Carlos Ivorra Castillo

TEORÍA DE CUERPOS DE CLASES

Esencialmente, el álgebra y el dinero determinan clases; la primera a nivel intelectual, el segundo a nivel práctico.

Simone Weil

Índice General

Introducción

En nuestro libro sobre teoría de números describimos una parte importante de los descubrimientos obtenidos durante el siglo XIX en este campo. El propósito del que aquí presentamos es relatar el desarrollo que estos hallazgos han tenido en la primera mitad de nuestro siglo. Si las figuras más relevantes en el siglo pasado fueron, como ya sabemos, Euler, Gauss, Legendre, Jacobi, Dirichlet y Kummer —entre muchos otros—, aquí nos encontraremos con nuevos nombres como Hilbert, Minkowski, Hasse, Takagi o Artin.

En realidad nuestra exposición no se ciñó fielmente a la cronología, de modo que nombres "modernos" como Hasse ya nos aparecieron en su momento, mientras que aquí tendremos ocasión (en el capítulo XIII) de reparar en la figura de un gran genio contemporáneo de Gauss, como fue la de Eisenstein.

La transición entre la teoría de números que suele llamarse "clásica" y la teoría moderna vino con el proceso de formalización y fundamentación que experimentó toda la matemática a principios de siglo. Esto no supuso un mero cambio de lenguaje, sino que la "nueva teoría" tenía una potencia muy superior a la de los medios clásicos, y permitió alcanzar un grado de profundidad y comprensión del comportamiento de los números inconcebible sin ella.

El proceso de formalización de la teoría de números consistió en la introducción del lenguaje algebraico moderno (del que nosotros nunca hemos prescindido). Este a su vez permitió formular en contextos mucho más generales los resultados clásicos. Uno de los matemáticos que más contribuyó a ello fue Richard Dedekind, a quien le preocupó especialmente el encontrar una respuesta precisa a la pregunta ¿Qué es un número? A Dedekind se le debe una de las construcciones clásicas de los números reales, y también fue él quien extrajo la definición moderna de ideal a partir del concepto práctico de Kummer de "divisor ideal", introdujo el concepto de entero algebraico y desarrolló una teoría general sobre cuerpos numéricos que incluía los teoremas sobre convergencia de las funciones dseta generalizadas.

Los conceptos nuevos requerían también programas nuevos que marcaran las direcciones más importantes a seguir en la investigación. Entre los matemáticos que más influyeron en este sentido destaca David Hilbert. La Sociedad Matemática Alemana le encargó un informe sobre los resultados alcanzados en la teoría algebraica de números durante el siglo XIX junto con las perspectivas para el siglo entrante. Hilbert presentó este (extenso) informe en 1897, y es conocido como el "Zahlberich". Constaba de cinco partes. Las dos primeras (Teoría Gene-

ral y Teoría de Galois) contenían los resultados básicos sobre la teoría de Galois y los cuerpos numéricos. Las dos siguientes (Cuerpos Cuadráticos y Cuerpos Ciclotómicos) exponían con enfoque moderno los resultados de las Disquisitiones Arithmeticae. Finalmente, la quinta parte (Cuerpos de Kummer) trataba de una clase especial de extensiones de cuerpos numéricos que tendremos ocasión de conocer en el capítulo VII.

Respecto a las nuevas perspectivas para la teoría de números, un buen resumen de sus criterios lo constituyen los problemas que presentó en su famosa charla en el Segundo Congreso Internacional de Matemáticas celebrado en Paris en 1900. Se trataba de los 23 problemas más importantes que a su juicio tenía planteada la matemática del siglo que pronto iba a comenzar. Los concernientes a la teoría algebraica de números ocupaban las posiciones 9–12. Entre ellos se encontraba, por supuesto, la demostración del último teorema de Fermat y, más en general, la obtención de un algoritmo para determinar si una ecuación diofántica arbitraria tiene o no solución (problema éste que fue resuelto negativamente a partir de los resultados de Gödel sobre indemostrabilidad). Los problemas relacionados con el contenido de este libro son el 9 y el 12:

El problema 9 pedía una generalización de la ley de reciprocidad cuadrática a exponentes mayores. Según veremos en el capítulo XIII, se trata de una cuestión que ya ocupó a Gauss y que Kummer y Eisenstein consideraron de gran importancia teórica. Ambos obtuvieron resultados parciales muy sofisticados, mientras que Hilbert pedía un resultado general.

El problema 12 trataba sobre clasificar las extensiones abelianas de un cuerpo numérico dado, en especial sobre $\mathbb{Q}$ y sobre los cuerpos cuadráticos. También se trata de un problema de raíces clásicas. Su motivación se remonta al trabajo de Abel sobre funciones elípticas, que le llevó a obtener resultados sobre extensiones y grupos abelianos (incluyendo lo que en términos modernos es el teorema de clasificación de los grupos abelianos finitos). Kronecker (alumno y amigo de Kummer) consideró que las investigaciones de Abel tenían gran interés y, continuándolo, conjeturó que las extensiones abelianas de $\mathbb{Q}$ son los subcuerpos de los cuerpos ciclotómicos (lo cual probaremos en el capítulo VIII). Así mismo llegó a una conjetura análoga, aunque más complicada, para el caso de cuerpos cuadráticos imaginarios y que se sale del alcance de este libro.

Aparte de estos precedentes, el problema 12 también estaba relacionado con el propio trabajo de Hilbert. Pocos años antes había conjeturado que si k es un cuerpo numérico y H es su grupo de clases (el cociente del grupo de ideales fraccionales de su anillo de enteros sobre el subgrupo generado por los ideales principales) existe una extensión de Galois K de k tal que el grupo de Galois $G(K/k)$ es isomorfo a H. Además esta extensión debía de estar muy relacionada con la aritmética de k. Por ejemplo, Hilbert conjeturó entre otras cosas que ningún primo de k se habría de ramificar en K y que los ideales primos que se escindirían completamente en K serían exactamente los principales (esto exige identificar de algún modo los ideales de k con parte de los ideales de K, lo que contituye un simple problema técnico en el que no vamos a detenernos aquí). A este cuerpo K lo llamó, de forma natural, "cuerpo de clases de k", y demostró su existencia para el caso en que k es un cuerpo cuadrático.

Estas conjeturas y pruebas son el embrión de lo que hoy se conoce como teoría de cuerpos de clases, que ha resultado ser una poderosa herramienta tanto para obtener nuevos resultados sobre números como para interpretar los ya conocidos. Antes de seguir con la historia vamos a detenernos y reparar en algunos hechos ya vistos en nuestro libro de teoría de números y que hacen sospechar de la existencia de una teoría más profunda que los explique. En primer lugar tenemos los ejemplos de la sección[1] [3.3], que muestran cómo factorizan los primos racionales en varios cuerpos numéricos. Cuando éstos son extensiones abelianas de $\mathbb{Q}$ (cuerpos cuadráticos, ciclotómicos, ciclotómicos reales), el criterio de factorización es extremadamente regular. Sucede que todas estas leyes de factorización son casos particulares de los resultados que proporciona la teoría de cuerpos de clases, válidos para extensiones abelianas de cuerpos numéricos arbitrarios.

Como muestra de la importancia de esta clase de resultados basta pensar en las factorizaciones de la función dseta de los cuerpos cuadráticos y ciclotómicos en términos de funciones L de Dedekind que obtuvimos en el [capítulo XII]. En las pruebas es esencial el conocimiento de las reglas de factorización de primos. A su vez, las factorizaciones nos sirvieron para probar el teorema de Dirichlet sobre primos en progresiones aritméticas y para obtener fórmulas para el número de clases de los cuerpos cuadráticos y ciclotómicos.

La teoría de cuerpos de clases permite obtener factorizaciones análogas para las funciones dseta de cualquier extensión abeliana de cuerpos numéricos, lo que nos da nuevas fórmulas para calcular números de clases de otros cuerpos (capítulo IX), así como generalizar el teorema de Dirichlet, de modo que podremos garantizar, por ejemplo, la existencia de infinitos primos de la forma $p = u^2 + 14v^2$ y, más aún, dar condiciones sencillas que determinen qué primos son de esta forma. Esto va más allá de la teoría de Gauss sobre formas cuadráticas y nos permite obtener resultados sobre representación de números por formas en casos en los cuales la teoría de Gauss no permite concluir nada (capítulo XI).

Volviendo al desarrollo histórico, los resultados básicos de la teoría de cuerpos de clases fueron demostrados por Takagi en 1920 (en una forma todavía no muy refinada). En realidad Takagi probó resultados más potentes que los conjeturados por Hilbert, pues no se limitó a considerar los grupos de clases usuales, definidos por Kummer y Dedekind, sino unos grupos de clases generalizados introducidos por Weber poco antes. Grosso modo, sin entrar en ciertos tecnicismos, Weber definió unos grupos $H(\mathfrak{m})$, donde $\mathfrak{m}$ es un ideal de un cuerpo numérico k, cuyos elementos son ciertas clases de equivalencia de ideales fraccionales primos con $\mathfrak{m}$, de modo que en el caso particular $k = \mathbb{Q}$ resultan ser los grupos de unidades módulo $\mathfrak{m}$. Si $\mathfrak{m} = 1$ se obtiene el grupo de clases usual. Estos grupos están relacionados por epimorfismos canónicos $f : H(\mathfrak{m}) \longrightarrow H(\mathfrak{m}')$, donde $\mathfrak{m}' \mid \mathfrak{m}$, de modo que un subgrupo $H \leq H(\mathfrak{m})$ puede venir inducido por un subgrupo de $H(\mathfrak{m}')$ (o sea, ser la antiimagen de un subgrupo de $H(\mathfrak{m}')$). Cada subgrupo H tiene asociado un mínimo ideal $\mathfrak{f}$ tal que H es inducido desde

[1] Todas las referencias que en lo sucesivo aparezcan entre corchetes remiten a mi libro de teoría de números.

$H(\mathfrak{f})$, al que se le llama el conductor de H. Takagi demostró que para cada subgrupo H de un grupo $H(\mathfrak{m})$ existe una extensión abeliana K de k cuyo grupo de Galois $G(K/k)$ es isomorfo al grupo de clases $H(\mathfrak{m})/H$. Los ideales primos de k (identificados adecuadamente con ideales de K) que se ramifican en K son exactamente los que dividen al conductor de H y, si un primo $\mathfrak{p}$ no divide a dicho conductor $\mathfrak{f}$ y f es el orden de $[\mathfrak{p}]$ en el grupo $H(\mathfrak{f})/H$, entonces el número de divisores primos de $\mathfrak{p}$ en K es h/f, donde $h = |H(\mathfrak{f}) : H|$. El lector reconocerá, pese a la imprecisión de la exposición, una forma general de los teoremas de descomposición de primos de los que hablábamos antes. En especial, la forma en que un primo $\mathfrak{p}$ de k se descompone en K sólo depende de su clase de equivalencia módulo H.

Las pruebas de Takagi eran esencialmente analíticas, basadas en funciones dseta y en ciertas generalizaciones de las funciones L debidas a Hecke. En un artículo posterior mostró una relación entre el isomorfismo que relaciona el grupo de clases con el grupo de Galois del cuerpo de clases y una generalización del símbolo de Legendre, con ayuda de la cual Hilbert había planteado su problema 9 sobre la ley de reciprocidad generalizada. Fue finalmente Artin quien consiguió en 1927 una descripción explícita de dicho isomorfismo (hoy conocido como isomorfismo de Artin), lo que supuso a la vez una simplificación y un avance en la teoría. Artin demostró la ley de reciprocidad general que hoy también lleva su nombre.

La teoría comenzó a tomar forma definitiva con el trabajo de Hasse. En 1925 publicó una recopilación sistemática de los resultados de Takagi. Pensaba publicar poco después una segunda parte, pero ésta se retrasó a causa de los resultados de Artin, y no apareció hasta 1930. En ella introdujo la mayor parte de la notación moderna y, lo que es más importante, aprovechó con eficiencia el concepto de "localización".

La idea se remonta a Hensel, un alumno de Kummer que extrajo de los prolijos cálculos de éste el concepto de números p-ádicos. Hensel observó que los conceptos asociados a cuerpos numéricos tienen análogos locales, que surgen al sustituir dichos cuerpos numéricos por sus compleciones respecto a ideales primos en el sentido del [capítulo VII], y postuló que las afirmaciones globales de un cuerpo numérico k pueden obtenerse a partir de las afirmaciones locales análogas para todos los primos de k, y viceversa. Por ejemplo, si k es un cuerpo numérico, para cada primo $\mathfrak{p}$ se puede definir el discriminante local $\Delta_\mathfrak{p}$ de k y se prueba que $\Delta_\mathfrak{p}$ es simplemente la máxima potencia de $\mathfrak{p}$ que divide al discriminante global Δ, de modo que el discriminante global puede obtenerse como el producto de los discriminantes locales.

Hasse era alumno de Hensel, y en su tesis doctoral dio un buen ejemplo de la validez de la conjetura de su maestro al demostrar una versión del teorema de Hasse–Minkowski [capítulo VIII]. Este teorema muestra también que, aunque las relaciones entre propiedades locales y globales pueden ser muy naturales, las pruebas no son necesariamente triviales.

Al aplicar estos principios a la teoría de cuerpos de clases dedujo de la teoría global una teoría local, más sencilla en algunos aspectos, demostró que la teoría global podía a su vez ser deducida de la teoría local, y planteó como problema

el construir la teoría local independientemente de la teoría global.

En los años posteriores las pruebas fueron simplificadas, básicamente por Artin, Herbrand y Chevalley. Un avance muy importante fue la introducción por Chevalley de los llamados elementos ideales. Se trata de un concepto técnico que trataremos con detalle en el capítulo VI. De momento digamos tan sólo que consiste en una generalización de la representación geométrica de los cuerpos numéricos [capítulo IV] que relaciona fuertemente los hechos locales con los globales.

Los resultados centrales de la teoría de cuerpos de clases tienen tal grado de profundidad que fueron muchos los esfuerzos dedicados a presentarlos desde diversos puntos de vista, con la esperanza de entenderlos lo mejor posible. Ciertamente, desde los trabajos originales de Takagi, bastante oscuros, hasta la introducción de los elementos ideales y el isomorfismo de Artin, se había recorrido un largo trecho, pero todavía quedaba mucho por hacer. Weil obtuvo una interesante presentación de la teoría en términos de álgebras, aunque pronto se vio que el único elemento relevante eran los cociclos que determinaban las álgebras involucradas. Con esto se llegó a una exposición en términos de la cohomología de grupos, que ha resultado ser muy iluminadora.

Ante el dilema de presentar la teoría en términos cohomológicos o en términos más clásicos, hemos optado por las dos soluciones a la vez. Primeramente la exponemos sin apoyarnos en la cohomología de grupos. Así conecta de forma directa con nuestro libro de teoría de números y, a nuestro parecer, resulta mucho más natural y accesible para una primera lectura. No obstante, en los tres últimos capítulos exponemos también la versión cohomológica, pues creemos que es el momento en que realmente puede apreciarse todo su valor.

Esperamos que el lector disfrute al econtrarse con la magnificencia de esta rama de las matemáticas, tanto en la elegancia de sus métodos como en la profundidad de sus resultados. Así mismo, al comparar con nuestro libro de teoría de números, el lector tendrá opción de comprender cómo una teoría de tal grado de abstracción ha surgido de forma natural a partir de los cálculos y observaciones concretas, cada vez más penetrantes, realizados por los matemáticos del siglo pasado.

Capítulo I

Dominios de Dedekind

Recordemos [3.1] que un *dominio de Dedekind* es un dominio íntegro en el que todo ideal propio se descompone de forma única salvo el orden en producto de ideales primos. Los dominios de Dedekind más importantes en la teoría de números son los órdenes maximales de los cuerpos numéricos [3.13], pero pronto nos vamos a encontrar con otros ejemplos de interés, por lo que nos conviene estudiarlos en general.

1.1 Resultados básicos

Recordemos [3.2] que si D es un dominio de Dedekind y K es su cuerpo de cocientes, un *ideal fraccional* de D es un D-módulo $M \subset K$ no nulo tal que existe un $d \in D$ no nulo de modo que $dM \subset D$.

Se cumple [3.4] que el conjunto de los ideales fraccionales de un dominio de Dedekind D es un grupo abeliano con el producto usual (MN es el D-módulo generado por los productos de elementos de M y N) y de hecho es el grupo abeliano libre generado por los ideales (primos) de D.

El resultado fundamental es el teorema de Dedekind [3.9], según el cual un anillo conmutativo y unitario D es un dominio de Dedekind si y sólo si cumple tres propiedades:

a) es noetheriano,

b) los ideales primos no nulos de D son maximales,

c) si un elemento b del cuerpo de cocientes de D es raíz de un polinomio mónico con coeficientes en D, entonces $b \in D$.

Vamos a probar analizar con más detalle propiedades a) y c).

Anillos y módulos noetherianos En este apartado daremos algunos criterios sencillos para garantizar que un anillo o un módulo dado es noetheriano. Recordemos las definiciones:

Definición 1.1 Sea A un anillo y M un A-módulo. Se dice que M es *noetheriano* si todos sus submódulos son finitamente generados.

Un anillo A es *noetheriano* si lo es como A-módulo, es decir, si todos sus ideales son finitamente generados. En particular todo dominio de ideales principales es noetheriano.

Las caracterizaciones siguientes suelen ser útiles:

Teorema 1.2 *Sea A un anillo y M un A-módulo. Las siguientes afirmaciones son equivalentes:*

a) M es noetheriano.

b) Toda sucesión creciente de submódulos

$$M_0 \subset M_1 \subset M_2 \subset M_3 \subset \cdots$$

es finalmente constante.

c) Toda familia no vacía de submódulos de M tiene un elemento maximal respecto a la inclusión.

Demostración: a) $\Rightarrow$ b) La unión de todos los módulos M_i es un submódulo de M, luego tiene un generador finito, que estará contenido en alguno de los módulos M_{i_0}. Entonces $M = M_{i_0}$ y por lo tanto $M = M_i$ para todo $i \geq i_0$.

b) $\Rightarrow$ c) Si existiera una familia de submódulos sin maximal podríamos tomar un módulo cualquiera M_0, que al no ser maximal estaría estrictamente contenido en otro módulo M_1 de la familia, que estaría contenido en otro M_2 y así formaríamos una cadena ascendente infinita, en contradicción con b).

c) $\Rightarrow$ a) Si N es un submódulo de M que no es finitamente generado entonces tomamos $m_0 \in N$ y se cumple $N \neq (m_0)$, luego existe un m_1 en $N \setminus (m_0)$ y $N \neq (m_0, m_1)$, luego existe un m_2 en $N \setminus (m_0, m_1)$ y $N \neq (m_0, m_1, m_2)$. De este modo construimos una familia de submódulos

$$(m_0) \subset (m_0, m_1) \subset (m_0, m_1, m_2) \subset \cdots$$

que no tiene maximal. ∎

Los teoremas siguientes justificarán de forma inmediata que todos los anillos y módulos que consideremos en lo sucesivo serán noetherianos:

Teorema 1.3 *Si A es un anillo y M es un A-módulo noetheriano, entonces todo submódulo y todo módulo cociente de M es noetheriano.*

Demostración: Sea N un submódulo de M. Entonces todo submódulo de N es también un submódulo de M, luego es finitamente generado y así N es noetheriano. Todo submódulo de M/N es de la forma R/N, donde $N \subset R \subset M$ y del hecho de que R es finitamente generado se sigue claramente que R/N también lo es. ∎

También se cumple un recíproco:

Teorema 1.4 *Sea A un anillo, M un A-módulo y N un submódulo de M. Si N y M/N son noetherianos entonces M también lo es.*

DEMOSTRACIÓN: A cada submódulo L de M le asociamos el par de módulos $\big(L \cap N, (L+N)/N\big)$. Notemos que si $E \subset F$ son dos submódulos de M y sus pares asociados son iguales entonces $E = F$. En efecto, si $x \in F$, como $(E+N)/N = (F+N)/N$, existen $u \in N$ y $v \in E$ tales que $x = u+v$. Entonces $u \in F \cap N = E \cap N$, luego $x \in E$.

A una sucesión ascendente de submódulos de M le corresponden dos sucesiones ascendentes de submódulos de N y de M/N respectivamente. Como éstas han de ser finalmente constantes, la dada también lo ha de ser, luego M es noetheriano. ∎

Teorema 1.5 *Sea A un anillo y M un A-módulo. Si E y F son submódulos noetherianos de M, entonces $E+F$ también es noetheriano.*

DEMOSTRACIÓN: Tenemos que E es noetheriano y $(E+F)/E \cong F/(E \cap F)$ también lo es, luego $E+F$ es noetheriano. ∎

Teorema 1.6 *Si A es un anillo noetheriano, entonces todo A-módulo finitamente generado es noetheriano.*

DEMOSTRACIÓN: Si M admite un generador con m elementos, entonces existe un epimorfismo de anillos $f : A^m \longrightarrow M$ (pues A^m es un módulo libre de rango m y podemos extender a un epimorfismo una biyección entre una base de A^m y un generador de M). Aplicando m veces el teorema anterior concluimos que A^m es un módulo noetheriano y M es isomorfo a un cociente de A^m, luego M es noetheriano. ∎

Teorema 1.7 (Teorema de Hilbert) *Si A es un anillo noetheriano entonces $A[x_1, \ldots, x_n]$ también lo es.*

DEMOSTRACIÓN: Basta probarlo para una indeterminada. Sea $\mathfrak{a}$ un ideal de $A[x]$. Sea $\mathfrak{b}_i$ el conjunto de los coeficientes directores de los polinomios de $\mathfrak{a}$ de grado i (más el 0).

Es claro que $\mathfrak{b}_i$ es un ideal de A, así como que $\mathfrak{b}_0 \subset \mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \mathfrak{b}_3 \subset \cdots$ (para ver que un elemento de $\mathfrak{b}_i$ está en $\mathfrak{b}_{i+1}$ basta multiplicar por x el polinomio que justifica que está en $\mathfrak{b}_i$). Como A es noetheriano, los ideales $\mathfrak{b}_i$ son iguales a partir de un $\mathfrak{b}_r$.

Sea $\mathfrak{b}_i = (b_{i1}, \ldots, b_{in})$ para $i = 0, \ldots, r$ (no es restricción suponer que el número de generadores es el mismo para todos los ideales, pues siempre podemos añadir generadores redundantes). Podemos suponer que los $b_{ij} \neq 0$.

Sea p_{ij} un polinomio en $\mathfrak{a}$ de grado i cuyo coeficiente de grado i sea b_{ij}. Vamos a probar que $\mathfrak{a} = (p_{ij} \mid i = 0, \ldots, r,\ j = 1, \ldots, n)$. Claramente este ideal está contenido en $\mathfrak{a}$.

Sea $f \in \mathfrak{a}$ un polinomio de grado d. Veremos que está en el ideal generado por los p_{ij} por inducción sobre d. El coeficiente director de f está en $\mathfrak{b}_d$. Si

$d > r$ notamos que los coeficientes directores de $x^{d-r}p_{r1}, \ldots, x^{d-r}p_{rn}$ son los números $b_{r1}, \ldots, b_{rn}$, que generan $\mathfrak{b}_d = \mathfrak{b}_r$. Por consiguiente existen elementos $c_1, \ldots, c_n$ en A tales que el polinomio $f - c_1x^{d-r}p_{r1} - \cdots - c_nx^{d-r}p_{rn}$ tiene grado menor que d y está en $\mathfrak{a}$, luego por hipótesis de inducción f está en el ideal generado por los p_{ij}.

Si $d \leq r$ obtenemos un polinomio $f - c_1p_{d1} - \cdots - c_np_{dn}$ de grado menor que d y contenido en $\mathfrak{a}$, con lo que se concluye igualmente. ∎

Teorema 1.8 *Si A es un anillo noetheriano y $B = A[b_1, \ldots, b_n]$ es un anillo finitamente generado sobre A, entonces B es noetheriano.*

(Porque B es isomorfo a un cociente de $A[x_1, \ldots, x_n]$).

Extensiones enteras La propiedad c) en el teorema de Dedekind está relacionada con la noción de "elemento entero", que el análogo en anillos a la de "elemento algebraico" en la teoría de extensiones de cuerpos. Necesitaremos los resultados básicos sobre extensiones enteras de dominios íntegros y su relación con las extensiones de sus cuerpos de cocientes.

Definición 1.9 Sea D un dominio íntegro y K un cuerpo que contenga a D. Un elemento $\alpha \in K$ es *entero* sobre D si es raíz de un polinomio mónico con coeficientes en D.

Cuando K es un cuerpo numérico y $D = \mathbb{Z}$, los elementos enteros son precisamente los enteros algebraicos. Todos los resultados que probaremos aquí son generalizaciones de hechos conocidos en este caso. Para empezar probaremos que los elementos enteros sobre un dominio íntegro forman un anillo, y para ello usaremos la siguiente caracterización de la integridad:

Teorema 1.10 *Sea D un dominio íntegro y K un cuerpo que contenga a D. Un elemento $\alpha \in K$ es entero sobre D si y sólo si existe un D-módulo finitamente generado no nulo $M \subset K$ tal que $\alpha M \subset M$.*

Demostración: Si α es entero entonces $\alpha^n + d_{n-1}\alpha^{n-1} + \cdots + d_1\alpha + d_0 = 0$, para ciertos $d_i \in D$. Basta considerar el módulo $M = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_D$.

Dado un módulo $M = \langle v_1, \ldots, v_n \rangle_D$ tal que $\alpha M \subset M$, existen elementos d_{ij} en D tales que

$$\alpha v_i = d_{i1}v_1 + \cdots + d_{in}v_n, \qquad \text{para } i = 1, \ldots, n.$$

Esto equivale a la ecuación vectorial $\alpha v = vA$, donde $v = (v_i)$ y $A = (d_{ij})$, o sea, α es un valor propio de la matriz A, luego es raíz de su polinomio característico, que claramente es mónico y con coeficientes en D. ∎

Teorema 1.11 *Sea D un dominio íntegro y K un cuerpo que contenga a D. Entonces el conjunto E de todos los elementos de K enteros sobre D es un subanillo de K.*

DEMOSTRACIÓN: Sean α, $\beta \in E$. Sean M y N dos D-módulos no nulos finitamente generados tales que $\alpha M \subset M$ y $\beta N \subset N$. Entonces es fácil ver que MN es un D-módulo no nulo finitamente generado y $(\alpha \pm \beta)MN \subset MN$, $\alpha\beta MN \subset MN$. Por lo tanto $\alpha \pm \beta \in E$ y $\alpha\beta \in E$. ∎

Definición 1.12 Sea E/D una *extensión* de dominios íntegros, es decir, D y E son dominios íntegros tales que D es un subanillo de E. Diremos que la extensión es *entera* si todo elemento de E es entero sobre D.

Vamos a probar que las extensiones enteras de dominios íntegros se comportan como las extensiones algebraicas de cuerpos. El teorema anterior implica que si adjuntamos a un anillo un conjunto de elementos enteros obtenemos una extensión entera. Ahora probamos que si adjuntamos un número finito de elementos obtenemos además una extensión finitamente generada.

Teorema 1.13 *Sean $D \subset E$ dominios íntegros tales que $E = D[a_1, \ldots, a_n]$ con los a_i enteros sobre D. Entonces E es un D-módulo finitamente generado.*

DEMOSTRACIÓN: Si tenemos una cadena $D \subset F \subset E$ de dominios íntegros de modo que E es un F-módulo finitamente generado y F es un D-módulo finitamente generado, entonces E es un D-módulo finitamente generado. Basta observar que si $E = \langle e_1, \ldots, e_n \rangle_F$ y $F = \langle f_1, \ldots, f_m \rangle_D$ entonces $E = \langle e_i f_j \rangle_D$.

De aquí se sigue que basta probar el teorema para una sola adjunción. Supongamos que $E = D[a]$ y que a es raíz de un polinomio mónico $p(x) \in D[x]$ de grado n. Todo elemento de E es de la forma $q(a)$ con $q(x) \in D[x]$.

Podemos dividir $q(x) = p(x)c(x) + r(x)$ con $\operatorname{grad} r(x) < n$, y entonces resulta que $q(a) = r(a)$. De aquí se sigue que $E = \langle 1, a, \ldots, a^{n-1} \rangle$. ∎

De aquí deducimos la transitividad de la integridad:

Teorema 1.14 *Si F/E y E/D son extensiones enteras entonces F/D también lo es.*

DEMOSTRACIÓN: Sea $\alpha \in F$. Entonces $\alpha^n + e_{n-1}\alpha^{n-1} + \cdots + e_1\alpha + e_0 = 0$ para ciertos $e_i \in E$. Sea $E' = D[e_0, \ldots, e_{n-1}]$. Por el teorema anterior E' es un D-módulo finitamente generado y $E'[\alpha]$ es un E'-módulo finitamente generado. Es fácil ver entonces que $E'[\alpha]$ es un D-módulo finitamente generado. Además es obvio que $\alpha E'[\alpha] \subset E'[\alpha]$, luego α es entero sobre D. ∎

Definición 1.15 Si D es un dominio íntegro contenido en un cuerpo K, el conjunto E de todos los elementos de K enteros sobre D se llama la *clausura entera* de D en K. El teorema 1.11 prueba que se trata de un dominio íntegro. Es la mayor extensión entera de D contenida en K.

Un dominio íntegro D contenido en un cuerpo K es *íntegramente cerrado* en K si todo elemento de K entero sobre D está en D o, equivalentemente, si D coincide con su clausura entera en K. Por el teorema anterior la clausura entera de un dominio íntegro en un cuerpo es íntegramente cerrada en éste.

Un dominio integro D es *íntegramente cerrado* si es íntegramente cerrado en su cuerpo de cocientes. Ésta es la condición c) de la caracterización algebraica de los dominios de Dedekind. Conviene notar que la comparten los dominios de factorización única:

Teorema 1.16 *Todo dominio de factorización única es íntegramente cerrado.*

DEMOSTRACIÓN: Sea D un dominio de factorización única. Si no es íntegramente cerrado es que hay un elemento α/β en su cuerpo de cocientes que es entero sobre D y no pertenece a D. Entonces existe un primo π que divide a β pero no divide a α. Sea

$$(\alpha/\beta)^n + d_{n-1}(\alpha/\beta)^{n-1} + \cdots + d_1(\alpha/\beta) + d_0 = 0, \qquad \text{para ciertos } d_i \in D.$$

Multiplicando por β^n queda $\alpha^n + d_{n-1}\beta\alpha^{n-1} + \cdots + d_1\beta^{n-1}\alpha + d_0\beta_n = 0$, de donde se sigue que $\pi \mid \alpha$, contradicción. ∎

Si E/D es una extensión de dominios íntegros podemos identificar el cuerpo de cocientes K de D con un subcuerpo del cuerpo de cocientes L de E, con lo que tenemos una extensión de cuerpos L/K. Vamos a estudiar la relación entre ambas extensiones. Por lo pronto, cuando digamos que E/D es una extensión *finita, separable, normal, etc.* nos referiremos a que lo es la extensión L/K de los cuerpos de cocientes.

Veamos ahora que el polinomio mínimo de un elemento algebraico determina si éste es o no entero.

Teorema 1.17 *Sea D un dominio íntegro y K su cuerpo de cocientes. Sea L/K una extensión finita. Entonces un elemento $\alpha \in L$ es entero sobre D si y sólo si su polinomio mínimo sobre K tiene coeficientes enteros sobre D. En particular la norma y la traza de un entero sobre D son enteras sobre D.*

DEMOSTRACIÓN: Es obvio que un K-monomorfismo de L en una clausura algebraica de L envía elementos enteros a elementos enteros, luego los conjugados de los enteros son enteros. Los coeficientes del polinomio mínimo de α dependen polinómicamente de los conjugados de α, luego si α es entero dichos coeficientes también lo son. La norma y la traza son dos de estos coeficientes. ∎

Si en el teorema anterior suponemos además que D es íntegramente cerrado, entonces resulta que un elemento algebraico sobre K es entero si y sólo si su polinomio mínimo sobre K está en $D[x]$, y en particular tenemos que la norma y la traza de un entero están en D.

Veamos ahora un resultado técnico elemental que necesitaremos en el teorema siguiente y en otras ocasiones.

Teorema 1.18 *Sea D un dominio íntegro y α un elemento algebraico sobre su cuerpo de cocientes. Entonces existe un $d \in D$ no nulo tal que $d\alpha$ es entero sobre D.*

DEMOSTRACIÓN: Por hipótesis $d_n\alpha^n + d_{n-1}\alpha^{n-1} + \cdots + d_1\alpha + d_0 = 0$ para ciertos $d_i \in D$ con $d_n \neq 0$. Multiplicando por d_n^{n-1} queda

$$(d_n\alpha)^n + d_{n-1}(d_n\alpha)^{n-1} + \cdots + d_1(d_n\alpha) + d_0 = 0,$$

luego $d_n\alpha$ es entero sobre D. ∎

Un hecho crucial en el estudio de los cuerpos numéricos es que el orden maximal de un cuerpo numérico de grado n es un $\mathbb{Z}$-módulo libre de rango n, lo que nos permite hablar de bases enteras. En el caso general, si L es una extensión finita del cuerpo de cocientes de un dominio íntegro D, no tenemos garantizado que la clausura entera de D en L esté finitamente generada sobre D como anillo y mucho menos como módulo. Para asegurarlo necesitamos imponer dos hipótesis: que el dominio sea noetheriano y que la extensión sea separable. Conviene tener presente que en los casos de mayor interés a los que se aplica todo lo que estamos viendo los dominios íntegros que aparecen son de característica 0, por lo que la separabilidad es trivial.

Teorema 1.19 *Sea D un dominio íntegro noetheriano íntegramente cerrado, sea K su cuerpo de cocientes y L una extensión finita separable de K. Entonces la clausura entera de D en L es un D-módulo finitamente generado.*

DEMOSTRACIÓN: Basta probar que la clausura entera de D en L está contenida en un D-módulo finitamente generado, pues tal módulo será noetheriano y en consecuencia la clausura entera será finitamente generada.

Sea $w_1, \ldots, w_n$ una K-base de L. Por el teorema anterior podemos suponer que los w_i son enteros sobre D. Sea $T : L \longrightarrow K$ la traza de la extensión. La matriz $\big(T(w_iw_j)\big)$ tiene determinante no nulo, pues en caso contrario existirían elementos $c_1, \ldots, c_n \in K$ no todos nulos tales que

$$0 = \sum_{j=1}^{n} c_j T(w_iw_j) = T\Big(w_i \sum_{j=1}^{n} c_j w_j\Big), \qquad \text{para } i = 1, \ldots, n.$$

Sea $\alpha = \sum_{j=1}^{n} c_j w_j$. Tenemos que $T(w_i\alpha) = 0$ para todo i. Para cada $\beta \in K$ sea $\beta\alpha^{-1} = \sum_{j=1}^{n} d_j w_j$, con $d_j \in K$. Entonces

$$T(\beta) = T\Big(\sum_{j=1}^{n} d_j\alpha w_j\Big) = \sum_{j=1}^{n} d_j T(\alpha w_j) = 0,$$

o sea, $T = 0$, lo cual es imposible en una extensión separable.

De aquí que existen elementos $z_1, \ldots, z_n \in L$ tales que

$$T(z_iw_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

(Las coordenadas de z_i en la base $w_1, \ldots, w_n$ han de satisfacer un sistema de ecuaciones lineales cuya matriz es $\big(T(w_iw_j)\big)$).

Sea $c \neq 0$ un elemento de D tal que cz_i es entero sobre D para $i = 1, \ldots, n$. Si x es cualquier elemento de L entero sobre D, entonces xcz_i es entero sobre D, luego lo mismo le sucede a $T(xcz_i)$ para cada i. Si $x = \sum_{j=1}^{n} b_j w_j$, con $b_j \in K$, entonces

$$T(xcz_i) = \sum_{j=1}^{n} cb_j T(z_i w_j) = cb_i \in K,$$

y como D es íntegramente cerrado, de hecho $cb_i \in D$ y

$$x = \sum_{j=1}^{n} b_j w_j = \sum_{j=1}^{n} (cb_j)(c^{-1}w_j) \in \left\langle c^{-1}w_1, \ldots, c^{-1}w_n \right\rangle_D .$$

Así pues, el módulo $\left\langle c^{-1}w_1, \ldots, c^{-1}w_n \right\rangle_D$ contiene a la clausura entera de D en L. ∎

Debemos tener presente que en las hipótesis de este teorema no podemos garantizar que la clausura entera de D en L sea un D-módulo libre. Evidentemente es libre de torsión, luego una condición suficiente para que sea libre es que D sea un dominio de ideales principales (por los teoremas de estructura de los módulos finitamente generados sobre dominios de ideales principales). Éste es el caso de $\mathbb{Z}$ y es por ello que podemos asegurar la existencia de bases enteras en los cuerpos numéricos. No obstante, si $D \subset E$ son órdenes maximales de cuerpos numéricos, no es necesariamente cierto que E tenga una base como D-módulo, por lo que en general nos tendremos que conformar con saber que E es un D-módulo finitamente generado, que es lo que afirma el teorema anterior.

Dominios de ideales principales En los términos introducidos en el párrafo anterior, el teorema de Dedekind afirma que los los dominios de Dedekind son los dominios íntegros noetherianos íntegramente cerrados cuyos ideales primos coinciden con los maximales (en lo sucesivo, cuando hablemos de *primos* en un dominio de Dedekind se entenderá que nos referimos a ideales primos no nulos).

Claramente todo dominio de ideales principales es un dominio de Dedekind (la clausura entera se sigue del teorema 1.16). Además un dominio de Dedekind es un dominio de ideales principales si y sólo si tiene factorización única (pues entonces cada ideal está generado por el máximo común divisor de sus generadores).

Los dominios de ideales principales son los dominios de Dedekind con mejor comportamiento (recordemos la observación final del apartado anterior). Aunque no son lo suficientemente generales como para que podamos limitarnos a este caso, lo cierto es que en muchas ocasiones podremos reducir problemas generales a problemas sobre dominios de ideales principales. En la sección siguiente estudiaremos una técnica general para ello. La idea será reducir los problemas al caso de dominios de Dedekind con un número finito de ideales primos, pues sucede que dichos anillos son siempre dominios de ideales principales. Para probarlo necesitamos la versión para ideales del teorema chino del resto.

Podríamos dar una prueba más simple para el caso particular de dominios de Dedekind, pero no merece la pena.

Teorema 1.20 (Teorema chino del resto) *Sea D un dominio íntegro y sean $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales de D tales que $\mathfrak{a}_i + \mathfrak{a}_j = D$ para $i \neq j$. Dados $\alpha_1, \ldots, \alpha_n \in D$ existe un $x \in D$ tal que $x \equiv \alpha_i \pmod{\mathfrak{a}_i}$ para $i = 1, \ldots, n$.*

DEMOSTRACIÓN: Para $n = 2$ tenemos que $a_1 + a_2 = 1$, para ciertos elementos $a_i \in \mathfrak{a}_i$, y basta tomar $x = \alpha_2 a_1 + \alpha_1 a_2$.

En el caso general, para cada $i \geq 2$ elegimos $a_i \in \mathfrak{a}_1$, $b_i \in \mathfrak{a}_i$ tales que $a_i + b_i = 1$. Entonces

$$1 = \prod_{i=2}^{n} (a_i + b_i) \in \mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i = D.$$

Por el caso ya probado existe un elemento $y_1 \in D$ tal que $y_1 \equiv 1 \pmod{\mathfrak{a}_1}$, $y_1 \equiv 0 \pmod{\mathfrak{a}_i}$ para $i \geq 2$. Similarmente podemos definir elementos $y_i \in D$ que cumplan

$$y_i \equiv 1 \pmod{\mathfrak{a}_i}, \qquad y_i \equiv 0 \pmod{\mathfrak{a}_j} \quad \text{para } j \neq i.$$

Basta tomar $x = \alpha_1 y_1 + \cdots + \alpha_n y_n$. ∎

Teorema 1.21 *Si D es un dominio de Dedekind con un número finito de ideales primos entonces D es un dominio de ideales principales y por lo tanto tiene factorización única.*

DEMOSTRACIÓN: Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los ideales primos de D. Sea $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Dado un ideal no nulo arbitrario $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$, por el teorema anterior existe un $\alpha \in D$ tal que $\alpha \equiv \pi_i^{r_i} \pmod{\mathfrak{p}_i^{r_i+1}}$. Es fácil ver que cada primo $\mathfrak{p}_i$ divide a α con multiplicidad exactamente r_i, de donde $(\alpha) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} = \mathfrak{a}$. ∎

1.2 Localización

En esta sección veremos cómo construir anillos a partir de uno dado de manera que desaparezcan todos los ideales primos salvo uno prefijado, y que éste conserve sus propiedades aritméticas. Esto supondrá una simplificación esencial para el tratamiento de muchos problemas.

Definición 1.22 Sea D un dominio íntegro. Un subconjunto S de D es *multiplicativo* si $1 \in S$, $0 \notin S$ y cuando $s, t \in S$ también $st \in S$. Si S es un subconjunto multiplicativo de D definimos

$$S^{-1}D = \{a/s \mid a \in D, s \in S\}.$$

Es fácil ver que $S^{-1}D$ es un subanillo del cuerpo de cocientes de D.

Si M es un D-módulo contenido en un cuerpo que contenga a D (en particular si M es un ideal de D), llamaremos

$$S^{-1}M = \{m/s \mid m \in M,\ s \in S\},$$

que es un $S^{-1}D$-módulo.

Notar que si $\mathfrak{p}$ es un ideal primo en D, entonces $S = D \setminus \mathfrak{p}$ es un subconjunto multiplicativo. En este caso el dominio íntegro $S^{-1}D$ se representa $D_{\mathfrak{p}}$ y se llama *localización* de D en $\mathfrak{p}$. Del mismo modo, escribiremos $M_{\mathfrak{p}}$ en lugar de $S^{-1}M$.

En definitiva, $D_{\mathfrak{p}}$ está formado por todas las fracciones en D cuyo denominador no está en $\mathfrak{p}$ (para un cierto representante a/s de la fracción). Una fracción a/s es una unidad de $D_{\mathfrak{p}}$ si y sólo si $a \notin \mathfrak{p}$, pues si $(a/s)(b/t) = 1$, entonces $ab = st \in D \setminus \mathfrak{p}$, luego $a \notin \mathfrak{p}$, y si $a \notin \mathfrak{p}$ entonces $(a/s)(s/a) = 1$.

Dicho de otro modo, un elemento $a/s \in D_{\mathfrak{p}}$ no es una unidad si y sólo si $a \in \mathfrak{p}$, o sea, si y sólo si a/s está en el ideal $\mathfrak{m} = S^{-1}\mathfrak{p}$. Esto implica que $\mathfrak{m}$ es el único ideal maximal del anillo $D_{\mathfrak{p}}$.

Se dice que un anillo A es *local* si tiene un único ideal maximal. Tenemos, pues, que cuando localizamos respecto a un ideal primo obtenemos un anillo local. Pronto veremos que cuando localizamos respecto a un primo $\mathfrak{p}$ en un dominio de Dedekind D, el ideal $\mathfrak{m}$ conserva las propiedades de $\mathfrak{p}$, mientras que los restantes ideales no tienen ningún reflejo en $D_{\mathfrak{p}}$.

En general se dice que una propiedad o un teorema es *local* si involucra a un único primo, mientras que si involucra a todo el sistema aritmético de un anillo se dice que la propiedad, o el teorema, es global. En estos términos, veremos que al localizar respecto a un primo se conservan las propiedades locales y se pierden las globales.

Hemos introducido la localización en términos de conjuntos multiplicativos arbitrarios porque, como veremos en la sección siguiente, otras elecciones de S nos permiten conservar un conjunto finito de primos en lugar de uno solo.

Veamos ahora las propiedades básicas de la localización:

Teorema 1.23 *Sea D un dominio íntegro y $S \subset D$ un subconjunto multiplicativo. Entonces se tienen los hechos siguientes:*

a) Si $\mathfrak{a}$ es un ideal de D, entonces $S^{-1}\mathfrak{a}$ es un ideal de $S^{-1}D$, y todos los ideales de $S^{-1}D$ son de esta forma.

b) Se cumple

$$S^{-1}\mathfrak{ab} = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$$

y

$$S^{-1}\mathfrak{a} = S^{-1}D \quad \textit{si y sólo si} \quad \mathfrak{a} \cap S \neq \varnothing.$$

c) Si un dominio E es entero sobre D entonces $S^{-1}E$ es entero sobre $S^{-1}D$.

d) Si B es la clausura entera de D en un cuerpo K, entonces $S^{-1}B$ es la clausura entera de $S^{-1}D$ en K.

e) Si D es íntegramente cerrado $S^{-1}D$ también lo es.

f) Si D es un dominio de Dedekind entonces $S^{-1}D$ también lo es y la aplicación S^{-1} es un epimorfismo del grupo de los ideales fraccionales de D en el grupo de los ideales fraccionales de $S^{-1}D$. El núcleo de este epimorfismo lo forman los ideales que cortan a S.

DEMOSTRACIÓN: a) Es inmediato que si $\mathfrak{a}$ es un ideal de D, entonces $S^{-1}\mathfrak{a}$ es un ideal de $S^{-1}D$. Recíprocamente, si $\mathfrak{b}$ es un ideal de $S^{-1}D$ entonces $\mathfrak{a} = \mathfrak{b} \cap D$ es un ideal de D y $\mathfrak{b} = S^{-1}\mathfrak{a}$. En efecto, una inclusión es clara, y si $x \in \mathfrak{b}$, entonces $x = a/s$ con $a \in D$, $s \in S$. Por lo tanto tenemos que $sx \in \mathfrak{b} \cap D = \mathfrak{a}$, luego $x \in S^{-1}\mathfrak{a}$.

b) Se prueba sin dificultad.

c) Sea $e/s \in S^{-1}E$, con $e \in E$, $s \in S$. Sea M un D-módulo finitamente generado tal que $eM \subset M$. Entonces $S^{-1}M$ es un $S^{-1}D$-módulo finitamente generado y $(e/s)S^{-1}M \subset S^{-1}M$.

d) Sea $\alpha \in K$ entero sobre $S^{-1}D$. Entonces $p(\alpha) = 0$, donde $p(x)$ es un polinomio mónico con coeficientes en $S^{-1}D$. Si s es el producto de los denominadores de los coeficientes de $p(x)$ elevado al grado de $p(x)$, es claro que $s \in S$ y que al multiplicar por s la igualdad $p(\alpha) = 0$ obtenemos que $s\alpha$ es raíz de un polinomio mónico con coeficientes en D. Consecuentemente $s\alpha \in E$ y así $\alpha \in S^{-1}E$.

Por el apartado anterior todos los elementos de $S^{-1}E$ son enteros sobre $S^{-1}D$, luego $S^{-1}E$ es la clausura entera de $S^{-1}D$ en K.

e) Es consecuencia inmediata de d).

f) Supongamos que D es un dominio de Dedekind. Los ideales de $S^{-1}D$ son de la forma $S^{-1}\mathfrak{a}$, donde $\mathfrak{a}$ es un ideal de D. Como $\mathfrak{a}$ es finitamente generado $S^{-1}\mathfrak{a}$ también lo es. Por lo tanto $S^{-1}D$ es noetheriano.

Por el apartado anterior $S^{-1}D$ es íntegramente cerrado.

Sea $S^{-1}\mathfrak{p}$ un ideal primo no nulo de $S^{-1}D$ y supongamos que $ab \in \mathfrak{p}$. Entonces uno de los dos factores, digamos a, está en $S^{-1}\mathfrak{p}$. Sea $a = p/s$, con $p \in \mathfrak{p}$, $s \in S$. Entonces $p = as$ y no puede ser que $s \in \mathfrak{p}$, pues entonces $S^{-1}\mathfrak{p} = 1$, luego $a \in \mathfrak{p}$. Así pues, $\mathfrak{p}$ es primo.

Como D es un dominio de Dedekind, $\mathfrak{p}$ es maximal. Si $S^{-1}\mathfrak{p} \subset S^{-1}\mathfrak{a}$ y existe un a/s en $S^{-1}\mathfrak{a}$ que no está en $S^{-1}\mathfrak{p}$, entonces $a \notin \mathfrak{p}$, luego $1 = p + da$, para cierto $p \in \mathfrak{p}$ y $d \in D$. Esto prueba que $1 \in S^{-1}\mathfrak{a} = S^{-1}D$, luego $S^{-1}\mathfrak{p}$ es un ideal maximal.

Con esto tenemos que $S^{-1}D$ es un dominio de Dedekind. El resto es fácil de comprobar. ∎

Centrémonos ahora en la localización respecto a un primo $\mathfrak{p}$ en un dominio de Dedekind D. Ya hemos visto que el anillo $D_{\mathfrak{p}}$ está formado por las fracciones

cuyo denominador no es divisible entre $\mathfrak{p}$. Ya hemos visto que $D_\mathfrak{p}$ tiene un único ideal maximal $\mathfrak{m} = S^{-1}\mathfrak{p}$ formado por las fracciones cuyo numerador está en $\mathfrak{p}$.

Además el teorema anterior nos da que $D_\mathfrak{p}$ es un dominio de Dedekind, luego los ideales restantes de $D_\mathfrak{p}$ han de ser las potencias de $\mathfrak{m}$, y los ideales fraccionales de $D_\mathfrak{p}$ son las potencias de $\mathfrak{m}$ con exponente entero.

Si $\mathfrak{q} \neq \mathfrak{p}$ es cualquier otro ideal primo de D entonces $\mathfrak{q}$ no puede estar contenido en $\mathfrak{p}$, luego corta a S y por lo tanto $S^{-1}\mathfrak{q} = 1$. Esto significa que el epimorfismo S^{-1} actúa sobre un ideal fraccional cualquiera eliminando todos sus factores distintos de $\mathfrak{p}$ y reemplazando a éste por $\mathfrak{m}$.

En resumen, tal y como habíamos anticipado, al localizar en $\mathfrak{p}$ estamos eliminando todos los ideales primos distintos de $\mathfrak{p}$, mientras que, como veremos, las propiedades de $\mathfrak{p}$ se transmiten muy bien a $\mathfrak{m}$. He aquí un primer ejemplo:

Teorema 1.24 *Sea D un dominio de Dedekind, sea $\mathfrak{p}$ un primo en D y sea n un número natural. Entonces*

a) Todo elemento de $D_\mathfrak{p}$ es congruente con un elemento de D módulo $\mathfrak{m}^n$.

b) Dos elementos de D son congruentes mód $\mathfrak{m}^n$ si y sólo si lo son mód $\mathfrak{p}^n$.

c) Los cocientes $D_\mathfrak{p}/\mathfrak{m}^n$ y $D/\mathfrak{p}^n$ son isomorfos.

DEMOSTRACIÓN: a) Sea d/s un elemento de $D_\mathfrak{p}$. El ideal $(s, \mathfrak{p}^n)$ es un divisor de $\mathfrak{p}^n$, luego es de la forma $\mathfrak{p}^r$ para $r \leq n$, pero $s \notin \mathfrak{p}$ y por lo tanto tampoco está en ninguna potencia de $\mathfrak{p}$ salvo en $\mathfrak{p}^0 = 1$. Así pues, $(s, \mathfrak{p}^n) = 1$ y en consecuencia $1 = sb + k$, donde $b \in D$ y $k \in \mathfrak{p}^n$. De aquí resulta que $d/s = db + k/s$, con $k/s \in \mathfrak{m}^n$ y $db \in$D.

b) Si $d \in \mathfrak{m}^n$ entonces $d = d'/s$, con $d' \in \mathfrak{p}^n$, pero entonces $\mathfrak{p}^n \mid sd$ y $\mathfrak{p}^n$ es primo con s, luego $\mathfrak{p}^n \mid d$, es decir, $d \in \mathfrak{p}^n$. El recíproco es obvio. De aquí se sigue inmediatamente b).

c) Es claro a partir de a) y b). ∎

Cuando D es un dominio de Dedekind el anillo $D_\mathfrak{p}$ es un dominio de Dedekind con un único primo, luego por el teorema 1.21 resulta ser un dominio de ideales principales.

En general, si D es un dominio de ideales principales local y $\mathfrak{m}$ es su ideal maximal, existe un primo $\pi \in D$ tal que $\mathfrak{m} = (\pi)$. Este primo está unívocamente determinado salvo unidades. Todo elemento $\alpha \in D$ no nulo se expresa de forma única como $\alpha = \epsilon\pi^n$, donde ϵ es una unidad de D y n es un número natural.

De hecho D es un dominio euclídeo considerando como norma euclídea la valoración inducida por π, es decir, $v(\epsilon\pi^n) = n$. La división de $\epsilon\pi^n$ entre $\delta\pi^m$ es

$$\begin{aligned} \epsilon\pi^n &= (\delta\pi^m)(\epsilon\delta^{-1}\pi^{n-m}) + 0 && \text{si } m \leq n \\ \epsilon\pi^n &= (\delta\pi^m)\cdot 0 + \epsilon\pi^n && \text{si } m > n. \end{aligned}$$

Observar que en el caso concreto de $D_\mathfrak{p}$ hemos llegado a que el ideal maximal $\mathfrak{m}$ es principal aun en el caso de que el ideal $\mathfrak{p}$ no lo sea.

1.3 Extensiones de dominios de Dedekind

Una buena parte de la teoría algebraica de números consiste en estudiar la relación entre la aritmética de un cuerpo numérico y la de una extensión finita. Para tratar esta cuestión con el grado de generalidad que necesitamos, probaremos ahora algunos resultados generales sobre extensiones de dominios de Dedekind.

Definición 1.25 Sean D y E dominios de Dedekind con cuerpos de cocientes k y K respectivamente ($k \subset K$). Diremos que E/D es una *extensión (finita) de dominios de Dedekind* si E es la clausura entera de D en K y además es un D-módulo finitamente generado.

Observar que en estas condiciones la extensión K/k ha de ser finita (si E está generado sobre D por n elementos, $|K : k| \leq n$). Llamaremos *grado* de E/D al grado de K/k. En general, cuando digamos que una extensión E/D de dominios de Dedekind es separable, de Galois, etc. se ha de entender que lo es la extensión K/k de los cuerpos de cocientes.

El teorema siguiente afirma que las extensiones separables de un dominio de Dedekind están en correspondencia biunívoca con las extensiones finitas separables de su cuerpo de cocientes.

Teorema 1.26 *Sea D un dominio de Dedekind y sea k su cuerpo de cocientes. Si K es una extensión finita separable de k y E es la clausura entera de D en K, entonces E/D es una extensión de dominios de Dedekind.*

Demostración: Ciertamente E es íntegramente cerrado. Por el teorema 1.19 tenemos que E es un D-módulo finitamente generado. En particular E es de la forma $E = D[a_1, \ldots, a_n]$ para ciertos elementos a_i, luego por el teorema 1.8 el anillo E es noetheriano. Falta ver que los ideales primos no nulos son maximales.

Sea $\mathfrak{P} \neq 0$ un ideal primo en E. Entonces $\mathfrak{p} = \mathfrak{P} \cap D$ es un ideal primo en D. Veamos que es no nulo.

Sea $\alpha \in \mathfrak{P}$ no nulo. Sea $p(x)$ el polinomio mínimo de α sobre el cuerpo de cocientes de D. Por el teorema 1.17 (y la observación posterior) sus coeficientes están en D. La ecuación $p(\alpha) = 0$ nos da que el término independiente de $p(x)$ está en $\mathfrak{p}$, y ciertamente es no nulo.

Como D es un dominio de Dedekind $\mathfrak{p}$ es un ideal maximal y el cociente $D/\mathfrak{p}$ es un cuerpo. Tenemos que $\mathfrak{p} \subset \mathfrak{P}$, lo que nos da la situación descrita por el esquema siguiente:

$$\begin{array}{ccc} D & \longrightarrow & E \\ \downarrow & & \downarrow \\ D/\mathfrak{p} & \longrightarrow & E/\mathfrak{P} \end{array}$$

La flecha horizontal superior es la inclusión, las flechas verticales son los epimorfismos canónicos y la flecha inferior es el monomorfismo que hace conmutativo el diagrama, definido de forma natural (a la clase de α le corresponde la clase de α).

Si $E = D[a_1, \ldots, a_n]$ es claro que también $E/\mathfrak{P} = (D/\mathfrak{p})\big[[a_1], \ldots, [a_n]\big]$. El hecho de que cada a_i sea entero sobre D implica que cada $[a_i]$ es algebraico sobre el cuerpo $D/\mathfrak{p}$, pero entonces $(D/\mathfrak{p})[[a_1], \ldots, [a_n]] = (D/\mathfrak{p})([a_1], \ldots, [a_n])$ es un cuerpo. Esto implica que $\mathfrak{P}$ es un ideal maximal. ∎

Las extensiones de $D = \mathbb{Z}$ son precisamente los órdenes maximales de los cuerpos numéricos. En este caso cada primo racional p puede descomponerse en primos de E y sabemos que conocer el modo en que factorizan los primos racionales es un dato muy importante sobre la aritmética de E. En el caso general no está claro qué sentido tiene hablar de factorizaciones en E de primos de D, pues ahora los primos no son elementos de D, sino ideales. Nuestro primer objetivo será, pues, probar que la aplicación que a cada ideal fraccional de E le asigna el ideal fraccional que genera en E es un monomorfismo de grupos, que nos permitirá considerar a los ideales de D como parte de los ideales de E. En realidad lo único que no es trivial es probar que dicha aplicación es un monomorfismo, o sea, que ideales distintos de (1) generan ideales distintos de (1). La clave será el teorema siguiente:

Teorema 1.27 (Lema de Nakayama) *Sea D un dominio íntegro, $\mathfrak{a}$ un ideal de D no nulo contenido en todos los ideales maximales de D y M un D-módulo finitamente generado tal que $\mathfrak{a}M = M$. Entonces $M = 0$.*

Demostración: Sea $M = \langle v_1, \ldots, v_n\rangle$. Entonces $v_n \in \mathfrak{a}M$, luego podemos expresar $v_n = a_1v_1 + \cdots + a_nv_n$, para ciertos $a_1, \ldots, a_n \in \mathfrak{a}$. De aquí que $(1 - a_n)v_n = a_1v_1 + \cdots + a_{n-1}v_{n-1}$.

Si $1 - a_n$ no fuera una unidad estaría en un ideal maximal $\mathfrak{m}$ de D, y por hipótesis tenemos que $a_n \in \mathfrak{a} \subset \mathfrak{m}$, luego $1 \in \mathfrak{m}$, lo cual es imposible. Así pues $1 - a_n$ es una unidad de D y podemos despejar v_n en la ecuación anterior para concluir que $M = \langle v_1, \ldots, v_{n-1}\rangle$. Repitiendo el argumento llegamos a que $M = \langle v_1\rangle$ y finalmente a que $v_1 = 0$. ∎

Teorema 1.28 *Sea D un dominio íntegro y E una extensión entera de D. Sea $\mathfrak{p}$ un primo en D. Entonces $\mathfrak{p}E \neq E$.*

Demostración: Supongamos que $\mathfrak{p}E = E$. Por el teorema 1.23 sabemos que $E_\mathfrak{p}$ es entero sobre $D_\mathfrak{p}$. Si llamamos $\mathfrak{m}$ al ideal maximal de $D_\mathfrak{p}$ es inmediato comprobar que $\mathfrak{m}E_\mathfrak{p} = E_\mathfrak{p}$. Así pues, el teorema es también falso en $D_\mathfrak{p}$, que además es un anillo local. Esto significa que basta probar el teorema en el caso en que D es local.

Si $\mathfrak{p}E = E$ entonces $1 = p_1e_1 + \cdots + p_ne_n$ para ciertos $p_i \in \mathfrak{p}$ y $e_i \in E$.

Sea $D' = D[e_1, \ldots, e_n]$. Por el teorema 1.13 tenemos que D' es un D-módulo finitamente generado y claramente $\mathfrak{p}D' = D'$. Puesto que $\mathfrak{p}$ está contenido en el único ideal maximal de D podemos aplicar el teorema anterior y concluir que $D' = 0$, lo cual es absurdo. ∎

Con esto estamos en condiciones de describir las relaciones básicas entre los primos de un dominio de Dedekind y los de una extensión.

Teorema 1.29 *Sea E/D una extensión de dominios de Dedekind.*

a) La aplicación que a cada ideal fraccional $\mathfrak{a}$ de D le asigna el ideal fraccional $\mathfrak{a}E$ es un monomorfismo de grupos.

b) La correspondencia anterior asigna a ideales primos entre sí imágenes primas entre sí. Si (α) es un ideal principal de D entonces su imagen es el ideal principal (α) generado por α en E.

c) Cada primo de E divide a un único primo de D.

Demostración: Es inmediato comprobar que si $\mathfrak{a}$ es un ideal fraccional de D entonces $\mathfrak{a}E$ es un ideal fraccional de E (ciertamente es un E-módulo, y si $c\mathfrak{a} \subset D$ entonces $c\mathfrak{a}E \subset DE = E$).

También es claro que si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales fraccionales de D entonces $\mathfrak{a}\mathfrak{b}E = (\mathfrak{a}E)(\mathfrak{b}E)$. Esto prueba que la aplicación que estamos considerando es un homomorfismo de grupos.

Si $\mathfrak{p}$ es un primo de D, el teorema anterior nos da que el ideal $\mathfrak{p}E$ que genera en E es un ideal propio (que desde luego ya no tiene por qué ser primo). Si $\mathfrak{P}$ es un factor primo de $\mathfrak{p}E$ en E, entonces $\mathfrak{p} \subset \mathfrak{p}E \subset \mathfrak{P}$, luego $\mathfrak{p} \subset \mathfrak{P} \cap D$. Por otra parte es obvio que $\mathfrak{P} \cap D$ es un ideal propio de D, y como $\mathfrak{p}$ es maximal ha de ser $\mathfrak{p} = \mathfrak{P} \cap D$.

En otras palabras, los primos de E que dividen a $\mathfrak{p}E$ son exactamente los primos $\mathfrak{P}$ que cumplen $\mathfrak{p} = \mathfrak{P} \cap D$, luego si $\mathfrak{p}$ y $\mathfrak{q}$ son primos distintos en D, entonces los primos que dividen a $\mathfrak{p}E$ son distintos de los primos que dividen a $\mathfrak{q}E$, es decir, $\mathfrak{p}E$ y $\mathfrak{q}E$ son ideales de E primos entre sí. En particular son distintos.

La unicidad de la factorización nos da ahora que ideales distintos de D generan ideales distintos de E, luego el homomorfismo es de hecho un monomorfismo.

Con esto queda probado a) y parte de b). El resto de b) es trivial. Respecto a c), si $\mathfrak{P}$ es un primo de E, en la prueba del teorema 1.26 se ve que $\mathfrak{p} = \mathfrak{P} \cap D$ es un ideal primo no nulo de D, y claramente $\mathfrak{p}E \subset \mathfrak{P}$, o sea, $\mathfrak{P} \mid \mathfrak{p}E$. La unicidad se sigue de b). ∎

En lo sucesivo escribiremos $\mathfrak{a}$ en lugar de $\mathfrak{a}E$, es decir, consideraremos a los ideales fraccionales de D como ideales fraccionales de E. Es importante tener claro que un ideal primo en D puede no ser primo en E. Ahora ya tiene sentido estudiar cómo factorizan en E los primos de D.

Definición 1.30 Sea E/D una extensión de dominios de Dedekind. Sea $\mathfrak{p}$ un primo en D y $\mathfrak{P}$ un primo en E tal que $\mathfrak{P} \mid \mathfrak{p}$. Llamaremos *índice de ramificación* de $\mathfrak{p}$ en $\mathfrak{P}$ a la multiplicidad de $\mathfrak{P}$ en $\mathfrak{p}$ y lo representaremos por $e = e(\mathfrak{P}/\mathfrak{p})$.

De este modo, si los primos que dividen a $\mathfrak{p}$ en E son $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ y e_i es el índice de ramificación de $\mathfrak{p}$ en $\mathfrak{P}_i$ entonces la descomposición de $\mathfrak{p}$ en E es $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$.

En el caso de los cuerpos numéricos, cuando $D = \mathbb{Z}$, sabemos que la norma impone una restricción al modo en que pueden factorizar los primos. Concretamente, si el grado del cuerpo es n y $N(\mathfrak{P}_i) = p^{f_i}$, entonces

$$p^n = \mathrm{N}(p) = \mathrm{N}(\mathfrak{P}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{P}_r r)^{e_r} = p^{f_1 e_1 + \cdots f_r e_r},$$

luego ha de ser

$$n = f_1 e_1 + \cdots + f_r e_r. \tag{1.1}$$

Para probar algo así en el caso general nos falta definir los números f_i. No vamos a definirlos a partir de la norma, sino que por el contrario definiremos la norma a partir de ellos. Observemos que si $\mathfrak{P}$ es un primo y $\mathrm{N}(\mathfrak{P}) = |E/\mathfrak{P}| = p^f$, entonces p es el único primo racional al que divide $\mathfrak{P}$ y f es el grado del cuerpo $E/\mathfrak{P}$ sobre su cuerpo primo $\mathbb{Z}/p\mathbb{Z}$. Todo esto tiene sentido en el caso general.

Definición 1.31 Si D es un dominio de Dedekind y $\mathfrak{p}$ es un primo en D, entonces el cociente $D/\mathfrak{p}$ es un cuerpo, al que en lo sucesivo llamaremos *cuerpo de restos* de $\mathfrak{p}$.

Si E es una extensión de D y $\mathfrak{P}$ es un primo en E que divide a $\mathfrak{p}$, razonando como en el teorema 1.26 podemos considerar al cuerpo de restos $\overline{E} = E/\mathfrak{P}$ como una extensión finita de $\overline{D} = D/\mathfrak{p}$ de forma natural (la clase de α se identifica con la clase de α).

Llamaremos *grado de inercia* de $\mathfrak{p}$ en $\mathfrak{P}$ al grado de la extensión de cuerpos $\overline{E}/\overline{D}$. Lo representaremos por $f = f(\mathfrak{P}/\mathfrak{p})$.

Ahora ya tiene sentido (1.1) en el caso general (donde n es el grado de la extensión E/D), si bien todavía no estamos en condiciones de probarla. Esta fórmula indica que cuanto mayor es el grado de inercia de un primo $\mathfrak{p}$ sobre un divisor en una extensión, el número de factores en que se descompone es menor, hasta el extremo de que si $f = n$ entonces $\mathfrak{p}$ se conserva primo en E.

Para llegar a (1.1) necesitamos estudiar los índices de ramificación y los grados de inercia. En primer lugar tenemos la transitividad. La prueba es inmediata.

Teorema 1.32 *Sea $D \subset E \subset F$ una cadena de extensiones de dominios de Dedekind. Sean $\mathfrak{p}$ un primo en F, $\mathfrak{q}$ un primo en E y $\mathfrak{r}$ un primo en D tales que $\mathfrak{p} \mid \mathfrak{q} \mid \mathfrak{r}$. Entonces*

$$e(\mathfrak{p}/\mathfrak{r}) = e(\mathfrak{p}/\mathfrak{q})e(\mathfrak{q}/\mathfrak{r}) \qquad y \qquad f(\mathfrak{p}/\mathfrak{r}) = f(\mathfrak{p}/\mathfrak{q})f(\mathfrak{q}/\mathfrak{r}).$$

Ahora vamos a estudiar la localización de la descomposición de un primo.

Teorema 1.33 *Sea E/D una extensión de dominios de Dedekind de grado n, sea $\mathfrak{p}$ un primo en D y supongamos que su factorización en E es $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, donde los primos $\mathfrak{P}_i$ son distintos dos a dos. Entonces*

a) $E_\mathfrak{p}/D_\mathfrak{p}$ es una extensión de dominios de Dedekind de grado n.

b) $E_\mathfrak{p}$ es un $D_\mathfrak{p}$-módulo libre de rango n.

c) $S^{-1}\mathfrak{p}$ es el único ideal primo de $D_\mathfrak{p}$ y $S^{-1}\mathfrak{P}_1, \ldots, S^{-1}\mathfrak{P}_r$ son los únicos ideales primos de $E_\mathfrak{p}$ (además son distintos dos a dos).

d) Los índices de ramificación y los grados de inercia de $S^{-1}\mathfrak{p}$ en cada $S^{-1}\mathfrak{P}_i$ son los mismos que los de $\mathfrak{p}$ en cada $\mathfrak{P}_i$.

DEMOSTRACIÓN: a) Estamos localizando respecto a $S = D \setminus \mathfrak{p}$, que es un subconjunto multiplicativo tanto de D como de E. Por el teorema 1.23 tanto $E_\mathfrak{p}$ como $D_\mathfrak{p}$ son dominios de Dedekind y $E_\mathfrak{p}$ es una extensión entera de $D_\mathfrak{p}$. Como los cuerpos de cocientes son los mismos, la extensión tiene también grado n.

b) Es claro que un generador de E como D-módulo es también un generador de $E_\mathfrak{p}$ como $D_\mathfrak{p}$-módulo, luego $E_\mathfrak{p}$ es un $D_\mathfrak{p}$-módulo finitamente generado, obviamente libre de torsión, y $D_\mathfrak{p}$ es un dominio euclídeo (ver el final de la sección anterior). Por lo tanto $E_\mathfrak{p}$ es libre.

Sean K y k los cuerpos de cocientes de E y D. Un sistema $D_\mathfrak{p}$-libre es también k-libre, pues multiplicando una combinación lineal con coeficientes en k por un elemento adecuado (no nulo) de $D_\mathfrak{p}$ obtenemos una combinación lineal con coeficientes en $D_\mathfrak{p}$ (teorema 1.18), luego el rango de $E_\mathfrak{p}$ es menor o igual que n. Por otra parte el teorema 1.18 nos da también que existe una k-base de K formada por elementos de $E_\mathfrak{p}$, que obviamente son $D_\mathfrak{p}$-libres, luego el rango de $E_\mathfrak{p}$ es exactamente n.

c) Ya sabemos que $S^{-1}\mathfrak{p}$ es el único ideal primo de $D_\mathfrak{p}$. Por el teorema 1.23 los ideales $S^{-1}\mathfrak{P}_i$ son todos no triviales, pues ninguno de los ideales $\mathfrak{P}_i$ corta a $S = D \setminus \mathfrak{p}$ (se cumple $\mathfrak{p} = \mathfrak{P}_i \cap D$).

Notar que si $a/s \in S^{-1}\mathfrak{P}_i$ con $s \in S$, entonces $a \in \mathfrak{P}_i$, pues $a/s = b/t$ para cierto $b \in \mathfrak{P}_i$, y así $at = bs \in \mathfrak{P}_i$ y como $t \in D \setminus \mathfrak{p}$ no puede ser $t \in \mathfrak{P}_i$, pues entonces $t \in \mathfrak{P}_i \cap D = \mathfrak{p}$. Por lo tanto $a \in \mathfrak{P}_i$.

De aquí se sigue inmediatamente que los ideales $S^{-1}\mathfrak{P}_i$ son primos. Además son distintos, pues si $S^{-1}\mathfrak{P}_i = S^{-1}\mathfrak{P}_j$ todo $a \in \mathfrak{P}_i$ cumpliría $a/1 \in S^{-1}\mathfrak{P}_j$, luego $a \in \mathfrak{P}_j$ y viceversa.

Si $\mathfrak{Q}$ es otro ideal de E entonces $\mathfrak{p} \neq \mathfrak{Q} \cap D$, luego $\mathfrak{Q}$ corta a S y es $S^{-1}\mathfrak{Q} = 1$. Por lo tanto todo ideal de $E_\mathfrak{p}$ se descompone en producto de ideales $S^{-1}\mathfrak{P}_1, \ldots, S^{-1}\mathfrak{P}_r$, luego éstos son los únicos ideales primos de $E_\mathfrak{p}$.

d) Aplicando S^{-1} a la factorización de $\mathfrak{p}$ vemos que los índices de ramificación se conservan. Para probar que lo mismo sucede con los grados de inercia fijemos un primo $\mathfrak{P} = \mathfrak{P}_i$. Como $\mathfrak{P} \subset S^{-1}\mathfrak{P}$ tenemos la situación siguiente:

$$\begin{array}{ccc} E/\mathfrak{P} & \longrightarrow & E_\mathfrak{p}/S^{-1}\mathfrak{P} \\ \uparrow & & \uparrow \\ D/\mathfrak{p} & \longrightarrow & D_\mathfrak{p}/S^{-1}\mathfrak{p} \end{array}$$

Todas las flechas indican monomorfismos de cuerpos definidos de forma natural: a la clase de un α le corresponde la clase de α. Las flechas verticales

determinan extensiones cuyos grados son los grados de inercia que queremos comparar. La flecha horizontal inferior es un isomorfismo por el teorema 1.24.

Basta probar que la flecha horizontal superior también es un isomorfismo, lo que equivale a probar que todo elemento de $E_\mathfrak{p}$ es congruente con uno de E módulo $S^{-1}\mathfrak{P}$, pero si $a/s \in E_\mathfrak{p}$ entonces $s \notin \mathfrak{P}$, luego es una unidad en $E/\mathfrak{P}$, es decir, existe un $b \in E$ de manera que $bs \equiv 1$ (mód $\mathfrak{P}$), de donde se sigue que $bs \equiv 1$ (mód $S^{-1}\mathfrak{P}$) y $a/s \equiv ab$ (mód $S^{-1}\mathfrak{P}$). ∎

Ahora ya podemos probar la relación (1.1). Notemos que la prueba se apoya en que al localizar una extensión obtenemos una extensión libre, de acuerdo con el apartado b) del teorema anterior.

Teorema 1.34 *Sea E/D una extensión de dominios de Dedekind de grado n. Sea $\mathfrak{p}$ un primo en D, sea $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ la factorización de $\mathfrak{p}$ en E y para cada i sea f_i el grado de inercia de $\mathfrak{p}$ en $\mathfrak{P}_i$. Entonces*

$$n = f_1e_1 + \cdots + f_re_r.$$

Demostración: Por el teorema anterior podemos localizar en $\mathfrak{p}$ y suponer que D es un anillo local, que E es un D-módulo libre de rango n y que $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ son los únicos primos de E.

Es claro que $E/\mathfrak{p}E$ es un espacio vectorial sobre $D/\mathfrak{p}$. Veamos que su dimensión es n.

Sea $\{w_1, \ldots, w_n\}$ una D-base de E. Es claro que $\{[w_1], \ldots, [w_n]\}$ es un generador de $E/\mathfrak{p}E$. Basta ver que es libre. Como D es un dominio de Dedekind con un único primo, el ideal $\mathfrak{p}$ es principal, o sea, $\mathfrak{p} = pD$, luego $\mathfrak{p}E = pE$.

Si $[d_1][w_1] + \cdots + [d_n][w_n] = 0$, entonces $d_1w_1 + \cdots + d_nw_n \in pE$, luego

$$d_1w_1 + \cdots + d_nw_n = p(c_1w_1 + \cdots + c_nw_n), \qquad \text{con } c_i \in D,$$

y por la unicidad $d_i = pc_i$. Así pues, $[d_i] = 0$ para $i = 1, \ldots, n$.

Para cada $i = 1, \ldots, r$ consideremos el epimorfismo canónico $E \longrightarrow E/\mathfrak{P}_i^{e_i}$. Estos epimorfismos inducen un homomorfismo

$$E \longrightarrow \prod_{i=1}^{r} E/\mathfrak{P}_i^{e_i}.$$

El teorema chino del resto nos da que este homomorfismo es en realidad un epimorfismo. Su núcleo está formado por los elementos de E divisibles entre todos los ideales , y como son primos entre sí, éstos son los múltiplos del producto de todos ellos, o sea, los múltiplos (los elementos) de $\mathfrak{p}E$. Por lo tanto tenemos un isomorfismo

$$E/\mathfrak{p}E \longrightarrow \prod_{i=1}^{r} E/\mathfrak{P}_i^{e_i}.$$

Los factores son también espacios vectoriales sobre $D/\mathfrak{p}$ y nuestro isomorfismo es también un isomorfismo de espacios vectoriales. El teorema quedará probado si vemos que la dimensión de cada factor $E/\mathfrak{P}_i^{e_i}$ es exactamente f_ie_i.

Por simplificar la notación fijemos $\mathfrak{P} = \mathfrak{P}_i$, $e = e_i$, $f = f_i$, para cierto índice i. Claramente $\mathfrak{P}^e \subset \mathfrak{P}^{e-1} \subset \cdots \subset \mathfrak{P}^2 \subset \mathfrak{P} \subset E$, luego

$$1 = \mathfrak{P}^e/\mathfrak{P}^e \subset \mathfrak{P}^{e-1}/\mathfrak{P}^e \subset \cdots \subset \mathfrak{P}^2/\mathfrak{P}^e \subset \mathfrak{P}/\mathfrak{P}^e \subset E/\mathfrak{P}^e,$$

donde cada término es un subespacio vectorial. La dimensión de $E/\mathfrak{P}^e$ es la suma de las dimensiones de los espacios cociente. Es fácil ver que

$$(E/\mathfrak{P}^e) \Big/ (\mathfrak{P}/\mathfrak{P}^e) \cong E/\mathfrak{P} \qquad \text{como } D/\mathfrak{p}\text{-espacios vectoriales}$$

(no es el teorema de isomorfía usual porque ni E ni $\mathfrak{P}$ son $D/\mathfrak{p}$-espacios vectoriales). Del mismo modo los cocientes restantes son isomorfos a los espacios $\mathfrak{P}^i/\mathfrak{P}^{i+1}$, para $i = 1, \ldots, e-1$.

Basta demostrar que todos estos espacios tienen dimensión f. Ciertamente, la dimensión de $E/\mathfrak{P}$ sobre $D/\mathfrak{p}$ es f por definición. Basta probar que todos los espacios $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ son isomorfos a $E/\mathfrak{P}$.

El anillo E es un dominio de Dedekind con un número finito de primos, luego es un dominio de ideales principales. Sea $\mathfrak{P} = (\pi)$. Entonces $\mathfrak{P}^i = (\pi^i)$.

La aplicación $\phi : E/\mathfrak{P} \longrightarrow \mathfrak{P}^i/\mathfrak{P}^{i+1}$ dada por $\phi([\alpha]) = [\pi^i\alpha]$ es claramente un isomorfismo de espacios vectoriales, luego el teorema queda probado. ∎

1.4 Extensiones de Galois

Los resultados que hemos obtenido se pueden mejorar cuando tratamos con extensiones finitas de Galois.

Sea E/D una extensión de Galois de dominios de Dedekind (lo cual significa, naturalmente, que la extensión K/k de los cuerpos de cocientes es finita de Galois). Sea $G(K/k)$ el grupo de Galois.

Es claro que cada $\sigma \in G(K/k)$ envía elementos de E a elementos de E (envía raíces de polinomios mónicos de $D[x]$ a raíces de polinomios mónicos de $D[x]$), luego $\sigma|_E$ es un automorfismo de E que deja fijos a los elementos de D. Recíprocamente, cada automorfismo de E que deja fijos a los elementos de D se extiende de forma natural a un k-automorfismo de K.

Llamaremos $G(E/D)$ al grupo de los D-automorfismos de E, es decir, al grupo de los automorfismos de E que dejan fijos a los elementos de D. Según lo que acabamos de observar resulta que los grupos $G(K/k)$ y $G(E/D)$ son isomorfos y no los distinguiremos. Puesto que $E \cap k = D$, los elementos de D son exactamente los elementos de E fijados por todos los automorfismos de $G(E/D)$.

Ahora, si $\sigma \in G(E/D)$ y $\mathfrak{a}$ es un ideal fraccional de E, definimos

$$\sigma(\mathfrak{a}) = \sigma[\mathfrak{a}] = \{\sigma(\alpha) \mid \alpha \in \mathfrak{a}\},$$

que claramente es un ideal fraccional de E, y es un ideal si $\mathfrak{a}$ lo es.

Vemos, pues, que cada $\sigma \in G(E/D)$ induce de este modo un automorfismo en el grupo de los ideales fraccionales de E que envía ideales a ideales, ideales

primos a ideales primos, conserva las factorizaciones y la divisibilidad y es compatible con la acción de σ sobre K, en el sentido de que $\sigma(\alpha E) = \sigma(\alpha)E$ para todo $\alpha \in K$.

Observar además que si $\mathfrak{a}$ es un ideal fraccional de D entonces $\sigma(\mathfrak{a}E) = \sigma(\mathfrak{a})E = \mathfrak{a}E$, o sea, que σ fija a los ideales de D. Sin embargo no es cierto que un ideal fijado por todos los D-automorfismos de E haya de ser un ideal de D. Enseguida veremos por qué.

Diremos que dos ideales fraccionales $\mathfrak{a}$ y $\mathfrak{b}$ de E son *conjugados* si existe un automorfismo $\sigma \in G(E/D)$ tal que $\sigma(\mathfrak{a}) = \mathfrak{b}$.

Teorema 1.35 *Sea E/D una extensión de Galois de dominios de Dedekind. Entonces dos ideales primos de E son conjugados si y sólo si dividen al mismo primo de D.*

Demostración: Sean $\mathfrak{P}$ y $\mathfrak{Q}$ primos en E. Si son conjugados por un automorfismo σ y $\mathfrak{P}$ divide a un primo $\mathfrak{p}$ de D entonces $\mathfrak{Q} = \sigma(\mathfrak{P}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}$.

Supongamos ahora que $\mathfrak{P} \mid \mathfrak{p}$ y $\mathfrak{Q} \mid \mathfrak{p}$ pero que $\sigma(\mathfrak{P}) \neq \mathfrak{Q}$ para todo automorfismo σ. Por el teorema chino del resto existe un $\alpha \in E$ tal que

$$\begin{aligned} &\alpha \equiv 0 \pmod{\mathfrak{Q}},\\ &\alpha \equiv 1 \pmod{\sigma(\mathfrak{P})} \quad \text{para todo } \sigma \in G(E/D). \end{aligned}$$

Pero entonces $\mathrm{N}(\alpha) = \prod_\sigma \sigma(\alpha) \equiv 1 \pmod{\mathfrak{P}}$ y por otra parte $\alpha \in \mathfrak{Q}$ y es uno de los factores de $\mathrm{N}(\alpha)$, luego $\mathrm{N}(\alpha) \in \mathfrak{Q} \cap D = \mathfrak{p} \subset \mathfrak{P}$, contradicción. ∎

De aquí se sigue que las factorizaciones de primos en extensiones de Galois son muy sencillas:

Teorema 1.36 *Sea E/D una extensión de Galois de grado n de dominios de Dedekind, sea $\mathfrak{p}$ un primo en D y sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ los primos de E que lo dividen. Entonces todos los índices de ramificación $e(\mathfrak{P}_i/\mathfrak{p})$ son iguales a un mismo número e y todos los grados de inercia $f(\mathfrak{P}_i/\mathfrak{p}))$ son iguales a un mismo número f. Por lo tanto la factorización de $\mathfrak{p}$ en E es de la forma*

$$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e,$$

y se cumple la relación $n = efr$.

Demostración: Dados i, j, existe un automorfismo σ tal que $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Como σ conserva la divisibilidad, es claro que conserva las multiplicidades, luego $e(\mathfrak{P}_i/\mathfrak{p}) = e(\mathfrak{P}_j/\mathfrak{p})$.

Por otra parte es claro que σ induce un isomorfismo $E/\mathfrak{P}_i \longrightarrow E/\mathfrak{P}_j$ que deja fijos a los elementos de $D/\mathfrak{p}$ (las clases con representante en D), luego los grados de $E/\mathfrak{P}_i$ y $E/\mathfrak{P}_j$ sobre $D/\mathfrak{p}$ coinciden, es decir, $f(\mathfrak{P}_i/\mathfrak{p}) = f(\mathfrak{P}_j/\mathfrak{p})$. La relación $n = efr$ es la particularización a este caso del teorema 1.34. ∎

Así pues, la descomposición de un primo en una extensión de Galois está determinada por los tres números e, f y r. Veamos ahora que cambiando el dominio base por otro mayor podemos hacer $r = 1$ conservando e y f.

Definición 1.37 Sea E/D una extensión de Galois de dominios de Dedekind, sea $G = G(E/D)$ y sea $\mathfrak{P}$ un primo en E. Llamaremos *grupo de descomposición* de $\mathfrak{P}$ al grupo

$$G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} \leq G.$$

Sea $\tau \in G$. Entonces $\sigma(\tau(\mathfrak{P})) = \tau(\mathfrak{P})$ si y sólo si $\tau^{-1}(\sigma(\tau(\mathfrak{P}))) = \mathfrak{P}$, es decir, si y sólo si $\tau\sigma\tau^{-1} \in G_{\mathfrak{P}}$, si y sólo si $\sigma \in \tau^{-1}G_{\mathfrak{P}}\tau = G^{\tau}_{\mathfrak{P}}$.

Así pues, tenemos que $G_{\tau(\mathfrak{P})} = G^{\tau}_{\mathfrak{P}}$, es decir, los grupos de descomposición de los primos conjugados con $\mathfrak{P}$ son los grupos conjugados del grupo de descomposición de $\mathfrak{P}$.

Notar también que $\sigma(\mathfrak{P}) = \tau(\mathfrak{P})$ si y sólo si $\tau\sigma^{-1} \in G_{\mathfrak{P}}$, por lo que si $G/G_{\mathfrak{P}}$ es el conjunto cociente para la congruencia por la derecha módulo $G_{\mathfrak{P}}$ (que no es un grupo en general) y $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ son los primos conjugados con $\mathfrak{P}$, entonces la aplicación $f : G/G_{\mathfrak{P}} \longrightarrow \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ dada por $f([\sigma]) = \sigma(\mathfrak{P})$ es biyectiva. Consecuentemente $|G_{\mathfrak{P}}| = n/r = ef$ (con la notación del teorema anterior).

Llamaremos *cuerpo de descomposición* de $\mathfrak{P}$ al cuerpo L fijado por $G_{\mathfrak{P}}$. El *dominio de descomposición* de $\mathfrak{P}$ será la clausura entera F de D en L, que por el teorema 1.26 es un dominio de Dedekind tal que $D \subset F \subset E$.

Teorema 1.38 *Sea E/D una extensión de Galois de dominios de Dedekind. Sea $\mathfrak{P}$ un primo en E y sea $\mathfrak{p} = \mathfrak{P} \cap D$. Sea F el dominio de descomposición de $\mathfrak{P}$ y sea $\mathfrak{p}' = \mathfrak{P} \cap F$. Entonces*

a) $e = e(\mathfrak{P}/\mathfrak{p}') = e(\mathfrak{P}/\mathfrak{p})$, $f = f(\mathfrak{P}/\mathfrak{p}') = f(\mathfrak{P}/\mathfrak{p})$, $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$.

b) $\mathfrak{p}' = \mathfrak{P}^e$.

c) F es el menor dominio de Dedekind intermedio T entre D y E tal que $\mathfrak{P}$ es el único primo que divide a $\mathfrak{P} \cap T$.

Demostración: En primer lugar observamos que E/F es una extensión de Galois cuyo grupo de Galois es $G_{\mathfrak{P}}$. Esto significa que $\mathfrak{P}$ es su único conjugado en esta extensión, luego por el teorema 1.35 tenemos que $\mathfrak{P}$ es el único primo de E que divide a $\mathfrak{p}'$.

a) Veamos que $f(\mathfrak{p}'/\mathfrak{p}) = 1$. Hemos de probar que el monomorfismo natural $D/\mathfrak{p} \longrightarrow F/\mathfrak{p}'$ es un isomorfismo, o sea, que todo elemento de F es congruente con un elemento de D módulo $\mathfrak{p}'$.

Sea $G = G(E/D)$. Si $\sigma \in G \setminus G_{\mathfrak{P}}$ entonces $\sigma(\mathfrak{P}) \neq \mathfrak{P}$, luego $\sigma^{-1}(\mathfrak{P}) \neq \mathfrak{P}$. Como $\mathfrak{P}$ es el único primo que divide a $\mathfrak{p}'$ resulta que $\mathfrak{p}'_\sigma = \sigma^{-1}(\mathfrak{P}) \cap F \neq \mathfrak{p}'$.

Sea $\alpha \in F$. Por el teorema chino del resto existe un elemento $\beta \in F$ tal que

$$\begin{aligned} \beta &\equiv \alpha \ (\text{mód } \mathfrak{p}'), \\ \beta &\equiv 1 \ (\text{mód } \mathfrak{p}'_\sigma), \qquad \text{para todo } \sigma \in G \setminus G_{\mathfrak{P}}. \end{aligned}$$

En particular

$$\begin{aligned} \beta &\equiv \alpha \ (\text{mód } \mathfrak{P}), \\ \beta &\equiv 1 \ (\text{mód } \sigma^{-1}(\mathfrak{P})), \qquad \text{para todo } \sigma \in G \setminus G_{\mathfrak{P}}. \end{aligned}$$

La segunda congruencia implica que $\sigma(\beta) \equiv 1$ (mód $\mathfrak{P}$) para todo $\sigma \in G \setminus G_{\mathfrak{P}}$. La norma de β en la extensión F/D es el producto de β por otros factores de la forma $\sigma(\beta)$ con $\sigma \in G \setminus G_{\mathfrak{P}}$, luego $\mathrm{N}(\beta) \equiv \alpha$ (mód $\mathfrak{P}$). Pero $\mathrm{N}(\beta) \in D$ y así $\mathrm{N}(\beta) - \alpha \in F \cap \mathfrak{P} = \mathfrak{p}'$, con lo que tenemos $\mathrm{N}(\beta) \equiv \alpha$ (mód $\mathfrak{p}'$) con $N(\beta) \in D$, que era lo que queríamos probar.

Así pues, $f(\mathfrak{p}'/\mathfrak{p}) = 1$. Por el teorema 1.32 concluimos que $f = f(\mathfrak{P}/\mathfrak{p}') = f(\mathfrak{P}/\mathfrak{p})$.

Ahora, el grado de la extensión E/F es el orden de $G_{\mathfrak{P}}$, que es ef (donde $e = e(\mathfrak{P}/\mathfrak{p})$). Por el teorema 1.36 (puesto que $r = 1$ para la extensión E/F) resulta que $e = e(\mathfrak{P}/\mathfrak{p}')$, y de la igualdad $e = e(\mathfrak{P}/\mathfrak{p}') = e(\mathfrak{P}/\mathfrak{p})$ se sigue, de nuevo por el teorema 1.32, que $e(\mathfrak{p}'/\mathfrak{p}) = 1$.

b) ya está probado.

c) Sea T un dominio de Dedekind intermedio tal que $\mathfrak{P}$ sea el único primo que divide a $\mathfrak{P} \cap T$. Esto significa que $\mathfrak{P}$ no tiene conjugados respecto a la extensión E/T, luego $G(E/T) \leq G_{\mathfrak{P}}$, luego $F \subset T$. ∎

Un caso especialmente notable se da cuando E/D es una extensión abeliana. Entonces todos los divisores en E de un primo $\mathfrak{p}$ de D tienen el mismo grupo de descomposición (pues dos cualesquiera son conjugados) y por lo tanto el mismo dominio de descomposición F. Así, si la factorización de $\mathfrak{p}$ en E es

$$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e,$$

el teorema anterior implica que la factorización en F tiene la forma

$$\mathfrak{p} = \mathfrak{p}'_1 \cdots \mathfrak{p}'_r, \tag{1.2}$$

donde los primos $\mathfrak{p}'_i$ son distintos y cada uno factoriza en E como $\mathfrak{p}'_i = \mathfrak{P}_i^e$. Además $f(\mathfrak{P}_i, \mathfrak{p}) = f(\mathfrak{P}_i, \mathfrak{p}'_i)$. Es decir, podemos descomponer la factorización de $\mathfrak{p}$ en dos fases. En la primera aparecen los r factores que han de aparecer en E pero con $e = f = 1$, y en la segunda fase cada factor se descompone con $r = 1$ pero con los mismos valores de e y f correspondientes a la extensión total E/D.

Si la extensión no es abeliana no podemos hablar en general de la descomposición intermedia (1.2), pero al menos tenemos una extensión E/F, distinta para cada primo $\mathfrak{P}_i$, donde éste ha perdido a sus conjugados conservando los números e y f. Ahora veremos que podemos separar e y f en dos extensiones sucesivas.

Si E/D es una extensión de Galois de dominios de Dedekind, $\mathfrak{p}$ es un primo en D y $\mathfrak{P}$ es un primo en E que divide a $\mathfrak{p}$, entonces cada $\sigma \in G_{\mathfrak{P}}$ induce de forma natural un $D/\mathfrak{p}$-automorfismo de $E/\mathfrak{P}$ dado por $\overline{\sigma}([\alpha]) = [\sigma(\alpha)]$ (es biyectivo porque tiene por inversa a la aplicación inducida por σ^{-1}). La aplicación $\sigma \mapsto \overline{\sigma}$ es un homomorfismo de grupos.

En general, la extensión $E/\mathfrak{P}$ sobre $D/\mathfrak{p}$ es normal y el homomorfismo anterior es un epimorfismo entre los grupos de Galois, pero la separabilidad puede perderse. Este problema no aparece en el caso de los cuerpos numéricos, pues en ellos los ideales primos dan cocientes finitos, luego perfectos.

Teorema 1.39 *Sea E/D una extensión de Galois de dominios de Dedekind con grupo de Galois G, sea $\mathfrak{p}$ un primo en D y $\mathfrak{P}$ un primo en E que divida a $\mathfrak{p}$. Sean $\overline{E} = E/\mathfrak{P}$ y $\overline{D} = D/\mathfrak{p}$. Supongamos que la extensión $\overline{E}/\overline{D}$ es separable. Entonces $\overline{E}/\overline{D}$ es de Galois y la aplicación $\sigma \mapsto \overline{\sigma}$ descrita arriba es un epimorfismo de $G_\mathfrak{P}$ sobre $G(\overline{E}/\overline{D})$.*

DEMOSTRACIÓN: Veamos que la extensión $\overline{E}/\overline{D}$ es normal. Dada una clase $[\alpha] \in \overline{E}$, sea $p(x)$ el polinomio mínimo de α en la extensión E/D. Como la extensión es de Galois, $p(x)$ se escinde en factores lineales y todas las raíces son elementos de E (porque son conjugadas de α). Tomando clases módulo $\mathfrak{P}$ en la factorización de $p(x)$ llegamos a que $[\alpha]$ es la raíz de un polinomio de $\overline{D}[x]$ que se escinde en $\overline{E}[x]$, luego el polinomio mínimo de $[\alpha]$ también se escinde y la extensión es normal.

Sea F el dominio de descomposición de $\mathfrak{P}$. Sea $\mathfrak{p}' = \mathfrak{P} \cap F$. Por el teorema anterior $f(\mathfrak{p}'/\mathfrak{p}) = 1$, lo que significa que $D/\mathfrak{p} = F/\mathfrak{p}'$, o sea, que la extensión $\overline{E}/\overline{D}$ es la misma que la extensión $\overline{E}/\overline{F}$. Por otra parte $G(E/F)_\mathfrak{P} = G(E/F) = G_\mathfrak{P}$, y todo esto nos da que podemos tomar como dominio base a F en lugar de D, es decir, podemos suponer que $G = G_\mathfrak{P}$.

Sea $[\alpha]$ un elemento primitivo de la extensión $\overline{E}/\overline{D}$ y sea $p(x)$ el polinomio mínimo de α sobre D. Entonces $p(x)$ se escinde en $E[x]$. Sean $\alpha_1, \ldots, \alpha_t$ todas sus raíces. Si $\overline{p}(x)$ es la imagen de $p(x)$ por el epimorfismo canónico de $D[x]$ sobre $\overline{D}[x]$ entonces $\overline{p}(x)$ se escinde en $\overline{E}[x]$ y sus raíces son $[\alpha_1], \ldots, [\alpha_t]$.

Un automorfismo $\tau \in G(\overline{E}/\overline{D})$ cumplirá $\tau([\alpha]) = [\alpha_i]$ para algún i, pero existe un automorfismo $\sigma \in G$ tal que $\sigma(\alpha) = \alpha_i$, luego $\bar{\sigma}([\alpha]) = [\alpha_i]$ y, como $[\alpha]$ es un elemento primitivo, esto implica que $\overline{\sigma} = \tau$. ∎

Definición 1.40 Sea E/D una extensión de Galois de dominios de Dedekind, sea $\mathfrak{p}$ un primo en D y $\mathfrak{P}$ un primo en E que divida a $\mathfrak{p}$ de modo que $E/\mathfrak{p}$ sea una extensión separable de $D/\mathfrak{p}$. Llamaremos *grupo de inercia* de $\mathfrak{P}$ al núcleo $T_\mathfrak{P}$ del epimorfismo descrito en el teorema anterior.

El teorema anterior nos da que $G_\mathfrak{P}/T_\mathfrak{P} \cong G(\overline{E}/\overline{D})$, y por lo tanto el orden de este grupo es f. Como $|G_\mathfrak{P}| = ef$ concluimos que $|T_\mathfrak{P}| = e$.

Teorema 1.41 *Sea E/D una extensión de Galois de grado n de dominios de Dedekind. Sea $\mathfrak{p}$ un primo en D y $\mathfrak{P}$ un primo en E que divida a $\mathfrak{p}$. Supongamos que $\overline{E} = E/\mathfrak{P}$ es una extensión separable de $\overline{D} = D/\mathfrak{p}$. Sean F y Z los anillos de enteros de los cuerpos fijados por el grupo de descomposición y el grupo de inercia de $\mathfrak{p}$ respectivamente. Llamemos $e = e(\mathfrak{P}/\mathfrak{p})$, $f = f(\mathfrak{P}/\mathfrak{p})$ y r al número de primos que dividen a $\mathfrak{p}$ en E. Sean $\mathfrak{p}' = \mathfrak{P} \cap F$, $\mathfrak{p}'' = \mathfrak{P} \cap Z$. Entonces se tienen los datos contenidos en la tabla siguiente:*

Grado	r	f	e	
Anillo	D	F	Z	E
Primo	$\mathfrak{p}$	$\mathfrak{p}'$	$\mathfrak{p}''$	$\mathfrak{P}$
Índ. de r.	1	1	e	
Grad. de i.	1	f	1	

DEMOSTRACIÓN: Ya sabemos que los grados son los indicados en la tabla. Los valores de la extensión F/D están dados en el teorema 1.38. Consideremos los cuerpos $\overline{D} = \overline{F} \subset \overline{Z} \subset \overline{E}$. Según el teorema 1.39 tenemos un epimorfismo $G(E/F) \longrightarrow G(\overline{E}/\overline{D})$ cuyo núcleo es por definición $T_{\mathfrak{P}} = G(E/Z)$. Así pues, el epimorfismo correspondiente a $G(E/Z) \longrightarrow G(\overline{E}/\overline{Z})$ tiene imagen trivial, luego $\overline{Z} = \overline{E}$. Esto nos da que $f(\mathfrak{P}/\mathfrak{p}'') = 1$.

Por otra parte, todos los automorfismos de $G(E/Z)$ fijan a $\mathfrak{P}$, luego el grado $e = |E : Z|$ coincide con el orden del grupo de descomposición de esta extensión, o sea, con $e(\mathfrak{P}/\mathfrak{p}'')f(\mathfrak{P}/\mathfrak{p}'')$. Por consiguiente $e(\mathfrak{P}/\mathfrak{p}'') = e$.

Con esto tenemos comprobados los valores correspondientes a las extensiones F/D y E/Z. Los de la extensión Z/F se siguen del teorema 1.32. ∎

De nuevo la situación descrita por el teorema anterior resulta más clara en el caso de extensiones abelianas, donde los dominios F y Z son los mismos para todos los divisores de un mismo primo $\mathfrak{p}$ de D. Al pasar a F la descomposición de $\mathfrak{p}$ es, según ya sabíamos, de la forma

$$\mathfrak{p} = \mathfrak{p}'_1 \cdots \mathfrak{p}'_r,$$

con $e(\mathfrak{p}'_i, \mathfrak{p}) = f(\mathfrak{p}'_i, \mathfrak{p}) = 1$. Al pasar a Z tenemos $\mathfrak{p}'_i = \mathfrak{p}''_i$, es decir, cada primo $\mathfrak{p}'_i$ se conserva primo en Z, pero el grado de inercia aumenta todo cuanto ha de aumentar de D a E. Finalmente, al pasar de Z a E tenemos $\mathfrak{p}''_i = \mathfrak{P}_i^e$, de manera que en este tramo se produce toda la ramificación sin que varíe el grado de inercia.

1.5 Normas de ideales

Ahora estamos en condiciones de extender a ideales la norma que tenemos definida sobre los elementos de cualquier extensión finita. Como ya habíamos observado, en el caso de un primo $\mathfrak{p}$ de un cuerpo numérico la norma viene dada por $\mathrm{N}(\mathfrak{p}) = p^f$, donde p es el único primo racional divisible entre p y f es el grado de inercia. La definición general sigue esta línea.

Definición 1.42 Sea E/D una extensión de dominios de Dedekind. Para cada primo $\mathfrak{P}$ de E definimos $\mathrm{N}_D^E(\mathfrak{P}) = \mathfrak{p}^f$, donde $\mathfrak{p} = \mathfrak{P} \cap D$ y $f = f(\mathfrak{P}/\mathfrak{p})$. Esta norma se extiende de forma única a un homomorfismo del grupo de los ideales fraccionales de E en el grupo de los ideales fraccionales de D. La norma de un ideal de E es un ideal de D.

Del teorema 1.32 se sigue que si tenemos dos extensiones F/E y E/D entonces $\mathrm{N}_D^F(\mathrm{N}_F^E(\mathfrak{a})) = \mathrm{N}_D^E(\mathfrak{a})$ para todo ideal fraccional $\mathfrak{a}$ de E. (Se prueba primero para ideales primos).

El teorema siguiente recoge otras propiedades básicas de la norma:

Teorema 1.43 *Sea E/D una extensión de dominios de Dedekind de grado n. Entonces*

a) Si $\mathfrak{a}$ es un ideal fraccional de D se cumple que $\mathrm{N}_D^E(\mathfrak{a}) = \mathfrak{a}^n$.

b) Si la extensión E/D es de Galois y $G = G(E/D)$ entonces

$$\mathrm{N}_D^E(\mathfrak{a}) = \prod_\sigma \sigma(\mathfrak{a}).$$

c) Si $\alpha \neq 0$ está en el cuerpo de cocientes de E entonces $\mathrm{N}_D^E(\alpha E) = \mathrm{N}_D^E(\alpha)D$.

Demostración: a) Basta probarlo cuando $\mathfrak{a}$ es primo y usar que las expresiones de los dos miembros conservan productos. El caso primo se sigue inmediatamente del teorema 1.34.

b) Por el mismo motivo que en a) basta probarlo para un ideal primo $\mathfrak{P}$. Sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ los conjugados de $\mathfrak{P}$ y sea $\mathfrak{q}$ el primo de D al que dividen. Teniendo en cuenta las observaciones hechas tras la definición 1.37, es claro que cuando σ recorre G la expresión $\sigma(\mathfrak{P})$ toma el valor $\mathfrak{P}_i$ exactamente $|G_\mathfrak{P}| = ef$ veces. Por lo tanto

$$\prod_{\sigma\in G} \sigma(p) = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^{ef} = \mathfrak{q}^f = \mathrm{N}_D^E(\mathfrak{P}).$$

c) Supongamos en primer lugar que E/D es separable y sea F la menor extensión de Galois sobre D que contiene a E. Por el apartado anterior

$$\mathrm{N}_D^F(\alpha F) = \prod_{\sigma\in G} \sigma(\alpha F) = \prod_{\sigma\in G} \sigma(\alpha)F = \mathrm{N}_D^F(\alpha)F = \mathrm{N}_D^F(\alpha)D.$$

(El último paso se debe a la identificación entre ideales de F e ideales de D).

Por lo tanto

$$\mathrm{N}_D^E(\mathrm{N}_E^F(\alpha F)) = \mathrm{N}_D^E(\mathrm{N}_E^F(\alpha))D,$$

pero si $m = |F : E|$ esto equivale a

$$\mathrm{N}_D^E((\alpha E)^m) = \mathrm{N}_D^E(\alpha^m)D,$$

de donde $\mathrm{N}_D^E(\alpha E)^m = (\mathrm{N}_D^E(\alpha)D)^m$, y por la factorización única ideal concluimos que $\mathrm{N}_D^E(\alpha E) = \mathrm{N}_D^E(\alpha)D$.

Si E/D no es separable, consideramos la clausura separable K del cuerpo de cocientes de D en el cuerpo de cocientes de E. Por el teorema 1.26, la clausura entera F de D en K es una extensión de D y obviamente E/F también es una extensión de dominios de Dedekind (E es finitamente generado sobre D, luego también sobre F). La transitividad de las normas y el caso ya probado reducen el problema a la extensión puramente inseparable E/F. Sea m el grado de la extensión. Entonces, todo $\alpha \in E$ cumple que $\alpha^m \in F$, luego por el apartado a) tenemos que

$$\mathrm{N}_F^E(\alpha E)^m = \mathrm{N}_F^E(\alpha^m E) = \alpha^{m^2} F = \big(\mathrm{N}_F^E(\alpha)F\big)^m.$$

Como en el caso anterior, podemos eliminar la m de ambos miembros. ∎

La norma de un ideal de un cuerpo numérico coincide con el número de elementos del anillo cociente que determina. Esto puede usarse para definir una

norma sobre los ideales de cualquier dominio de Dedekind con tal de que los anillos cociente sean finitos. Como éste será el caso en todos los dominios de Dedekind que nos van a interesar, conviene definir esta norma en un contexto general.

Definición 1.44 Diremos que un dominio de Dedekind D tiene *restos finitos* si para todo ideal primo $\mathfrak{p}$ de D se cumple que el cuerpo de restos $D/\mathfrak{p}$ es finito. En tal caso definimos la *norma absoluta* de $\mathfrak{p}$ como $\mathrm{N}\,\mathfrak{p} = |D/\mathfrak{p}|$. La norma absoluta se extiende multiplicativamente a todos los ideales fraccionales de D.

De este modo, si $\mathfrak{a}$ es un ideal fraccional, se cumple que $\mathrm{N}\,\mathfrak{a}$ es un número racional positivo, y es un número natural si $\mathfrak{a}$ es un ideal.

El teorema 1.24 implica que si $\mathfrak{p}$ es un primo de un dominio de Dedekind D con restos finitos y $D_\mathfrak{p}$ es la localización en $\mathfrak{p}$, entonces $D_\mathfrak{p}$ tiene restos finitos y, si $\mathfrak{m}$ es su único ideal maximal, se cumple $\mathrm{N}\,\mathfrak{m}^n = \mathrm{N}\,\mathfrak{p}^n$ para todo número entero n.

Teorema 1.45 *Sea D un dominio de Dedekind con restos finitos y sea $\mathfrak{a}$ un ideal de D. Entonces $\mathrm{N}\,\mathfrak{a} = |D/\mathfrak{a}|$.*

Demostración: La prueba es una variante de la del teorema 1.34. Supongamos primero que $\mathfrak{a} = \mathfrak{p}^e$. Sea p la característica de $D/\mathfrak{p}$ (que claramente es la misma que la del anillo $D/\mathfrak{p}^e$). Podemos localizar en $\mathfrak{p}$ y suponer que éste es el único ideal primo de D. Entonces

$$1 = \mathfrak{p}^e/\mathfrak{p}^e \subset \mathfrak{p}^{e-1}/\mathfrak{p}^e \subset \cdots \subset \mathfrak{p}^2/\mathfrak{p}^e \subset \mathfrak{p}/\mathfrak{p}^e \subset D/\mathfrak{p}^e,$$

y cada término es un subespacio vectorial de $D/\mathfrak{p}^e$ (considerado como espacio vectorial sobre $\mathbb{Z}/p\mathbb{Z}$). Como en el teorema 1.34 se prueba que cada cociente entre dos subespacios consecutivos es isomorfo a $D/\mathfrak{p}$, con lo que $|D/\mathfrak{p}^e| = |D/\mathfrak{p}|^e = (\mathrm{N}\,\mathfrak{p})^e = \mathrm{N}\,\mathfrak{p}^e$.

En general, si $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, la aplicación $D \longrightarrow \prod_{i=1}^r E/\mathfrak{p}_i^{e_i}$ que a cada elemento de D le asigna la r-tupla de sus clases módulo $\mathfrak{p}_i^{e_i}$ es un homomorfismo de anillos suprayectivo, por el teorema chino del resto, y su núcleo es obviamente igual a $\mathfrak{a}$. Así pues tenemos un isomorfismo

$$D/\mathfrak{a} \cong \prod_{i=1}^r E/\mathfrak{p}_i^{e_i}$$

de donde concluimos que

$$|D/\mathfrak{a}| = |\prod_{i=1}^r E/\mathfrak{p}_i^{e_i}| = \prod_{i=1}^r \mathrm{N}\,\mathfrak{p}_i^{e_i} = \mathrm{N}\,\mathfrak{a}.$$

■

Finalmente observamos que si D es un dominio de Dedekind con restos finitos y E es una extensión de D, entonces E también tiene restos finitos, pues si $\mathfrak{P}$ es un primo en E y $\mathfrak{p}$ es el primo en D al cual divide, entonces $E/\mathfrak{P}$ es una extensión finita del cuerpo finito $D/\mathfrak{p}$, luego también es un cuerpo finito. Más aún, se cumple $\mathrm{N}\,\mathfrak{P} = (\mathrm{N}\,\mathfrak{p})^f$, donde $f = f(\mathfrak{P}/\mathfrak{q})$.

Capítulo II

Compleciones

En el capítulo anterior hemos visto cómo la técnica de localización es de gran ayuda para obtener resultados aritméticos en dominios de Dedekind, eliminando los primos no involucrados y enriqueciendo la estructura algebraica disponible. Sin embargo, las localizaciones que realmente tienen valor teórico son las que se obtienen mediante compleciones de valores absolutos. Ya conocemos la teoría básica. Recordemos las definiciones principales:

Un *valor absoluto* en un cuerpo k es una función $|\ |$ de k en el cuerpo de los números reales que cumpla las propiedades siguientes:

a) $|\alpha| \geq 0$ y $|\alpha| = 0$ si y sólo si $\alpha = 0$.

b) $|\alpha + \beta| \leq |\alpha| + |\beta|$,

c) $|\alpha\beta| = |\alpha|\,|\beta|$.

Todo valor absoluto induce una distancia en el sentido topológico usual con la distancia dada por $d(\alpha, \beta) = |\alpha - \beta|$.

Un *cuerpo métrico* es un par $(k, \mathcal{T})$, donde k es un cuerpo y $\mathcal{T}$ es una topología inducida por un valor absoluto en k.

Dos valores absolutos en un cuerpo k son *equivalentes* si inducen la misma topología en k. El teorema [7.2] caracteriza la equivalencia de valores absolutos.

Un valor absoluto en un cuerpo k es *no arquimediano* si cumple

$$|\alpha + \beta| \leq \text{máx}\{|\alpha|, |\beta|\}, \qquad \text{para todo } \alpha, \beta \in k.$$

En caso contrario se dice que es *arquimediano.*

Se demuestra [7.5] que un valor absoluto es arquimediano si y sólo si existe un número natural n tal que $|n| > 1$, por lo que el carácter arquimediano de un valor absoluto en un cuerpo k depende sólo de su comportamiento sobre el cuerpo primo de k. Además esto implica que dos valores absolutos equivalentes son ambos arquimedianos o no lo es ninguno. Un cuerpo métrico es *arquimediano*

o *no arquimediano* según si los valores absolutos que inducen su topología son arquimedianos o no arquimedianos.

En todo cuerpo k de puede definir al menos el valor absoluto trivial $|\ |_0$ dado por

$$|\alpha|_0 = \begin{cases} 1 & \text{si } \alpha \neq 0, \\ 0 & \text{si } \alpha = 0. \end{cases}$$

El valor absoluto trivial induce la topología discreta y sólo es equivalente a sí mismo.

Una *valoración* en un cuerpo k es una aplicación $v : k \longrightarrow \mathbb{Z} \cup \{+\infty\}$ tal que:

a) v es suprayectiva y $v(\alpha) = +\infty$ si y sólo si $\alpha = 0$.

b) $v(\alpha\beta) = v(\alpha) + v(\beta)$ para todo α, $\beta \in k$,

c) $v(\alpha + \beta) \geq \text{mín}\{v(\alpha), v(\beta)\}$, para todo α, $\beta \in k$.

Una valoración en un cuerpo k induce un valor absoluto no arquimediano en k dado por $|\alpha| = \rho^{v(\alpha)}$, donde $0 < \rho < 1$, entendiendo que $|0| = \rho^{\infty} = 0$. Cuando ρ varía entre 0 y 1 recorremos una clase de equivalencia de valores absolutos.

Un cuerpo métrico es *discreto* si sus valores absolutos están inducidos por una valoración. En tal caso ésta es única.

Todo cuerpo métrico k tiene una *compleción* K, es decir, [7.8] un cuerpo métrico completo que contiene a k como subcuerpo denso. La compleción es única salvo isomorfismo topológico, es decir, si K_1 y K_2 son compleciones de k, la identidad en k se extiende a un isomorfismo topológico $\sigma : K_1 \longrightarrow K_2$ (un isomorfismo-homeomorfismo).

Es fácil generalizar esto ligeramente: todo isomorfismo topológico entre dos cuerpos métricos se extiende a un isomorfismo topológico entre sus compleciones.

Recordemos por último que todo valor absoluto en un cuerpo se extiende a su compleción y que, si el cuerpo es discreto, su valoración se extiende también.

2.1 Divisores primos

Sabemos [7.9] que cada ideal primo en un orden maximal de un cuerpo numérico K induce una valoración en K que convierte a éste en un cuerpo métrico discreto. Sin embargo, los cuerpos numéricos tienen otros valores absolutos no inducidos por primos (p. ej. el valor absoluto usual en $\mathbb{Q}$, que es arquimediano). Sucede que ciertos resultados de la teoría que vamos a desarrollar se expresan de forma más simétrica y elegante si a los primos de un cuerpo numérico añadimos ciertos "primos infinitos", definidos por valores absolutos arquimedianos y los tratamos formalmente como si fueran ideales primos. Para concretar estas ideas comenzamos dando la siguiente definición:

Definición 2.1 Sea k un cuerpo. Llamaremos *divisores primos* de k a las clases de equivalencia de valores absolutos en k distintas de la clase del valor absoluto trivial.

Un divisor primo es *arquimediano* o *no arquimediano* si lo son los valores absolutos que lo componen. Un divisor primo es *discreto* si sus valores absolutos están inducidos por una valoración. Todo divisor discreto es no arquimediano.

Si k es el cuerpo de cocientes de un dominio de Dedekind D y $\mathfrak{p}$ es un ideal primo en D se define el valor $\mathfrak{p}$-ádico de un elemento $\alpha \in D$ no nulo como el exponente $v_\mathfrak{p}(\alpha)$ de $\mathfrak{p}$ en la factorización del ideal (α). Si α/β es un elemento cualquiera de k definimos $v_\mathfrak{p}(\alpha/\beta) = v_\mathfrak{p}(\alpha) - v_\mathfrak{p}(\beta)$. Con esto tenemos una valoración en k que a su vez induce un divisor primo de k, al que seguiremos llamando $\mathfrak{p}$.

Observar que si $\mathfrak{p}$ y $\mathfrak{q}$ son ideales primos distintos de D y $|\ |_\mathfrak{p}$, $|\ |_\mathfrak{q}$, son valores absolutos inducidos por ellos en k, éstos no son equivalentes, pues si $\alpha \in \mathfrak{p} \setminus \mathfrak{q}$ y $\beta \in \mathfrak{q} \setminus \mathfrak{p}$ se cumple que $v_\mathfrak{p}(\alpha) \geq 1$, $v_\mathfrak{p}(\beta) = 0$, $v_\mathfrak{q}(\beta) \geq 1$, $v_\mathfrak{q}(\alpha) = 0$, luego

$$|\alpha|_\mathfrak{p} < 1 = |\beta|_\mathfrak{p}, \qquad |\beta|_\mathfrak{q} < 1 = |\alpha|_\mathfrak{q},$$

Así pues, ideales primos distintos inducen divisores primos distintos y podemos considerar que el conjunto de los divisores primos de k contiene a los ideales primos de D.

Recordemos que si $\mathfrak{p}$ es un divisor primo discreto en un cuerpo k, cuyos valores absolutos están inducidos por la valoración $v_\mathfrak{p}$, entonces podemos definir el anillo de enteros $D_\mathfrak{p} = \big\{\alpha \in k \bigm| |\alpha| \leq 1\big\} = \big\{\alpha \in k \bigm| v_\mathfrak{p}(\alpha) \geq 0\big\}$. Se trata de un anillo local cuyo único ideal maximal es $\mathfrak{p} = \{\alpha \in k \mid v_\mathfrak{p}(\alpha) \geq 1\}$. Los teoremas [7.12] y [7.13] describen su estructura.

De ellos se sigue en particular que $D_\mathfrak{p}$ es un dominio de Dedekind y que la valoración inducida por el ideal $\mathfrak{p}$ es precisamente $v_\mathfrak{p}$, luego determina en k el divisor $\mathfrak{p}$. Por este motivo usamos la misma notación para el divisor y para el ideal.

Si k es un cuerpo numérico y $\mathfrak{p}$ es un ideal primo en su orden maximal $\mathcal{O}$, el teorema [3.7] muestra que el anillo de enteros de k respecto al divisor $\mathfrak{p}$ coincide con la localización $\mathcal{O}_\mathfrak{p}$ respecto al ideal $\mathfrak{p}$ en el sentido del capítulo anterior (y por ello usamos la misma notación para ambos).

La divisibilidad entre ideales se puede expresar en términos de los divisores asociados:

Teorema 2.2 *Sea E/D una extensión separable de dominios de Dedekind y sea K/k la extensión de sus cuerpos de cocientes. Sea $\mathfrak{p}$ un ideal primo en D y $\mathfrak{P}$ un ideal primo en E. Entonces $\mathfrak{P} \mid \mathfrak{p}$ si y sólo si existe un valor absoluto asociado a $\mathfrak{p}$ que se extiende a un valor absoluto asociado a $\mathfrak{P}$. En tal caso cada valor absoluto asociado a $\mathfrak{p}$ se extiende a un único valor absoluto asociado a $\mathfrak{P}$ y la restricción a k de todo valor absoluto asociado a $\mathfrak{P}$ es un valor absoluto asociado a $\mathfrak{p}$.*

DEMOSTRACIÓN: Si $\mathfrak{P} \mid \mathfrak{p}$ sea e el índice de ramificación $e(\mathfrak{P}/\mathfrak{p})$. Entonces $\mathfrak{P}$ divide e veces a $\mathfrak{p}$, lo que se traduce en que las valoraciones asociadas a ambos primos satisfacen la relación $v_{\mathfrak{P}}(\alpha) = e\, v_{\mathfrak{p}}(\alpha)$, para todo $\alpha \in k$.

Cada valor absoluto asociado a $\mathfrak{p}$ es de la forma $|\alpha| = \rho^{v_{\mathfrak{p}}(\alpha)}$, para todo $\alpha \in k$, y se extiende al valor absoluto asociado a $\mathfrak{P}$ dado por $|\alpha| = (\rho^{1/e})^{v_{\mathfrak{P}}(a)}$ para todo $\alpha \in K$.

Recíprocamente, todo valor absoluto asociado a $\mathfrak{P}$ es de la forma $|\alpha| = \rho^{v_{\mathfrak{P}}(\alpha)}$, para todo $\alpha \in K$, y su restricción a k es de la forma $|\alpha| = (\rho^e)^{v_{\mathfrak{p}}(a)}$, luego está asociado a $\mathfrak{p}$.

Cada valor absoluto asociado a $\mathfrak{p}$ tiene extensión única asociada a $\mathfrak{P}$ porque dos extensiones serían equivalentes, luego una sería una potencia de la otra, y como en k coinciden, el exponente sería 1.

Finalmente, si existe un valor absoluto asociado a $\mathfrak{p}$ que se extiende a un valor absoluto asociado a $\mathfrak{P}$, entonces $\mathfrak{p}$ ha de ser el único ideal primo de k al que divide $\mathfrak{P}$, pues ya hemos visto que todas las restricciones de los valores absolutos de $\mathfrak{P}$ se corresponden con dicho primo. ∎

En los cuerpos numéricos podemos simplificar la situación eligiendo valores absolutos canónicos con el criterio siguiente:

Definición 2.3 Si p es un primo en $\mathbb{Z}$, llamaremos *valor absoluto canónico* asociado a p al valor absoluto en $\mathbb{Q}$ dado por $|r|_p = (1/p)^{v_p(r)}$, para todo $r \in \mathbb{Q}$.

Si $\mathfrak{p}$ es un ideal primo en un cuerpo numérico K (es decir, un ideal de su anillo de enteros algebraicos) y p es el único primo racional al cual divide, llamaremos *valor absoluto canónico* asociado a $\mathfrak{p}$ al único valor absoluto asociado a $\mathfrak{p}$ que extiende al valor absoluto canónico de p. Lo representaremos por $|\ |_{\mathfrak{p}}$.

Teorema 2.4 *Sea K/k una extensión de cuerpos numéricos, sea $\mathfrak{P}$ un ideal primo en K y $\mathfrak{p}$ un ideal primo en k. Se cumple que $\mathfrak{P} \mid \mathfrak{p}$ si y sólo si el valor absoluto canónico de $\mathfrak{P}$ extiende al valor absoluto canónico de $\mathfrak{p}$.*

DEMOSTRACIÓN: Si $\mathfrak{P} \mid \mathfrak{p}$ entonces la restricción a k del valor absoluto canónico de $\mathfrak{P}$ es un valor absoluto asociado a $\mathfrak{p}$ que extiende al valor absoluto canónico del único primo racional p al cual dividen ambos ideales, luego por la unicidad dicha restricción ha de ser el valor absoluto canónico de $\mathfrak{p}$. El recíproco es una consecuencia inmediata del teorema 2.2. ∎

Según comentábamos, hemos introducido la noción de "divisor primo" para añadir primos infinitos al conjunto de los ideales primos de un cuerpo numérico. Los primos que nos faltan son los inducidos por los valores absolutos siguientes:

Definición 2.5 Sea k un cuerpo numérico y $\sigma : k \longrightarrow \mathbb{C}$ un monomorfismo. Definimos el valor absoluto en k dado por

$$|\alpha|_\sigma = |\sigma(\alpha)|,$$

donde el valor absoluto del segundo miembro es el usual en $\mathbb{C}$.

Obviamente $|\ |_\sigma$ es un valor absoluto arquimediano en k. Ahora hemos de determinar si dos de ellos pueden ser equivalentes. La respuesta es que sí, pero sólo en un caso muy concreto.

Teorema 2.6 *Sea k un cuerpo numérico y sean σ, $\tau : k \longrightarrow \mathbb{C}$ dos monomorfismos. Entonces σ y τ inducen valores absolutos equivalentes en k si y sólo si $\sigma = \tau$ o bien $\sigma = \overline{\tau}$ (la composición de τ con la conjugación compleja).*

DEMOSTRACIÓN: Si σ y τ inducen valores absolutos equivalentes, entonces ambos dan lugar a la misma compleción K de k. Por otro lado, las clausuras $\overline{\sigma[k]}$ y $\overline{\tau[k]}$ son compleciones de $\sigma[k]$ y $\tau[k]$ respectivamente. Consecuentemente σ y τ se extienden a isomorfismos topológicos $\sigma : K \longrightarrow \overline{\sigma[k]}$ y $\tau : K \longrightarrow \overline{\tau[k]}$.

Ahora observamos que $\overline{\sigma[k]}$ y $\overline{\sigma[k]}$ son subcuerpos cerrados de $\mathbb{C}$ que contienen a $\mathbb{Q}$, luego a $\mathbb{R}$. Tienen que ser concretamente $\mathbb{R}$ o $\mathbb{C}$, y como $\tau^{-1} \circ \sigma$ es un isomorfismo entre ellos, tienen que ser iguales y $\tau^{-1} \circ \sigma$ es un $\mathbb{R}$-automorfismo entre ellos (es un automorfismo continuo que fija a $\mathbb{Q}$, luego por continuidad fija a $\mathbb{R}$).

Por consiguiente, $\tau^{-1} \circ \sigma$ es la identidad en $\mathbb{R}$, la identidad en $\mathbb{C}$ o bien la conjugación en $\mathbb{C}$. En cualquier caso $\sigma = \tau$ o bien $\sigma = \overline{\tau}$. Restringiendo a k tenemos la conclusión. ∎

Observar que si $\sigma = \overline{\tau}$, entonces los valores absolutos que inducen no sólo son equivalentes, sino que de hecho son iguales.

Definición 2.7 Siguiendo la notación usual [4.1], si k es un cuerpo numérico de grado n llamaremos $\sigma_1, \ldots, \sigma_s : k \longrightarrow \mathbb{R}$ a sus monomorfismos reales y $\sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t} : k \longrightarrow \mathbb{C}$ a sus monomorfismos complejos. De este modo $n = s + 2t$ y llamamos $r = s + t$.

Según el teorema anterior los r valores absolutos arquimedianos inducidos por $\sigma_1, \ldots, \sigma_r$ son no equivalentes dos a dos, luego inducen r divisores primos arquimedianos distintos en k. Los llamaremos *divisores primos infinitos* de k. Por oposición, los divisores primos inducidos por los ideales primos del orden maximal de k serán los *divisores primos finitos* de k. Un primo infinito de un cuerpo numérico es *real* o *complejo* según si está inducido por un monomorfismo real o complejo.

Así, por ejemplo, $\mathbb{Q}$ tiene un único primo arquimediano (real), correspondiente a la inclusión $\mathbb{Q} \longrightarrow \mathbb{R}$, y que representaremos por ∞.

En lo sucesivo, cuando hablemos de *divisores primos* de un cuerpo numérico sobrentenderemos que nos referimos únicamente a divisores de uno de estos tipos: o los divisores finitos inducidos por ideales o los divisores infinitos inducidos por monomorfismos. En el apéndice de este capítulo probamos que en realidad éstos son todos los divisores del cuerpo, pero nunca necesitaremos este hecho. En lo sucesivo nos bastará con el convenio de que no hablamos de ningún otro posible divisor.

Observemos que en el contexto de los cuerpos numéricos "divisor primo finito" es sinónimo de "divisor primo no arquimediano" o "divisor primo discreto", mientras que "divisor primo infinito" es sinónimo de "divisor primo arquimediano". A menudo diremos únicamente "primo", en vez de "divisor primo".

Podemos tomar como *valor absoluto canónico* para un divisor primo arquimediano $\mathfrak{p}$ de un cuerpo numérico al dado por la definición 2.5. Lo representaremos por $|\ |_\mathfrak{p}$. Observemos que si σ es un monomorfismo complejo, entonces σ y $\overline{\sigma}$ inducen el mismo valor absoluto, luego no tenemos dos valores absolutos canónicos para un mismo divisor.

Convertimos el teorema 2.4 en una definición para el caso arquimediano:

Sea K/k una extensión de cuerpos numéricos, sea $\mathfrak{p}$ un primo infinito de k y $\mathfrak{P}$ un primo infinito de K. Diremos que $\mathfrak{P}$ divide a $\mathfrak{p}$ si el valor absoluto canónico de $\mathfrak{P}$ extiende al valor absoluto canónico de $\mathfrak{p}$. Lo representaremos con la notación habitual: $\mathfrak{P} \mid \mathfrak{p}$.

Resultados elementales de la teoría de cuerpos nos dan que cada primo arquimediano de K divide a un único primo de k, así como que todo primo arquimediano de k es divisible entre al menos un primo de K. Los primos infinitos de un cuerpo numérico son exactamente los divisores del primo ∞ de $\mathbb{Q}$.

Si k es un cuerpo numérico y $\mathfrak{p}$ es un divisor primo en k, llamaremos $k_\mathfrak{p}$ a la compleción de k respecto a los valores absolutos de $\mathfrak{p}$. Llamaremos $|\ |_\mathfrak{p}$ a la extensión a $k_\mathfrak{p}$ del valor absoluto canónico de $\mathfrak{p}$ en k.

Las compleciones de los primos arquimedianos de un cuerpo numérico son fáciles de calcular:

Si $\mathfrak{p}$ es un primo infinito real de un cuerpo numérico k, inducido por un monomorfismo $\sigma : k \longrightarrow \mathbb{R}$, entonces σ es un isomorfismo topológico entre k con la topología inducida por $|\ |_\mathfrak{p}$ y la topología usual de $\mathbb{R}$, luego se extiende a un isomorfismo topológico entre $k_\mathfrak{p}$ y la compleción de $\sigma[k]$, que obviamente es $\mathbb{R}$. Así pues, $k_\mathfrak{p} \cong \mathbb{R}$. Similarmente, si $\mathfrak{p}$ es un primo infinito complejo de k entonces $k_\mathfrak{p} \cong \mathbb{C}$.

Las compleciones de los primos no arquimedianos las estudiamos en la sección siguiente.

2.2 Cuerpos $\mathfrak{p}$-ádicos

Si $\mathfrak{p}$ es un primo finito en un cuerpo numérico k, la compleción $k_\mathfrak{p}$ se conoce como cuerpo de los *números $\mathfrak{p}$-ádicos.* El teorema [7.14] afirma que el único ideal primo del anillo de enteros $D_\mathfrak{p}$ de $k_\mathfrak{p}$ (el anillo de los enteros $\mathfrak{p}$-ádicos) se comporta como el ideal $\mathfrak{p}$ del orden maximal $\mathcal{O}_k$, en el sentido de que tenemos los isomorfismos naturales $\mathcal{O}_k/\mathfrak{p}^n \cong D_\mathfrak{p}/\mathfrak{p}^n$ (dados por $[\alpha] \mapsto [\alpha]$).

A su vez, el teorema [7.15] nos da que las compleciones no arquimedianas de los cuerpos numéricos son cuerpos métricos localmente compactos (al igual que las arquimedianas).

Si K/k es una extensión de cuerpos numéricos, $\mathfrak{p}$ es un divisor primo en k y $\mathfrak{P}$ es un divisor primo en K que divide a $\mathfrak{p}$, entonces la clausura de k en $K_\mathfrak{p}$ es una compleción de k respecto a la restricción del valor absoluto canónico de $\mathfrak{P}$, que es el valor absoluto canónico de $\mathfrak{p}$, luego podemos identificar dicha clausura con $k_\mathfrak{p}$, o sea, podemos considerar que $k_\mathfrak{p} \subset K_\mathfrak{P}$. El hecho de que el valor absoluto canónico de $\mathfrak{P}$ en K extienda al de $\mathfrak{p}$ en k implica por continuidad que lo mismo vale para sus extensiones a las compleciones.

El teorema siguiente nos da una primera relación entre las extensiones K/k y $K_\mathfrak{P}/k_\mathfrak{p}$.

Teorema 2.8 *Sea K/k una extensión de cuerpos numéricos, sea E/D la extensión de sus anillos de enteros. Sea $\mathfrak{p}$ un primo finito en D y sea $\mathfrak{P}$ un primo en E que lo divida. Sea $e = e(\mathfrak{P}/\mathfrak{p})$ y $f = f(\mathfrak{P}/\mathfrak{p})$. Sean $K_\mathfrak{P}$ y $k_\mathfrak{p}$ las compleciones de ambos cuerpos y sean $E_\mathfrak{P}$ y $D_\mathfrak{p}$ los correspondientes anillos de enteros. Entonces*

a) La extensión $K_\mathfrak{P}/k_\mathfrak{p}$ es finita y su grado es ef.

b) $E_\mathfrak{P}$ es la clausura entera de $D_\mathfrak{p}$ en $K_\mathfrak{P}$, luego $E_\mathfrak{P}/D_\mathfrak{p}$ es una extensión de dominios de Dedekind.

c) Si $\mathfrak{m}_\mathfrak{p}$ y $\mathfrak{m}_\mathfrak{P}$ son los ideales maximales de $D_\mathfrak{p}$ y $E_\mathfrak{P}$, tenemos la situación descrita por el diagrama siguiente:

$$\begin{array}{ccc} E/\mathfrak{P} & \longrightarrow & E_\mathfrak{P}/\mathfrak{m}_\mathfrak{P} \\ \uparrow & & \uparrow \\ D/\mathfrak{p} & \longrightarrow & D_\mathfrak{p}/\mathfrak{m}_\mathfrak{p} \end{array}$$

Todas las aplicaciones están definidas de forma natural ($[\alpha] \mapsto [\alpha]$). Las flechas horizontales son los isomorfismos descritos en [7.14]. *Las flechas verticales son monomorfismos de cuerpos.*

d) Se cumple $e = e(\mathfrak{m}_\mathfrak{P}/\mathfrak{m}_\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$ y $f = f(\mathfrak{m}_\mathfrak{P}/\mathfrak{m}_\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$. En particular $\mathfrak{m}_\mathfrak{p} = \mathfrak{m}_\mathfrak{P}^e$.

Demostración: Sea $\alpha_1, \ldots, \alpha_n$ un generador de E como D-módulo. Sea $\gamma \in E_\mathfrak{P}$. Por [7.14] sabemos que $E_\mathfrak{P}$ es la clausura de E, luego existe una sucesión $\{x_k\}$ de elementos de E que converge a γ.

Digamos que $x_k = d_{k1}\alpha_1 + \cdots + d_{kn}\alpha_n$, para ciertos coeficientes $d_{kj} \in D$.

Como $D_\mathfrak{p}$ es compacto (es la bola unidad cerrada de $k_\mathfrak{p}$), también lo es $D_\mathfrak{p}^n$, y la sucesión $(d_{k1}, \ldots, d_{kn})$ tiene una subsucesión convergente a un cierto $(d_1, \ldots, d_n) \in D_\mathfrak{p}^n$. Entonces es claro que x_k converge a $d_1\alpha_1 + \cdots + d_n\alpha_n = \gamma$. Esto prueba que $\alpha_1, \ldots, \alpha_n$ es también un generador de $E_\mathfrak{P}$ como $D_\mathfrak{p}$-módulo.

En particular $E_\mathfrak{P} = D_\mathfrak{p}[\alpha_1, \ldots, \alpha_n]$ y, como los α_i son enteros sobre D, también lo son sobre $D_\mathfrak{p}$, con lo que $E_\mathfrak{P}$ es una extensión entera de $D_\mathfrak{p}$. Como $E_\mathfrak{p}$ es íntegramente cerrado (es DIP), tenemos que $E_\mathfrak{P}$ es la clausura entera de $D_\mathfrak{p}$ en $K_\mathfrak{P}$.

Otra consecuencia es que $k_\mathfrak{p}(\alpha_1,\dots,\alpha_n)$ es un cuerpo que contiene a $E_\mathfrak{P}$, y como $K_\mathfrak{P}$ es el cuerpo de cocientes de $E_\mathfrak{P}$, ha de ser $K_\mathfrak{P} = k_\mathfrak{p}(\alpha_1,\dots,\alpha_n)$. Los números $\alpha_1,\dots,\alpha_n$ son algebraicos sobre k, luego también sobre $k_\mathfrak{p}$, luego la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ es finita.

Con esto tenemos probado b). En c) no hay nada que probar, pero de c) se deduce que el grado de la extensión de la izquierda del diagrama coincide con el grado de la extensión de la derecha, o sea, que $f = f(\mathfrak{m}_\mathfrak{P}/\mathfrak{m}_\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$.

La relación entre la valoración inducida por $\mathfrak{P}$ y la valoración inducida por $\mathfrak{p}$ es que para todo $\alpha \in k$ se cumple $v_\mathfrak{P}(\alpha) = e\, v_\mathfrak{p}(\alpha)$. Como las valoraciones definidas por $\mathfrak{m}_\mathfrak{p}$ y $m_\mathfrak{P}$ extienden a éstas, se cumple $v_{\mathfrak{m}_\mathfrak{P}}(\alpha) = e\, v_{\mathfrak{m}_\mathfrak{p}}(\alpha)$ para todo $\alpha \in k$, y por continuidad para todo $\alpha \in k_\mathfrak{p}$. Esto implica que $e = e(\mathfrak{m}_\mathfrak{P}/\mathfrak{m}_\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$, con lo que queda probado d).

Por último, el grado de la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ es ef por el teorema 1.34. ∎

En particular vemos que todo cuerpo $\mathfrak{p}$-ádico $k_\mathfrak{p}$ es una extensión finita del cuerpo $\mathbb{Q}_p$, donde p es el único primo racional divisible entre $\mathfrak{p}$.

El teorema anterior no es todo lo que podemos decir en general sobre las extensiones K/k y $K_\mathfrak{P}/k_\mathfrak{p}$. Para precisar más aún la relación entre ambas extensiones necesitamos probar que toda extensión finita separable K de un cuerpo métrico discreto localmente compacto k es también un cuerpo métrico discreto localmente compacto. Para ello veremos que cada valor absoluto de k se extiende de forma única a K, con lo que la clausura entera en K del anillo de enteros de k será un dominio de Dedekind con un único primo (por 2.2, dos primos darían lugar a dos extensiones distintas del mismo valor absoluto de k). La conclusión será entonces inmediata.

La posibilidad de extender valores absolutos es consecuencia del teorema 2.2. Los resultados siguientes nos servirán para probar la unicidad de la extensión.

Definición 2.9 Sea K un cuerpo métrico y V un espacio vectorial sobre K. Una *norma* en V (para un valor absoluto prefijado en K) es una aplicación $\|\ \| : V \longrightarrow \mathbb{R}$ que cumpla las propiedades siguientes:

a) $\|v\| \geq 0$ para todo $v \in V$ y $\|v\| = 0$ si y sólo si $v = 0$,

b) $\|v + w\| \leq \|v\| + \|w\|$ para todo $v, w \in V$,

c) $\|\alpha v\| = |\alpha|\|v\|$ para todo $\alpha \in K$ y todo $v \in V$.

Claramente V es un espacio métrico con la distancia dada por $\|v - w\|$. Se comprueba sin dificultad que la suma y el producto en V son funciones continuas.

Dos normas $\|\ \|_1$ y $\|\ \|_2$ en un mismo espacio V son *equivalentes* si existen números reales $0 < m < M$ tales que

$$\|v\|_1 \leq m\|v\|_2 \qquad \text{y} \qquad \|v\|_2 \leq M\|v\|_1$$

para todo $v \in V$. Es obvio que dos normas equivalentes inducen la misma topología en V.

Teorema 2.10 *Sea K un cuerpo métrico en el que hemos prefijado un valor absoluto. Entonces la aplicación en K^n definida mediante*

$$\|x\| = \max\{|x_i| \mid i = 1, \dots, n\}$$

es una norma. Si K es completo entonces K^n es completo con esta norma.

DEMOSTRACIÓN: La comprobación de que en efecto es una norma es rutinaria. Observemos que $\|\ \|$ induce en K^n la topología producto (las bolas abiertas para la norma son productos de bolas abiertas en K del mismo radio). Es fácil ver que si una sucesión es de Cauchy en K^n, entonces sus coordenadas son de Cauchy en K, luego si K es completo convergen, y la sucesión dada también. ∎

Teorema 2.11 *Sea K un cuerpo métrico completo y sea V un K-espacio vectorial de dimensión finita. Entonces todas las normas sobre V (para un valor absoluto prefijado) son equivalentes y V es completo con cualquiera de ellas.*

DEMOSTRACIÓN: Supongamos primero que $V = K^n$. Sea $\|\ \|^*$ cualquier norma en K^n y sea $\|\ \|$ la norma definida en el teorema anterior. Basta ver que ambas son equivalentes. Sea $e_1, \dots, e_n$ la base canónica de K^n. Entonces para todo $x \in K^n$ se cumple

$$\|x\|^* = \|x_1e_1 + \cdots + x_ne_n\|^* \le |x_1|\|e_1\|^* + \cdots + |x_n|\|e_n\|^* \le M\|x\|,$$

donde $M = \|e_1\|^* + \cdots + \|e_n\|^*$.

Ahora hemos de probar la relación opuesta. Basta ver que existen constantes N_i de modo que si $x \in K^n$, entonces $|x_i| \le N_i\|x\|^*$, pues en tal caso $N = \max N_i$ cumple $\|x\| \le N\|x\|^*$. Lo probaremos por inducción sobre n.

Si $n = 1$ basta tomar $N_1 = 1/\|1\|^*$. Supuesto cierto para $n-1$, identificamos K^{n-1} con los elementos de K^n cuya última coordenada es nula. Las restricciones a K^{n-1} de las dos normas consideradas son normas en K^{n-1}. Por hipótesis de inducción son equivalentes y K^{n-1} es completo para la restricción de la norma $\|\ \|^*$, luego es cerrado en K^n para la topología inducida esta norma.

Supongamos, por reducción al absurdo, que para todo natural m existe un $w_m \in \mathbb{K}^n$ de manera que $|(w_m)_n| > m\|w_m\|^*$. Podemos suponer que $(w_m)_n = 1$ (basta dividir w_m entre $(w_m)_n$ si es preciso), y entonces la desigualdad se reduce a $\|w_m\|^* < 1/m$. Por otra parte esta condición adicional implica también que $w_m - e_n \in K^{n-1}$.

De este modo tenemos que $\{w_m\}$ tiende a 0 y que $w_m - e_n$ tiende a $-e_n$ pero, como K^{n-1} es cerrado, esto implica que $e_n \in K^{n-1}$, lo cual es absurdo. Por lo tanto existe un m tal que $|w_n| \le m\|w\|^*$ para todo $w \in K^n$. El mismo razonamiento se aplica a cualquier otro índice.

Si V es un espacio vectorial cualquiera de dimensión n sobre K, cada norma en V induce una en K^n a través de un isomorfismo de espacios vectoriales. Del hecho de que las normas inducidas sean equivalentes se sigue obviamente que las

normas de partida también lo sean. Igualmente se concluye que V es completo con cualquiera de ellas. ∎

Ahora ya podemos probar la unicidad de la extensión de los valores absolutos:

Teorema 2.12 *Sea K un cuerpo métrico completo y sea L una extensión finita de K. Si el valor absoluto de K admite una extensión a L entonces dicha extensión es única y L es con ella un cuerpo métrico completo.*

Demostración: Si $|\ |_1$ y $|\ |_2$ son dos valores absolutos en L que extienden al de K entonces podemos considerarlos como dos normas en L como K-espacio vectorial. Por el teorema anterior son equivalentes, luego inducen la misma topología en L, luego son equivalentes como valores absolutos, luego uno es una potencia del otro, pero como coinciden en K el exponente ha de ser 1, luego son iguales. El teorema anterior nos da también que L es completo. ∎

En el caso de cuerpos métricos discretos siempre es posible extender el valor absoluto a una extensión finita separable, y de aquí a cualquier extensión separable. En realidad el teorema vale para extensiones algebraicas de cuerpos completos cualesquiera, pero esto no no nos va a hacer falta y requeriría más trabajo (la prueba general está en el apéndice).

Teorema 2.13 *Sea k un cuerpo métrico discreto completo.*

a) Cada valor absoluto de k se extiende de forma única a cada una de sus extensiones separables.

b) Si K es una extensión finita separable de k, entonces la extensión de cualquier valor absoluto de k está inducida por una valoración con la que K resulta ser un cuerpo métrico discreto completo. Los anillos de enteros forman una extensión separable de dominios de Dedekind.

c) Cualquier k-isomorfismo entre dos extensiones separables de k es una isometría respecto a las extensiones de un mismo valor absoluto de k.

Demostración: Sea D el anillo de los enteros de k. Si K es cualquier extensión finita separable de k, entonces la clausura entera E de D en K es un dominio de Dedekind (teorema 1.26). Si $\mathfrak{P}$ es un primo de E (que dividirá al único primo $\mathfrak{p}$ de D), el teorema 2.2 nos da que cada valor absoluto de k se extiende a un valor absoluto en K inducido por la valoración asociada a $\mathfrak{P}$. El teorema anterior nos da que la extensión es única, de donde se sigue que $\mathfrak{P}$ es el único primo de E (dos primos distintos darían lugar a dos extensiones distintas). Así pues E es un anillo local, luego es el anillo de enteros de la valoración inducida por su único primo $\mathfrak{P}$. Por el teorema anterior K es localmente compacto, y así queda probado b).

Fijemos un valor absoluto $|\ |_k$ en k. Si K es una extensión separable de k, entonces sobre cada extensión finita intermedia L hay una única extensión del valor absoluto de k, llamémosla $|\ |_L$. Es claro que si $k \subset L \subset N \subset K$ entonces $|\ |_N$ extiende a $|\ |_L$.

Para cada $\alpha \in K$, la extensión $k(\alpha)/k$ es finita separable, y podemos definir $|\alpha| = |\alpha|_{k(\alpha)}$. Por la unicidad es claro que si $L \subset K$ es cualquier extensión finita de k y $\alpha \in L$ entonces $|\alpha| = |\alpha|_L$. De aquí se sigue inmediatamente que $|\ |$ es un valor absoluto sobre K que extiende al valor absoluto de k. La extensión es única pues, si tuviéramos dos, coincidirían sobre todas las extensiones finitas de k, luego sobre todos los elementos de K. Esto prueba a).

Si $\sigma : K \longrightarrow L$ es un k-isomorfismo entre dos extensiones algebraicas de k, entonces es claro que $|\alpha|^* = |\sigma(\alpha)|$ es un valor absoluto en K que extiende al de k, luego por la unicidad es precisamente el valor absoluto de K, y por tanto $|\alpha| = |\sigma(\alpha)|$ para todo $\alpha \in K$, es decir, σ es una isometría. ∎

La parte principal de este teorema puede expresarse estrictamente en términos de cuerpos métricos, es decir, en función de sus topologías y no de sus valores absolutos:

Teorema 2.14 *Sea k un cuerpo métrico discreto completo y K una extensión separable de k. Entonces K admite una única topología de cuerpo métrico que induce la topología de k. Si la extensión es finita entonces K es discreto y completo. Cualquier k-isomorfismo entre dos extensiones separables de k es un isomorfismo topológico.*

Demostración: Sea D el anillo de enteros de k y $\mathfrak{p}$ su único primo. Si la extensión K/k es finita, y E es la clausura entera de D en K, entonces el teorema anterior nos da que E es un dominio de Dedekind con un único primo $\mathfrak{P}$. Puesto que obviamente $\mathfrak{P} \mid \mathfrak{p}$, por el teorema 2.2 cada valor absoluto de k se extiende a un valor absoluto de K asociado a $\mathfrak{P}$, y por el teorema anterior la extensión es única.

Cualquier valor absoluto en K que induzca la topología de k es extensión de un valor absoluto de $\mathfrak{p}$, luego es uno de los valores absolutos de $\mathfrak{P}$ y por consiguiente induce la topología $\mathfrak{P}$-ádica. Por el teorema anterior K es discreto y completo.

Si la extensión K/k no es finita basta observar que un valor absoluto en K está completamente determinado por su restricción a las extensiones finitas de k. La afirmación sobre los k-isomorfismos se sigue inmediatamente del teorema anterior. ∎

Como aplicación tenemos los resultados prometidos sobre extensiones de cuerpos $\mathfrak{p}$-ádicos. Notemos que los cuerpos numéricos son perfectos, por lo que al aplicarles el teorema anterior podemos sustituir "extensión separable" por "extensión algebraica".

Teorema 2.15 *Sea K/k una extensión de cuerpos numéricos, sea E/D la extensión de sus anillos de enteros. Sea $\mathfrak{p}$ un primo en D y sea $\mathfrak{P}$ un primo en E que lo divida.*

a) Si $K = k(A)$, para cierto conjunto $A \subset K$, entonces $K_{\mathfrak{P}} = k_{\mathfrak{p}}(A)$.

b) En particular $K_{\mathfrak{P}} = k_{\mathfrak{p}}K$.

c) Si la extensión K/k es de Galois, la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ también lo es.

DEMOSTRACIÓN: a) Podemos suponer que A es finito. Entonces tenemos $k_\mathfrak{p} \subset k_\mathfrak{p}(A) \subset K_\mathfrak{P}$, y la extensión $k_\mathfrak{p}(A)/k_\mathfrak{p}$ es finita, luego por el teorema anterior $k_\mathfrak{p}(A)$ es completo, luego es cerrado en $K_\mathfrak{P}$. Por otra parte $K \subset k_\mathfrak{p}(A)$ y K es denso en $K_\mathfrak{P}$, luego ha de ser $K_\mathfrak{P} = k_\mathfrak{p}(A)$.

b) es inmediato a partir de a).

c) Si K/k es una extensión de Galois entonces $K = k(A)$, donde A es el conjunto de las raíces de un polinomio de $k[x]$, y como $K_\mathfrak{P} = k_\mathfrak{P}(A)$ la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ también es de Galois. ∎

Definición 2.16 En lo sucesivo, para cada primo finito $\mathfrak{p}$ de un cuerpo numérico k fijaremos una clausura algebraica $\mathbb{K}_\mathfrak{p}$ del cuerpo $\mathfrak{p}$-ádico $k_\mathfrak{p}$. Según el teorema 2.13 el valor absoluto canónico de $k_\mathfrak{p}$ se extiende de forma única a $\mathbb{K}_\mathfrak{p}$. Representaremos esta extensión por $|\ |_\mathfrak{p}$ y la llamaremos *valor absoluto canónico* de $\mathbb{K}_\mathfrak{p}$. Dicho teorema implica también que todo $k_\mathfrak{p}$-isomorfismo entre dos extensiones algebraicas de $k_\mathfrak{p}$ (contenidas en $\mathbb{K}_\mathfrak{p}$) es una isometría respecto al valor absoluto canónico.

Observemos que si p es el primo racional al que divide $\mathfrak{p}$, entonces $k_\mathfrak{p}$ es una extensión finita de $\mathbb{Q}_p$, luego $\mathbb{K}_\mathfrak{p}$ es también una clausura algebraica de $\mathbb{Q}_p$, es decir, $\mathbb{K}_\mathfrak{p}$ es topológicamente isomorfo a $\mathbb{K}_p$ (e isométrico respecto a los valores absolutos canónicos). De este modo, para cuestiones puramente algebraicas es suficiente tratar con los cuerpos $\mathbb{K}_p$, pero debemos tener presente que si $\mathfrak{p}$ y $\mathfrak{q}$ son dos divisores de p en un mismo cuerpo métrico k, entonces la isometría entre $\mathbb{K}_\mathfrak{p}$ y $\mathbb{K}_\mathfrak{q}$ no es la identidad sobre k, (o de lo contrario $|\ |_\mathfrak{p}$ y $|\ |_\mathfrak{q}$ serían el mismo valor absoluto), por lo que no podemos identificar ambos cuerpos a ciertos efectos. En particular no podemos identificar ambos con $\mathbb{K}_p$.

Notemos que el criterio de irreducibilidad de Eisenstein es aplicable al anillo de enteros de $\mathbb{Q}_p$, lo que nos da polinomios irreducibles en $\mathbb{Q}_p[x]$ de grado arbitrariamente grande. Por consiguiente $\mathbb{K}_p$ tiene grado infinito sobre $\mathbb{Q}_p$.

Ahora probaremos un sencillo resultado técnico que nos será útil en varias ocasiones más adelante. De momento lo usaremos para probar, entre otras cosas, que la clausura algebraica de $\mathbb{Q}$ es densa en $\mathbb{K}_p$. La prueba de este teorema y los siguientes se basa en el teorema 2.13, que tenemos probado para cuerpos métricos discretos completos aunque ya comentamos que vale en realidad para cuerpos completos arbitrarios. Admitiendo esto, las demostraciones que veremos a continuación son válidas para cuerpos métricos completos no arquimedianos cualesquiera.

Teorema 2.17 (Lema de Krasnel) *Sea k un cuerpo métrico discreto completo y sean α y β dos elementos de su clausura separable K. Supongamos que para todo k-monomorfismo $\sigma : k(\alpha) \longrightarrow K$ distinto de la identidad se cumple $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$. Entonces $k(\alpha) \subset k(\beta)$.*

DEMOSTRACIÓN: Se entiende que el valor absoluto que aparece en el enunciado es la extensión a K de cualquier valor absoluto en k (cuya existencia está garantizada por el teorema 2.13).

Basta ver que todo $k(\beta)$-monomorfismo $\tau : k(\alpha,\beta) \longrightarrow K$ fija a α. El teorema 2.13 nos da que τ es una isometría, luego $|\tau(\beta-\alpha)| = |\beta-\alpha|$. Entonces

$$|\tau(\alpha)-\alpha| = |\tau(\alpha)-\beta+\beta-\alpha| \leq \text{máx}\big\{|\tau(\alpha-\beta)|, |\beta-\alpha|\big\} = |\beta-\alpha| < |\sigma(\alpha)-\alpha|$$

para todo $\sigma : k(\alpha) \longrightarrow K$ distinto de la identidad, luego τ ha de ser la identidad en $k(\alpha)$. ∎

Geométricamente, el teorema anterior afirma que, si α es separable sobre k, entonces $k(\alpha)$ está contenido en cualquier extensión de k que contenga a un punto de una bola de centro α en la clausura separable de k que no contenga a ningún conjugado de α aparte de a él mismo.

Con esto podemos probar una especie de continuidad de las raíces de un polinomio respecto de sus coeficientes.

Si k es un cuerpo métrico discreto completo y fijamos en él un valor absoluto, para cada polinomio $g \in k[x]$ definimos $\|g\|$ como el máximo de los valores absolutos de sus coeficientes. Es claro que esta aplicación es una norma en $k[x]$.

Teorema 2.18 *Sea k un cuerpo métrico discreto completo. Para cada polinomio $f(x) \in k[x]$ mónico irreducible separable de grado n, existe un $\delta > 0$ tal que si $g(x) \in k[x]$ es mónico de grado n y $\|f-g\| < \delta$, entonces g es irreducible en $k[x]$ y cada raíz α de f (en una clausura algebraica fija de k) se corresponde biunívocamente con una raíz β de g de modo que $k(\alpha) = k(\beta)$.*

DEMOSTRACIÓN: Sea C una clausura separable de k. Entonces sobre C tenemos definido un único valor absoluto que extiende al de k. Si $g \in k[x]$ es un polinomio mónico de grado n, podemos expresarlo en la forma

$$g(x) = x^n(1 + a_{n-1}x^{-1} + \cdots + a_1x_1^{-n} + a_0x^{-n}).$$

Así queda claro que si un $x \in C$ cumple $|x| \geq 2\|g\|$ entonces

$$|a_{n-1}x^{-1} + \cdots + a_1x_1^{-n} + a_0x^{-n}| \leq 1/2,$$

$$|1 + a_{n-1}x^{-1} + \cdots + a_1x_1^{-n} + a_0x^{-n}| \geq 1/2,$$

de donde $|g(x)| \geq 1$. En particular toda raíz de g en C ha de cumplir $|\alpha| < 2\|g\|$.

Fijemos un polinomio $f \in k[x]$ mónico separable de grado n. Para todo polinomio g mónico y de grado n y todo $\alpha \in C$, tomando M tal que $M > 1$, $M > |\alpha|$ tenemos que $|f(\alpha) - g(\alpha)| \leq \|f-g\|M^n$.

De aquí se sigue que si una sucesión de polinomios mónicos de grado n converge a f en norma, entonces converge puntualmente a f. En particular, si α es una raíz de g en C, se cumple

$$|f(\alpha)| = |f(\alpha) - g(\alpha)| \leq \|f-g\|(2\|g\|)^n \leq 2^n\|f-g\|(\|f-g\| + \|f\|),$$

y de aquí deducimos que para todo $\epsilon > 0$ existe un $\delta > 0$ tal que si g es un polinomio mónico de grado n con $\|f - g\| < \delta$, entonces $|f(\alpha)| < \epsilon^n$ para toda raíz α de g en C.

Descomponiendo f en producto de factores lineales es claro que si un $\alpha \in C$ dista de cada raíz de f más que ϵ, entonces $|f(x)| \geq \epsilon^n$. Reuniendo lo dicho concluimos que para cada $\epsilon > 0$ existe un $\delta > 0$ tal que si g es un polinomio mónico de grado n con $\|f - g\| < \delta$ entonces cada raíz de g en C dista menos de ϵ de una raíz de f.

Más aún, tomando δ suficientemente pequeño podemos asegurar que, fijada una raíz β de f, todo polinomio g mónico de grado n tal que $\|f - g\| < \delta$ tiene una raíz en C que dista de β menos que ϵ. En efecto, en caso contrario existiría una sucesión de polinomios mónicos de grado n, digamos $\{g_i\}$, que convergería a f en norma y de modo que las raíces de cada g_i en C se acercaran a las restantes raíces de f, pero eso implicaría que el valor absoluto de $g_i(x)$ estaría acotado inferiormente en un entorno de β, mientras que por otra parte $g_i(\beta)$ debería tender a 0.

Ahora supongamos que f es irreducible. Sea ϵ menor que la distancia entre dos cualesquiera de sus raíces. Sea $\delta > 0$ tal que si $\|f - g\| < \delta$ entonces las raíces de g en C distan menos que ϵ de las raíces de f. Por la elección de ϵ una misma raíz de g en C no puede distar menos que ϵ de dos raíces distintas de f, y como f tiene n raíces distintas, lo mismo le sucede a g y cada raíz β de g dista menos que ϵ de una única raíz α de f. En particular g es separable, y si α y β se corresponden en este sentido, $|\beta - \alpha| < \epsilon < |\gamma - \alpha|$, para cualquier otra raíz γ de f. El teorema anterior implica entonces que $k(\alpha) \subset k(\beta)$, pero como α es raíz de un polinomio irreducible de grado n, tenemos $|k(\alpha) : k| = n$, y como β es raíz de un polinomio de grado n, ha de ser $k(\alpha) = k(\beta)$, de donde se sigue que g es irreducible. ∎

Veamos algunas aplicaciones de estos teoremas. Llamaremos *cuerpos p-ádicos* a las extensiones finitas de $\mathbb{Q}_p$.

Teorema 2.19 *Sea K un cuerpo p-ádico. Entonces existe un cuerpo numérico $k \subset K$ tal que $|k : \mathbb{Q}| = |K : \mathbb{Q}_p|$ y k es denso en K.*

Demostración: Si $p = \infty$ el resultado es trivial. Supongamos que p es finito. Sea $K = \mathbb{Q}_p(\alpha)$. Basta aplicar el teorema anterior tomando como f el polinomio mínimo de α y como g un polinomio mónico con coeficientes racionales lo suficientemente cercano a f. Si β es una raíz de éste último (que está en K por el teorema anterior), definimos $k = \mathbb{Q}(\beta)$. ∎

En particular, tal y como afirmábamos, la clausura algebraica de $\mathbb{Q}$ es densa en $\mathbb{K}_p$. Las observaciones siguientes (hasta el final de la sección) no serán necesarias en el resto del libro.

Si k es un cuerpo numérico, su clausura en $\mathbb{Q}_p$ es $k\mathbb{Q}_p$, luego tiene grado finito sobre $\mathbb{Q}_p$. Si p es finito esto implica que $\overline{k} \neq \mathbb{K}_p$ (pues hemos visto que la extensión $\mathbb{K}_p/\mathbb{Q}_p$ es infinita). El teorema anterior implica que $\mathbb{K}_p$ es la unión de las clausuras de los cuerpos numéricos, que son subcuerpos propios cerrados. Es inmediato que todo subcuerpo propio de un cuerpo métrico tiene interior

vacío, luego el teorema de Baire implica que, si p es un primo finito, entonces la clausura algebraica $\mathbb{K}_p$ no es completa (al contrario de lo que ocurre para $p = \infty$). Por otra parte su compleción sigue siendo algebraicamente cerrada:

Teorema 2.20 *Sea k un cuerpo métrico discreto completo, sea $\mathbb{K}$ su clausura algebraica y $\overline{\mathbb{K}}$ su compleción. Entonces $\overline{\mathbb{K}}$ es algebraicamente cerrado.*

DEMOSTRACIÓN: En primer lugar probamos que $\overline{\mathbb{K}}$ es un cuerpo perfecto. Hemos de ver que si tiene característica prima p, entonces todos sus elementos tienen raíz p-ésima.

Ahora bien, cada $x \in \overline{\mathbb{K}}$ es el límite de una sucesión $\{x_n\}$ de elementos de $\mathbb{K}$, cada uno de los cuales tiene una (única) raíz p-ésima en $\mathbb{K}$, por ser éste algebraicamente cerrado. La sucesión $\{\sqrt[p]{x_n}\}$ es de Cauchy, pues

$$|\sqrt[p]{x_m} - \sqrt[p]{x_m}| = (|\sqrt[p]{x_m} - \sqrt[p]{x_m}|^p)^{1/p} = |x_m - x_n|^{1/p}.$$

Claramente $\lim_n \sqrt[p]{x_n}$ es una raíz p-ésima de x en $\overline{\mathbb{K}}$.

Sea ahora $f(x) \in \overline{\mathbb{K}}[x]$ un polinomio mónico irreducible. Según acabamos de probar, f es separable. Podemos aproximar sus coeficientes desde $\mathbb{K}$ y obtener así un polinomio $g(x) \in \mathbb{K}[x]$ mónico y del mismo grado al que podemos aplicar el teorema 2.18. Entonces $g(x)$ es irreducible (en $\overline{K}[x]$, luego también en $\mathbb{K}[x]$) luego tiene grado 1 y f también. ∎

2.3 La aritmética de los cuerpos numéricos

Con lo visto hasta ahora estamos en condiciones de demostrar los resultados básicos de la aritmética de los cuerpos numéricos. Una de sus características fundamentales es que los resultados que hacen referencia a un solo primo valen tanto para primos finitos como para primos infinitos, y los que involucran a todos los primos requieren que se consideren tanto los primos finitos como los infinitos.

En la sección anterior hemos convenido en llamar $\mathbb{K}_\mathfrak{p}$ a la clausura algebraica de la compleción $k_\mathfrak{p}$ de un cuerpo numérico k respecto a un primo finito $\mathfrak{p}$. Para unificar la notación, extendemos este convenio al caso infinito, de modo que si $\mathfrak{p}$ es un primo infinito entonces $k_\mathfrak{p}$ es isomorfo a $\mathbb{R}$ o $\mathbb{C}$ y su clausura algebraica es, por consiguiente, $\mathbb{K}_\mathfrak{p} = \mathbb{C}$. El valor absoluto canónico en $\mathbb{K}_\mathfrak{p}$ será en este caso el valor absoluto usual en $\mathbb{C}$.

Conviene tener presente que muchos de los resultados que hemos probado para compleciones respecto a primos finitos resultan trivialmente ciertas para primos infinitos. Por ejemplo, si K/k es una extensión de cuerpos numéricos, $\mathfrak{p}$ es un primo en k y $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en K, la igualdad $K_\mathfrak{P} = k_\mathfrak{p} K$, que el teorema 2.15 prueba en el caso finito, también vale en el caso infinito, pues el miembro derecho ha de ser $\mathbb{R}$ o $\mathbb{C}$, completo en cualquier caso, luego cerrado en $K_\mathfrak{P}$, y al contener a K es denso.

Definición 2.21 Sea K/k una extensión de cuerpos numéricos, sea $\mathfrak{p}$ un primo en k y $\mathfrak{P}$ un primo en K que divida a $\mathfrak{p}$. Definimos el *grado local* de la extensión en $\mathfrak{P}$ como

$$n(\mathfrak{P}/\mathfrak{p}) = |K_{\mathfrak{P}} : k_{\mathfrak{p}}|.$$

Teorema 2.22 *Sea K/k una extensión de grado n de cuerpos numéricos y sea $\mathfrak{p}$ un primo en k. Entonces*

$$n = \sum_{\mathfrak{P}|\mathfrak{p}} n(\mathfrak{P}/\mathfrak{p}).$$

DEMOSTRACIÓN: Se entiende que la suma recorre los divisores primos de $\mathfrak{p}$ en K. En el caso finito el teorema 2.8 nos da que $n(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$, y la relación buscada es consecuencia inmediata de 1.34.

Supongamos ahora que $\mathfrak{p}$ es un primo infinito, digamos que inducido por el monomorfismo $\sigma : k \longrightarrow \mathbb{C}$. Veamos que hay exactamente n monomorfismos $\tau : K \longrightarrow \mathbb{C}$ que extienden a σ. En efecto, fijado uno de ellos, cualquier otro es de la forma $\tau \circ \rho$, donde ρ es un $\sigma[k]$-monomorfismo de $\tau[K]$, y ρ puede tomar n valores posibles.

Estos n monomorfismos determinan todos los divisores de $\mathfrak{p}$ en K, pero hemos de tener presente que cada par de monomorfismos conjugados dan lugar al mismo divisor. Si $\mathfrak{p}$ es un primo complejo, entonces todas las extensiones de σ serán monomorfismos complejos y todos los grados locales serán $n(\mathfrak{P}/\mathfrak{p}) = 1$. Por otra parte, la conjugación de una extensión de σ ya no será una extensión de σ, luego las n extensiones son no conjugadas dos a dos y dan lugar a n divisores distintos. La relación buscada es en este caso $n = 1 + \cdots + 1$.

Si $\mathfrak{p}$ es real, entonces σ puede tener s extensiones reales y t pares de extensiones conjugadas. Tenemos entonces que $n = s + 2t$. Las extensiones reales dan lugar a s primos reales distintos en K para los cuales $n(\mathfrak{P}/\mathfrak{p}) = 1$. Las extensiones complejas dan lugar a t primos complejos distintos para los cuales $n(\mathfrak{P}/\mathfrak{p}) = 2$. Claramente también en este caso se cumple la relación entre los grados. ∎

La relación $n(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$ sólo tiene sentido, en principio, para primos finitos. Podemos extenderla al caso infinito adoptando el convenio de que si $\mathfrak{P}$ y $\mathfrak{p}$ son primos infinitos tales que $\mathfrak{P} \mid \mathfrak{p}$, entonces su *grado de inercia* es $f(\mathfrak{P}/\mathfrak{p}) = 1$ y su *índice de ramificación* es $e(\mathfrak{P}/\mathfrak{p}) = n(\mathfrak{P}/\mathfrak{p})$.

Para completar la analogía convendremos también en que un primo infinito factoriza como producto de los primos que lo dividen con las multiplicidades determinadas por los índices de ramificación.

Por ejemplo, en los cuerpos cuadráticos reales el primo ∞ de $\mathbb{Q}$ se escinde en dos factores reales distintos: $\infty = \infty_1\infty_2$, mientras que en los cuerpos cuadráticos imaginarios se ramifica: $\infty = \infty_1^2$.

En el teorema anterior hemos empleado argumentos completamente distintos para los primos finitos y para los infinitos. Ahora probaremos un resultado que generaliza la construcción que hemos hecho de los primos arquimedianos de

un cuerpo numérico y la extiende al caso de los primos finitos. Con su ayuda podremos probar muchos resultados sobre primos sin necesidad de distinguir si son finitos o no.

Teorema 2.23 *Sea K/k una extensión de cuerpos numéricos y $\mathfrak{p}$ un divisor primo de k. Entonces:*

a) Para cada k-monomorfismo $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ existe un primo $\mathfrak{P}$ en K divisor de $\mathfrak{p}$ tal que $|\alpha|_\mathfrak{P} = |\sigma(\alpha)|_\mathfrak{p}$ para todo $\alpha \in K$.

b) Para cada primo $\mathfrak{P}$ de K que divide a $\mathfrak{p}$, los k-monomorfismos que inducen el primo $\mathfrak{P}$ según el apartado a) son exactamente las restricciones a K de los $k_\mathfrak{p}$-monomorfismos $\sigma : K_\mathfrak{P} \longrightarrow \mathbb{K}_\mathfrak{p}$, y hay exactamente $n(\mathfrak{P}/\mathfrak{p})$ de ellos.

c) Dos k-monomorfismos σ y τ inducen el mismo valor absoluto si y sólo si existe un $k_\mathfrak{p}$-automorfismo $\phi : \mathbb{K}_\mathfrak{p} \longrightarrow \mathbb{K}_\mathfrak{p}$ tal que $\sigma \circ \phi = \tau$.

DEMOSTRACIÓN: Si $\mathfrak{P}$ es un divisor primo de $\mathfrak{p}$ en K, el teorema 2.12 implica que cada $k_\mathfrak{p}$-monomorfismo $\tau : K_\mathfrak{P} \longrightarrow \mathbb{K}_\mathfrak{p}$ es una isometría, pues el valor absoluto en $K_\mathfrak{P}$ dado por $|\alpha| = |\tau(\alpha)|_\mathfrak{p}$ extiende al valor absoluto canónico de $k_\mathfrak{p}$, luego ha de ser el valor absoluto canónico de $K_\mathfrak{P}$.

Por lo tanto, su restricción a K es un k-monomorfismo $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ que cumple $|\alpha|_\mathfrak{P} = |\sigma(\alpha)|_\mathfrak{p}$, para todo $\alpha \in K$, es decir, que induce el primo $\mathfrak{P}$ en el sentido del apartado a).

Como K es denso en $K_\mathfrak{P}$, las restricciones de dos $k_\mathfrak{p}$-monomorfismos distintos han de ser dos k-monomorfismos distintos, luego así obtenemos $n(\mathfrak{P}/\mathfrak{p})$ de ellos.

Además, dos k-monomorfismos obtenidos por restricción desde dos compleciones correspondientes a primos distintos en K han de ser distintos entre sí, pues cada uno induce en K valor absoluto distinto. Por el teorema anterior, si el grado de K/k es n, tenemos n monomorfismos distintos que cumplen el apartado a), pero éstos son todos los k-monomorfismos de K, luego a) es cierto para todos los k-monomorfismos. Este razonamiento prueba también b).

c) Si σ y τ inducen el mismo valor absoluto en K, digamos $|\ |_\mathfrak{P}$, por b) ambos se extienden a sendos $k_\mathfrak{p}$-monomorfismos $\sigma, \tau : K_\mathfrak{P} \longrightarrow \mathbb{K}_\mathfrak{p}$. Entonces $\sigma^{-1} \circ \tau : \sigma[K_\mathfrak{P}] \longrightarrow \tau[K_\mathfrak{P}]$ es un $k_\mathfrak{p}$-isomorfismo que se extiende a un $k_\mathfrak{p}$-automorfismo $\phi : \mathbb{K}_\mathfrak{p} \longrightarrow \mathbb{K}_\mathfrak{p}$ (porque $\mathbb{K}_\mathfrak{p}$ es la clausura algebraica de los cuerpos $\sigma[K_\mathfrak{p}]$ y $\tau[K_\mathfrak{p}]$). Claramente entonces $\sigma \circ \phi = \tau$.

Recíprocamente, supongamos que $\sigma \circ \phi = \tau$ para un cierto $k_\mathfrak{p}$-automorfismo ϕ. Entonces para todo $\alpha \in K$ se tiene $|\tau(\alpha)|_\mathfrak{p} = |\phi(\sigma(\alpha))|_\mathfrak{p} = |\sigma(\alpha)|_\mathfrak{p}$, porque los $k_\mathfrak{p}$-automorfismos son isometrías (en el caso infinito son la identidad en $\mathbb{R}$ o $\mathbb{C}$ o la conjugación compleja). Vemos, pues, que ambos monomorfismos inducen el mismo valor absoluto. ∎

De este teorema se siguen relaciones muy importantes entre los primos de un cuerpo numérico.

Definición 2.24 Sea K/k una extensión de cuerpos numéricos. Sea $\mathfrak{p}$ un primo en k y $\mathfrak{P}$ un primo en K que divida a $\mathfrak{p}$. Llamaremos *norma local* $\mathrm{N}_\mathfrak{P}$ y *traza local* $\mathrm{Tr}_\mathfrak{P}$ a la norma y la traza de la extensión $K_\mathfrak{P}/k_\mathfrak{p}$.

Si $\alpha \in K$, la norma de α (en la extensión K/k) es el producto las imágenes de α por los k-monomorfismos de K. Sin más que agrupar los factores correspondientes a monomorfismos que inducen un mismo primo $\mathfrak{P}$ según el teorema anterior obtenemos que

$$\mathrm{N}_k^K(\alpha) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_\mathfrak{P}(\alpha), \tag{2.1}$$

y análogamente para la traza:

$$\mathrm{Tr}_k^K(\alpha) = \sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{Tr}_\mathfrak{p}(\alpha). \tag{2.2}$$

Más aún, en el caso en que $k = \mathbb{Q}$ y $\mathfrak{p} = p$ es un primo racional (finito o no), entonces $\mathrm{N}_\mathfrak{P}(\alpha)$ es el producto de todos los conjugados de α por los monomorfismos que inducen el valor absoluto de $\mathfrak{P}$, o sea por los monomorfismos que cumplen $|\alpha|_\mathfrak{P} = |\sigma(\alpha)|_p$. Por lo tanto, si llamamos $n_\mathfrak{P} = n(\mathfrak{P}/p)$, resulta que $|\,\mathrm{N}_\mathfrak{P}(\alpha)|_p = |\alpha|_\mathfrak{P}^{n_\mathfrak{P}}$. Por consiguiente

$$|\,\mathrm{N}_\mathbb{Q}^K(\alpha)|_p = \prod_{\mathfrak{P}|p} |\alpha|_\mathfrak{P}^{n_\mathfrak{P}}. \tag{2.3}$$

De aquí se sigue una relación importante entre los valores absolutos de un cuerpo numérico:

Teorema 2.25 (Fórmula del producto) *Sea K un cuerpo numérico. Para cada primo $\mathfrak{p}$ de K sea p el primo racional divisible entre $\mathfrak{p}$ y sea $n_\mathfrak{p}$ el grado local $n(\mathfrak{p}/p)$. Entonces para todo $\alpha \in K$ no nulo se cumple*

$$\prod_\mathfrak{p} |\alpha|_\mathfrak{p}^{n_\mathfrak{p}} = 1,$$

donde $\mathfrak{p}$ recorre todos los primos de K.

Demostración: Notemos en primer lugar que si r es un número racional no nulo y p recorre todos los primos de $\mathbb{Q}$ se cumple

$$\prod_p |r|_p = 1.$$

En efecto, si q es un número primo entonces

$$|q|_p = \begin{cases} 1/q & \text{si } p = q, \\ 1 & \text{si } q \neq p \neq \infty \\ q & \text{si } p = \infty \end{cases}$$

Claramente entonces la fórmula es cierta para todo primo q. Trivialmente es cierta para ± 1 y, como el producto es multiplicativo, la fórmula es válida para todo número racional no nulo.

Por la fórmula (2.3) concluimos

$$1 = \prod_p |\,\mathrm{N}(\alpha)|_p = \prod_p \prod_{\mathfrak{p}|p} |\alpha|_{\mathfrak{p}}^{n_{\mathfrak{p}}} = \prod_{\mathfrak{p}} |\alpha|_{\mathfrak{p}}^{n_{\mathfrak{p}}}.$$

■

Definición 2.26 Sea $\mathfrak{p}$ un primo de un cuerpo numérico K, sea p el primo racional al cual divide y sea $n_{\mathfrak{p}}$ el grado local $n(\mathfrak{p}/p)$. Para cada $\alpha \in K$ definimos

$$\|\alpha\|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^{n_{\mathfrak{p}}}.$$

Claramente $\|\ \|_{\mathfrak{p}}$ es un valor absoluto asociado a $\mathfrak{p}$ excepto cuando $\mathfrak{p}$ es un primo complejo, en cuyo caso se trata del cuadrado del valor absoluto canónico. En estos términos la fórmula del producto se expresa como

$$\prod_p \|\alpha\|_{\mathfrak{p}} = 1. \tag{2.4}$$

En el caso de los primos no arquimedianos $\|\ \|_{\mathfrak{p}}$ es un valor absoluto muy natural. En efecto, si $v_{\mathfrak{p}}(\pi) = 1$ y p es el primo racional divisible entre $\mathfrak{p}$ (digamos $p = \mathfrak{p}^e$), entonces $p = \epsilon\pi^e$, para una cierta unidad ϵ (de $K_{\mathfrak{p}}$). Así, $1/p = |p|_p = |p|_{\mathfrak{p}} = |\pi^e|_{\mathfrak{p}}$, luego $|\pi|_{\mathfrak{p}} = (1/p)^{1/e}$ y, en definitiva,

$$\|\pi\|_{\mathfrak{p}} = \left(\frac{1}{p^{1/e}}\right)^{ef} = \frac{1}{p^f} = \frac{1}{N\mathfrak{p}}. \tag{2.5}$$

Esto caracteriza a $\|\ \|_{\mathfrak{p}}$ como el valor absoluto dado por $\|\alpha\|_{\mathfrak{p}} = (1/N\mathfrak{p})^{v_{\mathfrak{p}}(\alpha)}$.

Comentemos ahora otra consecuencia del teorema 2.23. En la sección anterior hemos visto que si p es un primo finito, la clausura algebraica $\mathbb{K}_p$ no es completa, pero si $K \subset \mathbb{K}_p$ es un cuerpo numérico (notemos que $\mathbb{K}_p$ contiene una clausura algebraica de $\mathbb{Q}$, y por lo tanto a todos los cuerpos numéricos) entonces la inclusión de K en $\mathbb{K}_p$ es un $\mathbb{Q}$-monomorfismo que determina un primo $\mathfrak{p}$ en K. Dicha inclusión se extiende a una isometría $K_{\mathfrak{p}} \longrightarrow \mathbb{K}_p$, cuya imagen es la clausura de K en $\mathbb{K}_p$. Así pues, $\overline{K}$ es completo aunque $\mathbb{K}_p$ no lo sea.

Veamos ahora qué podemos añadir para extensiones de Galois. Para empezar, el grupo de Galois actúa sobre los primos. Conviene dar una definición en el caso general:

Definición 2.27 Sea $\sigma : K \longrightarrow L$ un isomorfismo de cuerpos numéricos y sea $\mathfrak{p}$ un divisor primo en K. Definimos $\tau(\mathfrak{p})$ como el divisor primo de L inducido por el valor absoluto dado por $|\alpha|_{\sigma(\mathfrak{p})} = |\sigma^{-1}(\alpha)|_{\mathfrak{p}}$ para todo $\alpha \in L$.

Entonces σ es una isometría si en K consideramos el valor absoluto de $\mathfrak{p}$ y en L el de $\sigma(\mathfrak{p})$, luego σ se extiende a una isometría $\sigma : K_{\mathfrak{p}} \longrightarrow L_{\sigma(\mathfrak{p})}$.

Pasemos ya al caso en que K/k es una extensión de Galois de cuerpos numéricos y $\sigma \in G(K/k)$. Entonces si $\mathfrak{p}$ es un primo de k y $\mathfrak{P} \mid \mathfrak{p}$ se cumple que $\sigma(\mathfrak{P}) \mid \mathfrak{p}$ (pues el valor absoluto $|\ |_{\sigma(\mathfrak{P})}$ extiende al valor absoluto de $\mathfrak{p}$), o sea, que σ permuta los divisores de $\mathfrak{p}$.

Observar que si el primo $\mathfrak{P}$ es no arquimediano entonces el primo $\sigma(\mathfrak{P})$ que acabamos de definir es el definido en la sección 1.4 pues, considerados como ideales, $\alpha \in \sigma(\mathfrak{p})$ si y sólo si $|\alpha|_{\sigma(\mathfrak{p})} < 1$, si y sólo si $|\sigma^{-1}(\alpha)|_{\mathfrak{p}} < 1$, si y sólo si $\sigma^{-1}(\alpha) \in \mathfrak{p}$, si y sólo si $\alpha \in \sigma[\mathfrak{p}]$.

Ahora podemos definir el *grupo de descomposición*

$$G_{\mathfrak{p}} = \{\sigma \in G(K/k) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\} \leq G(K/k),$$

para cualquier divisor primo de K, incluso si es infinito. El teorema siguiente generaliza los resultados que probamos en el capítulo anterior para el caso finito.

Teorema 2.28 *Sea K/k una extensión de Galois de cuerpos numéricos. Sea $\mathfrak{p}$ un divisor primo en k. Entonces*

a) Si $\mathfrak{P}_1$ y $\mathfrak{P}_2$ son divisores de $\mathfrak{p}$ en K existe un automorfismo $\sigma \in G(K/k)$ tal que $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.

b) Si $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en K, el grupo de Galois local $G(K_{\mathfrak{p}}/k_{\mathfrak{p}})$ es isomorfo al grupo de descomposición $G_{\mathfrak{P}}$ (el isomorfismo es la restricción). En particular $|G_{\mathfrak{P}}| = n(\mathfrak{P}/\mathfrak{p})$.

c) Si $\tau \in G(K/k)$ y $\mathfrak{P}$ es un primo de K, entonces $G_{\tau(\mathfrak{P})} = G_{\mathfrak{p}}^{\tau}$.

Demostración: a) Tomamos como $\mathbb{K}_{\mathfrak{p}}$ una clausura algebraica de $K_{\mathfrak{P}_2}$ y así $K_{\mathfrak{P}_2} \subset \mathbb{K}_{\mathfrak{p}}$, y el valor absoluto asociado a $\mathfrak{P}_2$ coincide con el de $K_{\mathfrak{p}}$.

Sea $\sigma : K \longrightarrow \mathbb{K}_{\mathfrak{p}}$ que induce el valor absoluto de $\mathfrak{P}_1$, es decir, tal que $|\alpha|_{\mathfrak{P}_1} = |\sigma(\alpha)|_{\mathfrak{p}} = |\sigma(\alpha)|_{\mathfrak{P}_2}$.

Como K/k es de Galois se cumple que $\sigma \in G(K/k)$, y así $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$.

b) Si $\sigma \in G(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ entonces $\sigma : K_{\mathfrak{P}} \longrightarrow K_{\mathfrak{P}}$ es una isometría, luego su restricción a K es una isometría para el valor absoluto de $\mathfrak{P}$, luego $\sigma(\mathfrak{P}) = \mathfrak{P}$.

Recíprocamente, si $\sigma(\mathfrak{P}) = \mathfrak{P}$ entonces σ se extiende a un automorfismo de $K_{\mathfrak{p}}$ que fija a k, luego a $k_{\mathfrak{p}}$ (por continuidad).

La restricción es inyectiva porque K es denso en $K_{\mathfrak{P}}$, y claramente es un isomorfismo de grupos.

c) El argumento empleado en el caso finito es válido en general. ∎

Observar que el teorema anterior implica que en las extensiones de Galois el índice de ramificación de todos los divisores de un mismo primo es constante (los grupos tienen todos el mismo número de elementos).

Hasta aquí hemos descrito cuidadosamente las relaciones entre los cuerpos numéricos, sus compleciones y sus localizaciones. En lo sucesivo, si E es el anillo de enteros de un cuerpo numérico K, no distinguiremos entre un ideal primo $\mathfrak{p}$ de E, el único ideal maximal de la localización $E_{\mathfrak{p}}$ y el único ideal primo del anillo de enteros de la compleción $K_{\mathfrak{p}}$. También identificaremos los isomorfismos de cuerpos con sus extensiones a las compleciones. Los teoremas que hemos demostrado garantizarán la consistencia de cualquier doble interpretación que pueda surgir al adoptar estas identificaciones.

Como aplicación de los resultados de esta sección probaremos un teorema sobre escisión de primos.

Definición 2.29 Sea K/k una extensión de grado n de cuerpos numéricos. Diremos que un divisor primo $\mathfrak{p}$ de k se *escinde completamente* en K si tiene exactamente n divisores en K. Por el teorema 2.22 esto equivale a que los grados locales $n(\mathfrak{P}/\mathfrak{p})$ sean 1 para todos los divisores $\mathfrak{P}$ de $\mathfrak{p}$ en K, lo que a su vez equivale a que $e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = 1$.

Teorema 2.30 *Se cumple:*

a) Si $k \subset K \subset L$ son cuerpos numéricos, un primo $\mathfrak{p}$ de k se escinde completamente en L si y sólo si se escinde completamente en K y cada divisor de $\mathfrak{p}$ en K se escinde completamente en L.

b) Si K/k y L/k son extensiones de cuerpos numéricos, $\mathfrak{p}$ es un primo de k que se escinde completamente en K y $\mathfrak{P}$ es un primo en L que divide a $\mathfrak{p}$, entonces $\mathfrak{P}$ se escinde completamente en KL.

c) Si K/k y L/k son extensiones de cuerpos numéricos y $\mathfrak{p}$ es un primo de k que se escinde completamente en K y en L, entonces $\mathfrak{p}$ se escinde completamente en KL.

DEMOSTRACIÓN: a) es inmediato a partir de la definición.

c) es consecuencia de a) y b): todo divisor de $\mathfrak{p}$ en L se escinde completamente en KL, luego $\mathfrak{p}$ se escinde completamente en KL.

Para probar b) observemos en general que cada divisor de $\mathfrak{p}$ en una extensión T de k de grado n viene determinado por uno de los k-monomorfismos $T \longrightarrow \mathbb{K}_\mathfrak{p}$. Como hay n de ellos, $\mathfrak{p}$ se escindirá completamente si y sólo si no hay dos k-monomorfismos que determinen el mismo valor absoluto. Pero sabemos que dos k-monomorfismos σ y τ determinan el mismo valor absoluto si y sólo si $\sigma = \tau \circ \phi$, donde ϕ es un $k_\mathfrak{p}$-monomorfismo de $\mathbb{K}_\mathfrak{p}$. La conclusión es, pues, que $\mathfrak{p}$ se escinde en T si y sólo si para todo k-monomorfismo $\sigma : T \longrightarrow \mathbb{K}_\mathfrak{p}$ se cumple que cualquier $k_\mathfrak{p}$-monomorfismo de $\mathbb{K}_\mathfrak{p}$ es la identidad en $\sigma[T]$, o sea, si para todo k-monomorfismo σ se cumple que $\sigma[T] \subset k_\mathfrak{p}$.

Ahora notamos que, puesto que $K_\mathfrak{P}/k_\mathfrak{p}$ es una extensión finita, la clausura algebraica $\mathbb{K}_\mathfrak{P}$ es también una clausura algebraica de $k_\mathfrak{p}$, luego podemos considerar $\mathbb{K}_\mathfrak{P} = \mathbb{K}_\mathfrak{p}$.

Para ver que $\mathfrak{P}$ se escinde completamente en KL consideramos un L-monomorfismo $\sigma : KL \longrightarrow \mathbb{K}_\mathfrak{P}$. Puesto que σ se restringe a un k-monomorfismo $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ y $\mathfrak{p}$ se escinde completamente en K, ha de ser $\sigma[K] \subset k_\mathfrak{p}$ y, dado que σ fija a los elementos de L, resulta que $\sigma[KL] \subset k_\mathfrak{p}L = L_\mathfrak{P}$. Por lo tanto $\mathfrak{P}$ se escinde completamente en KL. ∎

Ejemplo Consideremos un cuerpo cúbico puro $\mathbb{Q}(\sqrt[3]{m})$. Su clausura normal se obtiene adjuntando una raíz cúbica de la unidad o, equivalentemente, adjuntando $\sqrt{-3}$, pues una raíz cúbica de la unidad es $\omega = (-1+\sqrt{-3})/2$ y los conjugados de $\sqrt[3]{m}$ son $\omega\sqrt[3]{m}$ y $\omega^2\sqrt[3]{m}$.

Por lo tanto, el cuerpo $K = \mathbb{Q}(\sqrt[3]{m}, \sqrt{-3})$ es una extensión finita de Galois sobre $\mathbb{Q}$ de grado 6. El teorema anterior nos permite determinar la factorización en K de los primos racionales a partir de la factorización en $\mathbb{Q}(\sqrt[3]{m})$ y en $\mathbb{Q}(\sqrt{-3})$, ambas vistas en [Sec. 3.3].

La tabla siguiente recoge todos los casos posibles (la notación es la introducida en [Sec. 3.3]):

Casos		$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt[3]{m})$	K	e	f
$p \nmid ab$	$p \equiv 1(3)$ $x^3 \equiv ab^2(p)$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6$	1	1
	$x^3 \not\equiv ab^2(p)$	$\mathfrak{p}_1\mathfrak{p}_2$	p	$\mathfrak{p}_1\mathfrak{p}_2$	1	3
	$p \equiv -1(3)$	p	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	2
$p \mid ab$	$p \equiv 1(3)$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}^3$	$(\mathfrak{p}_1\mathfrak{p}_2)^3$	3	1
	$p \equiv -1(3)$	p	$\mathfrak{p}^3$	$\mathfrak{p}^3$	3	2
$p = 3$	Tipo I	$\mathfrak{p}^2$	$\mathfrak{p}^3$	$\mathfrak{p}^6$	6	1
	Tipo II	$\mathfrak{p}^2$	$\mathfrak{p}_1\mathfrak{p}_2^2$	$(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$	2	1

La primera fila se obtiene aplicando el teorema anterior: p se escinde completamente tanto en $\mathbb{Q}(\sqrt{-3})$ como en $\mathbb{Q}(\sqrt[3]{m})$, luego se escinde completamente en el producto. Las restantes se deducen elementalmente usando la transitividad de e y f. Tomemos por ejemplo la tercera fila. Sabemos que f ha de ser múltiplo de 2 (porque vale 2 en $\mathbb{Q}(\sqrt{-3})$) y divisor de 6, pero no puede ser 6 porque el número de primos ha de ser $r \geq 2$ (por $\mathbb{Q}(\sqrt[3]{m})$), luego ha de ser $f = 2$, y la única posibilidad es $r = 3$, $f = 2$, $e = 1$. En los demás casos se razona de forma similar. ∎

Ejercicio: Factorizar ∞ en las tres extensiones del ejemplo anterior.

Terminamos la sección con un teorema muy útil sobre valores absolutos que generaliza al teorema chino del resto.

Teorema 2.31 (Teorema de aproximación (Artin-Whaples)) *Sea K un cuerpo y sean $|\ |_1, \ldots, |\ |_n$ valores absolutos en K no triviales y no equivalentes dos a dos. Sean $x_1, \ldots, x_n \in K$ y $\epsilon > 0$. Entonces existe un $x \in K$ tal que $|x - x_i|_i < \epsilon$ para $i = 1, \ldots, n$.*

Demostración: Notemos en primer lugar que si dos valores absolutos no triviales cumplen que cuando $|\alpha|_1 \leq 1$ también $|\alpha|_2 \leq 1$, entonces ambos son equivalentes.

En efecto, existe un cierto $c \in K$ tal que $0 < |c|_2 < 1$. De este modo $|\alpha|_1 < 1$ implica que $|\alpha^n|_1 \leq |c|_1$ para n suficientemente grande, luego $|\alpha^n/c|_1 \leq 1$, luego

$|\alpha^n/c|_2 \leq 1$, luego $|\alpha^n|_2 \leq |c|_2 < 1$, y por lo tanto $|\alpha|_2 < 1$. Recíprocamente, $|\alpha|_1 \geq 1$ implica que $|1/\alpha|_1 \leq 1$, luego $|1/\alpha|_2 \leq 1$ y $|\alpha|_2 \geq 1$.

Así pues, $|\alpha|_1 < 1$ si y sólo si $|\alpha|_2 < 1$. De aquí se sigue claramente la equivalencia.

Ahora las hipótesis del teorema nos dan que existen $\alpha, \beta \in K$ tales que

$$|\alpha|_1 < 1, \quad |\alpha|_2 \geq 1, \quad |\beta|_1 \geq 1, \quad |\beta|_2 < 1.$$

Llamando $y = \beta/\alpha$ resulta que $|y|_1 > 1$, $|y|_2 < 1$.

Veamos por inducción sobre n que existe un cierto $y \in K$ tal que $|y|_1 > 1$, $|y|_i < 1$ para $i = 2, \ldots, n$. Lo tenemos probado para $n = 2$. Supongamos que existe un $y \in K$ tal que $|y|_1 > 1$, $|y|_i < 1$ para $i = 2, \ldots, n-1$. Tomemos también un $z \in K$ que cumpla $|z|_1 > 1$, $|z|_n < 1$.

Si se cumple $|y|_n \leq 1$ entonces $y^m z$ cumple lo pedido cuando m es suficientemente grande. Si $|y|_n > 1$ consideramos la sucesión $u_m = y^m/(1+y^m)$, que claramente tiende a 1 respecto a los valores absolutos $|\ |_1$ y $|\ |_n$ y tiende a 0 respecto a los restantes. Cuando m es suficientemente grande $u_m z$ cumple lo pedido.

Sea, pues, $y \in K$ tal que $|y|_1 > 1$, $|y|_i < 1$ para $i = 2, \ldots, n$. Usamos de nuevo que la sucesión $y^m/(1+y^m)$ tiende a 1 respecto al primer valor absoluto y tiende a 0 respecto a los demás. Multiplicándola por x_1 y tomando un término suficientemente lejano obtenemos un elemento $y_1 \in K$ tal que $|x_1 - y_1|_1 < \epsilon/n$ y $|y_1|_i < \epsilon/n$ para $i = 2, \ldots, n$.

Del mismo modo podemos obtener elementos y_i tales que $|x_i - y_i|_i < \epsilon/n$, $|y_i|_j < \epsilon/n$ para $j \neq i$. El teorema se cumple con $x = y_1 + \cdots + y_n$. ∎

2.4 Extensiones no ramificadas

En esta sección y en la siguiente estudiaremos ciertas clases de extensiones de cuerpos discretos completos. Si k es un cuerpo métrico discreto completo k y D es su anillo de enteros, sabemos que D es un dominio de Dedekind con un único primo $\mathfrak{p}$. En particular D es un dominio euclídeo. Representaremos por $\overline{k}$ al cuerpo de restos $\overline{k} = D/\mathfrak{p}$.

Las extensiones finitas separables de cuerpos métricos discretos completos están descritas en el teorema 2.13: si K es una extensión separable de grado n de un cuerpo métrico discreto completo k entonces K también es un cuerpo discreto completo y sus anillos de enteros forman una extensión E/D de dominios de Dedekind.

La aritmética de E se relaciona con la de D a través del índice de ramificación $e = e(\mathfrak{P}/\mathfrak{p})$, dado por $\mathfrak{p} = \mathfrak{P}^e$, y el grado de inercia $f = f(\mathfrak{P}/\mathfrak{p}) = |\overline{K} : \overline{k}|$, donde $\overline{k}$ se identifica con un subcuerpo de $\overline{K}$ de forma natural. Sabemos que $ef = n$.

Recordemos, por último, que E es un D-módulo finitamente generado libre de torsión y, como D es un dominio euclídeo, E es de hecho un D-módulo libre, necesariamente de rango n.

Ya hemos comentado que la hipótesis de separabilidad puede eliminarse: todos los hechos que acabamos de citar son ciertos siempre que K/k es una extensión finita de cuerpos discretos completos. Damos la prueba en el apéndice. Para no añadir hipótesis superfluas, en los resultados de esta sección y la siguiente hemos optado por enunciar los teoremas para extensiones finitas arbitrarias, con lo cual admiten una doble lectura: o bien se acepta la validez de los hechos citados para extensiones finitas, o bien se supone que los cuerpos involucrados tienen todos[1] característica 0, en cuyo caso las hipótesis de separabilidad que necesitamos se satisfacen trivialmente.

Recalcamos que en los capítulos posteriores aplicaremos estos resultados exclusivamente a las compleciones no arquimedianas de los cuerpos numéricos, por lo que la hipótesis de característica nula no nos supondrá ninguna restricción en la práctica.

En esta sección estudiamos con más detalle la relación entre las extensiones finitas de un cuerpo métrico discreto k y las extensiones finitas de su cuerpo de restos $\overline{k}$. Fijemos una clausura algebraica $\mathbb{K}$ de k y sea $\mathbb{E}$ la clausura entera de D en $\mathbb{K}$ (donde D es el anillo de enteros de k). Cuando hablemos de extensiones algebraicas de k entenderemos que las tomamos en $\mathbb{K}$. Para cada extensión finita K de k, su anillo de enteros E_k tiene un único ideal primo $\mathfrak{P}_k$, y es fácil ver que la unión de todos los ideales $\mathfrak{P}_K$ forma un ideal primo $\mathfrak{P}$ de $\mathbb{E}$. Dos elementos de $\mathbb{E}$ son congruentes módulo $\mathfrak{P}$ si y sólo si lo son módulo $\mathfrak{P}_K$, para cualquier extensión finita K de k que los contenga. Esto permite identificar de forma natural a cada cuerpo de restos $\overline{K}$ con un subcuerpo de $\overline{\mathbb{K}} = \mathbb{E}/\mathfrak{P}$.

También es fácil ver que $\overline{\mathbb{K}}$ es una clausura algebraica de $\overline{k}$. En efecto, cada elemento de $\overline{\mathbb{K}}$ es la clase de un elemento de $\alpha \in \mathbb{E}$, cuyo polinomio mínimo f sobre k tiene coeficientes en D, por lo que $[\alpha]$ es la raíz de la proyección natural $\overline{f}$ de f en $\overline{k}[x]$. Esto prueba que $\overline{\mathbb{K}}$ es una extensión algebraica de $\overline{k}$. Por otra parte, todo polinomio de $\overline{k}[x]$ es la proyección de un polinomio $f \in \mathbb{E}[x]$ del mismo grado. Como las raíces de un polinomio con coeficientes enteros son enteras, f se escinde en $\mathbb{E}[x]$, luego $\overline{f}$ se escinde en $\overline{\mathbb{K}}[x]$.

Así pues, cuando hablemos de extensiones algebraicas de $\overline{k}$ entenderemos que están contenidas en $\overline{\mathbb{K}}$. Es claro que la correspondencia $K \mapsto \overline{K}$ es una aplicación suprayectiva entre las extensiones finitas de k y las extensiones finitas de $\overline{k}$. Sin embargo no es inyectiva. Lo que haremos en esta sección es estudiar una familia de extensiones finitas de k que se corresponden biunívocamente con las extensiones finitas separables de $\overline{k}$.

Definición 2.32 Sea K/k una extensión de grado n de cuerpos métricos discretos completos y sea E/D la extensión de sus anillos de enteros. Sea $\mathfrak{P}$ el ideal primo de E y $\mathfrak{p}$ el ideal primo de D. Diremos que $\mathfrak{P}$ es *no ramificado* sobre $\mathfrak{p}$, o que la extensión K/k es *no ramificada* si $e = 1$ (o, equivalentemente, si $f = n$) y el cuerpo de restos $E/\mathfrak{P}$ es una extensión separable de $D/\mathfrak{p}$.

[1]Esta hipótesis no incluye a los cuerpos de restos $D/\mathfrak{p}$, que en los casos de mayor interés serán cuerpos finitos.

Así pues, K/k es no ramificada si $\overline{K}/\overline{k}$ es separable y $|K : k| = |\overline{K} : \overline{k}|$. Vamos a comprobar que la relación entre una extensión no ramificada y la extensión de sus cuerpos de restos es mucho más fuerte que la de tener el mismo grado. En primer lugar necesitamos un resultado técnico.

Teorema 2.33 *Sea E/D una extensión de Galois de dominios de Dedekind. Sea K/k la extensión de los cuerpos de cocientes. Sea $\mathfrak{p}$ un primo en D y supongamos que $\mathfrak{p}$ es divisible entre un único primo $\mathfrak{P}$ de E. Supongamos también que $E/\mathfrak{P}$ es separable sobre $D/\mathfrak{p}$. Consideremos un polinomio mónico irreducible $f(x) \in D[x]$ con una raíz en E. Entonces la imagen $\overline{f}$ de f en $(D/\mathfrak{p})[x]$ es potencia de un polinomio irreducible.*

DEMOSTRACIÓN: Puesto que K/k es una extensión finita de Galois, tenemos que $f(x)$ se escinde en $K[x]$ y, como E es la clausura entera de D en K, sabemos que todas las raíces de $f(x)$ están en E. Consecuentemente $f(x)$ se escinde en $E[x]$ y $\overline{f}$ se escinde en $(E/\mathfrak{P})[x]$.

Dos raíces cualesquiera de $\overline{f}$ son las clases de equivalencia de dos raíces de f, que son conjugadas en E por un k-automorfismo que fija a $\mathfrak{P}$ (por ser el único primo de $\mathfrak{P}$). Según el teorema 1.39, este automorfismo induce un $D/\mathfrak{p}$-automorfismo de $E/\mathfrak{P}$ que conjuga las raíces dadas, luego las raíces de $\overline{f}$ son todas conjugadas, con lo que $\overline{f}$ no puede ser divisible entre dos polinomios irreducibles distintos. ∎

Teorema 2.34 *Sea K/k una extensión finita de cuerpos métricos discretos completos.*

a) Si K/k es no ramificada y $\overline{K} = \overline{k}([\alpha])$ para cierto entero $\alpha \in K$, entonces la extensión K/k es separable, $K = k(\alpha)$ y el polinomio mínimo de α en k es irreducible en $\overline{k}[x]$.

b) Si $K = k(\alpha)$ para un cierto entero $\alpha \in K$ cuyo polinomio mínimo no tenga raíces múltiples en $\overline{K}$, entonces K/k es no ramificada y $\overline{K} = \overline{k}([\alpha])$.

DEMOSTRACIÓN: a) Sea $f(x)$ el polinomio mínimo de α sobre k. Como α es entero, se cumple que $f(x)$ tiene coeficientes enteros en k, y su imagen $\overline{f}$ es un polinomio mónico con raíz $[\alpha]$. Como la extensión es no ramificada el grado de $\overline{K}$ sobre $\overline{k}$ coincide con el grado n de K/k. Claramente entonces $n \le \operatorname{grad} \overline{f} = \operatorname{grad} f \le n$, luego se da la igualdad y por lo tanto $\overline{f}$ es el polinomio mínimo de $[\alpha]$. Esto implica que $\overline{f}$ es separable, y entonces f también ha de serlo. La conclusión es ahora obvia.

b) Es obvio que $\overline{K} = \overline{k}([\alpha])$, y por hipótesis $[\alpha]$ es separable sobre $\overline{k}$. Así pues, la extensión $\overline{K}/\overline{k}$ es separable.

Pero la hipótesis implica también que el polinomio mínimo de α no tiene raíces múltiples, luego la extensión K/k es separable también. Podemos aplicar el teorema anterior a la menor extensión de Galois de k que contiene a K. Concluimos que la imagen $\overline{f}$ del polinomio mínimo de α es irreducible en $\overline{k}$.

Esto prueba que $|\overline{K}:\overline{k}| \geq |K:k|$ y, como la otra desigualdad siempre es cierta, de hecho tenemos la igualdad. El teorema es ahora inmediato. ∎

Observemos que si K/k es una extensión no ramificada entonces por definición $\overline{K}/\overline{k}$ es separable, luego tiene un elemento primitivo. Por consiguiente el apartado a) prueba que las extensiones no ramificadas son siempre separables.

El apartado b) afirma que la condición necesaria y suficiente para que al adjuntarle a k un entero separable α obtengamos una extensión no ramificada es que las raíces de su polinomio mínimo permanezcan distintas en los cuerpos de restos.

Ahora podemos probar las propiedades básicas de las extensiones no ramificadas:

Teorema 2.35 *Sea k un cuerpo métrico discreto completo.*

a) Si $k \subset K \subset L$ es una cadena de extensiones finitas, entonces L/k es no ramificada si y sólo si L/K y K/k son no ramificadas.

b) Si K/k es una extensión finita no ramificada y L/k es una extensión finita, entonces KL/L es no ramificada.

c) Si K/k y L/k son extensiones finitas no ramificadas entonces KL/k también lo es.

Demostración: a) es inmediato a partir de la definición.

b) Sea $\overline{K} = \overline{k}([\alpha])$ para cierto entero $\alpha \in K$ y sea $f(x)$ el polinomio mínimo de α sobre k. Por el teorema anterior sabemos que $K = k(\alpha)$ y que $f(x)$ es irreducible en $\overline{k}\,[x]$ (luego separable). Claramente $KL = L(\alpha)$ y el polinomio mínimo de α sobre L divide a f, luego será separable también. Por el teorema anterior la extensión KL/L es no ramificada.

c) Por b) la extensión KL/L es no ramificada, luego por a) KL/k también lo es. ∎

Con estas propiedades ya podemos demostrar que las extensiones no ramificadas de un cuerpo k se corresponden biunívocamente con las extensiones separables del cuerpo de restos:

Teorema 2.36 *Sea k un cuerpo métrico discreto completo.*

a) Si K y L son extensiones finitas de k tales que K/k es no ramificada y $\overline{K} = \overline{L}$, entonces $K \subset L$.

b) La correspondencia $K \mapsto \overline{K}$ biyecta las extensiones no ramificadas de k con las extensiones finitas separables de $\overline{k}$.

c) Si K/k es una extensión no ramificada entonces K/k es separable, y K/k es de Galois si y sólo si lo es $\overline{K}/\overline{k}$. En tal caso, el epimorfismo descrito en el teorema 1.39 *es un isomorfismo entre $G(K/k)$ y $G(\overline{K}/\overline{k})$.*

DEMOSTRACIÓN: a) Claramente $\overline{KL} = \overline{K}\,\overline{L} = \overline{L}$, y por el teorema anterior la extensión KL/L es no ramificada. Por consiguiente $|KL : L| = |\overline{KL} : \overline{L}| = 1$, es decir, $KL = L$, luego $K \subset L$.

b) Toda extensión separable de $\overline{k}$ es de la forma $\overline{k}([\alpha])$, donde α es un entero en una extensión de k. El polinomio mínimo de $[\alpha]$ en $\overline{k}$ será de la forma $\overline{f}$, donde $f \in k[x]$ es un polinomio mónico con coeficientes enteros. Descomponiéndolo en factores lineales y tomando clases, concluimos que existe una raíz β de $f(x)$ tal que $[\beta] = [\alpha]$. Equivalentemente, podemos suponer que α es raíz de $f(x)$.

Como el polinomio mínimo de α sobre k divide a f, no puede tener raíces múltiples en $\overline{\mathbb{K}}$, luego el teorema 2.34 nos da que $K = k(\alpha)$ es una extensión no ramificada de k, y ciertamente $\overline{K}$ es la extensión dada. La unicidad se sigue del apartado anterior.

c) Ya sabemos que las extensiones no ramificadas son separables. Si K/k es de Galois el teorema 1.39 nos da que $\overline{K}/\overline{k}$ también lo es, y tenemos el epimorfismo $G(K/k) \longrightarrow G(\overline{K}/\overline{k})$ descrito allí (observemos que como K tiene un único primo el grupo de descomposición es todo el grupo de Galois). Por otra parte los dos grupos de Galois tienen orden n, luego el epimorfismo es en realidad un isomorfismo.

Supongamos ahora que la extensión $\overline{K}/\overline{k}$ es de Galois. Sea $\overline{K} = \overline{k}([\alpha])$. Según el teorema 2.34 se cumple que $K = k(\alpha)$ y el polinomio mínimo f de α sobre k induce el polinomio mínimo de $[\alpha]$ sobre $\overline{k}$. Basta probar que todas las raíces de f están en K. Ahora bien, si β es una raíz de f, entonces $[\beta]$ es una raíz de $\overline{f}$ y, como $\overline{K}/\overline{k}$ es de Galois, $[\beta] \in \overline{K}$. Más aún, puesto que $[\beta]$ tiene el mismo polinomio mínimo que $[\alpha]$, se cumple $\overline{K} = \overline{k}([\beta])$.

Resulta entonces que el cuerpo $L = k(\beta)$ es una extensión no ramificada de k con el mismo cuerpo de restos, luego el apartado a) nos da que $L = K$, y por consiguiente $\beta \in K$. ∎

Como ya hemos dicho, estos teoremas vamos a aplicarlos al caso de las compleciones de los cuerpos numéricos, en las cuales los cuerpos de restos son finitos. Todas las extensiones finitas de los cuerpos finitas son de Galois, cíclicas de hecho, luego en este caso se cumple:

Teorema 2.37 *Toda extensión no ramificada de un cuerpo métrico discreto localmente compacto es finita de Galois con grupo de Galois cíclico.*

(Recordemos de [7.15] que la compacidad local en un cuerpo métrico discreto completo equivale a que el cuerpo de restos sea finito.)

2.5 Extensiones totalmente ramificadas

Definición 2.38 Sea k un cuerpo métrico discreto completo. Una extensión K/k de grado n es *totalmente ramificada* si cumple que $e = n$ (o, equivalentemente, $f = 1$). Si $\mathfrak{p}$ es el único primo de k y $\mathfrak{P}$ es el único primo de K, también se dice que $\mathfrak{P}$ está *totalmente ramificado* sobre $\mathfrak{p}$.

De este modo, las extensiones totalmente ramificadas son las que presentan un comportamiento enteramente opuesto al de las extensiones no ramificadas. Observemos que K/k es no ramificada si y sólo si $\overline{K} = \overline{k}$. En general una extensión no tiene por qué ser no ramificada o totalmente ramificada, pero toda extensión (cuya extensión de cuerpos de restos sea separable) se descompone en dos extensiones de estos tipos:

Teorema 2.39 *Sea k un cuerpo métrico discreto completo y sea K una extensión finita de k tal que la extensión $\overline{K}/\overline{k}$ sea separable. Sea K_{nr} el producto de todos los cuerpos intermedios no ramificados sobre k. Entonces la extensión K_{nr}/k es no ramificada y la extensión K/K_{nr} es totalmente ramificada.*

DEMOSTRACIÓN: La extensión K_{nr}/k es no ramificada por el teorema 2.35.

Según el teorema 2.36 existe una extensión no ramificada L de k tal que $\overline{L} = \overline{K}$. Por el apartado a) de este mismo teorema se cumple de hecho que $L \subset K$, luego $k \subset L \subset K_{nr}$. Consecuentemente, $\overline{K} = \overline{L} \subset \overline{K}_{nr} \subset \overline{K}$, luego $\overline{L} = \overline{K}_{nr}$ y, de nuevo por 2.36, $L = K_{nr}$. Así pues, $\overline{K}_{nr} = \overline{K}$, lo que implica que la extensión K/K_{nr} es totalmente ramificada. ∎

Recordemos que un *polinomio de Eisenstein* para un primo π en un dominio de factorización única es un polinomio mónico cuyos coeficientes sean todos divisibles entre π excepto el coeficiente director y cuyo término independiente no sea divisible entre π^2. El criterio de irreducibilidad de Eisenstein afirma que los polinomios de Eisenstein son siempre irreducibles.

Teorema 2.40 *Sea k un cuerpo métrico discreto completo y K una extensión de k de grado n.*

a) Si K/k es totalmente ramificada y $\mathfrak{P} = (\pi)$ es el primo de K, entonces el polinomio mínimo de π en K es un polinomio de Eisenstein de grado n.

b) Si $K = k(\pi)$ y π es la raíz de un polinomio de Eisenstein con coeficientes en K, entonces la extensión es totalmente ramificada y π es primo en K.

DEMOSTRACIÓN: a) Consideremos una clausura algebraica de k, donde tenemos definido un valor absoluto que extiende a uno prefijado de k. Como los k-automorfismos son isometrías, todos los conjugados de π tienen el mismo valor absoluto, y éste es menor que 1.

Los coeficientes distintos del director del polinomio mínimo de π se obtienen de sumas de productos de los conjugados de π, y como el valor absoluto es no arquimediano resulta que todos tienen valor absoluto menor que 1. Esto significa que todos son divisibles entre el único primo de k. El término independiente es, concretamente, el producto de todos los conjugados de π, luego su valor absoluto es $|\pi|^n$. Como el único primo de k es precisamente $\mathfrak{p} = \mathfrak{P}^n$, es claro que dicho término independiente no es divisible entre $\mathfrak{p}^2$.

b) Sea ρ un primo en k, con lo que $\mathfrak{p} = (\rho)$, y supongamos que π es una raíz de un polinomio de Eisenstein de grado n con coeficientes en k.

Entonces el valor absoluto del término independiente es $|\rho|$, y por otra parte dicho término independiente es el producto de los n conjugados de π (pues el polinomio es irreducible, luego $|\pi|^n = |\rho| < 1$

Por lo tanto, $|\pi^n/\rho| = 1$, o sea, que π^n/ρ es una unidad y, como ideal en K, se tiene $\mathfrak{p} = (\pi)^n$. De aquí se sigue que π es primo, pues el índice de ramificación no puede ser mayor que el grado de la extensión. Así pues, $\mathfrak{P} = (\pi)$ y la extensión es totalmente ramificada. ∎

Veamos una aplicación de este teorema:

Teorema 2.41 *Sea k un cuerpo métrico localmente compacto perfecto y sea n un número natural. Entonces k tiene sólo un número finito de extensiones de grado $\leq n$.*

Demostración: Cada extensión de grado $\leq n$ de k se descompone en una extensión no ramificada de grado $\leq n$ seguida de una extensión totalmente ramificada también de grado $\leq n$. (Observar que $\overline{k}$ es finito, luego perfecto, y por consiguiente podemos aplicar el teorema 2.39). El teorema 2.36 nos da que hay sólo un número finito de extensiones no ramificadas de k de grado $\leq n$ (porque un cuerpo finito tiene sólo un número finito de extensiones de grado $\leq n$). Basta ver que cada una de estas extensiones admite sólo un número finito de extensiones totalmente ramificadas de grado $\leq n$. Puesto que tales extensiones son localmente compactas (tienen cuerpos de restos finitos), basta probar que todo cuerpo métrico localmente compacto k tiene sólo un número finito de extensiones totalmente ramificadas de un grado fijo e.

Sea $\mathfrak{p} = (\pi)$ el primo de k. Cada extensión está determinada por un polinomio de Eisenstein de la forma

$$x^e + \alpha_{e-1}x^{e-1} + \cdots + \alpha_1 x + u_0\pi,$$

donde los coeficientes α_i están en $\mathfrak{p}$ y u_0 es una unidad de k. Si llamamos U al grupo de las unidades tenemos que cada polinomio de Eisenstein de grado e está determinado por un elemento de $\mathfrak{p} \times \overset{e-2}{\cdots} \times \mathfrak{p} \times U$. Recíprocamente, cada elemento de este espacio determina a lo sumo e extensiones de k.

El teorema 2.18 (y aquí usamos que k es perfecto) afirma que cada punto de este espacio tiene un entorno (respecto a la topología producto) cuyos puntos determinan las mismas extensiones de k. Por compacidad hay tan sólo un número finito de extensiones. ∎

La ramificación de los primos es una de las partes más delicadas de la teoría que estamos estudiando. No entraremos a fondo en ella hasta el capítulo X, pero de momento nos conviene dar un paso más, con el cual aislaremos la situación más difícil de manejar. Para ello introducimos los conceptos siguientes:

Definición 2.42 Una extensión finita K/k de cuerpos métricos completos discretos es *dominadamente ramificada* si la extensión $\overline{K}/\overline{k}$ es separable y la característica de estos cuerpos no divide al índice de ramificación e. En caso contrario se dice que la extensión es *libremente ramificada.* Alternativamente, si $\mathfrak{p}$ es el

primo de k y $\mathfrak{P}$ el de K, se dice que $\mathfrak{P}$ está dominada o libremente ramificado sobre $\mathfrak{p}$.

Observemos que las extensiones dominadamente ramificadas contienen a las no ramificadas. Si los cuerpos de restos tienen característica 0 todas las extensiones son dominadamente ramificadas y lo que diremos a continuación se vuelve trivial. Ahora necesitamos un resultado técnico.

Teorema 2.43 *Sea K/k una extensión totalmente ramificada de cuerpos métricos discretos completos cuyos cuerpos de restos tengan característica prima p. Sea e un número natural no divisible entre p, sea $\mathfrak{p} = (\rho)$ el ideal primo de k y sea $\pi \in K$ tal que $|\pi|^e = |\rho|$. Entonces existe una unidad ϵ en k tal que una de las raíces del polinomio $x^e - \epsilon\rho$ está contenida en $k(\pi)$.*

Demostración: Sea $\delta = \pi^e/\rho$, que por hipótesis cumple $|\delta| = 1$, luego es una unidad de K. Sea $\mathfrak{P}$ el ideal primo de K. Como $\mathfrak{P}$ está totalmente ramificado sobre $\mathfrak{p}$ se cumple que $\overline{K} = \overline{k}$, luego existe una unidad $\epsilon \in k$ tal que $\delta \equiv \epsilon \pmod{\mathfrak{P}}$.

Así pues, existe un $\gamma \in \mathfrak{P}$ tal que $\delta = \epsilon + \gamma$, es decir, $\pi^e = \epsilon\rho + \gamma\rho$. Como $|\gamma| < 1$ resulta que $|\pi^e - \epsilon\rho| < |\rho|$.

Sea $f(x) = x^e - \epsilon\rho$ y sean $\alpha_1, \ldots, \alpha_e$ sus raíces (que son distintas porque f es separable, ya que si K tiene característica prima, ésta ha de ser igual a p y tenemos que $p \nmid e$). Entonces

$$|f(\pi)| = |\pi - \alpha_1| \cdots |\pi - \alpha_e| = |\pi^e - \epsilon\rho| < |\rho| = |\pi|^e,$$

luego alguna de las raíces, digamos α_1, ha de cumplir $|\pi - \alpha_1| < |\pi|$.

De la ecuación $f(\alpha_i) = 0$ se sigue que $|\alpha_i|^e = |\pi|^e$, luego $|\alpha_i| = |\pi|$ y en particular tenemos $|\pi - \alpha_1| < |\alpha_1|$.

Como $p \nmid e$ podemos afirmar que $e \notin \mathfrak{p}$, luego $|e| = 1$. Teniendo esto en cuenta llegamos a que

$$|f'(\alpha_1)| = |\alpha_1|^{e-1} = |\alpha_1 - \alpha_2| \cdots |\alpha_1 - \alpha_e|,$$

pero $|\alpha_1 - \alpha_i| \le |\alpha_1|$, pues el valor absoluto es no arquimediano y $|\alpha_1| = |\alpha_i|$. Esto implica que $|\alpha_1 - \alpha_i| = |\alpha_1|$ para todo $i = 2, \ldots, e$.

En resumen tenemos que $|\pi - \alpha_1| < |\alpha_1| = |\alpha_i - \alpha_1|$ para $i = 2, \ldots, e$. El teorema se sigue ahora de 2.17. Notemos que según el enunciado de 2.17 haría falta que π fuera separable sobre k, pero si analizamos la prueba vemos que basta con que α sea separable y que el valor absoluto de k se extienda a una extensión que contenga a β (π en nuestro caso) y a todos los conjugados de α. ∎

El teorema siguiente mejora a 2.40 para las extensiones totalmente ramificadas con ramificación dominada. Esencialmente afirma que una extensión K/k totalmente ramificada de grado n no divisible entre la característica de $\overline{k}$ tiene ramificación dominada si y sólo si podemos tomar como primo en K a una raíz n-sima de un primo en k.

Teorema 2.44 *Sea k un cuerpo métrico discreto completo y sea K una extensión de k de grado n. Sea $\mathfrak{p}$ y $\mathfrak{P}$ los primos de k y K respectivamente. Sea p la característica de $\overline{k}$.*

a) Si K/k es total y dominadamente ramificada entonces existen $\pi \in K$ y $\rho \in k$ de modo que $K = k(\pi)$, $\mathfrak{P} = (\pi)$, $\mathfrak{p} = (\rho)$ y el polinomio mínimo de π sobre k es $x^n - \rho$.

b) Si $K = k(\pi)$, donde π es una raíz de un polinomio de la forma $x^e - \rho$, con ρ entero en k y e un natural no divisible entre p, entonces la extensión K/k es dominadamente ramificada, y será totalmente ramificada si además la multiplicidad de $\mathfrak{p}$ en ρ es prima con e.

DEMOSTRACIÓN: a) Sea $\mathfrak{P} = (\pi)$ y $\mathfrak{p} = (\rho)$. Como la extensión es totalmente ramificada tenemos que $(\rho) = \mathfrak{p} = \mathfrak{P}^n = (\pi^n)$, y por ser dominadamente ramificada se cumple además que $p \nmid e = n$. El teorema anterior nos dice que podemos elegir ρ adecuadamente (multiplicándolo por una unidad) de manera que una raíz α del polinomio $x^n - \rho$ esté contenida en $k(\pi)$. Pero éste es un polinomio de Eisenstein, luego el teorema 2.40 nos da que α es primo en $k(\alpha) \subset k(\pi) \subset K$ y, comparando los grados, resulta que $K = k(\alpha)$, luego se cumple a) tomando π igual a este α que hemos obtenido.

b) En primer lugar observamos que $\overline{K} = \overline{k}([\pi])$, y $[\pi]$ es separable sobre $\overline{k}$, pues el polinomio $x^e - [\rho]$ es primo con su derivada. Así pues, la extensión $\overline{K}/\overline{k}$ es separable.

Sea $f(x) = x^e - \rho$. Sea $\rho = \epsilon\tau^r$, donde ϵ es una unidad en k y τ es un primo. Fijemos una raíz e-ésima primitiva de la unidad ζ y raíces e-ésimas de ϵ y τ, a las que llamaremos $\epsilon^{1/e}$ y $\tau^{1/e}$. Entonces $\epsilon^{1/e}\tau^{r/e}$ es una raíz de $f(x)$ y dos raíces cualesquiera se diferencian en una potencia de ζ. Por lo tanto $K = k(\pi) \subset k(\zeta, \epsilon^{1/e}, \tau^{1/e})$.

Los polinomios mínimos de ζ y $\epsilon^{1/e}$ dividen respectivamente a $x^e - 1$ y $x^e - \epsilon$, que son primos con sus derivadas (en K y en $\overline{K}$). Podemos aplicar dos veces el teorema 2.34 y concluir que $L = k(\zeta, \epsilon^{1/e})$ es una extensión de k no ramificada. De aquí se sigue que τ sigue siendo primo en L.

Por otra parte, el teorema 2.40 nos da que la extensión $L(\tau^{1/e})/L$ es totalmente ramificada, pues $\tau^{1/e}$ es raíz del polinomio de Eisenstein $x^e - \tau$. Además su grado es e, luego también es dominadamente ramificada.

El índice de ramificación de $L(\tau^{1/e})/k$ es igual a e (pues el de L/k vale 1), y el índice de ramificación de K/k divide a éste, luego es primo con p y por lo tanto K/k es dominadamente ramificada.

Si además la multiplicidad de $\mathfrak{p}$ en ρ (o sea, r) es prima con e, existen enteros racionales s y t tales que $se + tr = 1$. Sea $\beta = \pi^t\tau^s$. Entonces $\beta^e/\tau = \pi^{te}\tau^{se-1} = (\pi^e\tau^{-r})^t$ y, como $\pi^e = \rho = \epsilon\tau^r$ resulta que β^e/τ es una unidad. Deducimos que $v_{\mathfrak{P}}(\tau) = v_{\mathfrak{P}}(\beta^e) = ev_{\mathfrak{P}}(\beta) \geq e$ (observar que de estas igualdades se sigue que $v_{\mathfrak{P}}(\beta) > 0$, pues $v_{\mathfrak{P}}(\tau) > 0$).

Esto implica que $e \leq e(\mathfrak{P}/\mathfrak{p}) \leq |K : k| \leq e$. En consecuencia la extensión es totalmente ramificada. ∎

La ramificación dominada se conserva en los mismos casos que la no ramificación:

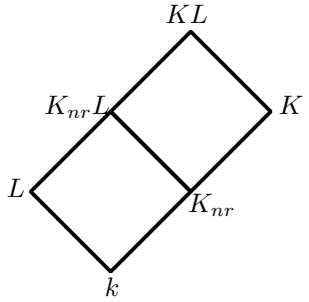
Teorema 2.45 *Sea k un cuerpo métrico discreto completo.*

a) Si $k \subset K \subset L$ es una cadena de extensiones finitas, entonces L/k es dominadamente ramificada si y sólo si L/K y K/k son dominadamente ramificadas.

b) Si K/k y L/k son extensiones finitas y K/k es dominadamente ramificada, entonces KL/L es dominadamente ramificada.

c) Si K/k y L/k son extensiones dominadamente ramificadas entonces KL/k también lo es.

DEMOSTRACIÓN: a) es evidente y c) es consecuencia de a) y b). Para probar b) consideremos el cuerpo K_{nr} definido en el teorema 2.39. La situación es la siguiente:



La extensión K_{nr}/k es no ramificada y por el teorema 2.35 lo mismo le ocurre a la extensión $K_{nr}L/L$. Sabemos que K/K_{nr} es total y dominadamente ramificada y usando el teorema anterior en los dos sentidos concluimos que $KL/K_{nr}L$ también es dominadamente ramificada. Como el índice de ramificación de esta extensión es el mismo que el de KL/K, tenemos b). ∎

Como en el caso de las extensiones no ramificadas, este teorema nos permite construir una máxima extensión con ramificación dominada.

Teorema 2.46 *Sea K/k una extensión de cuerpos métricos discretos completos. Supongamos que $\overline{k}$ tiene característica prima p y que la extensión $\overline{K}/\overline{k}$ es separable. Sea K_d el producto de todos los cuerpos intermedios dominadamente ramificados sobre k. Entonces la extensión K_d/k es dominadamente ramificada y K/K_d es totalmente ramificada y el grado $|K : K_d|$ es potencia de p.*

DEMOSTRACIÓN: El teorema anterior garantiza que la extensión K_d/k es dominadamente ramificada. Claramente $K_{nr} \subset K_d$, luego la extensión K/K_d es totalmente ramificada. Sea e el índice de ramificación de K/k, que es el mismo que el de K/K_{nr}. Sea $e = mp^r$, donde $(m, p) = 1$. Sea $\mathfrak{P}$ el primo de K y $\mathfrak{p}$ el primo de K_{nr}. Entonces $\mathfrak{p} = \mathfrak{P}^e$. De aquí se sigue que si $\mathfrak{P} = (\pi)$ y $\mathfrak{p} = (\rho)$, entonces $|\pi^e| = |\rho|$ y si $\tau = \pi^{p^r}$ podemos aplicar el teorema 2.43 tomando $e = m$

y $\pi = \tau$ (y la extensión K/K_{nr}, que es totalmente ramificada). Concluimos que $K_{nr}(\tau)$ contiene una raíz α del polinomio $x^m - \rho$. Este polinomio es irreducible en $K_{nr}[x]$ por ser un polinomio de Eisenstein. Si llamamos $L = K_{nr}(\alpha)$ el teorema 2.44 nos da que L/K_{nr} es total y dominadamente ramificada, luego el índice de ramificación de L/K_{nr} es el grado de la extensión, o sea, m.

Obviamente L/k es dominadamente ramificada, también con índice de ramificación m. Por lo tanto la extensión K/L tiene índice de ramificación p^r y, como es totalmente ramificada (porque $K_{nr} \subset L$), se cumple $|K : L| = p^r$.

En consecuencia $L = K_d$, pues LK_d/L es dominadamente ramificada y tiene grado potencia de p, lo cual obliga a que $|LK_d : L| = 1$. ∎

2.6 Complementos

Recogemos aquí algunos hechos variados de interés sobre los cuerpos numéricos y sus compleciones. Ninguno de ellos será necesario después

Los divisores primos de los cuerpos numéricos Comenzamos probando que los únicos divisores primos en un cuerpo numérico k son los que de hecho estamos considerando, es decir, los inducidos por los monomorfismos $k \longrightarrow \mathbb{K}_p$ para cada primo racional p (finito o infinito). Esto se prueba fácilmente una vez lo tenemos para $\mathbb{Q}$:

Teorema 2.47 (Teorema de Ostrowski) *Los únicos divisores primos de $\mathbb{Q}$ son los inducidos por los primos de $\mathbb{Z}$ y el divisor ∞ inducido por el valor absoluto usual.*

Demostración: Fijemos un valor absoluto no trivial en $\mathbb{Q}$. Supongamos en primer lugar que existe un número natural a tal que $|a| > 1$. Puesto que, para todo natural n,

$$|n| = |1 + \cdots + 1| \leq |1| + \cdots + |1| = n,$$

se cumple $|a| = a^\alpha$, con $0 < \alpha \leq 1$.

Cada número natural N puede expresarse en base a, es decir, en la forma

$$N = x_0 + x_1 a + \cdots + x_{k-1} a^{k-1},$$

donde cada x_i es un número natural $0 \leq x_i < a$ y $x_{k-1} \neq 0$. De aquí se sigue que $a^{k-1} \leq N < a^k$. Entonces

$$|N| \leq |x_0| + |x_1|\,|a| + \cdots + |x_{k-1}|\,|a|^{k-1} \leq (a-1)(1 + a^\alpha + \cdots + a^{(k-1)\alpha})$$

$$= (a-1)\,\frac{a^{k\alpha} - 1}{a^\alpha - 1} < (a-1)\,\frac{a^{k\alpha}}{a^\alpha - 1} = \frac{(a-1)a^\alpha}{a^\alpha - 1}\,a^{(k-1)\alpha} \leq KN^\alpha,$$

donde K es una constante que no depende de N. Cambiando N por N^m obtenemos $|N|^m \leq KN^{m\alpha}$, luego $|N| \leq \sqrt[m]{K}\,N^\alpha$, y haciendo tender m a infinito llegamos a que $|N| \leq N^\alpha$, para todo natural N.

Ahora tomamos $N = a^k - b$, donde $0 < b \leq a^k - a^{k-1}$. Por la desigualdad triangular

$$|N| \geq |a^k| - |b| = a^{\alpha k} - |b| \geq a^{\alpha k} - b^\alpha \geq a^{\alpha k} - (a^k - a^{k-1})^\alpha$$

$$= \left(1 - \left(1 - \frac{1}{a}\right)^\alpha\right) a^{\alpha k} = K_1 a^{\alpha k} > K_1 N^\alpha,$$

donde la constante K_1 no depende de N.

De nuevo cambiamos N por N^m, lo que nos da $|N|^m > K_1 N^{m\alpha}$, y de aquí $|N| > \sqrt[n]{K_1}\, N^\alpha$. Haciendo tender m a infinito queda $|N| \geq N^\alpha$.

En resumen, hemos probado que $|N| = N^\alpha$ para todo número natural N, y es claro que de aquí se sigue que $|r| = |r|_\infty^\alpha$ para todo $r \in \mathbb{Q}$, luego el valor absoluto dado induce el primo ∞.

Supongamos ahora que $|a| \leq 1$ para todo número natural a. No puede ser que $|a| = 1$ para todo número natural, pues en tal caso el valor absoluto sería trivial. Claramente ha de haber un primo p tal que $|p| < 1$. Veamos que es único. Si $|q| < 1$ para otro primo q, entonces podemos tomar exponentes k y l tales que $|p^k| < 1/2$ y $|q^l| < 1/2$. Existen enteros u y v tales que $up^k + vq^l = 1$, y esto nos lleva a una contradicción:

$$1 = |1| = |up^k + vq^l| \leq |u|\,|p^k| + |v|\,|q^l| < \frac{1}{2} + \frac{1}{2} < 1.$$

Así pues, $|q| = 1$ para todo primo $q \neq p$. Sea $|p| = \rho < 1$. Todo número racional no nulo puede expresarse como $r = p^m(a/b)$, donde $m \in \mathbb{Z}$ y a y b son números naturales primos con p. Claramente entonces $|r| = \rho^m$, luego el valor absoluto dado es el inducido por p. ∎

En la prueba del teorema se ve que los únicos valores absolutos arquimedianos de $\mathbb{Q}$ son los de la forma $|\ |_\infty^\alpha$, para $0 < \alpha \leq 1$. De aquí se sigue que cada valor absoluto arquimediano en $\mathbb{R}$ ha de ser también de esta forma, luego cada valor absoluto arquimediano de $\mathbb{R}$ se extiende a un valor absoluto en $\mathbb{C}$ equivalente al usual (usando [7.3]).

Teorema 2.48 *Los únicos divisores en un cuerpo numérico $k$son los inducidos por los monomorfismos $k \longrightarrow \mathbb{K}_p$, donde p es un primo en $\mathbb{Q}$.*

Demostración: Fijemos un valor absoluto no trivial en k y veamos que su restricción a $\mathbb{Q}$ no puede ser trivial. En efecto, si lo fuera tomamos una $\mathbb{Q}$-base de k, digamos $v_1, \ldots, v_n$, y entonces todo $x \in k$ se expresa en la forma $x = r_1 v_1 + \cdots + r_n v_n$, con lo que

$$|x| \leq |x_1|\,|v_1| + \cdots + |x_n|\,|v_n| \leq |v_1| + \cdots + |v_n|,$$

pero un valor absoluto no trivial no puede estar acotado (existe un $x \in k$ con $|x| > 1$ y sus potencias tienen valor absoluto arbitrariamente grande).

Según el teorema anterior, la restricción a $\mathbb{Q}$ del valor absoluto dado es el inducido por un primo p de $\mathbb{Q}$ (finito o infinito).

Sea $\overline{k}$ la compleción de k respecto al valor absoluto dado. Entonces la clausura de $\mathbb{Q}$ en $\overline{k}$ es topológicamente isomorfa a $\mathbb{Q}_p$ y el cuerpo $\mathbb{Q}_p\, k$ es una extensión finita de $\mathbb{Q}_p$, luego es completo por el teorema 2.13. En definitiva, es cerrado y denso en $\overline{k}$, luego $\overline{k} = \mathbb{Q}_p\, k$. Podemos tomar una clausura algebraica $\mathbb{K}_p$ de $\mathbb{Q}_p$ que contenga a $\overline{k}$, y entonces la inclusión $k \longrightarrow \mathbb{K}_p$ induce el valor absoluto de partida. ∎

Cuerpos completos arquimedianos Ahora probamos que los únicos cuerpos métricos completos arquimedianos son $\mathbb{R}$ y $\mathbb{C}$ con sus divisores usuales.

En efecto, sea K un cuerpo arquimediano completo. Fijado un valor absoluto en K, su restricción a $\mathbb{Q}$ ha de corresponder al único divisor primo arquimediano de $\mathbb{Q}$, es decir, a la clase de equivalencia del valor absoluto usual. Por lo tanto, la clausura de $\mathbb{Q}$ en K es un cuerpo isomorfo a $\mathbb{R}$ (al que llamaremos $\mathbb{R}$) y la restricción a $\mathbb{R}$ del valor absoluto de K es equivalente al valor absoluto usual en $\mathbb{R}$. Basta probar que la extensión $K/\mathbb{R}$ es algebraica, pues entonces K será $\mathbb{R}$ o $\mathbb{C}$, y su valor absoluto será equivalente al usual por el teorema 2.12.

Fijemos $\xi \in K$ y veamos que es algebraico sobre $\mathbb{R}$. Para cada $z \in \mathbb{C}$, los números $z + \overline{z}$ y $z\overline{z}$ son reales, luego podemos definir la aplicación $f : \mathbb{C} \longrightarrow \mathbb{R}$ dada por $f(z) = |\xi^2 - (z + \overline{z})\xi + z\overline{z}|$, donde el valor absoluto es el de K.

La aplicación f es continua, pues

$$|f(z_1) - f(z_2)| \leq |(z_2 + \overline{z}_2) - (z_1 + \overline{z}_1)|\,|\xi| + |z_1\overline{z}_1 - z_2\overline{z}_2|$$

$$\leq |z_2 - z_1|\,|\xi| + |\overline{z}_2 - \overline{z}_1|\,|\xi| + |z_1\overline{z}_1 - z_2\overline{z}_2|,$$

considerando en $\mathbb{C}$ la extensión de la restricción a $\mathbb{R}$ del valor absoluto de K (ver el comentario tras el teorema de Ostrowski).

Por otra parte, $\lim\limits_{z\to\infty} f(z) = +\infty$, pues

$$f(z) \geq |z\overline{z}| - |\xi^2| - |z + \overline{z}|\,|\xi| \geq |z|^2 - |\xi^2| - 2|\xi|\,|z|,$$

(pues la conjugación es una isometría).

Sea $m = \text{ínf}\{f(z) \mid z \in \mathbb{C}\} \geq 0$. El hecho de que f tienda a infinito en infinito implica que m es también el ínfimo de f en un compacto, luego existe un $z \in \mathbb{C}$ tal que $f(z) = m$.

Sea $S = \{z \in \mathbb{C} \mid f(z) = m\}$. Se trata de un compacto no vacío, luego existe un número $z_0 \in S$ tal que $|z_0| \geq |z|$ para todo $z \in S$.

Basta probar que $m = 0$, pues entonces la ecuación $f(z_0) = 0$ probará que ξ es algebraico sobre $\mathbb{R}$. SI m es positivo tomamos $0 < \epsilon < \text{mín}\{m, 1\}$ y consideramos el polinomio

$$g(x) = x^2 - (z_0 + \overline{z}_0)x + z_0\overline{z}_0 + \epsilon \in \mathbb{R}[x].$$

Sean z_1, z_2 sus raíces en $\mathbb{C}$. Entonces $z_1 z_2 = z_0\overline{z}_0 + \epsilon$, luego $|z_1| > |z_0|$ o bien $|z_2| > |z_0|$. Supongamos por ejemplo la primera desigualdad. Entonces $z_1 \notin S$.

Tomemos un número natural $n \geq 1$ y definamos

$$G(x) = (x^2 - (z_0 + \overline{z}_0)x + z_0\overline{z}_0)^n - (-\epsilon)^n.$$

Entonces $G(x)$ es un polinomio en $\mathbb{R}[x]$ de grado $2n$. Sean $\beta_1, \ldots, \beta_{2n}$ sus raíces en $\mathbb{C}$. Como $G(z_1) = 0$ podemos suponer que $z_1 = \beta_1$. Se cumple

$$G(x) = \prod_{i=1}^{2n} (x - \beta_i) = \prod_{i=1}^{2n} (x - \overline{\beta}_i),$$

luego

$$G(x)^2 = \prod_{i=1}^{2n} (x - \beta_i)(x - \overline{\beta}_i) = \prod_{i=1}^{2n} \big(x^2 - (\beta_i + \overline{\beta}_i)x + \beta_i \overline{\beta}_i\big).$$

Como todos los factores son polinomios en $\mathbb{R}[x]$ tiene sentido calcular

$$|G(\xi)^2| = \prod_{i=1}^{2n} f(\beta_i) \geq f(z_1)\, m^{2n-1}.$$

Por otra parte

$$|G(\xi)| \leq f(z_0)^n + \epsilon^n = m^n + \epsilon^n.$$

Uniendo ambas desigualdades resulta que $f(z_1)m^{2n-1} \leq (m^n + \epsilon^n)^2$, luego

$$\frac{f(z_1)}{m} \leq \left(1 + \left(\frac{\epsilon}{m}\right)^n\right)^2,$$

y haciendo tender n a infinito queda $f(z_1) \leq m$, luego $f(z_1) = m$ y $z_1 \in S$, contradicción. ∎

Capítulo III

Diferentes y discriminantes

Es conocida la utilidad de los discriminantes a la hora de trabajar con cuerpos numéricos concretos, en especial a la hora de calcular sus anillos de enteros. También hemos vislumbrado su significado teórico, principalmente en el caso de los cuerpos cuadráticos. Con los resultados de los capítulos anteriores estamos en condiciones de comprender mucho mejor su papel en la teoría, a la vez que multiplicaremos su utilidad práctica.

Recordemos que el discriminante de un cuerpo numérico es en definitiva el discriminante de una base entera, en el sentido de [2.6], pero si K/k es una extensión de cuerpos numéricos, el anillo de enteros de K no es necesariamente un módulo libre sobre el anillo de enteros de k, es decir, no tenemos necesariamente bases enteras (salvo que k tenga factorización única). Sin embargo, este inconveniente no afecta sustancialmente a la teoría de los discriminantes. Definiremos el discriminante de la extensión como un cierto ideal del cuerpo base k, de modo que si K admite una base entera sobre k, entonces el discriminante será el ideal principal generado por el discriminante de la base.

A menudo será más conveniente trabajar con un concepto muy próximo al de discriminante: el diferente. El diferente de una extensión K/k será un ideal de K, de modo que el discriminante será la norma del diferente.

Antes de todo esto hemos de profundizar en un concepto que tocamos superficialmente al introducir el discriminante: la dualidad que la traza induce en una extensión separable de cuerpos.

3.1 Módulos complementarios

Si K/k es una extensión finita de cuerpos, la aplicación $(\alpha, \beta) \mapsto \mathrm{Tr}(\alpha\beta)$ es una forma bilineal en K. Su matriz en una k-base de K dada, digamos $w_1, \ldots, w_n$, es claramente $\big(\mathrm{Tr}(w_i w_j)\big)$. En la prueba del teorema 1.19 vimos que si la extensión K/k es separable entonces esta matriz tiene determinante no nulo, por lo que la forma bilineal es regular e induce un isomorfismo entre K y su k-espacio vectorial dual (el espacio de las aplicaciones lineales de K en k). En general, cada base de un espacio vectorial de dimensión finita tiene asociada

una base en su espacio dual. En nuestro caso podemos considerar su antiimagen por el isomorfismo inducido por la traza y obtenemos así otra k-base de K, a la que llamamos base dual de la base de partida.

El teorema siguiente recoge los hechos que vamos a necesitar en la práctica sobre todo lo dicho. Notemos que está probado casi en su totalidad en la demostración del teorema 1.19.

Teorema 3.1 *Sea K/k una extensión de cuerpos finita separable, consideremos la traza $\mathrm{Tr} : K \longrightarrow k$ y sea $w_1, \ldots, w_n$ una k-base de K. Entonces*

a) La matriz $\big(\mathrm{Tr}(w_i w_j)\big)$ tiene determinante no nulo.

b) Existen unos únicos elementos $z_1, \ldots, z_n$ en K de modo que

$$\mathrm{Tr}(w_i z_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Estos elementos forman una k-base de K a la que llamaremos base dual *de la base dada.*

Demostración: El apartado a) está probado en la demostración del teorema 1.19. También vimos allí la existencia de los elementos $z_1, \ldots, z_n$, y es clara su unicidad, pues las coordenadas de los z_i en la base w_j son la solución de un sistema de n ecuaciones lineales con n incógnitas cuya matriz de coeficientes es la del apartado a). Esto mismo implica que $z_1, \ldots, z_n$ forman una k-base de K. ∎

Introducimos ahora un concepto muy relacionado con las bases duales, tal y como veremos enseguida:

Definición 3.2 Sea E/D una extensión separable de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes. Sea $\mathrm{Tr} : K \longrightarrow k$ la traza de la extensión. Si L es un subgrupo aditivo de K definimos el *complementario* de L como el conjunto L' de todos los elementos $\alpha \in K$ tales que $\mathrm{Tr}[\alpha L] \subset D$, o sea, $\mathrm{Tr}(\alpha\beta) \in D$ para todo $\beta \in L$.

El teorema siguiente recoge las propiedades básicas de los conjuntos complementarios. El apartado d) describe los módulos complementarios en el único caso en que nos van a interesar.

Teorema 3.3 *Sea E/D una extensión separable de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes asociados. Sean L y M subgrupos aditivos de K. Entonces*

a) L' es un subgrupo aditivo de K.

b) Si L es un D-módulo (o un E-módulo) entonces L' también lo es.

c) Si $L \subset M$ entonces $M' \subset L'$.

d) Si $w_1, \dots, w_n$ es una k-base de K y $w'_1, \dots, w'_n$ es su base dual, entonces el módulo complementario de $L = \langle w_1, \dots, w_n \rangle_D$ es $L' = \langle w'_1, \dots, w'_n \rangle_D$.

e) Si L es un ideal fraccional de K entonces L' también lo es.

DEMOSTRACIÓN: a) Si $\alpha_1, \alpha_2 \in L'$ entonces

$$\mathrm{Tr}\big((\alpha_1 - \alpha_2)\beta\big) = \mathrm{Tr}(\alpha_1\beta) - \mathrm{Tr}(\alpha_2\beta) \in D$$

para todo $\beta \in L$.

b) Si $\alpha \in L'$ y $d \in D$ (o $d \in E$) entonces $d\beta \in L$ para todo $\beta \in L$, luego $\mathrm{Tr}(d\alpha\beta) = \mathrm{Tr}\big(\alpha(d\beta)\big) \in D$ para todo $\beta \in L$.

c) es evidente.

d) Sea $\alpha \in L'$. Entonces $\alpha = a_1 w'_1 + \cdots a_n w'_n$ para ciertos elementos $a_i \in K$. Pero sucede que $a_i = \mathrm{Tr}(\alpha w_i) \in D$, luego $\alpha \in \langle w'_1, \dots, w'_n \rangle_D$.

Recíprocamente, si $\alpha = a_1 w'_1 + \cdots + a_n w'_n$, para ciertos elementos $a_i \in D$, entonces $\mathrm{Tr}(\alpha w_i) = a_i \in D$, y por linealidad es claro que $\mathrm{Tr}(\alpha\beta) \in D$ para todo $\beta \in L$, luego $\alpha \in L'$.

e) Si L es un ideal fraccional de K, por b) sabemos que L' es un E-módulo. Existe un $\alpha \in K$ no nulo tal que $\alpha L \subset E$, luego $\mathrm{Tr}[\alpha L] \subset \mathrm{Tr}[E] \subset D$, luego $\alpha \in L'$ que, por consiguiente, es no nulo.

Falta probar que existe un $\alpha \in K$ no nulo tal que $\alpha L' \subset E$. En primer lugar observamos que L contiene una k-base de K. En efecto, por 1.18 existe una k-base de K formada por elementos de E. Si la multiplicamos por cualquier elemento no nulo de L obtenemos la base buscada. Sea, pues, $w_1, \dots, w_n$ una k-base de K contenida en L. Entonces $\langle w_1, \dots, w_n \rangle_D \subset L$ y, por c) y d), tenemos que $L' \subset \langle w'_1, \dots, w'_n \rangle_D$.

Como D es noetheriano, el D-módulo $\langle w'_1, \dots, w'_n \rangle_D$ también lo es, luego L' es un D-módulo finitamente generado. Digamos $L' = \langle x_1, \dots, x_r \rangle_D$. Aplicando el teorema 1.18 encontramos un elemento no nulo $\alpha \in D$ tal que $\alpha x_i \in E$ para todo i, con lo que $\alpha L' \subset E$, como había que probar. ∎

En realidad sólo nos van a interesar los complementarios de los ideales fraccionales. Para ellos probamos, en primer lugar, que conmutan con las localizaciones:

Teorema 3.4 *Sea E/D una extensión separable de dominios de Dedekind, sea S un subconjunto multiplicativo de D y sea $\mathfrak{a}$ un ideal fraccional de E. Entonces $S^{-1}(\mathfrak{a}') = (S^{-1}\mathfrak{a})'$.*

DEMOSTRACIÓN: Notar que al localizar los cuerpos de cocientes no varían, luego la traza de la extensión $S^{-1}E/S^{-1}D$ es la misma que la de la E/D.

Si $\alpha/s \in S^{-1}(\mathfrak{a}')$ y $a/t \in S^{-1}\mathfrak{a}$, entonces $\mathrm{Tr}(\alpha a/st) = \mathrm{Tr}(\alpha a)/st \in S^{-1}D$, luego tenemos la inclusión $S^{-1}(\mathfrak{a}') \subset (S^{-1}\mathfrak{a})'$.

Por definición de ideal fraccional existe un $a \in E$ no nulo tal que $a\mathfrak{a} \subset E$. Puesto que E es un D-módulo finitamente generado y D es noetheriano, también

$a\mathfrak{a}$ es finitamente generado, y de aquí que lo mismo le sucede a $\mathfrak{a}$. Sea, pues, $\mathfrak{a} = \langle a_1, \ldots, a_n\rangle_D$. Si $\alpha \in (S^{-1}\mathfrak{a})'$ entonces se cumple $\mathrm{Tr}(\alpha a_i) \in S^{-1}D$ para $i = 1, \ldots, n$. Digamos $\mathrm{Tr}(\alpha a_i) = d_i/s_i$. Sea $s = s_1 \cdots s_n$.

Entonces $\mathrm{Tr}(s\alpha a_i) = s\,\mathrm{Tr}(\alpha a_i) \in D$, de donde por linealidad se cumple $\mathrm{Tr}(s\alpha\beta) \in D$ para todo $\beta \in \mathfrak{a}$. Esto significa que $s\alpha \in \mathfrak{a}'$ y así $\alpha \in S^{-1}(\mathfrak{a}')$. ∎

En las condiciones del teorema anterior, si $\mathfrak{p}$ es un primo en D, sus divisores primos en E son $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ y $S = D \setminus \mathfrak{p}$, el teorema 1.33 nos permite identificar a $\mathfrak{p}$ con el único primo de $D_\mathfrak{p}$ y a $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ con los únicos primos de $E_\mathfrak{p}$. Lo que afirma entonces el teorema es que el complementario local $\mathfrak{a}'_\mathfrak{p}$ está formado por las potencias de $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ que dividen al complementario global $\mathfrak{a}'$. Si identificamos cada $\mathfrak{a}_\mathfrak{p}$ con un ideal fraccional de E tenemos

$$\mathfrak{a}' = \prod_\mathfrak{p} \mathfrak{a}'_\mathfrak{p},$$

donde $\mathfrak{p}$ recorre los primos de D. De esta fórmula se desprende que todos los factores son iguales a 1 salvo a lo sumo un número finito de ellos.

Veamos un último resultado sobre complementarios de ideales fracionales:

Teorema 3.5 *Sea E/D una extensión finita de dominios de Dedekind y sea $\mathfrak{a}$ un ideal fraccional de E. Entonces $\mathfrak{a}' = E'\mathfrak{a}^{-1}$.*

Demostración: Claramente $\mathrm{Tr}[E'\mathfrak{a}^{-1}\mathfrak{a}] \subset \mathrm{Tr}[E'E] \subset D$, de donde se sigue que $E'\mathfrak{a}^{-1} \subset \mathfrak{a}'$. Así mismo $\mathrm{Tr}[\mathfrak{a}'\mathfrak{a}E] = \mathrm{Tr}[\mathfrak{a}'\mathfrak{a}] \subset D$, con lo que $\mathfrak{a}'\mathfrak{a} \subset E'$, y de aquí que $\mathfrak{a}' \subset E'\mathfrak{a}^{-1}$. ∎

Por lo tanto el cálculo de ideales complementarios se reduce al cálculo de E'. Llegamos así al concepto de diferente de una extensión.

3.2 Diferentes

Definición 3.6 Sea E/D una extensión separable de dominios de Dedekind. Llamaremos *diferente* de la extensión a $\mathfrak{D} = (E')^{-1}$. Por la definición de complementario es obvio que $E \subset E'$, de donde $\mathfrak{D} = (E')^{-1} \subset E^{-1} = E$, es decir, $\mathfrak{D}$ es un ideal de E.

En estos términos el teorema 3.5 afirma que si $\mathfrak{a}$ es un ideal fraccional de E entonces $\mathfrak{a}' = (\mathfrak{D}\mathfrak{a})^{-1}$. Así mismo, del teorema 3.4 se sigue que si $\mathfrak{p}$ es un ideal primo de D, entonces la localización $\mathfrak{D}_\mathfrak{p}$ del diferente es el diferente de la extensión local $E_\mathfrak{p}/D_\mathfrak{p}$. Por consiguiente podemos factorizar

$$\mathfrak{D} = \prod_\mathfrak{p} \mathfrak{D}_\mathfrak{p},$$

donde $\mathfrak{p}$ recorre los primos de D. En particular, todos los diferentes locales son unitarios salvo a lo sumo una cantidad finita de ellos.

El diferente de una extensión E/D es muy fácil de calcular cuando E es una extensión simple de D, es decir, cuando E es de la forma $D[\alpha]$. Para verlo necesitamos el resultado siguiente:

Teorema 3.7 *Sea $K = k(\alpha)$ una extensión de cuerpos separable de grado n. Sea $f \in k[x]$ el polinomio mínimo de α. Sea*

$$\frac{f(x)}{x-\alpha} = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}.$$

Entonces la base dual de $1, \alpha, \ldots, \alpha^{n-1}$ es

$$\frac{b_0}{f'(\alpha)}, \cdots, \frac{b_{n-1}}{f'(\alpha)}.$$

DEMOSTRACIÓN: Sean $\alpha_1, \ldots, \alpha_n$ las raíces de f. Si $0 \le r \le n-1$ se cumple que

$$\sum_{i=1}^{n} \frac{f(x)}{x-\alpha_i}\,\frac{\alpha_i^r}{f'(\alpha_i)} = x^r.$$

En efecto, la diferencia entre ambos miembros es un polinomio de grado menor o igual que $n-1$ y tiene por raíces a todos los α_i, luego es idénticamente nulo. Los sumandos del miembro izquierdo son todos los conjugados del polinomio

$$\frac{f(x)}{x-\alpha}\,\frac{\alpha^r}{f'(\alpha)},$$

luego la suma tiene por coeficientes a las trazas de los coeficientes de este último polinomio.

El coeficiente i-ésimo es $f'(\alpha)^{-1}b_i\alpha^r$, luego hemos obtenido que

$$\mathrm{Tr}\left(\frac{b_i}{f'(\alpha)}\,\alpha^r\right) = \begin{cases} 1 & \text{si } i = r, \\ 0 & \text{si } i \neq r. \end{cases}$$

∎

Teorema 3.8 *Sea E/D una extensión separable de dominios de Dedekind tal que existe un $\alpha \in E$ de manera que $E = D[\alpha]$. Sea $f(x)$ el polinomio mínimo de α. Entonces el diferente de la extensión es $\mathfrak{D} = (f'(\alpha))$.*

DEMOSTRACIÓN: Hay que probar que $E' = E/f'(\alpha)$. Por hipótesis $E = \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle_D$ y, por 3.3 y el teorema anterior (con la notación de éste último),

$$E' = \left\langle \frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)} \right\rangle_D.$$

Ahora bien, si $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in D[x]$, entonces la igualdad

$$f(x) = (x-\alpha)(b_0 + b_1 x + \cdots + b_{n-1}x^{n-1})$$

nos da las relaciones

$$a_i = b_{i-1} - \alpha b_i, \quad i = 1, \ldots, n-1, \qquad b_{n-1} = 1.$$

Por recurrencia resulta

$$\begin{aligned} b_{n-1} &= 1 \\ b_{n-2} &= a_{n-1} + \alpha \\ b_{n-3} &= a_{n-1} + a_{n-2}\alpha + a_{n-1}\alpha^2 \\ \cdots &\quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ b_0 &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n \end{aligned}$$

De aquí se sigue que

$$E' = \frac{1}{f'(\alpha)}\,\langle b_0, b_1, \ldots, b_{n-1}\rangle_D = \frac{1}{f'(\alpha)}\,\langle 1, \alpha, \ldots, \alpha^{n-1}\rangle_D = \frac{1}{f'(\alpha)}\,E.$$

∎

Este teorema nos permite calcular los diferentes de las extensiones más sencillas, como son los cuerpos cuadráticos y ciclotómicos (sobre $\mathbb{Q}$). Por ejemplo, el diferente de $\mathbb{Z}\big[\sqrt{7}\,\big]/\mathbb{Z}$ es $\mathfrak{D} = (2\sqrt{7}\,)$.

Un hecho muy importante es la transitividad de los diferentes:

Teorema 3.9 *Sea $D \subset E \subset F$ una cadena de extensiones separables de dominios de Dedekind. Entonces $\mathfrak{D}_{F/D} = \mathfrak{D}_{F/E}\mathfrak{D}_{E/D}$ (considerándolos a todos como ideales en F).*

Demostración: Hay que probar que $F'_{F/D} = F'_{F/E}E'_{E/D}$. Sean $k \subset K \subset L$ los cuerpos de cocientes correspondientes. Entonces

$$\begin{aligned} \mathrm{Tr}_k^L[F'_{F/E}E'_{E/D}F] &= \mathrm{Tr}_k^K\big[\mathrm{Tr}_K^L[F'_{F/E}E'_{E/D}F]\big] \\ &= \mathrm{Tr}_k^K\big[E'_{E/D}\,\mathrm{Tr}_K^L[F'_{F/E}F]\big] \subset \mathrm{Tr}_k^K[E'_{E/D}E] \subset D, \end{aligned}$$

luego $F'_{F/E}E'_{E/D} \subset F'_{F/D}$.

Sea $\alpha \in F'_{F/D}$. Entonces $\mathrm{Tr}_k^L[\alpha F] \subset D$, pero como $EF = F$ resulta que

$$\mathrm{Tr}_k^L[\alpha F] = \mathrm{Tr}_k^K\big[\mathrm{Tr}_K^L[\alpha F]\big] = \mathrm{Tr}_k^K\big[\mathrm{Tr}_K^L[\alpha EF]\big] = \mathrm{Tr}_k^K\big[E\,\mathrm{Tr}_K^L[\alpha F]\big] \subset D,$$

luego $\mathrm{Tr}_K^L[\alpha F] \subset E'_{E/D}$ y, en consecuencia, $(E'_{E/D})^{-1}\,\mathrm{Tr}_K^L[\alpha F] \subset E$. Como $(E'_{E/D})^{-1} \subset K$, esto equivale a que $\mathrm{Tr}_K^L[\alpha(E'_{E/D})^{-1}F] \subset E$, luego tenemos que $\alpha(E'_{E/D})^{-1} \subset F'_{F/E}$, y así concluimos que $\alpha \in F'_{F/E}E'_{E/D}$. ∎

Veamos ahora que los diferentes también se comportan consistentemente con las compleciones.

Teorema 3.10 *Sea K/k una extensión de cuerpos numéricos y sea E/D la extensión de sus anillos de enteros. Sea $\mathfrak{p}$ un primo en D y sea $\mathfrak{P}$ un primo en E que divida a $\mathfrak{p}$. Sea $K_\mathfrak{P}/k_\mathfrak{p}$ la extensión de las compleciones y $E_\mathfrak{P}/D_\mathfrak{p}$ la extensión de enteros correspondiente. Entonces el diferente local $\mathfrak{D}_\mathfrak{P} = \mathfrak{D}_{E_\mathfrak{P}/D_\mathfrak{p}}$*

es la mayor potencia de $\mathfrak{P}$ que divide al diferente global $\mathfrak{D} = \mathfrak{D}_{E/D}$. Consecuentemente

$$\mathfrak{D} = \prod_{\mathfrak{P}} \mathfrak{D}_{\mathfrak{P}},$$

donde $\mathfrak{P}$ recorre los primos de E.

DEMOSTRACIÓN: Sean $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ los primos de E que dividen a $\mathfrak{p}$. Supongamos por ejemplo que $\mathfrak{P} = \mathfrak{P}_1$. Sea $\mathrm{Tr} : K \longrightarrow k$ la traza de la extensión K/k y sean $\mathrm{Tr}_i : K_{\mathfrak{P}_i} \longrightarrow k_{\mathfrak{p}}$ las trazas locales.

Sea $S = D \setminus \mathfrak{p}$. Claramente $S^{-1}E \subset E_{\mathfrak{P}}$. Vamos a probar que $(S^{-1}E)'$ es denso en $(E_{\mathfrak{P}})'$ (el primer complementario respecto a la extensión $S^{-1}E/S^{-1}D$, el segundo respecto a $E_{\mathfrak{P}}/D_{\mathfrak{p}}$).

En primer lugar probamos que $(S^{-1}E)' \subset (E_{\mathfrak{P}})'$. Sea $x \in (S^{-1}E)'$ y sea $y \in E_{\mathfrak{P}}$. Hemos de comprobar que $\mathrm{Tr}_1(xy) \in D_{\mathfrak{p}}$, o sea, que $|\,\mathrm{Tr}_1(xy)| \leq 1$.

Por densidad existe un elemento de K arbitrariamente próximo a y respecto al valor absoluto de $\mathfrak{P}_1$, y aplicándole el teorema de aproximación obtenemos un elemento $\alpha \in K$ arbitrariamente próximo a y respecto a $\mathfrak{P}_1$ y arbitrariamente próximo a 0 respecto a los otros primos.

En particular, puesto que $|y|_{\mathfrak{P}_1} \leq 1$, podemos exigir que $|\alpha|_{\mathfrak{P}_i} \leq 1$ para $i = 1, \dots, r$, con lo que $\alpha \in S^{-1}E$ (pues α se expresa como una fracción de modo que los primos de $S^{-1}E$ dividen al numerador con multiplicidad mayor o igual que al denominador y, puesto que $S^{-1}E$ tiene factorización única, podemos simplificarlos hasta obtener un elemento de $S^{-1}E$). Por consiguiente tenemos que $\mathrm{Tr}(x\alpha) \in S^{-1}D \subset D_{\mathfrak{p}}$.

Por otro lado, las trazas Tr_i son continuas, luego tomando aproximaciones adecuadas podemos exigir que $|\,\mathrm{Tr}_1(xy) - \mathrm{Tr}_1(x\alpha)| \leq 1$ y $|\,\mathrm{Tr}_i(x\alpha)| \leq 1$ para $i = 2, \dots, r$. Ahora aplicamos la relación (2.2):

$$\mathrm{Tr}(x\alpha) = \mathrm{Tr}_1(x\alpha) + \sum_{i=2}^{r} \mathrm{Tr}_i(x\alpha),$$

y vemos que tanto el miembro izquierdo como los términos del sumatorio están en $D_{\mathfrak{p}}$, luego también $\mathrm{Tr}_1(x\alpha) \in D_{\mathfrak{p}}$, es decir, $|\,\mathrm{Tr}_1(x\alpha)| \leq 1$ y por consiguiente $|\,\mathrm{Tr}_1(xy)| \leq 1$, como había que probar.

Ahora tomemos un $x \in (E_{\mathfrak{P}})'$ y vamos a encontrarle elementos arbitrariamente próximos en $(S^{-1}E)'$. Como K es denso en $K_{\mathfrak{P}}$ podemos encontrar un elemento de K arbitrariamente próximo a x y, aplicando a éste el teorema de aproximación, llegamos a un $\alpha \in K$ arbitrariamente próximo a x respecto a $\mathfrak{P}_1$ y arbitrariamente próximo a 0 respecto a los demás valores absolutos.

Veamos que $\alpha \in (S^{-1}E)'$. Para ello tomamos $y \in S^{-1}E$ y probamos que $\mathrm{Tr}(\alpha y) \in S^{-1}D$, es decir, que $|\,\mathrm{Tr}(\alpha y)| \leq 1$. Sabemos que $|\,\mathrm{Tr}_1(xy)| \leq 1$.

Con aproximaciones adecuadas podemos exigir que $|\,\mathrm{Tr}_1(xy) - \mathrm{Tr}_1(\alpha y)| \leq 1$ y $|\,\mathrm{Tr}_i(\alpha y)| \leq 1$ para $i = 2, \dots, r$ (y, de hecho, para $i = 1$ también).

La relación entre las trazas nos da ahora que $|\,\mathrm{Tr}(\alpha y)| \leq 1$, como queríamos probar. No obstante esto no justifica que $\alpha \in (S^{-1}E)'$, porque en realidad la

elección de α que hemos hecho para que se cumpla $\mathrm{Tr}_1(\alpha y) \in S^{-1}D$ depende de y. Ahora bien, podemos encontrar un mismo α que haga $\mathrm{Tr}_1(\alpha y) \in S^{-1}D$ para un conjunto finito fijo de elementos $y \in S^{-1}E$, y como $S^{-1}E$ es un $S^{-1}D$-módulo finitamente generado, basta asegurarlo para los elementos de un generador.

Tenemos, pues, que $(S^{-1}E)'$ es denso en $(E_{\mathfrak{P}})'$. Por otra parte es claro que $S^{-1}E$ es denso en $E_{\mathfrak{P}}$ (pues $E \subset S^{-1}E$ es denso en $E_{\mathfrak{P}}$).

El anillo $S^{-1}E$ es un dominio de Dedekind con un número finito de primos, luego es un dominio de ideales principales. En particular el diferente de la extensión $S^{-1}E/S^{-1}D$ será de la forma $\mathfrak{D}_{\mathfrak{p}} = (\alpha) = \alpha S^{-1}E$, luego $(S^{-1}E)' = \alpha^{-1}S^{-1}E$. Tomando clausuras queda $(E_{\mathfrak{P}})' = \alpha^{-1}E_{\mathfrak{P}} = (\alpha)^{-1}$, de donde $\mathfrak{D}_{\mathfrak{P}} = (\alpha) = \mathfrak{P}^n$, donde $n = v_{\mathfrak{P}}(\alpha)$ es el exponente de $\mathfrak{P}$ en α, o sea, en $\mathfrak{D}_{\mathfrak{p}}$, y por el teorema anterior también en el diferente global $\mathfrak{D}$. ∎

Como consecuencia, si K/k es una extensión de cuerpos numéricos, E/D es la extensión de sus anillos de enteros, $\mathfrak{p}$ es un primo en D, $\mathfrak{D}_{\mathfrak{p}}$ es el diferente de la extensión $S^{-1}E/S^{-1}D$ (donde $S = D \setminus \mathfrak{p}$) y para cada primo $\mathfrak{P}$ que divida a $\mathfrak{p}$ en E llamamos $\mathfrak{D}_{\mathfrak{P}}$ al diferente de la extensión de compleciones $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, los teoremas anteriores prueban que

$$\mathfrak{D}_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{D}_{\mathfrak{P}}.$$

Así pues, una forma de calcular diferentes es calcular los diferentes locales. Una de las razones por las que este planteamiento resulta ventajoso es que los diferentes locales siempre pueden ser calculados mediante el teorema 3.8. Para demostrarlo veremos primero un resultado técnico.

Teorema 3.11 *Sea E/D una extensión finita de dominios de Dedekind. Supongamos que D tiene un único primo $\mathfrak{p}$ y que E tiene un único primo $\mathfrak{P}$. Sea $\alpha \in E$ tal que $E/\mathfrak{P} = (D/\mathfrak{p})[\alpha]$ y sea $\pi \in E$ tal que $\mathfrak{P} = (\pi)$. Entonces $E = D[\alpha, \pi]$.*

Demostración: Llamemos $F = D[\alpha, \pi]$. Basta probar que $\mathfrak{p}E + F = E$, pues entonces, considerando a E y F como D-módulos, $\mathfrak{p}(E/F) = E/F$, y el teorema 1.27 nos da que $E/F = 0$, o sea, $E = F$.

Pero $\mathfrak{p}E$ es simplemente $\mathfrak{p}$ visto como ideal en E, es decir, $\mathfrak{p}E = \mathfrak{P}^e$ para cierto natural e. Lo que hay que probar es que todo elemento de E es congruente módulo $\mathfrak{P}^e$ con uno de F. Tenemos

$$\mathfrak{P}^e \subset \mathfrak{P}^{e-1} \subset \cdots \subset \mathfrak{P}^2 \subset \mathfrak{P} \subset E.$$

Es claro que la aplicación $f : E/\mathfrak{P} \longrightarrow \mathfrak{P}^i/\mathfrak{P}^{i+1}$ definida por $f([u]) = [\pi^i u]$ es un isomorfismo de $D/\mathfrak{p}$-espacios vectoriales. Una base de $E/\mathfrak{P}$ la forman las clases de los elementos $1, \alpha, \ldots, \alpha^{f-1}$, luego una base de $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ es $\pi^i\alpha^j$, para $j = 0, \ldots, f-1$.

Es claro que la unión de estas bases, es decir, el conjunto de elementos de la forma $\pi^i\alpha^j$, para $i = 0, \ldots, e-1$, $j = 0, \ldots, f-1$, forma un generador de $E/\mathfrak{P}^e$ como $D/\mathfrak{p}$-espacio vectorial. De aquí se sigue inmediatamente lo buscado. ∎

Teorema 3.12 *Sea E/D una extensión de dominios de Dedekind. Supongamos que E tiene un único primo $\mathfrak{P}$ y que D tiene un único primo $\mathfrak{p}$ de modo que $E/\mathfrak{P}$ sea una extensión separable de $D/\mathfrak{p}$. Entonces existe un $\alpha \in E$ tal que $E = D[\alpha]$ y cualquier β suficientemente próximo a α cumple igualmente $E = D[\beta]$.*

DEMOSTRACIÓN: Sea $E/\mathfrak{P} = (D/\mathfrak{p})[\gamma]$. Sea $f(x) \in D[x]$ un polinomio mónico tal que su imagen en $(D/\mathfrak{p})[x]$ sea el polinomio mínimo de $[\gamma]$. Sea $\mathfrak{P} = (\rho)$.

Los dos primeros términos del desarrollo de Taylor de f alrededor de γ tienen coeficientes enteros, luego el resto es un polinomio con coeficientes enteros y divisible entre $(x-\gamma)^2$. Evaluando en $\gamma + \rho$ queda

$$f(\gamma + \rho) \equiv f(\gamma) + f'(\gamma)\rho \pmod{\mathfrak{P}^2}.$$

Como γ es separable (mód $\mathfrak{P}$) tenemos $f'(\gamma) \not\equiv 0 \pmod{\mathfrak{P}}$, por lo que $f'(\gamma)\rho \not\equiv 0 \pmod{\mathfrak{P}^2}$. Esto significa que o bien $f(\gamma+\rho)$ o bien $f(\gamma)$ no es congruente con 0 (mód $\mathfrak{P}^2$). Tomamos $\alpha = \gamma + \rho$ o $\alpha = \gamma$ de modo que $\pi = f(\alpha) \not\equiv 0 \pmod{\mathfrak{P}^2}$.

El cualquier caso tenemos $\alpha \equiv \gamma \pmod{\mathfrak{P}}$, luego $E/\mathfrak{P} = (D/\mathfrak{p})[\alpha]$ y así mismo $\pi \equiv f(\gamma) \equiv 0 \pmod{\mathfrak{P}}$, luego $\mathfrak{P} = (\pi)$. Además $\pi = f(\alpha) \in D[\alpha]$. Por el teorema anterior $E = D[\alpha, \pi] = D[\alpha]$.

La última afirmación de sigue de la continuidad de f en α y de que $f(\alpha) = \pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, que es un abierto. Si β está cerca de α se cumplirá que $\pi' = f(\beta)$ estará en $\mathfrak{P} \setminus \mathfrak{P}^2$, luego se cumplirá $\mathfrak{P} = (\pi')$ y podemos concluir igual que con α y π. ∎

Ahora veremos que localizando y aplicando el teorema anterior y el teorema 3.8 podemos generalizar éste último a extensiones cualesquiera.

Teorema 3.13 *Sea K/k una extensión de cuerpos numéricos y sea E/D la extensión de sus anillos de enteros. Entonces el diferente de la extensión es el máximo común divisor de todos los números $f'(\alpha)$, donde $\alpha \in E$ cumple $K = k(\alpha)$ y $f \in D[x]$ es el polinomio mínimo de α.*

DEMOSTRACIÓN: Sea $K = k(\alpha)$ con $\alpha \in E$ y sea f su polinomio mínimo. Entonces $D[\alpha] = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle_D \subset E$. El mismo razonamiento empleado en el teorema 3.8 nos da ahora que $E' \subset E/f'(\alpha)$, luego $(f'(\alpha)) \subset \mathfrak{D}$, es decir, $\mathfrak{D} \mid f'(\alpha)$.

Para demostrar que $\mathfrak{D}$ es el máximo común divisor de todos estos elementos basta probar que para todo primo $\mathfrak{P}$ existe un α tal que el orden de multiplicidad de $\mathfrak{P}$ en $\mathfrak{D}$ es el mismo que en $f'(\alpha)$.

Sea $\mathfrak{p}$ el primo en D divisible entre $\mathfrak{P}$. Tomemos una clausura algebraica $\mathbb{K}_\mathfrak{p}$ de $k_\mathfrak{p}$ que contenga a $K_\mathfrak{P}$. De este modo, el valor absoluto de $\mathfrak{P}$ está inducido por la identidad de K en $\mathbb{K}_\mathfrak{p}$.

Por el teorema anterior existe un $\beta \in E$ tal que $E_\mathfrak{P} = D_\mathfrak{p}[\beta]$. Veamos que tomando adecuadamente $a = 0, 1$ se cumple que $|\lambda(\beta) - a| = 1$ para todo $k_\mathfrak{p}$-automorfismo λ de $\mathbb{K}_\mathfrak{p}$.

En efecto, sea L la adjunción a $K_\mathfrak{P}$ de todos los $\lambda(\beta)$. Sea $\mathfrak{Q}$ su único primo y $F_\mathfrak{Q}$ su anillo de enteros. Entonces las clases $[\lambda(\beta)]$ módulo $\mathfrak{Q}$ son conjugadas sobre $D_\mathfrak{p}/\mathfrak{p}$. Si son todas nulas entonces $|\lambda(\beta)| < 1$ para todo λ, luego sirve $a = 1$. Si ninguna es nula entonces $|\lambda(\beta)| = 1$ para todo λ, luego sirve $a = 0$.

Sea $\sigma_1, \ldots, \sigma_r : K \longrightarrow \mathbb{K}_\mathfrak{p}$ un conjunto de k-monomorfismos no equivalentes que induzcan todos los valores absolutos en K correspondientes a divisores de $\mathfrak{p}$. Podemos suponer que σ_1 es la identidad y por lo tanto induce el valor absoluto de $\mathfrak{P}$. Sea $\epsilon > 0$. Por el teorema chino del resto existe un $\alpha \in E$ tal que

$$|\alpha - \beta|_\mathfrak{P} < \epsilon, \qquad |\alpha - a|_{\mathfrak{P}'} < \epsilon,$$

para todo primo $\mathfrak{P}' \neq \mathfrak{P}$ que divida a $\mathfrak{p}$ (usamos el teorema chino del resto y no el teorema de aproximación para garantizar que $\alpha \in E$). Equivalentemente, en términos del valor absoluto de $\mathbb{K}_\mathfrak{p}$,

$$|\alpha - \beta| < \epsilon, \qquad |\sigma_i(\alpha) - a| < \epsilon, \quad \text{para } i = 2, \ldots, r. \tag{3.1}$$

Sea $K = k(\gamma)$. Sea $\pi \in \mathfrak{p}$. Entonces $K = k(\pi^m\gamma)$ para cualquier $m \geq 0$. Si tomamos m suficientemente grande como para que $|\pi^m\gamma|$ sea menor que la distancia entre dos conjugados cualesquiera de α, es claro que los números $\alpha' + \pi^m\gamma'$, cuando α' varía en los conjugados de α y γ' en los conjugados de γ, son distintos dos a dos, pero cada conjugado de $\alpha + \pi^m\gamma$ es de la forma $\alpha' + \pi^m\gamma'$, donde γ' recorre todos los conjugados de γ y α' es un conjugado de α que depende de γ'. Concluimos que $\alpha + \pi^m\gamma$ tiene tantos conjugados como γ, luego $K = k(\alpha + \pi^m\gamma)$.

Si exigimos además que $|\pi^m\gamma| < \epsilon$, tenemos que $\alpha + \pi^m$ cumple también (3.1), es decir, podemos suponer que $K = k(\alpha)$.

Si tomamos ϵ suficientemente pequeño podemos aplicar el teorema anterior y concluir que $E_\mathfrak{P} = D_\mathfrak{p}[\beta] = D_\mathfrak{p}[\alpha]$.

Notar que, en general, si f es un polinomio mónico e irreducible con raíz α, entonces f se descompone como producto de $x - \alpha'$, donde α' recorre los conjugados de α, y al derivar se obtiene que $f'(\alpha)$ se descompone como producto de $\alpha - \alpha'$, donde α' recorre los conjugados de α distintos de él mismo.

El teorema 3.8 nos da que el diferente local $\mathfrak{D}_\mathfrak{P}$ es el producto de todos los $\alpha - \sigma(\alpha)$, donde σ recorre los k-monomorfismos $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ que se extienden a $K_\mathfrak{P}$, es decir, que son equivalentes a la identidad σ_1, pero distintos de ella.

Por otro lado, si f es el polinomio mínimo de α sobre K, tenemos también que $f'(\alpha)$ es el producto de los $\alpha - \sigma(\alpha)$, donde σ recorre los k-monomorfismos $\sigma : K \longrightarrow \mathbb{K}_\mathfrak{p}$ distintos de la identidad.

Por el teorema 10 sabemos que el exponente de $\mathfrak{P}$ en el diferente global $\mathfrak{D}$ es el mismo que en $\mathfrak{D}_\mathfrak{P}$, y lo que queremos probar es que coincide con el exponente de $\mathfrak{P}$ en $f'(\alpha)$, luego basta probar que $\mathfrak{P}$ no divide a ningún factor $\alpha - \sigma(\alpha)$, donde $\sigma : K \longrightarrow K_\mathfrak{p}$ es un k-monomorfismo que no se extiende a $K_\mathfrak{P}$, es decir, que determina un primo de K distinto de $\mathfrak{P}$.

Un tal σ será equivalente a un cierto σ_i para $i = 2, \ldots, r$, o sea, existe un $k_\mathfrak{p}$-automorfismo λ de $\mathbb{K}_\mathfrak{p}$ tal que $\sigma(\alpha) = \lambda(\sigma_i(\alpha))$. Así pues

$$|\alpha - \sigma(\alpha)| = |\alpha - \lambda(\sigma_i(\alpha))| = |\lambda^{-1}(\alpha) - \sigma_i(\alpha)| = |\lambda^{-1}(\alpha) - a + a - \sigma_i(\alpha)|.$$

Como $|\lambda^{-1}(\alpha) - a| = 1$ y $|a - \sigma_i(\alpha)| < \epsilon$, concluimos que $|\alpha - \sigma(\alpha)| = 1$, luego el factor no es divisible entre $\mathfrak{P}$. ∎

Terminamos esta sección con el primer resultado importante en torno a la aritmética de los cuerpos numéricos. Vamos a determinar los primos ramificados de una extensión.

Definición 3.14 Los términos que introdujimos en el capítulo anterior para extensiones locales tienen sentido globalmente: Sea $\mathfrak{p}$ un primo en un cuerpo numérico, sea $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en una extensión de grado n, sea p el primo racional al cual dividen. Diremos que

a) $\mathfrak{p}$ es *no ramificado* en $\mathfrak{P}$ si $e(\mathfrak{P}/\mathfrak{p}) = 1$,

b) $\mathfrak{p}$ es *ramificado* en $\mathfrak{P}$ si $e(\mathfrak{P}/\mathfrak{p}) > 1$,

c) $\mathfrak{p}$ es *totalmente ramificado* en $\mathfrak{P}$ si $e(\mathfrak{P}/\mathfrak{p}) = n$,

d) $\mathfrak{p}$ es *dominadamente ramificado* en $\mathfrak{P}$ si $p \nmid e(\mathfrak{P}/\mathfrak{p})$,

e) $\mathfrak{p}$ es *libremente ramificado* en $\mathfrak{P}$ si $p \mid e(\mathfrak{P}/\mathfrak{p})$.

También diremos que $\mathfrak{P}$ es *ramificado, totalmente ramificado, etc.* sobre $\mathfrak{p}$.

Teorema 3.15 *Sea K/k una extensión de cuerpos numéricos. Sea $\mathfrak{p}$ un primo en k, sea $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en K, sea $e = e(\mathfrak{P}/\mathfrak{p})$ y $\mathfrak{D}$ el diferente de la extensión. Entonces:*

a) Se cumple que $\mathfrak{P}^{e-1} \mid \mathfrak{D}$.

b) Si $\mathfrak{P}$ es libremente ramificado sobre $\mathfrak{p}$ entonces $\mathfrak{P}^e \mid \mathfrak{D}$.

c) Si $\mathfrak{P}$ es no ramificado sobre $\mathfrak{p}$ entonces $\mathfrak{P} \nmid \mathfrak{D}$.

d) En particular $\mathfrak{P}$ es ramificado sobre $\mathfrak{p}$ si y sólo si $\mathfrak{P} \mid \mathfrak{D}$. El número de primos ramificados en K es finito.

Demostración: Teniendo en cuenta que al localizar se conserva el exponente de $\mathfrak{P}$ en el diferente así como el grado de ramificación e, es claro que podemos localizar y suponer que los cuerpos K y k son completos.

Si $\mathfrak{P}$ es no ramificado entonces $\mathfrak{P} = \mathfrak{p} = (\pi)$ para un cierto $\pi \in D$. Sea $\alpha \in E$ tal que $E/\mathfrak{P} = (D/\mathfrak{p})[\alpha]$. Por el teorema 3.11 concluimos que $E = D[\alpha, \pi] = D[\alpha]$. El teorema 3.8 nos da entonces que $\mathfrak{D} = (f'(\alpha))$, donde $f(x) \in D[x]$ es el polinomio mínimo de α. El teorema 2.34 implica que la imagen de f en $(D/\mathfrak{p})[x]$ es el polinomio mínimo de $[\alpha]$, luego $f'(\alpha) \not\equiv 0 \pmod{\mathfrak{P}}$, es decir, $\mathfrak{P} \nmid \mathfrak{D}$, luego $\mathfrak{D} = 1$. Esto prueba c).

Consideremos la cadena de extensiones $k \subset K_{nr} \subset K$ (ver el teorema 2.39). Hemos probado que el diferente de K_{nr}/k es igual a 1, luego el diferente de K/k es el mismo que el de K/K_{nr}. Así mismo, el índice de ramificación de K_{nr}/k vale 1 luego el índice de ramificación de K/k es el mismo que el de K/K_{nr}.

De aquí se sigue que para probar a) y b) podemos suponer que $k = K_{nr}$ o, equivalentemente, que $\mathfrak{P}$ es totalmente ramificado.

Entonces $E/\mathfrak{P} = D/\mathfrak{p}$, luego el teorema 3.11 nos da $E = D[1,\pi] = D[\pi]$, donde $\pi \in D$ cumple $\mathfrak{P} = (\pi)$. Por el teorema 2.40 el polinomio mínimo de π es de la forma $f(x) = x^e + a_{e-1}x^{e-1} + \cdots + a_1x + a_0$, donde todos los $a_i \in D$ son divisibles entre $\mathfrak{p}$ (o sea, entre $\mathfrak{P}^e$).

En consecuencia $f'(\pi) \equiv e\pi^{e-1}$ (mód $\mathfrak{P}^e$). Por el teorema 3.8 tenemos que $\mathfrak{D} = (f'(\pi))$, luego se cumple que $\mathfrak{P}^{e-1} \mid \mathfrak{D}$ y, si además $\mathfrak{P}$ es libremente ramificado, entonces $p \mid e$, luego $\mathfrak{P}^e \mid \mathfrak{D}$. ∎

3.3 Discriminantes

Ahora relacionamos el concepto de diferente de una extensión con el ya conocido de discriminante. Como ya hemos anticipado, la relación básica entre ellos es que el discriminante es la norma del diferente. El discriminante contiene un poco menos de información que el diferente pero a cambio está en el cuerpo base, y por ello es más fácil de manejar.

Definición 3.16 Sea K/k una extensión de cuerpos separable de grado n. Sean $\sigma_1, \ldots, \sigma_n$ los k-monomorfismos de K en una clausura algebraica. Para cada conjunto de n elementos $W = \{w_1, \ldots, w_n\} \subset K$ se define el *discriminante* de W como

$$\Delta[W] = \big(\det(\sigma_i(w_j))\big)^2 = \det\big((\sigma_k(w_i))(\sigma_k(w_j))\big) = \det\big(\mathrm{Tr}(w_iw_j)\big) \in k.$$

Los hechos siguientes son generalizaciones naturales de [2.7]:

Es claro que $\Delta[W]$ no depende del orden de los elementos de W ni del de los monomorfismos. Si W es un sistema ligado sobre k entonces las columnas de la matriz $\big(\sigma_i(w_j)\big)$ son linealmente dependientes, luego $\Delta[W] = 0$.

Si W y W' son dos k-bases de K y $D^W_{W'}$ es la matriz del cambio de base (cuyas filas son las coordenadas de los elementos de W' en la base W) es fácil comprobar que

$$\Delta[W'] = |D^W_{W'}|^2\Delta[W].$$

Si $K = k(\alpha)$, entonces una k-base de K es $1, \alpha, \ldots, \alpha^{n-1}$, y

$$\Delta[\alpha] = \Delta[1, \alpha, \ldots, \alpha^{n-1}] = \prod_{i<j}\big(\sigma_j(\alpha) - \sigma_i(\alpha)\big)^2 \neq 0,$$

pues el determinante que aparece es del tipo de Vandermonde.

Uniendo todos estos hechos concluimos que $\Delta[W] = 0$ si y sólo si W es linealmente dependiente.

Otra propiedad fácil de comprobar es que

$$\Delta[\alpha w_1, \ldots, \alpha w_n] = \mathrm{N}(\alpha)^2\Delta[w_1, \ldots, w_n].$$

Si E/D es una extensión separable de dominios de Dedekind y K/k es la extensión de los cuerpos de cocientes, es claro que si $W \subset E$ entonces $\Delta[W] \in D$.

Cuando $D = \mathbb{Z}$ todo D-módulo $M \subset K$ es libre y podemos definir $\Delta[M]$ como el discriminante de cualquier base de M (entendiendo que es 0 si el rango de M es menor que n). Si W y W' son dos bases de M entonces la matriz de cambio de base tiene determinante ± 1, luego $\Delta(W) = \Delta(W')$, y por lo tanto $\Delta(M)$ no depende de la elección de la base.

En el caso general no es cierto que todo D-módulo sea libre, y aún en tal caso los discriminantes de dos bases de un módulo libre no tienen por qué coincidir (se diferencian en el cuadrado de una unidad de D, que ya no tiene por qué ser igual a ± 1). Todo esto nos lleva a definir el discriminante de un D-módulo como otro D-módulo.

Definición 3.17 Sea E/D una extensión separable de grado n de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes. Si $M \subset K$ es un D-módulo llamaremos *discriminante* de M al D-módulo $\Delta[M]$ generado por los discriminantes $\Delta[W]$, donde W recorre los subconjuntos de M con n elementos.

Llamaremos *discriminante* de la extensión a $\Delta = \Delta[E]$. El teorema siguiente prueba entre otras cosas que Δ es un ideal no nulo de D.

Teorema 3.18 *Sea E/D una extensión separable de grado n de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes. Sea $M \subset K$ un D-módulo. Entonces*

a) Si M admite una base W con n elementos, entonces $\Delta[M] = \langle \Delta[W] \rangle_D$.

b) Si $M \subset E$ entonces $\Delta[M]$ es un ideal de D.

c) Si M es un ideal no nulo (fraccional) de E entonces $\Delta[M]$ es un ideal no nulo (fraccional) de D.

d) Si $M \subset N \subset E$ son D-módulos libres de rango n entonces $\Delta[N] \mid \Delta[M]$ y $\Delta[M] = \Delta[N]$ si y sólo si $M = N$.

Demostración: a) Una inclusión es obvia. Si W' es un subconjunto de M con n elementos, entonces W y W' son dos k-bases de K y la matriz $D^W_{W'}$ de cambio de base tiene sus coeficientes en D. Por lo tanto

$$\Delta[W'] = |D^W_{W'}|^2 \Delta[W] \in \langle \Delta[W] \rangle_D ,$$

y así tenemos la igualdad.

b) Si $M \subset E$ todos los discriminantes $\Delta[W]$ con $W \subset M$ están en D, luego $\Delta[M] \subset D$ y un D-módulo contenido en D es un ideal de D.

c) Si M es un ideal de E entonces $\Delta[M]$ es un ideal de D por el apartado b). Sea W una k-base de K. Por el teorema 1.18 existe un $d \in D$ no nulo tal que $dW \subset E$, y dW sigue siendo una k-base de K. Si $M \neq 0$ tomamos $\alpha \in M \cap D$ no nulo, y entonces $\alpha dW \subset M$ y es una k-base, luego $0 \neq \Delta[\alpha dW] \in \Delta[M]$.

El mismo razonamiento prueba que si M es un ideal fraccional (no nulo) entonces $\Delta[M]$ es un D-módulo no nulo (y está contenido en k). Sea $\alpha \in K$ no

nulo tal que $\alpha M \subset E$. Entonces $\Delta[\alpha M] = \mathrm{N}(\alpha)^2\Delta[M] \subset D$, luego $\Delta[M]$ es un ideal fraccional de D.

d) Sea W una base de N y W' una base de M. Entonces la matriz $D^W_{W'}$ de cambio de base tiene coeficientes en D, luego $|D^W_{W'}| \in D$. Tenemos que $\Delta(W') = |D^W_{W'}|^2\Delta(W)$ y, como $\Delta[M] = (\Delta[W'])$, $\Delta[N] = (\Delta[W])$, concluimos que $\Delta[M] \subset \Delta[N]$ o, lo que es lo mismo, $\Delta[N] \mid \Delta[M]$, y que se da la igualdad si y sólo si $|D^W_{W'}|^2$ es una unidad en D, lo cual equivale a que la matriz $D^W_{W'}$ tenga inversa en D y a que W' sea también una base de N. ∎

Aunque tenemos un concepto de discriminante de un módulo válido en cualquier caso, el teorema anterior muestra que su comportamiento es mejor sobre los módulos libres de rango máximo. Cuando $D = \mathbb{Z}$ sabemos que todos los ideales fraccionales de E son de este tipo (por [2.17]). Otro caso importante en el que esto sucede es cuando D tiene un único primo, pues entonces D es un dominio euclídeo (ver las observaciones tras el teorema 1.24) y los ideales fraccionales de E son D-módulos finitamente generados y libres de torsión, luego son libres. El hecho de que sus discriminantes sean no nulos prueba que tienen rango máximo. (Respecto al carácter finitamente generado de los ideales fraccionales, observar que E es finitamente generado por el teorema 1.19 y como D es noetheriano también lo son los ideales de E, y de aquí que lo mismo vale para los ideales fraccionales).

En el caso $D = \mathbb{Z}$, la única información que se pierde al considerar los discriminantes como módulos en lugar de como números racionales es el signo, pues dos números racionales generan el mismo $\mathbb{Z}$-módulo si y sólo si se diferencian tan sólo en el signo. Por otra parte, en virtud de la relación $\Delta[W'] = |D^W_{W'}|^2\Delta[W]$, sucede que todos los discriminantes de todos los $\mathbb{Z}$-módulos de un cuerpo numérico K tienen el mismo signo. Veamos que este signo es fácil de recuperar, con lo que en realidad trabajar con módulos no supone ningún inconveniente.

Teorema 3.19 *Sea K un cuerpo numérico y W una $\mathbb{Q}$-base de K. Entonces el signo de $\Delta[W]$ es $(-1)^t$, donde t es el número de primos infinitos complejos de K.*

Demostración: Por los comentarios anteriores basta analizar el signo del discriminante de una base concreta. Sea $K = \mathbb{Q}(\alpha)$ y consideremos

$$\Delta[\alpha] = \prod_{i<j} \big(\sigma_j(\alpha) - \sigma_i(\alpha)\big)^2.$$

Dividamos los pares de índices (i, j) en tres grupos según que los monomorfismos asociados sean ambos reales, uno real y otro complejo o ambos complejos.

Es claro que si σ_i y σ_j son ambos reales entonces $\big(\sigma_j(\alpha) - \sigma_i(\alpha)\big)^2 > 0$, luego los factores del primer grupo no influyen en el signo.

Los factores del segundo tipo pueden ser agrupados en parejas formadas por un monomorfismo real acompañado por dos monomorfismos complejos conjugados. Entonces, si $\big(\sigma_j(\alpha) - \sigma_i(\alpha)\big)^2$ es uno de estos factores, su pareja es

$\big(\overline{\sigma_j(\alpha)-\sigma_i(\alpha)}\big)^2$, y el producto de ambos es $|\sigma_j(\alpha)-\sigma_i(\alpha)|^4>0$, luego los factores de este tipo tampoco contribuyen al signo.

Entre los factores del tercer tipo distingamos a su vez los formados por pares de monomorfismos conjugados y el resto. Si $\big(\sigma_j(\alpha)-\sigma_i(\alpha)\big)^2$ es uno de los factores restantes donde σ_i no es el conjugado de σ_j, entonces otro de los factores de este tipo es $\big(\overline{\sigma_j(\alpha)-\sigma_i(\alpha)}\big)^2$, y concluimos como antes.

De esta manera, los únicos factores que influyen en el signo son los de tipo $\big(\sigma_j(\alpha)-\sigma_i(\alpha)\big)^2$ donde σ_i y σ_j son conjugados. Entonces $\sigma_j(\alpha)-\sigma_i(\alpha)$ es imaginario puro y, por lo tanto, $\big(\sigma_j(\alpha)-\sigma_i(\alpha)\big)^2<0$. El número de factores de este tipo es claramente igual a t, de donde se concluye el teorema. ∎

Las propiedades básicas de los discriminantes las deduciremos de su comportamiento local, que estudiamos seguidamente.

Teorema 3.20 *Sea E/D una extensión separable de dominios de Dedekind y S un subconjunto multiplicativo de D. Sea $\mathfrak{a}$ un ideal fraccional de E. Entonces $S^{-1}\Delta[\mathfrak{a}]=\Delta[S^{-1}\mathfrak{a}]$.*

En particular si $\mathfrak{p}$ es un ideal primo de D y $\Delta_\mathfrak{p}$ es el discriminante de la extensión local $E_\mathfrak{p}/D_\mathfrak{p}$, entonces $\Delta_\mathfrak{p}$ es la mayor potencia de $\mathfrak{p}$ que divide al discriminante global Δ. Consecuentemente

$$\Delta=\prod_\mathfrak{p}\Delta_\mathfrak{p}.$$

Demostración: Si $W\subset S^{-1}\mathfrak{a}$, llamando s al producto de los denominadores (en S) de los elementos de W podemos expresar $W=W'/s$, donde $W'\subset\mathfrak{a}$. Entonces

$$\Delta[W]=\mathrm{N}(1/s)\Delta[W']=\frac{\Delta(W')}{s^n}\in S^{-1}\Delta[\mathfrak{a}],$$

luego $\Delta[S^{-1}\mathfrak{a}]\subset S^{-1}\Delta[\mathfrak{a}]$.

Por otra parte $S^{-1}\Delta[\mathfrak{a}]$ está generado como $S^{-1}D$-módulo por los elementos de la forma $\Delta[W]$, con $W\subset\mathfrak{a}\subset S^{-1}\mathfrak{a}$, pero $\Delta[W]\in\Delta[S^{-1}\mathfrak{a}]$, con lo que $S^{-1}\Delta(\mathfrak{a})\subset\Delta[S^{-1}\mathfrak{a}]$. ∎

La primera consecuencia es la versión general de un resultado que ya conocíamos para el caso $D=\mathbb{Z}$ (de hecho lo tomamos como definición de norma de un módulo [2.32]).

Teorema 3.21 *Sea E/D una extensión separable de dominios de Dedekind, sea Δ su discriminante y sea $\mathfrak{a}$ un ideal fraccional de E. Entonces*

$$\Delta[\mathfrak{a}]=\mathrm{N}(\mathfrak{a})^2\Delta.$$

Demostración: Para probar esta igualdad de ideales fraccionales basta tomar un primo arbitrario $\mathfrak{p}$ de D y ver que su multiplicidad en ambos miembros es la misma. Para ello podemos localizar tomando $S=D\setminus\mathfrak{p}$ y demostrar que $\Delta[S^{-1}\mathfrak{a}]=\mathrm{N}(S^{-1}\mathfrak{a})^2\Delta[S^{-1}E]$.

En efecto, por el teorema anterior tenemos que

$$\Delta[S^{-1}\mathfrak{a}] = S^{-1}\Delta[\mathfrak{a}] \quad \text{y} \quad \Delta[S^{-1}E] = S^{-1}\Delta[E],$$

luego la multiplicidad de $\mathfrak{p}$ en $\Delta[\mathfrak{a}]$ y $\Delta[E]$ es la misma que la multiplicidad de $S^{-1}\mathfrak{p}$ en $\Delta(S^{-1}\mathfrak{a})$ y $\Delta(S^{-1}E)$.

Así mismo, el exponente de $\mathfrak{p}$ en $\mathrm{N}(\mathfrak{a})$ es la suma de los productos de los grados de inercia de los divisores de $\mathfrak{p}$ en E por sus multiplicidades en $\mathfrak{a}$, y todo esto se conserva al localizar, luego también el exponente de $\mathfrak{p}$ en $\mathrm{N}(\mathfrak{a})^2$ es el mismo que el exponente de $S^{-1}\mathfrak{p}$ en $\mathrm{N}(S^{-1}\mathfrak{a})^2$.

Equivalentemente, podemos suponer que $\mathfrak{p}$ es el único primo de D, pero entonces D es un dominio euclídeo y E es un dominio de ideales principales (teorema 1.21).

Sea K/k la extensión de los cuerpos de cocientes. Sea $\mathfrak{a} = (\alpha) = \alpha E$, con $\alpha \in K$. Toda k-base de K contenida en $\mathfrak{a}$ es de la forma αW, donde W es una k-base contenida en E y, recíprocamente, dada W, la base αW está contenida en $\mathfrak{a}$. De la relación $\Delta[\alpha W] = \mathrm{N}(\alpha)^2\Delta[W]$ se sigue que $\Delta[\alpha E] = \mathrm{N}(\alpha)^2\Delta[E]$, o sea, $\Delta(\mathfrak{a}) = \mathrm{N}(\mathfrak{a})^2\Delta$. ∎

Ahora estamos en condiciones de demostrar la relación ya anunciada entre el diferente y el discriminante de una extensión:

Teorema 3.22 *Sea E/D una extensión separable de dominios de Dedekind y sea K/k la extensión de los cuerpos de cocientes. Entonces el discriminante Δ y el diferente $\mathfrak{D}$ de la extensión verifican que $\Delta = \mathrm{N}(\mathfrak{D})$.*

Demostración: El mismo argumento que en el teorema anterior nos permite suponer que D tiene un único primo. Entonces E es un D-módulo libre de rango máximo (ver las observaciones tras el teorema 3.18). Sea $W = (w_i)$ una base y sea W' la base dual. Por el teorema 3.3 sabemos que W' es base de E'.

$$\Delta[W]\Delta[W'] = \det\big(\sigma_i(w_j)\big)^2 \det(\sigma_i(w'_j)\big)^2 = \det\big(\mathrm{Tr}(w_i w'_j)\big)^2 = 1,$$

luego $\Delta[E]\Delta[E'] = 1$. Usando esto y el teorema anterior obtenemos que

$$\Delta^{-1} = \Delta[E]^{-1} = \Delta[E'] = \Delta(\mathfrak{D}^{-1}) = \mathrm{N}(\mathfrak{D}^{-1})^2\Delta,$$

con lo que $\mathrm{N}(\mathfrak{D})^2 = \Delta^2$ y, en consecuencia, $\mathrm{N}(\mathfrak{D}) = \Delta$. ∎

De aquí se sigue una versión débil del teorema 3.15 en términos de discriminantes:

Teorema 3.23 *Sea E/D una extensión separable de dominios de Dedekind y sea $\mathfrak{p}$ un primo en D. Entonces $\mathfrak{p}$ se ramifica (sobre alguno de sus divisores) en E si y sólo si $\mathfrak{p} \mid \Delta$.*

Demostración: Si $\mathfrak{p}$ se ramifica sobre algún divisor $\mathfrak{P}$ entonces $\mathfrak{P} \mid \mathfrak{D}$, luego $\mathfrak{p} \mid \mathrm{N}(\mathfrak{P}) \mid \mathrm{N}(\mathfrak{D}) = \Delta$.

Si $\mathfrak{p} \mid \Delta = \mathrm{N}(\mathfrak{D})$, entonces algún divisor $\mathfrak{P}$ de $\mathfrak{p}$ cumple $\mathfrak{P} \mid \mathfrak{D}$, luego $\mathfrak{p}$ se ramifica sobre $\mathfrak{P}$. ∎

Sabemos [4.13] que el discriminante de un cuerpo numérico distinto de $\mathbb{Q}$ nunca es igual a ± 1, luego en todo cuerpo numérico existen siempre primos ramificados sobre $\mathbb{Q}$. Sin embargo el discriminante relativo de un cuerpo numérico respecto de un subcuerpo puede ser 1. Para ver un ejemplo demostraremos primero dos hechos generales de gran utilidad en la práctica. El primero es una consecuencia inmediata de los teoremas 3.9 y 3.22.

Teorema 3.24 *Sea $D \subset E \subset F$ una cadena de extensiones separables de dominios de Dedekind de grados m y n respectivamente. Entonces*

$$\Delta_{F/D} = \mathrm{N}_D^E(\Delta_{F/E})\,\Delta_{E/D}^n.$$

Demostración: Sean $k \subset K \subset L$ los cuerpos de cocientes. Tomando normas en la igualdad del teorema 3.9 queda

$$\begin{aligned}\Delta_{F/D} &= \mathrm{N}_k^L(\mathfrak{D}_{F/D}) = \mathrm{N}_k^L(\mathfrak{D}_{F/E})\,\mathrm{N}_k^L(\mathfrak{D}_{E/D}) = \mathrm{N}_k^K(\Delta_{F/E})\,\mathrm{N}_k^K(\mathfrak{D}_{E/D})^n\\ &= \mathrm{N}_D^E(\Delta_{F/E})\Delta_{E/D}^n.\end{aligned}$$

■

Teorema 3.25 *Sean K y L dos cuerpos numéricos de grados m y n respectivamente cuyos discriminantes sean primos entre sí. Entonces sus anillos de enteros cumplen $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$ y además $\Delta_{KL} = \Delta_K^n\Delta_L^m$.*

Demostración: Por la transitividad del diferente tenemos que

$$\mathfrak{D}_{KL/\mathbb{Q}} = \mathfrak{D}_{KL/K}\mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{KL/L}\mathfrak{D}_{L/\mathbb{Q}}.$$

Por hipótesis $\mathfrak{D}_{K/\mathbb{Q}}$ y $\mathfrak{D}_{L/\mathbb{Q}}$ tienen normas primas entre sí, luego son primos entre sí. Vamos a probar que los dos factores restantes también son primos entre sí, con lo que podremos concluir que

$$\mathfrak{D}_{KL/K} = \mathfrak{D}_{L/\mathbb{Q}} \quad \text{y} \quad \mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{KL/L}. \tag{3.2}$$

Supongamos que existe un primo $\mathfrak{P}$ en KL tal que $\mathfrak{P} \mid \mathfrak{D}_{KL/K}$ y $\mathfrak{P} \mid \mathfrak{D}_{KL/L}$. Sean p, $\mathfrak{p}$ y $\mathfrak{p}'$ los primos en $\mathbb{Q}$, K y L respectivamente divisibles entre $\mathfrak{P}$. El teorema 3.15 nos da que $e(\mathfrak{P}/\mathfrak{p})$ y $e(\mathfrak{P}/\mathfrak{p}')$ son ambos mayores que 1. Si consideramos las compleciones respecto a estos primos resulta que $KL_{\mathfrak{P}}/K_{\mathfrak{p}}$ y $KL_{\mathfrak{P}}/L_{\mathfrak{p}'}$ son ambas ramificadas, luego por el teorema 2.35 b) llegamos a que $K_{\mathfrak{p}}/\mathbb{Q}_p$ y $L_{\mathfrak{p}'}/\mathbb{Q}_p$ también son ramificadas, pero entonces el teorema 3.15 nos da que $\mathfrak{p} \mid \mathfrak{D}_{K/\mathbb{Q}}$ y $\mathfrak{p}' \mid \mathfrak{D}_{L/\mathbb{Q}}$, luego $p \mid \Delta_K$ y $p \mid \Delta_L$, contradicción.

Sea W una $\mathbb{Z}$-base de $\mathcal{O}_K$. Sea W' la base dual. Entonces W' es una $\mathbb{Z}$-base de $(\mathfrak{D}_{K/\mathbb{Q}})^{-1}$, luego es también un generador como $\mathcal{O}_L$-módulo del ideal fraccional generado por $(\mathfrak{D}_{K/\mathbb{Q}})^{-1}$ en KL, que por (3.2) es $(\mathfrak{D}_{KL/L})^{-1}$. Dualizando de nuevo concluimos que W es un generador de $\mathcal{O}_{KL}$ como $\mathcal{O}_L$-módulo. Así pues, $\mathcal{O}_{KL} = \mathcal{O}_L[W] = \mathcal{O}_L\mathbb{Z}[W] = \mathcal{O}_L\mathcal{O}_K$.

La relación entre los discriminantes se obtiene tomando normas en

$$\mathfrak{D}_{KL/\mathbb{Q}} = \mathfrak{D}_{KL/K}\mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{L/\mathbb{Q}}\mathfrak{D}_{K/\mathbb{Q}}.$$

En principio así obtenemos la igualdad como ideales, pero el signo es también correcto. Para probarlo observamos que $K \cap L = \mathbb{Q}$, ya que el discriminante de $K \cap L$ da lugar a un factor común en los discriminantes de K y L (por el teorema 3.24), luego ha de ser 1 y, en consecuencia (por [4.13]), $K \cap L = \mathbb{Q}$. De aquí que los monomorfismos de KL se expresen de forma única como producto de los monomorfismos de K por los monomorfismos de L (una base de KL es el producto de una base de K por una base de L). Si K y L tienen t y t' primos complejos respectivamente, entonces tienen $2t$ y $2t'$ monomorfismos complejos, y KL tiene $2tn+2t'm-4tt'$ monomorfismos complejos (un producto de monomorfismos es complejo si y sólo si lo es al menos uno de los factores), luego KL tiene $tn + t'm - 2tt'$ primos complejos, y el teorema 3.19 nos da que el signo es correcto. ∎

3.4 Ejemplos y aplicaciones

Vamos a dar algunos ejemplos que ilustren la potencia de la teoría que hemos desarrollado hasta aquí. Comenzamos con dos ejemplos de discriminante relativo igual a 1.

Ejemplo Consideremos el cuerpo $K = \mathbb{Q}(\sqrt{5}, \sqrt{-5})$. Como $\mathbb{Q}(\sqrt{5})$ es un cuerpo real y por lo tanto no contiene a $\sqrt{-5}$, es claro que K es un cuerpo numérico de grado 4. Además K es el cuerpo de escisión de $(x^2+5)(x^2-5)$, luego K es una extensión de Galois de $\mathbb{Q}$.

Es claro que el grupo de Galois es producto de dos grupos cíclicos, y sus tres subgrupos propios se corresponden con los cuerpos intermedios $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-5})$ y $\mathbb{Q}(i)$.

Los discriminantes de estos cuerpos son respectivamente 5, -20 y -4, luego podemos aplicar el teorema 3.25 a $\mathbb{Q}(\sqrt{5})$ y a $\mathbb{Q}(i)$ para concluir que el discriminante de K es $\Delta = 400$. El teorema 3.24 nos da entonces que el discriminante de K relativo a $\mathbb{Q}(\sqrt{-5})$ es 1. ∎

Ejemplo (Artin) Sea $K_5 = \mathbb{Q}(\alpha)$, donde α es una raíz del polinomio $f(x) = x^5 - x + 1$. Es fácil ver que $f(x)$ es irreducible módulo 3, luego es irreducible en $\mathbb{Q}[x]$ y por consiguiente K_5 tiene grado 5 sobre $\mathbb{Q}$. Se cumple que $\Delta[\alpha] = 19 \cdot 151$ (ver el ejemplo y el ejercicio siguiente tras el teorema [2.8]). Como es libre de cuadrados podemos afirmar que el discriminante de K_5 es $\Delta = 19 \cdot 151$.

Sea K el cuerpo de escisión de $f(x)$ sobre $\mathbb{Q}$. Vamos a probar que tiene grado 120 o, equivalentemente, que $G \cong \Sigma_5$, donde $G = G(K/\mathbb{Q})$ y Σ_5 es el grupo de permutaciones de 5 elementos. Si identificamos estos 5 elementos con

las cinco raíces de f, entonces $G \leq \Sigma_5$. Ahora consideramos las factorizaciones

$$\begin{aligned} f(x) &\equiv (x-6)^2(x^3+12x^2+13x+9) \text{ (mód 19)},\\ f(x) &\equiv (x-9)(x^4+9x^3+12x^2+16x+15) \text{ (mód 23)}. \end{aligned}$$

Según el teorema [3.16], el 19 tiene un divisor en K_5 con grado de inercia 3, y el 23 tiene un divisor con grado de inercia 4. Por lo tanto $60 = 5\cdot 4\cdot 3 \,\big|\, |G|$. Esto nos deja únicamente dos posibilidades para G: o bien $G = A_5$ o bien $G = \Sigma_5$. De la definición de discriminante se sigue que $\sqrt{\Delta} \in K$, luego $k = \mathbb{Q}\big(\sqrt{\Delta}\,\big) \subset K$. Así pues, G contiene a $G(K/k)$ como subgrupo normal de índice 2, lo que implica que $G = \Sigma_5$ y $G(K/k) = A_5$.

Vamos a probar que ningún primo de k se ramifica en K. En primer lugar probaremos que los primos de $\mathbb{Q}$ que se ramifican en K son a lo sumo 19 y 151. Para ello acotaremos el diferente de la extensión. Notemos que al adjuntar una a una las raíces de $f(x)$ obtenemos una cadena de cuerpos

$$\mathbb{Q} \subset K_5 \subset K_{20} \subset K_{60} \subset K.$$

Basta probar que el diferente de cada paso es divisible a lo sumo entre divisores primos de 19 y 151. Ahora bien, si K_i/K_j es uno de los pasos intermedios, tenemos que $K_i = K_j(\alpha)$, donde α es una raíz de $f(x)$. Si llamamos $g(x)$ al polinomio mínimo de α sobre K_j, entonces $g(x) \mid f(x)$, por lo que $g'(\alpha) \mid f'(\alpha)$. Por el teorema 3.13 sabemos que el diferente de K_i/K_j divide a $f'(\alpha)$ y, por otra parte, considerando las extensiones $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K_i$, podemos calcular

$$\mathrm{N}_{\mathbb{Q}}^{K_i}\big(f'(\alpha)\big) = \mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}\big(f'(\alpha)\big)^{|K_i:\mathbb{Q}(\alpha)|} = \Delta^{|K_i:\mathbb{Q}(\alpha)|},$$

ya que $f'(\alpha)$ es el diferente de $\mathbb{Q}(\alpha)/\mathbb{Q}$ por el teorema 3.8 (notar que todo lo dicho antes para K_5 vale $\mathbb{Q}(\alpha)$, que es uno de sus conjugados).

Así pues, todo primo que divide al diferente de K_i/K_j divide a Δ, es decir, a 19 o a 151 y éstos son, pues, los únicos primos de $\mathbb{Q}$ que pueden ramificarse en K. Vamos a ver que su índice de ramificación vale exactamente 2.

La factorización de $f(x)$ módulo 19 que hemos calculado antes nos muestra que 19 se descompone en K_5 como producto de un primo al cuadrado con grado de inercia 1 por otro primo con grado de inercia 3. Las compleciones de K_5 respecto a estos primos dan lugar a dos extensiones de $\mathbb{Q}_{19}$, una de grado 2 y otra de grado 3. Llamémoslas L_2 y L_3. Ambas son de Galois: la primera por ser de grado 2 y la segunda por ser no ramificada (teorema 2.37). Cada una de ellas se obtiene adjuntando a $\mathbb{Q}_{19}$ una raíz de $f(x)$, luego L_2 contiene a dos raíces y L_3 a las otras tres.

Sea ahora $\mathfrak{P}$ un divisor de 19 en K. La compleción $K_{\mathfrak{P}}$ se obtiene adjuntando a $\mathbb{Q}_{19}$ las raíces de $f(x)$, luego $K_{\mathfrak{P}} = L_2L_3$. Por consiguiente $|K_{\mathfrak{P}} : \mathbb{Q}_{19}| = 6$ y, claramente, $e = 2$, $f = 3$.

En definitiva, la factorización de 19 en K consta de 20 primos al cuadrado con grado de inercia 3.

El 151 se trata de forma similar, a partir de la factorización

$$f(x) \equiv (x-9)(x-39)^2(x^2+87x+61) \text{ (mód 151)}.$$

Ahora vemos que $f(x)$ tiene ya una raíz en $\mathbb{Q}_{151}$, mientras que las otras cuatro dan lugar a dos extensiones cuadráticas, una con $e = 2$ y otra con $f = 2$. La conclusión es que 151 se descompone en 30 factores primos al cuadrado con grado de inercia 2.

Evidentemente 19 y 151 se ramifican en k, es decir, $19 = \mathfrak{p}^2$ y $151 = \mathfrak{q}^2$. Es claro entonces que $\mathfrak{p}$ y $\mathfrak{q}$ son no ramificados en K. El primero se descompone en 20 primos distintos con grado de inercia 3 y el segundo en 30 primos distintos con grado de inercia 2. Ningún otro primo puede ramificarse, luego no hay primos ramificados y el diferente es trivial: $\mathfrak{D}_{K/k} = 1$. ∎

Ejercicio: Probar que el cuerpo K_5 del ejemplo anterior tiene factorización única.

Ahora vamos a calcular el discriminante y el anillo de enteros de los cuerpos ciclotómicos de orden potencia de primo. Para ello necesitamos el hecho siguiente:

Teorema 3.26 *Sea p un número primo, r un número natural no nulo y ζ una raíz p^r-ésima primitiva de la unidad sobre $\mathbb{Q}$. Entonces $\zeta - 1$ es primo en el anillo de enteros de $\mathbb{Q}(\zeta)$ y $p = (\zeta - 1)^{\phi(p^r)}$.*

Demostración: Las raíces p^r-ésimas primitivas de la unidad son las raíces de $x^{p^r} - 1$ que no son raíces de $x^{p^{r-1}} - 1$, luego el polinomio ciclotómico p^r-ésimo es

$$\frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{p^{r-1}(p-1)} + x^{p^{r-1}(p-2)} + \cdots + x^{p^{r-1}} + 1.$$

Evaluando en 1 queda que

$$p = \prod_i (1 - \zeta^i),$$

donde i recorre los números menores que p^r no divisibles entre p.

Ahora notamos que $(1-\zeta^i)/(1-\zeta) = 1+\zeta+\cdots+\zeta^{i-1}$ es entero, pero ζ y ζ^i son dos raíces primitivas cualesquiera, luego $(1-\zeta)/(1-\zeta^i)$ también es entero, es decir, que $1 - \zeta^i$ es un asociado de $1 - \zeta$ para todo i, luego podemos poner

$$p = \epsilon(1 - \zeta)^{\phi(p^r)},$$

para cierta unidad ciclotómica ϵ. Como p no puede descomponerse en más de $\phi(p^r)$ factores podemos afirmar que $1 - \zeta$ es primo. Es claro entonces que la factorización de p en ideales es la indicada en el enunciado. ∎

Teorema 3.27 *Sea p un número primo, r un número natural no nulo y ζ una raíz p^r-ésima primitiva de la unidad sobre $\mathbb{Q}$. Entonces el anillo de enteros del cuerpo ciclotómico $\mathbb{Q}(\zeta)$ es $\mathbb{Z}[\zeta]$ y el discriminante es*

$$\Delta = (-1)^{\phi(p^r)/2} \frac{p^{r\phi(p^r)}}{p^{\phi(p^r)/(p-1)}}.$$

DEMOSTRACIÓN: El signo es consecuencia del teorema 3.19. Ocupémonos del valor absoluto. Si llamamos $f(x)$ al polinomio ciclotómico tenemos que $x^{p^r} - 1 = f(x)(x^{p^{r-1}} - 1)$, luego derivando y sustituyendo en ζ queda

$$p^r \zeta^{p^r-1} = f'(\zeta)(\zeta^{p^{r-1}} - 1),$$

luego $f'(\zeta) \mid p^r$. Por el teorema 3.13 podemos afirmar que $\mathfrak{D} \mid f'(\zeta) \mid p^r$, y al tomar normas queda que el discriminante Δ es potencia de p. Así pues, $\Delta = \Delta_p$.

Si llamamos E al anillo de enteros ciclotómicos, al localizar en p el teorema anterior nos da que E_p tiene un único primo (salvo asociados), que es $\zeta - 1$. Más aún, $\zeta - 1$ es totalmente ramificado sobre p, luego el grado de inercia es 1 y el teorema 3.11 nos da que

$$E_p = \mathbb{Z}_p[1, \zeta - 1] = \mathbb{Z}_p[\zeta - 1] = \mathbb{Z}_p[\zeta].$$

Por lo tanto $\Delta_p = \Delta[\zeta]$, y este discriminante no depende de si se calcula en la extensión local o en la global (pues los cuerpos de cocientes son los mismos, y los monomorfismos también). Así pues, $\Delta = \Delta(\mathbb{Z}[\zeta])$ y por el teorema 3.18 d) concluimos que $E = \mathbb{Z}[\zeta]$.

Por el teorema 3.8 resulta que $\mathfrak{D} = (f'(\zeta))$ y $\Delta = \pm \mathrm{N}(f'(\zeta))$. Concretamente tenemos que $f'(\zeta) = p^r \zeta^{p^r-1}/(\zeta^{p^{r-1}} - 1)$.

Es claro que $\mathrm{N}(p^r) = p^{r\phi(p^r)}$, $\mathrm{N}(\zeta) = 1$ y sólo queda calcular $\mathrm{N}(\zeta^{p^{r-1}} - 1)$. Ahora bien, $\omega = \zeta^{p^{r-1}}$ es una raíz p-ésima primitiva de la unidad, luego el teorema 26 nos da que $\omega - 1$ es primo en $\mathbb{Q}(\omega)$ y $p = (\omega - 1)^{p-1}$. De aquí se sigue que $\mathrm{N}(\omega - 1) = p$, donde N es ahora la norma de $\mathbb{Q}(\omega)$.

La norma de $\omega - 1$ en $\mathbb{Q}(\zeta)$ se obtiene por la transitividad elevando la anterior al grado de $\mathbb{Q}(\zeta)/\mathbb{Q}(\omega)$, es decir, $\mathrm{N}(\zeta^{p^{r-1}} - 1) = p^{\phi(p^r)/(p-1)}$. ∎

Ahora podemos aplicar el teorema 3.25 para extender el teorema anterior a cuerpos ciclotómicos arbitrarios.

Teorema 3.28 *Sea m un número natural no nulo y ζ una raíz m-sima primitiva de la unidad sobre $\mathbb{Q}$. Entonces el anillo de enteros del cuerpo ciclotómico $\mathbb{Q}(\zeta)$ es $\mathbb{Z}[\zeta]$ y el discriminante es*

$$\Delta = (-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p \mid m} p^{\phi(m)/(p-1)}}$$

DEMOSTRACIÓN: Basta observar que si $(m, n) = 1$, ζ es una raíz m-sima primitiva de la unidad y ω es una raíz n-sima primitiva de la unidad entonces $\zeta\omega$ es una raíz mn-ésima primitiva de la unidad y $\mathbb{Q}(\zeta\omega) = \mathbb{Q}(\zeta)\mathbb{Q}(\omega)$. Después se aplica inductivamente el teorema 3.25. ∎

En particular tenemos caracterizados los primos que ramifican en un cuerpo ciclotómico:

Teorema 3.29 *Sea $m > 1$ un número natural y K el cuerpo ciclotómico de orden m. Entonces un primo impar p se ramifica en K si y sólo si $p \mid m$. El 2 se ramifica en K si y sólo si $4 \mid m$.*

Capítulo IV

El símbolo de Artin

Vamos a introducir ahora uno de los conceptos fundamentales de la teoría de cuerpos de clases. A modo de primera aproximación podemos pensar que, así como los diferentes y los discriminantes nos han permitido estudiar el comportamiento de los primos ramificados, el estudio de los primos no ramificados (en extensiones abelianas) se funda en el símbolo de Artin. Para definirlo necesitamos estudiar primero un concepto relacionado.

4.1 El símbolo de Frobenius

Consideremos una extensión finita de Galois de dominios de Dedekind E/D con restos finitos, de modo que para cada primo $\mathfrak{p}$ en D está definida su norma absoluta $\mathrm{N}\,\mathfrak{p}$, igual al número de elementos cuerpo de restos $D/\mathfrak{p}$. Sea K/k la extensión de sus cuerpos de cocientes. Sea $\mathfrak{P}$ un primo en E y sea $\mathfrak{p}$ el primo de D al cual divide. Llamemos $\overline{k} = D/\mathfrak{p}$ y $\overline{K} = E/\mathfrak{P}$.

Supongamos que $\mathfrak{P}$ es no ramificado sobre $\mathfrak{p}$. Esta hipótesis equivale a que el grupo de inercia de $\mathfrak{P}$ sea trivial (ver 1.40). Entonces, según el teorema 1.39 el grupo de descomposición de $\mathfrak{P}$ es isomorfo al grupo de Galois de la extensión $\overline{K}/\overline{k}$. Ésta es una extensión de cuerpos finitos, luego su grupo de Galois es cíclico y, concretamente, es sabido que un generador de $G(\overline{K}/\overline{k})$ es el *automorfismo de Frobenius* σ dado por $\sigma(c) = c^{\mathrm{N}\,\mathfrak{p}}$, para todo $c \in \overline{K}$.

Definición 4.1 En las condiciones anteriores, llamaremos *símbolo de Frobenius* de $\mathfrak{P}$ a la antiimagen de σ por el isomorfismo descrito en el teorema 1.39. Lo representaremos por

$$\left(\frac{K/k}{\mathfrak{P}}\right) \in G_{\mathfrak{P}}.$$

De este modo el símbolo de Frobenius es por definición el único automorfismo $\tau \in G_{\mathfrak{P}}$ que cumple $\tau([\alpha]) = [\alpha]^{\mathrm{N}\,\mathfrak{p}}$ para todo $\alpha \in E$ o, lo que es lo mismo, $\tau(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}}$ (mód $\mathfrak{P}$) para todo $\alpha \in E$.

En realidad el símbolo de Frobenius es el único automorfismo de todo el grupo de Galois $G(K/k)$ con esta propiedad. Lo demostramos en el teorema siguiente junto con otras propiedades elementales.

Teorema 4.2 *Sea E/D una extensión finita de Galois de dominios de Dedekind con restos finitos. Sea K/k la extensión de los cuerpos de cocientes. Sea $\mathfrak{P}$ un primo en E y sea $\mathfrak{p}$ el primo de D al cual divide. Supongamos que $e(\mathfrak{P}/\mathfrak{p}) = 1$. Entonces:*

a) $\left(\frac{K/k}{\mathfrak{P}}\right)$ *es un generador del grupo de descomposición $G_{\mathfrak{P}}$ (luego su orden es $f(\mathfrak{P}/\mathfrak{p})$).*

b) Para todo $\alpha \in E$ se cumple

$$\left(\frac{K/k}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}} \pmod{\mathfrak{P}}.$$

c) $\left(\frac{K/k}{\mathfrak{P}}\right)$ *es el único k-automorfismo de K que cumple b).*

d) Para todo $\tau \in G(K/k)$ se cumple

$$\left(\frac{K/k}{\tau(\mathfrak{P})}\right) = \tau^{-1}\left(\frac{K/k}{\mathfrak{P}}\right)\tau = \left(\frac{K/k}{\mathfrak{P}}\right)^{\tau}.$$

e) Si L es un cuerpo intermedio y $\mathfrak{p}'$ es el primo de L divisible entre $\mathfrak{P}$, entonces

$$\left(\frac{K/L}{\mathfrak{P}}\right) = \left(\frac{K/k}{\mathfrak{P}}\right)^{f(\mathfrak{p}'/\mathfrak{p})}.$$

f) En las condiciones de e), si además la extensión L/k es de Galois, se cumple que

$$\left(\frac{K/k}{\mathfrak{P}}\right)\Big|_L = \left(\frac{L/k}{\mathfrak{p}'}\right)$$

y $\left(\frac{K/k}{\mathfrak{P}}\right) \in G(K/L)$ *si y sólo si $f(\mathfrak{p}'/\mathfrak{p}) = 1$.*

g) Si L es otra extensión finita separable de k, $\mathfrak{P}'$ es un primo en KL que divida a $\mathfrak{P}$ y $\mathfrak{p}'$ es el primo de L divisible entre $\mathfrak{P}'$, entonces KL/L es una extensión finita de Galois, $\mathfrak{P}'$ es no ramificado sobre $\mathfrak{p}'$ y

$$\left(\frac{KL/L}{\mathfrak{P}'}\right)\Big|_K = \left(\frac{K/k}{\mathfrak{P}}\right)^{f(\mathfrak{p}'/\mathfrak{p})}.$$

Demostración: a), b) Por la definición del símbolo de Frobenius.

c) Basta probar que si $\tau \in G(K/k)$ cumple $\tau(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}} \pmod{\mathfrak{P}}$ para todo $\alpha \in E$, entonces $\tau \in G_{\mathfrak{P}}$. Ahora bien, si $\alpha \in \mathfrak{P}$ entonces $\mathfrak{P} \mid \alpha$ y $\mathfrak{P} \mid \tau(\alpha) - \alpha^{\mathrm{N}\,\mathfrak{p}}$, luego $\mathfrak{P} \mid \tau(\alpha)$, es decir, $\tau(\mathfrak{P}) \subset \mathfrak{P}$, y por maximalidad $\tau(\mathfrak{P}) = \mathfrak{P}$.

d) En primer lugar, $e(\tau(\mathfrak{P})/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) = 1$, luego está definido $\left(\frac{K/k}{\tau(\mathfrak{P})}\right)$. Se cumple

$$\left(\frac{K/k}{\mathfrak{P}}\right)\left(\tau^{-1}(\alpha)\right) \equiv \tau^{-1}(\alpha)^{\mathrm{N}\,\mathfrak{p}} \text{ (mód } \mathfrak{P}),$$

luego aplicando τ queda

$$\left(\frac{K/k}{\mathfrak{P}}\right)^{\tau}(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}} \text{ (mód } \tau(\mathfrak{P})).$$

Concluimos aplicando c).

e) Por la transitividad del índice de ramificación tenemos que $e(\mathfrak{P}/\mathfrak{p}') = 1$. Así mismo es claro que $\mathrm{N}\,\mathfrak{p}' = (\mathrm{N}\,\mathfrak{p})^f$, donde $f = f(\mathfrak{p}', \mathfrak{p})$. Se cumple que

$$\left(\frac{K/k}{\mathfrak{P}}\right)^{f}(\alpha) \equiv \alpha^{(\mathrm{N}\,\mathfrak{p})^f} \text{ (mód } \mathfrak{P}),$$

para todo $\alpha \in E$, y basta aplicar c).

f) De nuevo por la transitividad se cumple $e(\mathfrak{p}'/\mathfrak{p}) = 1$. Tenemos que

$$\left(\frac{K/k}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}} \text{ (mód } \mathfrak{P}),$$

para todo $\alpha \in E$, luego en particular, si llamamos F a la clausura entera de D en L,

$$\left(\frac{K/k}{\mathfrak{P}}\right)\Big|_L(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}} \text{ (mód } \mathfrak{p}'),$$

para todo $\alpha \in F$, luego podemos aplicar c). Además

$$\left(\frac{K/k}{\mathfrak{P}}\right) \in G(K/L) \text{ si y sólo si } \left(\frac{K/k}{\mathfrak{P}}\right)\Big|_L = 1,$$

$$\text{si y sólo si } \left(\frac{L/k}{\mathfrak{p}'}\right) = 1, \text{ si y sólo si } f(\mathfrak{p}'/\mathfrak{p}) = 1,$$

pues $f(\mathfrak{p}'/\mathfrak{p})$ es el orden del símbolo de Frobenius.

g) Es un hecho conocido que en estas circunstancias la extensión KL/L es finita de Galois. Localizando en los primos involucrados y aplicando el teorema 2.35 concluimos que $\mathfrak{P}'$ es no ramificado sobre $\mathfrak{p}'$. Además $\mathrm{N}\,\mathfrak{p}' = (\mathrm{N}\,\mathfrak{p})^f$, donde $f = f(\mathfrak{p}'/\mathfrak{p})$.

Es claro que tanto $\left(\frac{KL/L}{\mathfrak{P}'}\right)\Big|_K$ como $\left(\frac{K/k}{\mathfrak{P}}\right)^{f(\mathfrak{p}'/\mathfrak{p})}$ dejan fijo a $\mathfrak{P}$ (es decir, están en el grupo de descomposición $G_{\mathfrak{P}}$). Sea F la clausura entera de D en KL. Entonces

$$\left(\frac{KL/L}{\mathfrak{P}'}\right)(\alpha) \equiv \alpha^{(\mathrm{N}\,\mathfrak{p})^f} \text{ (mód } \mathfrak{P}')$$

para todo $\alpha \in F$ y, en particular,

$$\left(\frac{KL/L}{\mathfrak{P}'}\right)\Big|_K (\alpha) \equiv \alpha^{(\mathrm{N}\,\mathfrak{p})^f} \equiv \left(\frac{K/k}{\mathfrak{P}}\right)^f (\alpha) \text{ (mód } \mathfrak{P})$$

para todo $\alpha \in E$, luego ambos automorfismos inducen el mismo automorfismo en $\overline{E}/\overline{D}$. Como la correspondencia es un isomorfismo, ha de ser

$$\left(\frac{KL/L}{\mathfrak{P}'}\right)\Big|_K = \left(\frac{K/k}{\mathfrak{P}}\right)^f.$$

■

4.2 El símbolo de Artin

Definición 4.3 Sea E/D una extensión abeliana de dominios de Dedekind con restos finitos. Sea K/k la extensión de los cuerpos de cocientes. Sea $\mathfrak{p}$ un primo de D cuyo índice de ramificación (sobre cualquiera de sus divisores en E) sea 1. En estas circunstancias el apartado d) del teorema anterior implica que el símbolo de Frobenius $\left(\frac{K/k}{\mathfrak{P}}\right)$ es el mismo automorfismo para cualquier divisor $\mathfrak{P}$ de $\mathfrak{p}$ en E. A este automorfismo lo llamaremos *símbolo de Artin,* y lo representaremos por

$$\left(\frac{K/k}{\mathfrak{p}}\right)$$

Sea Δ el discriminante de la extensión E/D (que es un ideal en D). Sea $I(\Delta)$ el grupo de los ideales fraccionales de D primos con Δ, es decir, los ideales fraccionales de la forma

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_\mathfrak{p}},$$

donde $\mathfrak{p}$ recorre los ideales primos de D que no dividen a Δ y los números $m_\mathfrak{p}$ son enteros y casi todos nulos.

Puesto que todos estos primos $\mathfrak{p}$ son no ramificados en E, podemos definir el símbolo de Artin del ideal fraccional $\mathfrak{a}$ como

$$\left(\frac{K/k}{\mathfrak{a}}\right) = \prod_{\mathfrak{p}} \left(\frac{K/k}{\mathfrak{p}}\right)^{m_\mathfrak{p}}.$$

(Observar que esto no tendría sentido si el grupo de Galois no fuera abeliano).

Así tenemos definido un homomorfismo de grupos $\omega : I(\Delta) \longrightarrow G(K/k)$, que recibe el nombre de *homomorfismo de Artin.*

Las propiedades del símbolo de Artin se deducen inmediatamente de las del símbolo de Frobenius.

Teorema 4.4 *Sea E/D una extensión abeliana de dominios de Dedekind con restos finitos. Sea K/k la extensión de sus cuerpos de cocientes y sea Δ el discriminante de la extensión.*

a) Si $\mathfrak{p} \in I(\Delta)$ *es un ideal primo, entonces el símbolo de Artin cumple*

$$\left(\frac{K/k}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}} \ (\text{mód } \mathfrak{p}),$$

para todo $\alpha \in E$*, y es el único* k*-automorfismo de* K *con esta propiedad. Su orden es el grado de inercia* f *de* $\mathfrak{p}$ *respecto a cualquiera de sus divisores en* E*.*

b) Si L *es un cuerpo intermedio y* $\mathfrak{a} \in I(\Delta)$*, entonces*

$$\left(\frac{L/k}{\mathfrak{a}}\right) = \left(\frac{K/k}{\mathfrak{a}}\right)\Big|_L.$$

c) Si L *es un cuerpo intermedio,* $\mathfrak{a}$ *es un ideal fraccional de* L *y* $\mathrm{N}(\mathfrak{a}) \in I(\Delta)$ *(donde* $\mathrm{N}(\mathfrak{a})$ *es la norma de la extensión* L/k*), entonces*

$$\left(\frac{K/L}{\mathfrak{a}}\right) = \left(\frac{K/k}{\mathrm{N}(\mathfrak{a})}\right)$$

d) Si L *es una extensión abeliana de* k*,* $\mathfrak{a}$ *es un ideal fraccional en* L *y* $\mathrm{N}(\mathfrak{a}) \in I(\Delta)$*, (donde* $\mathrm{N}(\mathfrak{a})$ *es la norma de la extensión* L/k*), entonces*

$$\left(\frac{KL/L}{\mathfrak{a}}\right)\Big|_K = \left(\frac{K/k}{\mathrm{N}(\mathfrak{a})}\right).$$

Demostración: a) Tenemos que $\mathfrak{p}$ se descompone en factores primos distintos en E (es decir, con multiplicidad 1), y cada uno de ellos divide a

$$\left(\frac{K/k}{\mathfrak{p}}\right)(\alpha) - \alpha^{\mathrm{N}\,\mathfrak{p}},$$

para todo $\alpha \in E$, luego su producto $\mathfrak{p}$ también divide a este elemento.

Si un automorfismo τ cumple $\tau(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}}$ (mód $\mathfrak{p}$) para todo $\alpha \in E$, en particular cumple $\tau(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}}$ (mód $\mathfrak{P}$), donde $\mathfrak{P}$ es cualquier divisor de $\mathfrak{p}$ en E, luego τ es el símbolo de Artin de $\mathfrak{p}$.

El orden del símbolo de Artin es f por 4.2 a).

b) Del teorema 4.2 f) se sigue que esta propiedad se cumple para ideales primos, luego por multiplicatividad es cierta para ideales fraccionales cualesquiera. Notar que si los primos que dividen a $\mathfrak{a}$ no se ramifican en K tampoco se ramifican en L.

c) es un caso particular de d).

d) La teoría de Galois nos da que la extensión KL/L es también abeliana y, usando el teorema 2.35, es fácil ver que los dos símbolos de Artin están definidos. Por la multiplicatividad basta probar el teorema para un ideal primo $\mathfrak{p}'$, pero este caso es consecuencia del teorema 4.2 g). Si llamamos $\mathfrak{P}'$ a un divisor de

$\mathfrak{p}'$ en KL, $\mathfrak{P}$ al primo de K divisible entre $\mathfrak{P}'$ y $\mathfrak{p}$ al primo de k divisible entre todos éstos, tenemos:

$$\left(\frac{KL/L}{\mathfrak{p}'}\right)\Big|_K = \left(\frac{KL/L}{\mathfrak{P}'}\right)\Big|_K = \left(\frac{K/k}{\mathfrak{P}}\right)^{f(\mathfrak{p}'/\mathfrak{p})} = \left(\frac{K/k}{\mathfrak{p}}\right)^{f(\mathfrak{p}'/\mathfrak{p})} = \left(\frac{K/k}{\mathrm{N}(\mathfrak{p}')}\right).$$

■

Veamos algunas aplicaciones del símbolo de Artin. Como primera muestra de la potencia de la teoría que tenemos ahora a nuestra disposición daremos una prueba sencilla y libre de cálculos de la irreducibilidad sobre $\mathbb{Q}$ del polinomio ciclotómico.

Observar que si ζ es una raíz m-sima primitiva de la unidad y $K = \mathbb{Q}(\zeta)$, entonces todo automorfismo $\sigma \in G(K/\mathbb{Q})$ ha de enviar a ζ a otra raíz primitiva, es decir, ha de ser $\sigma(\zeta) = \zeta^r$, para cierto entero r tal que $(r, m) = 1$. Además r está determinado módulo m y determina completamente a σ, luego la aplicación que a cada σ le asigna la clase de r módulo m es un monomorfismo del grupo de Galois $G(K/\mathbb{Q})$ en el grupo U_m de las unidades de $\mathbb{Z}/m\mathbb{Z}$.

La irreducibilidad del polinomio ciclotómico equivale a que el grado de la extensión $K/\mathbb{Q}$ sea $\phi(m)$, lo que a su vez equivale a que el monomorfismo que hemos descrito sea suprayectivo.

Esto es lo que prueba el teorema siguiente, donde el único hecho que se usa sobre K es que si r es un primo que no divide a m, entonces r no se ramifica en K. Esto se puede demostrar directamente como sigue: sea $f(x)$ el polinomio mínimo de ζ. Entonces tenemos que $f(x) \mid x^m - 1$, luego $f'(\zeta) \mid m\zeta^{m-1}$, y cualquier primo que se ramifique en K ha de dividir al diferente de K, que divide a $f'(\zeta)$, que divide a m.

Teorema 4.5 *Sea $m > 2$ un número natural, sea ζ una raíz m-sima primitiva de la unidad y sea $K = \mathbb{Q}(\zeta)$. Si r es un número natural primo con m entonces el símbolo de Artin de r viene determinado por*

$$\left(\frac{K/\mathbb{Q}}{r}\right)(\zeta) = \zeta^r.$$

Demostración: Por la multiplicatividad basta probar el teorema cuando r es primo. En general sabemos que la imagen de ζ ha de ser una raíz m-sima primitiva de la unidad, es decir,

$$\left(\frac{K/\mathbb{Q}}{r}\right)(\zeta) = \zeta^t, \qquad \text{con } (t, m) = 1.$$

Aplicando el teorema 4.4 a) se ha de cumplir $\zeta^t \equiv \zeta^r \pmod{r}$. Ahora bien, si $\mathfrak{r}$ es un primo de K que divida a r, esto implica que $\zeta^t \equiv \zeta^r \pmod{\mathfrak{r}}$, pero en el cuerpo $E/\mathfrak{r}$ el polinomio $x^m - 1$ tiene todas sus raíces distintas, pues su derivada es mx^{m-1}, que sólo se anula en 0, luego si ζ^t y ζ^r coinciden módulo $\mathfrak{r}$ es que son iguales, es decir,

$$\left(\frac{K/\mathbb{Q}}{r}\right)(\zeta) = \zeta^r.$$

■

Observar que el caso en que $2 \mid m$ pero no se ramifica no necesita ser considerado, pues esto ocurre cuando $m = 2m'$, con m' impar, pero entonces el cuerpo ciclotómico m-simo es el mismo que que el cuerpo ciclotómico m'-ésimo, ya que si ζ' es una raíz m'-ésima primitiva de la unidad, entonces $\zeta = -\zeta'$ es una raíz m-sima primitiva de la unidad. De todos modos, teniendo esto en cuenta es fácil ver que el símbolo de Artin de 2 viene dado por

$$\left(\frac{K/\mathbb{Q}}{2}\right)(\zeta) = -\left(\frac{K/\mathbb{Q}}{2}\right)(\zeta') = -\zeta'^2 = -\zeta^2 = \zeta^{m/2}\zeta^2 = \zeta^{(m+4)/2}.$$

El valor del símbolo de Artin se debe esencialmente a que el orden del símbolo de Artin de un primo coincide con su grado de inercia, y conocido el grado de inercia (de un primo no ramificado) conocemos completamente el modo en que factoriza. Veámoslo en la práctica en el caso de los cuerpos ciclotómicos. Es interesante comparar la prueba del teorema siguiente con la de [3.20].

Teorema 4.6 *Sea $m > 2$ un número natural y sea K el cuerpo ciclotómico m-simo sobre $\mathbb{Q}$.*

a) Sea p un primo que no divida a m, sea $f = \mathrm{o}_m(p)$ el orden de p módulo m y sea $r = \phi(m)/f$. Entonces la factorización de p en K es de la forma $p = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, donde todos los factores son distintos y el grado de inercia es f.

b) Sea $m = p^i m'$, con $(p, m') = 1$, sea $e = \phi(p^i)$, $f = \mathrm{o}_{m'}(p)$ y $r = \phi(m')/f$. Entonces la factorización de p en K es de la forma $p = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$, donde todos los factores son distintos y su grado de inercia es f.

Demostración: a) El grado de inercia de p es igual al orden de su símbolo de Artin, que es el automorfismo que corresponde con $[p]$ a través del isomorfismo entre el grupo de Galois y el grupo de unidades módulo m, luego dicho grado es $f = \mathrm{o}_m(p)$. El resto es obvio.

b) Supongamos que $p^i \neq 2$. El caso contrario se reduce al caso a) teniendo en cuenta que entonces K es también la extensión ciclotómica de orden m'.

Sea L la extensión ciclotómica de orden p^i y sea M la extensión ciclotómica de orden m'. Vimos en el capítulo anterior que $K = LM$. Sea $\mathfrak{P}$ un primo que divida a p en K y sean $\mathfrak{p}_1$, $\mathfrak{p}_2$ los primos de L y M respectivamente divisibles entre $\mathfrak{P}$.

Por el teorema 3.26 sabemos que $e(\mathfrak{p}_1/p) = \phi(p^i) = e$ y, como p no divide al discriminante de M, tenemos que $e(\mathfrak{p}_2/p) = 1$. Localizando y aplicando el teorema 2.35 concluimos que $e(\mathfrak{P}/\mathfrak{p}_1) = 1$, luego se cumple que $e(\mathfrak{P}/p) = \phi(p^i)$, como afirma el enunciado.

Así pues $e(\mathfrak{P}/\mathfrak{p}_2) = e$. Como $|K : M| = e$, necesariamente $f(\mathfrak{P}/\mathfrak{p}_2) = 1$, y por lo tanto $f(\mathfrak{P}/p) = f(\mathfrak{p}_2/p) = \mathrm{o}_{m'}(p)$ por a). El resto es obvio. ∎

Con esto la aritmética básica de los cuerpos ciclotómicos queda completamente determinada.

Ejemplo Ahora vamos a usar los símbolos de Artin para analizar la descomposición en primos en el cuerpo $K = \mathbb{Q}(\sqrt{5}, \sqrt{-5}\,)$ que estudiamos en el capítulo anterior. Se trata de una extensión finita de Galois cuyo grupo de Galois es de tipo $C_2 \times C_2$. El discriminante vale, según calculamos, $\Delta = 400$. Por lo tanto los únicos primos que se ramifican son 2 y 5.

Si p es cualquier otro primo, su comportamiento en K depende exclusivamente del orden de su símbolo de Artin: si es igual a 2 tendremos $f = 2$, luego $p = \mathfrak{p}_1\mathfrak{p}_2$, para ciertos primos $\mathfrak{p}_1$ y $\mathfrak{p}_2$ de K. Si el orden es 1 entonces $f = 1$, luego $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$.

De este modo, el comportamiento de un primo depende sólo de si su símbolo de Artin es o no la identidad. Para averiguarlo podemos calcular la restricción a los distintos cuerpos cuadráticos contenidos en K y razonar a la inversa: si un primo se escinde en un cuerpo cuadrático su símbolo de Artin es la identidad, y si se conserva es la conjugación.

El comportamiento de un primo en los cuerpos $\mathbb{Q}(\sqrt{5}\,)$, $\mathbb{Q}(\sqrt{-5}\,)$ y $\mathbb{Q}(i)$ depende de su resto módulo 5, 20 y 4 respectivamente, luego para contemplar todos los casos hemos de trabajar módulo 20. La tabla siguiente recoge todas las posibilidades:

p (mód 20)	$\sqrt{5}$	$\sqrt{-5}$	$\sqrt{-1}$
1, 9	+	+	+
3, 7	−	−	−
11, 19	+	−	−
13, 17	−	−	+

Un signo positivo indica que los primos congruentes con los números de la fila correspondiente se escinden en el cuerpo de la columna correspondiente, mientras que el signo negativo indica que se conservan. Equivalentemente, el símbolo de Artin es la identidad si el signo es + y la conjugación si el signo es − (por lo tanto la imagen de $\sqrt{d}$ por el símbolo de Artin es $\pm\sqrt{d}$ según el signo de la tabla). Omitimos las comprobaciones por ser de sobra conocidas (ver [Tabla 3.1]).

Esto determina completamente la factorización de los primos distintos de 2 y 5. Vemos que el símbolo de Artin sólo es la identidad sobre los primos congruentes con 1 y con 9 módulo 20, luego éstos son los que se escinden completamente en cuatro factores. Los restantes se escinden en dos factores. De aquí también se deduce la factorización en K de los primos de los tres cuerpos intermedios. Por ejemplo, un primo $p \equiv 11$ (mód 20) se descompone como $p = \mathfrak{p}_1\mathfrak{p}_2$ en $\mathbb{Q}(\sqrt{5}\,)$ y, como su descomposición en K es del mismo tipo, concluimos que cada $\mathfrak{p}_i$ se conserva primo en K.

Las factorizaciones de 2 y 5 pueden ser obtenidas comparando sus factorizaciones en los cuerpos $\mathbb{Q}(\sqrt{5}\,)$ y $\mathbb{Q}(\sqrt{-1}\,)$, teniendo en cuenta que sus discriminantes son primos entre sí. Concretamente se obtiene que $2 = \mathfrak{p}^2$ y $5 = (\mathfrak{p}_1\mathfrak{p}_2)^2$. Observar que ningún primo de $\mathbb{Z}$ se conserva primo en K. ∎

Ejemplo En el ejemplo anterior el símbolo de Artin nos ha permitido calcular las factorizaciones en un cuerpo mayor a partir de las factorizaciones en cuerpos menores. También es posible proceder en sentido contrario. Por ejemplo, sea K

el cuerpo ciclotómico de orden 13 y consideremos $k = K \cap \mathbb{R}$. Es claro que k es un cuerpo de grado 6 sobre $\mathbb{Q}$. La factorización de los primos en K depende de su resto módulo 13. Ésta es la tabla del orden de los restos módulo 13:

p (mód 13)	1	2	3	4	5	6	7	8	9	10	11	12
orden ($= f$)	1	12	3	6	4	12	12	4	3	6	12	2
r	12	1	4	2	3	1	1	3	4	2	1	6

La última fila es el número r de primos en que se descompone en K un primo racional cuyo resto módulo 13 sea el de la columna correspondiente.

La aplicación que a cada automorfismo de K le asigna su restricción a k es un epimorfismo de grupos cuyo núcleo es el único automorfismo de orden 2. Si un automorfismo tiene, por ejemplo, orden 6 eso significa que su cubo es el automorfismo de orden 2, luego la restricción a k de dicho cubo es la identidad, luego la restricción pasa a tener orden 3. En general, el orden de la restricción a k de un automorfismo de orden par es la mitad del orden del automorfismo de partida.

Si un automorfismo tiene orden impar, ninguna de sus potencias es el automorfismo de orden 2, luego las restricciones a k de estas potencias no son la identidad en k hasta que no llegamos a la identidad en K, es decir, el orden se conserva.

Concluimos que el orden del símbolo de Artin de un primo en k es la mitad del orden de su símbolo de Artin en K si este orden es par y el mismo si es impar. He aquí la tabla:

p (mód 13)	1	2	3	4	5	6	7	8	9	10	11	12
orden en K	1	12	3	6	4	12	12	4	3	6	12	2
orden en k	1	6	3	3	2	6	6	2	3	3	6	1
r (en k)	6	1	2	2	3	1	1	3	2	2	1	6

Por ejemplo, los primos racionales que se conservan primos en K son exactamente los congruentes con 2, 6, 7, 11 (mód 13). La tabla determina totalmente la factorización en k salvo por el primo 13, pero como 13 se ramifica totalmente en K ($f = 1$, $e = 12$) es claro que lo mismo le sucede en k. (Comparar con [3.22]). ∎

Reflexionemos sobre estos resultados: La forma en que un primo racional factoriza en la extensión ciclotómica m-sima depende únicamente de su resto módulo m. Sabemos que en los cuerpos cuadráticos el tipo de descomposición depende sólo del resto módulo el discriminante, en $\mathbb{Q}(\sqrt{5}, \sqrt{-5}\,)$ hay que considerar clases módulo 20 (mientras que el discriminante es 400) y en el último ejemplo la factorización depende de los restos módulo 13. ¿Podemos encontrar una relación entre estos fenómenos?

Ante todo notemos que el hecho de que la descomposición de los primos de una extensión dependa sólo del resto módulo un cierto número no es algo trivial. Por ejemplo, en el caso de los cuerpos cuadráticos es una consecuencia de la ley de reciprocidad cuadrática. Además hay cuerpos en los que no sucede nada parecido.

La clave del buen comportamiento de los ejemplos que hemos considerado está en el teorema siguiente:

Teorema 4.7 *Si k es un subcuerpo del cuerpo ciclotómico de grado m, entonces la descomposición en k de los primos racionales que no dividen a m depende sólo de su resto módulo m.*

DEMOSTRACIÓN: El discriminante de k divide al de la extensión ciclotómica m-sima, llamémosla K, luego los primos que no dividen a m son no ramificados en k. Si dos de ellos son congruentes módulo m entonces su símbolo de Artin en K es el mismo, luego también lo es su restricción a k, que es el símbolo de Artin en k, luego factorizan igual. ∎

Respecto al caso de los cuerpos cuadráticos, observemos que si p es primo y ζ es una raíz p-ésima primitiva de la unidad, entonces el cuerpo $\mathbb{Q}(\zeta)$ tiene grupo de Galois cíclico de orden $p-1$, luego contiene un único cuerpo cuadrático K. Como el discriminante de K ha de dividir al del cuerpo ciclotómico, que es potencia de p, ha de ser necesariamente $K = \mathbb{Q}(\sqrt{p})$ o bien $K = \mathbb{Q}(\sqrt{-p}\,)$. El signo es el que hace que $\pm p \equiv 1 \pmod 4$, pues con el signo contrario el discriminante de K sería $4p$. Ahora bien, como $\sqrt{-p} = i\sqrt{p}$, si $\mathbb{Q}(\zeta)$ contiene a uno de estos dos cuerpos cuadráticos, el otro está contenido en $\mathbb{Q}(\zeta, i)$, que es el cuerpo ciclotómico de orden $4p$. Más en general tenemos:

Teorema 4.8 *El cuerpo cuadrático de discriminante Δ está contenido en el cuerpo ciclotómico de orden $|\Delta|$.*

DEMOSTRACIÓN: Sea d un entero impar libre de cuadrados $d \equiv 1 \pmod 4$. Entonces podemos factorizarlo como $d = p_1 \cdots p_r$, donde los números p_i son primos impares con el signo adecuado para que sean congruentes con 1 módulo 4. Según la observación previa al teorema,

$$\mathbb{Q}(\sqrt{d}\,) = \mathbb{Q}(\sqrt{p_1}\,) \cdots \mathbb{Q}(\sqrt{p_r}\,) \subset \mathbb{Q}(\zeta),$$

donde ζ es una raíz de la unidad de orden $|d|$ (pues $\mathbb{Q}(\zeta)$ contiene a los cuerpos ciclotómicos de órdenes p_i). Como el discriminante de $\mathbb{Q}(\sqrt{d}\,)$ es d, el teorema está probado en este caso.

Para $-d$ el discriminante es $-4d$ y, por otro lado,

$$\mathbb{Q}(\sqrt{-d}\,) = \mathbb{Q}(\sqrt{d}, i) \subset \mathbb{Q}(\zeta, i),$$

y el último cuerpo es el cuerpo ciclotómico de orden $4d$, luego también se cumple el teorema.

Finalmente, el discriminante de $\mathbb{Q}(\sqrt{\pm 2d}\,)$ es $\pm 8d$ y, si $\omega = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\,i$, entonces es claro que $i, \sqrt{2} \in \mathbb{Q}(\omega)$, luego $\mathbb{Q}(\sqrt{\pm 2d}\,) = Q(\sqrt{d}, \sqrt{\pm 2}\,) \subset \mathbb{Q}(\zeta, \omega)$, y el último cuerpo es el cuerpo ciclotómico de orden $|8d|$. ∎

A la luz de este teorema, el hecho de que la factorización de un primo en un cuerpo cuadrático dependa sólo de su resto módulo el discriminante es un caso particular del teorema 4.7. Es razonable conjeturar que mediante el símbolo de

Artin podremos obtener las leyes de descomposición de los primos en cuerpos cuadráticos a partir de las leyes correspondientes para cuerpos ciclotómicos, pero las primeras son equivalentes a la ley de reciprocidad cuadrática, luego no debería ser difícil probar ésta última. El primero en observar que la ley de reciprocidad se deduce de las propiedades de factorización de los primos en los cuerpos ciclotómicos (de orden primo) fue Kronecker, alumno y amigo de Kummer. Por supuesto, la prueba que sigue dista mucho de ser la original.

La ley de reciprocidad cuadrática Nos apoyaremos en una de las leyes complementarias: $(-1/p) = (-1)^{(p-1)/2}$, cuya prueba es tan simple que no merece la pena abordarla desde un punto de vista abstracto (ver [12.3]).

En general, si K es un cuerpo cuadrático de discriminante Δ, su anillo de enteros es de la forma $E = \mathbb{Z}[\omega]$, donde el polinomio mínimo de ω tiene discriminante Δ. Si q es un primo impar que no divide a Δ y $\mathfrak{q}$ es un divisor de q en E, entonces $E/\mathfrak{q} = (\mathbb{Z}/(q))[\omega]$, luego q se escinde en K si y sólo si $[\omega] \in \mathbb{Z}/(q)$, si y sólo si el discriminante del polinomio mínimo de ω es un cuadrado en $\mathbb{Z}/(q)$, si y sólo si $(\Delta/q) = 1$.

Consideremos dos primos impares distintos p y q de modo que $p \equiv 1 \pmod 4$. Sea ζ una raíz p-ésima primitiva de la unidad. Según el teorema 4.8 tenemos que $\mathbb{Q}(\sqrt{p}\,) \subset \mathbb{Q}(\zeta)$. Según acabamos de ver

$$q \text{ se escinde en } \mathbb{Q}(\sqrt{p}\,) \Leftrightarrow \left(\frac{p}{q}\right) = 1$$

El grupo de Galois $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ es cíclico de orden $p-1$ y es isomorfo al grupo U_p de las unidades módulo p. El grupo $G(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{p}\,))$ es su único subgrupo de índice 2, que se corresponde con el único subgrupo de índice 2 de U_p, que es el núcleo del homomorfismo definido por el símbolo de Legendre $(\ /p)$. Es decir, el automorfismo de $\mathbb{Q}(\zeta)$ correspondiente a la clase $[q]$ fija a $\mathbb{Q}(\sqrt{p}\,)$ si y sólo si $(q/p) = 1$. Pero el automorfismo asociado a q es el símbolo de Artin de q, luego

$$\left(\frac{q}{p}\right) = 1 \Leftrightarrow \left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{q}\right) \in G\big(\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{p}\,)\big) \Leftrightarrow \left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{q}\right)\Big|_{\mathbb{Q}(\sqrt{p}\,)} = 1$$

$$\Leftrightarrow \left(\frac{\mathbb{Q}(\sqrt{p}\,)/\mathbb{Q}}{q}\right) = 1 \Leftrightarrow q \text{ se escinde en } \mathbb{Q}(\sqrt{p}\,) \Leftrightarrow \left(\frac{p}{q}\right) = 1.$$

Supongamos ahora que $p,\ q \equiv -1 \pmod 4$. Entonces $\mathbb{Q}(\sqrt{-p}) \subset Q(\zeta)$ y el razonamiento anterior es válido con la única variante de que q se escinde en $\mathbb{Q}(\sqrt{-p})$ si y sólo si $(-p/q) = (-1/q)(p/q) = 1$, o sea, si y sólo si $(p/q) = -1$.

También podemos probar la fórmula para $(2/p)$. El razonamiento anterior nos lleva a que si $p \equiv 1 \pmod 4$ entonces $(2/p) = 1$ si y sólo si 2 se escinde en $\mathbb{Q}(\sqrt{p}\,)$, lo que equivale a que el polinomio $x^2 - x + (p-1)/4$ tenga sus raíces en $\mathbb{Z}/(2)$, lo que a su vez equivale a que $2 \mid (p-1)/4$, o sea, a que $p \equiv 1 \pmod 8$. Si $p \equiv -1 \pmod 4$ razonamos con $-p$ y llegamos a que $(2/p) = 1$ si y sólo si 2 se escinde en $\mathbb{Q}(\sqrt{-p})$, lo que nos lleva análogamente a que $-p \equiv 1 \pmod 8$.

En resumen tenemos que $(2/p) = 1$ si y sólo si $p \equiv \pm 1$ (mód 8). ∎

Ahora vemos que la razón por la que la descomposición de los primos racionales en $K = \mathbb{Q}(\sqrt{5}, \sqrt{-5}\,)$ depende de su resto módulo 20 es que $K = \mathbb{Q}(\sqrt{5}, i)$ está contenido en el cuerpo ciclotómico de orden 20.

Kronecker conjeturó que toda extensión abeliana de $\mathbb{Q}$ está contenida en un cuerpo ciclotómico, lo que implica que, en cualquiera de ellas, la factorización de los primos depende sólo de su resto módulo un entero fijo. La conjetura es correcta, si bien no es nada fácil de probar y aún no estamos en condiciones de hacerlo, pero conviene tenerla presente porque explica la razón por la que los cuerpos ciclotómicos van a tener tanta importancia en la teoría que estamos desarrollando.

Ejemplo Ahora calcularemos el grupo de inercia y el grupo de descomposición de un primo en una cierta extensión. Por ejemplo, sea K el cuerpo ciclotómico de orden 40 y el primo racional $p = 5$. Como el orden de 5 módulo 8 es 2, el teorema 4.6 nos da la factorización $5 = (\mathfrak{pq})^4$.

El grado de la extensión es $n = 16$, el índice de ramificación es $e = 4$ y el grado de inercia es $f = 2$. El grupo de descomposición de p tendrá orden $ef = 8$ y fijará a un cuerpo F de grado 2 sobre $\mathbb{Q}$.

El teorema 1.38 nos dice que la descomposición de 5 en F será de la forma $5 = \mathfrak{p}'\mathfrak{q}'$. De hecho, si encontramos un cuerpo F' en el que 5 factorice de este modo podemos asegurar que la factorización de $\mathfrak{p}'$ en K será de la forma $\mathfrak{p}' = \mathfrak{p}^4$, pues no pueden aparecer más primos y el índice de ramificación ha de ser 4. El teorema 1.41 nos garantiza que $F \subset F'$ y, si además F' tiene grado 2 sobre $\mathbb{Q}$, tendremos la igualdad.

Ahora bien, conocemos un cuerpo intermedio donde 5 factoriza de este modo: el cuerpo ciclotómico de orden 8, llamémoslo K_8. Así pues, $F \subset K_8$.

El teorema 4.6 nos da que en K_8 las constantes de 5 son $e = 1$, $f = 2$, luego ciertamente tenemos $5 = \mathfrak{p}'\mathfrak{q}'$ y el grupo de descomposición de $\mathfrak{p}'$ tendrá orden 2 y fijará a un cuerpo de grado 2 sobre $\mathbb{Q}$ en el que 5 se descompondrá también en dos factores. Por lo tanto el cuerpo que buscamos es precisamente el cuerpo de descomposición de $\mathfrak{p}'$ en K_8.

Como 5 es no ramificado en K_8, sabemos que el grupo de descomposición de $\mathfrak{p}'$ está generado por el símbolo de Artin de 5, que es el automorfismo σ dado por $\sigma(\zeta) = \zeta^5$ (donde ζ es una raíz octava primitiva de la unidad). Si tomamos por ejemplo $z = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\,i$ se ve claramente que $K_8 = \mathbb{Q}(\sqrt{2}, i)$ (una inclusión es obvia y los grados coinciden). Además $\sqrt{2} = \zeta + \zeta^7$, $i = \zeta^2$, lo que nos permite calcular $\sigma(\sqrt{2}) = -\sqrt{2}$ y $\sigma(i) = i$.

Ahora es claro que el cuerpo fijado por σ es $F = \mathbb{Q}(i)$ y éste es el cuerpo de descomposición de 5 en K.

Obviamente, podríamos haber pensado directamente en $\mathbb{Q}(i)$ y nos habríamos ahorrado pasar por K_8, pero de todos modos necesitamos las consideraciones anteriores para calcular el grupo de descomposición.

Claramente se trata de la imagen de $G(K_5/\mathbb{Q})\times\langle\sigma\rangle$ a través del isomorfismo $G(K_5/\mathbb{Q})\times G(K_8/\mathbb{Q})\cong G(K_{40}/\mathbb{Q})$ o, usando la representación en términos de clases de enteros, la imagen de $U_5\times\langle[5]\rangle$ a través del isomorfismo $U_5\times U_8\cong U_{40}$. Teniendo en cuenta que $U_5=\langle[2]\rangle$, Esta imagen es el grupo $G_5=\langle[17],[21]\rangle$.

Ahora calcularemos el cuerpo de inercia de 5. Llamémoslo Z. Sabemos que Z tiene grado 4 sobre $\mathbb{Q}$, contiene a F y las constantes de 5 para $Z/\mathbb{Q}$ son $e=1$, $f=2$. De hecho Z es el único cuerpo que cumple esto, ya que en estas condiciones, si $\mathfrak{p}$ es un divisor de 5 en Z, su grado de inercia en K/Z es $f=1$, luego todo automorfismo de $G(K/Z)$ induce la identidad en el cuerpo de restos $\overline{K}$ (induce un automorfismo que fija a $\overline{Z}=\overline{K}$), luego $G(K/Z)$ está contenido en el grupo de inercia y, al tener el mismo orden, ambos grupos coinciden.

Como K_8 cumple estas condiciones concluimos que es el cuerpo de inercia buscado y el grupo es la imagen de $U_5\times 1$ por el isomorfismo $U_5\times U_8\cong U_{40}$, que es el grupo generado por [15].

La tabla siguiente resume lo que hemos obtenido:

	$\mathbb{Q}$	$F=\mathbb{Q}(i)$	$Z=\mathbb{Q}(\sqrt{2},i)$	K
Factorización	5	$\mathfrak{p}'\mathfrak{q}'$	$\mathfrak{p}''\mathfrak{q}''$	$(\mathfrak{pq})^4$
Grado	1	2	4	16
e (sobre $\mathbb{Q}$)	1	1	1	4
f (sobre $\mathbb{Q}$)	1	1	2	2

Tenemos así una ilustración de la situación descrita por el teorema 1.38. ∎

4.3 El homomorfismo de Artin

Terminamos el capítulo con algunos comentarios sobre los objetivos que nos proponemos perseguir. Nuestra meta a medio plazo será estudiar las propiedades del homomorfismo de Artin

$$\omega : I(\Delta) \longrightarrow G(K/k).$$

En particular determinaremos su núcleo y su imagen. Concretamente resulta que el homomorfismo de Artin es siempre suprayectivo, pero esto no es fácil de probar, y constituye uno de los resultados básicos de la teoría de cuerpos de clases. De las propiedades del homomorfismo de Artin deduciremos muchos resultados importantes sobre la aritmética de los cuerpos numéricos.

Ejercicio: Admitiendo la suprayectividad de ω, probar que una extensión abeliana de dominios de Dedekind contiene primos que se conservan si y sólo si su grupo de Galois es cíclico.

La estructura del núcleo es más complicada. Es claro que un primo $\mathfrak{p}$ está en el núcleo de ω si y sólo si $f=1$, o sea, si $\mathfrak{p}$ se escinde completamente en K. Otra observación de interés es que si $\mathfrak{q}$ es un primo en k y $\mathfrak{P}$ es uno de sus divisores en K, entonces por definición de norma $\mathrm{N}(\mathfrak{P})=\mathfrak{p}^f$, donde $f=f(\mathfrak{P}/\mathfrak{p})$, pero f

es precisamente el orden del símbolo de Artin de $\mathfrak{p}$, luego $\omega\big(\mathrm{N}(\mathfrak{P})\big) = 1$. De la multiplicatividad de la norma se sigue que si $\mathfrak{a}$ es cualquier ideal fraccional de K tal que $\mathrm{N}(\mathfrak{a}) \in I(\Delta)$ se cumple $\omega\big(\mathrm{N}(\mathfrak{a})\big) = 1$.

Definición 4.9 Si E/D es una extensión de dominios de Dedekind de discriminante Δ, llamaremos *grupo de normas* $\mathrm{N}(\Delta)$ al grupo de las normas $\mathrm{N}(\mathfrak{a})$, donde $\mathfrak{a}$ es un ideal fraccional de E tal que $\mathrm{N}(\mathfrak{a}) \in I(\Delta)$.

Acabamos de probar el teorema siguiente:

Teorema 4.10 *Sea K/k una extensión abeliana de cuerpos numéricos de discriminante Δ. Entonces el grupo de normas $\mathrm{N}(\Delta)$ está contenido en el núcleo del homomorfismo de Artin.*

Más aún, un primo $\mathfrak{p} \nmid \Delta$ está en el núcleo de ω si y sólo si $f = 1$, si y sólo si $\mathrm{N}(\mathfrak{P}) = \mathfrak{p}$ (donde $\mathfrak{P}$ es cualquiera de sus divisores primos en K) si y sólo si $\mathfrak{p} \in \mathrm{N}(\Delta)$. De momento no podemos decir más. Observar que no podemos afirmar que el núcleo de ω esté generado por los primos que contenga.

Capítulo V

Similitud de ideales

Nos ocupamos ahora del concepto de similitud de ideales y grupo de clases, cuya utilidad es bien conocida. Recordemos que en un cuerpo numérico arbitrario tenemos definido el grupo de clases [4.15] y los grupos de clases de sus órdenes no maximales [4.16]. En los cuerpos cuadráticos tenemos además la distinción entre grupos de clases estrictas y no estrictas. Aquí definiremos una familia mucho más amplia de grupos abelianos finitos asociados a un cuerpo numérico dado, a los que llamaremos grupos de clases, y que contendrán a todos estos ejemplos como casos particulares. La teoría de cuerpos de clases confiere un significado muy profundo a estos grupos, pues probaremos que si K/k es una extensión abeliana de cuerpos numéricos con discriminante Δ y N es el núcleo del homomorfismo de Artin $\omega : I(\Delta) \longrightarrow G(K/k)$ (que, según anticipamos al final del capítulo anterior, es suprayectivo), entonces el cociente $I(\Delta)/N$ será uno de los grupos de clases de k, isomorfo, por consiguiente, al grupo de Galois de la extensión. Más aún, esta correspondencia que a cada extensión abeliana de k le asigna un grupo de clases es esencialmente biyectiva, con lo que los grupos de clases representan los grupos de Galois de las extensiones abelianas del cuerpo k. Estos hechos conectan íntimamente la aritmética de k con sus extensiones abelianas, pues los grupos de clases se definen estrictamente en términos de la aritmética ideal del cuerpo, generalizada levemente para que intervengan los primos infinitos.

De momento no estamos en condiciones de probar estos hechos. Simplemente introduciremos y estudiaremos los grupos de clases de un cuerpo numérico.

5.1 Divisores

Acabamos de comentar que los grupos de clases de un cuerpo numérico se definen en términos de su aritmética ideal, pero hemos de extender el concepto de ideal para admitir factores primos infinitos. Ello nos lleva al concepto de divisor. La definición siguiente es la que cabría esperar salvo por ciertas restricciones que imponemos arbitrariamente a presencia de divisores primos infinitos en las factorizaciones de los divisores. Enseguida las justificaremos.

Definición 5.1 Sea k un cuerpo numérico. Un *divisor* de k es una aplicación $\mathfrak{m}$ que asigna a cada divisor primo $\mathfrak{p}$ de K le asigna un número natural $\mathfrak{m}_\mathfrak{p}$, de tal modo que

a) $\mathfrak{m}_\mathfrak{p} = 0$ para todos los divisores primos de k salvo un número finito de ellos.

b) $\mathfrak{m}_\mathfrak{p} = 0$ para todo primo arquimediano complejo.

c) $\mathfrak{m}_\mathfrak{p} \leq 1$ para todo primo arquimediano real.

Definimos el producto de dos divisores $\mathfrak{m}$ y $\mathfrak{n}$ como el divisor que cumple

a) $(\mathfrak{mn})_\mathfrak{p} = \mathfrak{m}_\mathfrak{p} + \mathfrak{n}_\mathfrak{p}$ para todo primo no arquimediano de K

b) $(\mathfrak{mn})_\mathfrak{p} = \text{máx}\{\mathfrak{m}_\mathfrak{p}, \mathfrak{n}_\mathfrak{p}\}$ para todo primo arquimediano de K.

Claramente este producto es asociativo y conmutativo, y tiene por elemento neutro al divisor 1 dado por $1_\mathfrak{p} = 0$ para todo divisor primo $\mathfrak{p}$.

Si identificamos cada divisor primo $\mathfrak{p}$ (que no sea arquimediano y complejo) con el divisor que cumple

$$\mathfrak{m}_\mathfrak{q} = \begin{cases} 1 & \text{si } \mathfrak{q} = \mathfrak{p}, \\ 0 & \text{si } \mathfrak{q} \neq \mathfrak{p}, \end{cases}$$

tenemos que cada divisor $\mathfrak{m} \neq 1$ se expresa como producto de divisores primos $\mathfrak{m} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, y la expresión es única salvo el orden si exigimos además que todos los exponentes sean no nulos y que los primos reales aparezcan con exponente 1. Observar que si $\mathfrak{p}$ es un primo infinito real, se cumple $\mathfrak{pp} = \mathfrak{p}$.

También podemos identificar de forma natural cada ideal de k con un divisor. Si k tiene s primos arquimedianos reales $\infty_1, \ldots, \infty_s$, todo divisor de k se expresa de forma única salvo el orden como

$$\mathfrak{m} = \mathfrak{m}_f \infty_1^{e_1} \cdots \infty_s^{e_s},$$

donde $\mathfrak{m}_f$ es un ideal de k, al que llamaremos *parte finita* de $\mathfrak{m}$, y los exponentes e_i son todos 0 o 1.

Finalmente, identificaremos todos los primos arquimedianos complejos de k con el divisor 1, con lo que admitiremos que tales divisores aparezcan también como factores.

Si K/k es una extensión de cuerpos numéricos podemos identificar a los divisores primos de k con parte de los divisores de K, y a partir de aquí podemos considerar a todo divisor de k como divisor de K.

Por ejemplo, si K es un cuerpo cuadrático real con dos divisores primos infinitos ∞_1, ∞_2, entonces el divisor primo ∞ de $\mathbb{Q}$ se identifica con el divisor de K (que ya no es primo) $\infty = \infty_1\infty_2$. Si K es imaginario, entonces $\infty = 1$ en K, aunque $\infty \neq 1$ en $\mathbb{Q}$.

Tiene sentido hablar de divisibilidad entre divisores. Es obvio que todo par de divisores de k tiene un único máximo común divisor y un único mínimo

común múltiplo. Dos divisores son primos entre sí si no son divisibles entre un mismo primo (finito o infinito real).

La razón por la que hemos introducido los divisores primos infinitos es que ciertas definiciones de la teoría de cuerpos de clases (entre ellas la de grupo de clases) se expresan de forma natural si definimos adecuadamente la congruencia módulo un divisor primo real. Sin embargo, la congruencia módulo una potencia de un primo real o módulo un primo complejo carece de significado. Por ello no hemos admitido que en las factorizaciones de los divisores aparezcan divisores complejos o potencias de divisores reales.

Definición 5.2 Sea k un cuerpo numérico y $\mathfrak{p}$ un divisor primo arquimediano real de k. Sea $\sigma : k \longrightarrow \mathbb{R}$ su monomorfismo asociado. Si $\alpha,\ \beta \in k \setminus \{0\}$ definimos

$$\alpha \equiv^* \beta \ (\text{mód } \mathfrak{p}) \quad \text{si y sólo si} \quad \sigma(\alpha/\beta) > 0,$$

y en tal caso diremos que α y β son *congruentes* módulo $\mathfrak{p}$.

Claramente esta relación es reflexiva, simétrica y transitiva y determina dos clases de equivalencia en k (con representantes 1 y -1). El asterisco $(*)$ indica que la congruencia es compatible con el producto de k, pero no con la suma. Si alguna vez conviene y no hay confusión, lo omitiremos.

Por ejemplo, dos números racionales son congruentes módulo ∞ si y sólo si tienen el mismo signo. Como ya hemos comentado, la congruencia módulo un primo complejo no tiene ningún significado. En todo caso, cuando $\mathfrak{p}$ es un primo complejo podemos definir $\alpha \equiv^* \beta$ (mód $\mathfrak{p}$) como una afirmación siempre verdadera.

Si D es el anillo de enteros de k, diremos que dos números $\alpha,\ \beta \in D$ no nulos son *congruentes* módulo un divisor $\mathfrak{m}$ (en signos $\alpha \equiv^* \beta$ (mód $\mathfrak{m}$)) si y sólo si α y β son congruentes módulo la parte finita de $\mathfrak{m}$ y módulo cada primo infinito que divide a $\mathfrak{m}$. Obviamente la congruencia módulo un divisor es una relación de equivalencia en $D \setminus \{0\}$ compatible con el producto (es decir, si $\alpha \equiv^* \beta$ (mód $\mathfrak{m}$) y $\gamma \equiv^* \delta$ (mód $\mathfrak{m}$), entonces $\alpha\gamma \equiv^* \beta\delta$ (mód $\mathfrak{m}$)).

Ejemplo La clase de congruencia de 3 módulo el divisor $5\,\infty$ está formada por los números $\{3, 8, 13, 18, \dots\}$, mientras que la clase de congruencia módulo 5 contiene también a los enteros negativos $-2, -7, -12, \dots$ Notar que la clase de 5 módulo 5 en este sentido no coincide completamente con la clase usual, porque no contiene al 0. ∎

El hecho de que la congruencia módulo un divisor $\mathfrak{m}$ no sea en general compatible con la suma hace que no podamos definir un anillo cociente $D/\mathfrak{m}$, pero sí es posible definir un grupo multiplicativo que, en el caso en que $\mathfrak{m}$ sea un ideal, no es sino el grupo de unidades $(D/\mathfrak{m})^*$ del anillo cociente.

Definición 5.3 Sea k un cuerpo numérico, sea D su anillo de enteros y sea $\mathfrak{m}$ un divisor de k. Llamamos *grupo numérico* módulo $\mathfrak{m}$ al conjunto

$$k(\mathfrak{m}) = \{\alpha/\beta \mid \alpha, \beta \in D \setminus \{0\},\ (\mathfrak{m}, \alpha\beta) = 1\}.$$

Claramente se trata de un subgrupo de $k^* = k \setminus \{0\} = k_1$. El máximo común divisor $(\mathfrak{m}, \alpha\beta)$ se ha de entender como un máximo común divisor entre divisores de k, lo que supone identificar el número $\alpha\beta$ con el ideal que genera. Como un elemento de D nunca puede tener divisores infinitos, es claro que $k(\mathfrak{m})$ depende sólo de la parte finita de $\mathfrak{m}$.

Es fácil ver que $D \cap k(\mathfrak{m})$ es el conjunto de elementos de $D \setminus \{0\}$ primos con $\mathfrak{m}$. Así, si $\alpha \in D \cap k(\mathfrak{m})$ entonces $(\alpha) + \mathfrak{m}_f = 1$, luego existe un $\beta \in D$ tal que $\alpha\beta \equiv 1 \pmod{\mathfrak{m}_f}$. Llamando $x = \alpha\beta^2 \in D$ se cumple igualmente

$$\alpha x = \alpha^2\beta^2 \equiv 1 \pmod{\mathfrak{m}_f}$$

y además αx es congruente con 1 módulo cualquier divisor primo infinito (real), pues $\alpha x/1$ es un cuadrado, luego su imagen por cualquier monomorfismo real es positiva. En conclusión, $\alpha x \equiv^* 1 \pmod{\mathfrak{m}}$.

De aquí se sigue que si α, β, γ, $\delta \in D \cap k(\mathfrak{m})$, $\alpha/\beta = \gamma/\delta$ y $\alpha \equiv^* \beta \pmod{\mathfrak{m}}$, entonces también $\gamma \equiv^* \delta \pmod{\mathfrak{m}}$. En efecto, según hemos probado, existe un $x \in D$ tal que $\alpha x \equiv^* 1 \pmod{\mathfrak{m}}$, luego

$$\delta \equiv^* x\alpha\delta = x\beta\gamma \equiv^* x\alpha\gamma \equiv^* \gamma \pmod{\mathfrak{m}}.$$

Esto nos permite extender la congruencia módulo $\mathfrak{m}$ a todo el grupo $k(\mathfrak{m})$. Para ello definimos el *grupo numérico unitario* módulo $\mathfrak{m}$ como

$$k_{\mathfrak{m}} = \{\alpha/\beta \mid \alpha, \beta \in D \setminus \{0\},\ (\mathfrak{m}, \alpha\beta) = 1,\ \alpha \equiv^* \beta \pmod{\mathfrak{m}}\},$$

que es un subgrupo de $k(\mathfrak{m})$.

Lo que hemos probado es que si α, $\beta \in D \cap k(\mathfrak{m})$, entonces

$$\alpha \equiv \beta \pmod{k_{\mathfrak{m}}} \Leftrightarrow \frac{\alpha}{\beta} \in k_{\mathfrak{m}} \Leftrightarrow \alpha \equiv^* \beta \pmod{\mathfrak{m}}.$$

En lo sucesivo, si x, $y \in k(\mathfrak{m})$, representaremos por $x \equiv^* y \pmod{\mathfrak{m}}$ a la congruencia módulo el subgrupo $k_{\mathfrak{m}}$. Acabamos de ver que esta definición es consistente con la que ya teníamos, con la ventaja de que ahora es una congruencia en el sentido usual de la teoría de grupos. En estos términos, trivialmente

$$k_{\mathfrak{m}} = \{x \in k(\mathfrak{m}) \mid x \equiv^* 1 \pmod{\mathfrak{m}}\}.$$

Como regla mnemotécnica establecemos que una notación del tipo $X(\mathfrak{m})$ siempre indicará "elementos primos con $\mathfrak{m}$", mientras que una notación del tipo $X_{\mathfrak{m}}$ hará referencia a "elementos $\equiv^* 1 \pmod{\mathfrak{m}}$".

Ahora estamos en condiciones de describir los cocientes determinados por las congruencias:

Teorema 5.4 *Sea k un cuerpo numérico, D su anillo de enteros y $\mathfrak{m}$ un divisor de k. Entonces*

$$k(\mathfrak{m})/k_{\mathfrak{m}} \cong \prod_{\mathfrak{p}|\mathfrak{m}_f} (D_{\mathfrak{p}}/\mathfrak{p}^{\mathfrak{m}_{\mathfrak{p}}})^* \times \prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ \mathfrak{p}\ \textit{real}}} k^*/k_{\mathfrak{p}} \cong (D/\mathfrak{m}_f)^* \times \prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ \mathfrak{p}\ \textit{real}}} k^*/k_{\mathfrak{p}}$$

DEMOSTRACIÓN: Notar que todo elemento de $k(\mathfrak{m})$ es una unidad del anillo local $D_\mathfrak{p}$, para todo primo $\mathfrak{p} \mid \mathfrak{m}_f$, luego también del cociente $D_\mathfrak{p}/\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}$. Por lo tanto está bien definida la aplicación que a cada elemento de $k(\mathfrak{m})$ le hace corresponder la n-tupla de sus clases en cada grupo $(D_\mathfrak{p}/\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}})^*$ y en $k^*/k_\mathfrak{p}$ si $\mathfrak{p}$ es real. También es claro que esta aplicación es un homomorfismo de grupos. Su núcleo es $k_\mathfrak{m}$ y el teorema de aproximación implica que es suprayectivo. Esto nos da el primer isomorfismo.

Para el segundo observamos que cada anillo $D_\mathfrak{p}/\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}$ es isomorfo a $D/\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}$, luego también son isomorfos sus grupos de unidades, o sea,

$$(D_\mathfrak{p}/\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}})^* \cong (D/\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}})^*.$$

La aplicación que a cada elemento de D le asigna sus clases en $D/\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}})$ es un homomorfismo de anillos cuyo núcleo es el ideal $\mathfrak{m}_f$, y es suprayectivo por el teorema chino del resto (o bien porque ambos anillos tienen el mismo número de elementos). Por lo tanto el producto de los grupos de unidades $(D/\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}})^*$, que es el grupo de unidades del producto, es isomorfo a $(D/\mathfrak{m}_f)^*$. ∎

Definición 5.5 Sea k un cuerpo numérico. Llamaremos *función de Euler* generalizada de k a la función que a cada divisor $\mathfrak{m}$ de k le hace corresponder el cardinal de su grupo cociente

$$\Phi(\mathfrak{m}) = |k(\mathfrak{m})/k_\mathfrak{m}|.$$

El teorema anterior muestra que Φ es multiplicativa, es decir, si $(\mathfrak{m}, \mathfrak{n}) = 1$, entonces $\Phi(\mathfrak{mn}) = \Phi(\mathfrak{m})\Phi(\mathfrak{n})$.

Si $\mathfrak{p}$ es un primo real es claro que $\Phi(\mathfrak{p}) = 2$, pues $k(\mathfrak{p}) = k \setminus \{0\}$ y

$$k_\mathfrak{p} = \{\alpha \in k \setminus \{0\} \mid \sigma(\alpha) > 0\},$$

donde $\sigma : k \longrightarrow \mathbb{R}$ es el monomorfismo que determina a $\mathfrak{p}$, luego el cociente se reduce a $k(\mathfrak{p})/k_\mathfrak{p} = \big\{[\pm 1]\big\}$.

También por el teorema anterior, si $\mathfrak{m}$ es un ideal del anillo de enteros D de k, entonces $\Phi(\mathfrak{m}) = |(D/\mathfrak{m})^*|$, luego la función Φ que acabamos de definir extiende a la definida en [3.23] y sobre ideales puede calcularse mediante el teorema [3.24].

Terminamos la sección enunciando un resultado técnico sobre los grupos $k(\mathfrak{m})$, consecuencia inmediata de [3.7].

Teorema 5.6 *Sea k un cuerpo numérico, D su anillo de enteros y $\mathfrak{m}$ un divisor de k. Sean α, $\beta \in k \setminus \{0\}$. Entonces $\alpha/\beta \in k(\mathfrak{m})$ si y sólo si $v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(\beta)$ para todo primo $\mathfrak{p} \mid \mathfrak{m}_f$.*

5.2 Clases de ideales

Definición 5.7 Sea k un cuerpo numérico, sea D su anillo de enteros y sea $\mathfrak{m}$ un divisor de k. Llamaremos *grupo de ideales* módulo $\mathfrak{m}$ al grupo $I(\mathfrak{m})$ de los

ideales fraccionales de D primos con $\mathfrak{m}$ (es decir, ideales fraccionales de la forma $\mathfrak{a}/\mathfrak{b}$, donde $\mathfrak{a}$ y $\mathfrak{b}$ son ideales que cumplen $(\mathfrak{ab},\mathfrak{m})=1$). En particular $I=I(1)$ es el grupo de todos los ideales fraccionales. Obviamente $I(\mathfrak{m})$ sólo depende de la parte finita del divisor $\mathfrak{m}$.

Definimos el *grupo unitario* de ideales módulo $\mathfrak{m}$ como

$$P_{\mathfrak{m}}=\{(\alpha)/(\beta)\mid \alpha/\beta\in k_{\mathfrak{m}}\},$$

que claramente es un subgrupo de $I(\mathfrak{m})$. El particular $P=P_1$ es el grupo generado por los ideales principales de D.

El *grupo de clases* de k módulo $\mathfrak{m}$ es el grupo cociente $H(\mathfrak{m})=I(\mathfrak{m})/P_{\mathfrak{m}}$. La relación de congruencia módulo $P_{\mathfrak{m}}$ se llama *similitud* módulo $\mathfrak{m}$.

En particular $H=H(1)$ es el grupo de clases usual ([4.15]), que —como ya sabemos— es finito. Seguidamente demostramos que todos los grupos de clases son finitos.

Llamaremos *número de clases* módulo $\mathfrak{m}$ al orden $h_{\mathfrak{m}}$ del grupo $H(\mathfrak{m})$. En particular h_1 será el número de clases de k en el sentido usual.

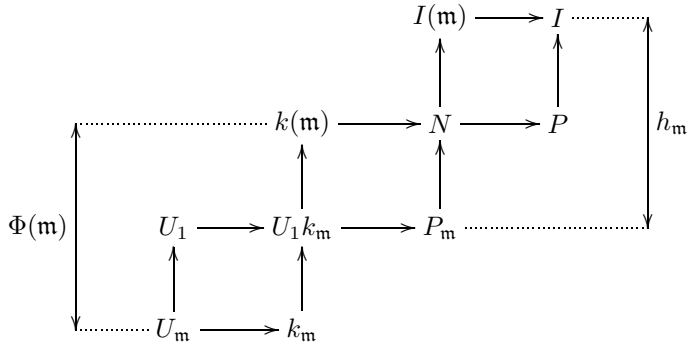
Teorema 5.8 *Sea k un cuerpo numérico, sea D su anillo de enteros y $\mathfrak{m}$ un divisor de k. Sea U_1 el grupo de las unidades de D y*

$$U_{\mathfrak{m}}=\{\epsilon\in U_1\mid \epsilon\equiv^* 1\ (\text{mód }\mathfrak{m})\}.$$

Entonces el índice $|U_1:U_{\mathfrak{m}}|$ divide a $\Phi(\mathfrak{m})$ y

$$h_{\mathfrak{m}}=\frac{\Phi(\mathfrak{m})}{|U_1:U_{\mathfrak{m}}|}\,h_1.$$

Demostración: El esquema siguiente resume la prueba:



En primer lugar consideramos la aplicación de $I(\mathfrak{m})$ en $H=I/P$ que a cada ideal fraccional le hace corresponder su clase. Veamos que es suprayectiva. Sean $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ los divisores primos de $\mathfrak{m}_f$. Fijemos $\rho_i\in\mathfrak{p}_i\setminus\mathfrak{p}_i^2$. Por el teorema chino del resto existe un entero π_i tal que

$$\pi_i\equiv\rho_i\ (\text{mód }\mathfrak{p}_i^2),\qquad \pi_i\equiv 1\ (\text{mód }\mathfrak{p}_j)\quad \text{para } j\neq i.$$

Es claro entonces que

$$v_{\mathfrak{p}_j}(\pi_i) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Si $\mathfrak{a} \in I$, es claro que multiplicando o dividiendo adecuadamente los π_i podemos formar un $\alpha \in k^*$ tal que $v_{\mathfrak{p}_i}(\alpha) = v_{\mathfrak{p}_i}(\mathfrak{a})$, para $i = 1, \ldots, r$. Consecuentemente el ideal fraccional $\alpha^{-1}\mathfrak{a}$ está en $I(\mathfrak{m})$ y su clase módulo P es la misma que la de α.

Tenemos así un epimorfismo $I(\mathfrak{m}) \longrightarrow I/P$, cuyo núcleo es $N = I(\mathfrak{m}) \cap P$. Un ideal fraccional está en N si y sólo si se expresa como $\mathfrak{a}/\mathfrak{b} = (\alpha)/(\beta)$, con $(\mathfrak{ab}, \mathfrak{m}) = 1$, pero esto equivale a que $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\beta)$ para todo $\mathfrak{p} \mid \mathfrak{m}_f$, y por el teorema 5.6 concluimos que

$$N = \{(\alpha)/(\beta) \mid \alpha, \beta \in D \setminus \{0\},\ \alpha/\beta \in k(\mathfrak{m})\}.$$

En particular vemos que $P_{\mathfrak{m}} \leq N$. Tenemos el isomorfismo

$$(I(\mathfrak{m})/P_{\mathfrak{m}})/(N/P_{\mathfrak{m}}) \cong I(\mathfrak{m})/N \cong H,$$

de modo que el grupo H es un cociente de $H(\mathfrak{m})$ y $h_{\mathfrak{m}} = |N : P_{\mathfrak{m}}|\, h_1$. Para calcular el primer factor consideramos el epimorfismo de $k(\mathfrak{m})$ en $N/P_{\mathfrak{m}}$ que a cada α/β le asigna $(\alpha)/(\beta)$.

Un número α/β está en el núcleo de este epimorfismo si y sólo si cumple $(\alpha)/(\beta) \in P_{\mathfrak{m}}$, es decir, si $(\alpha)/(\beta) = (\gamma)/(\delta)$, donde $\gamma/\delta \in k_{\mathfrak{m}}$. Esto equivale a $(\alpha\delta) = (\gamma\beta)$, o sea, a que $\alpha\delta = \epsilon\gamma\beta$, para cierto $\epsilon \in U_1$, luego $\alpha/\beta = \epsilon\gamma/\delta$. En resumen, el núcleo es $U_1 k_{\mathfrak{m}}$ (notar que $U_1 \leq k(\mathfrak{m})$).

De este modo hemos llegado a que $N/P_{\mathfrak{m}} \cong k(\mathfrak{m})/(U_1 k_{\mathfrak{m}})$, luego el índice que buscamos es un divisor de $|k(\mathfrak{m}) : k_{\mathfrak{m}}| = \Phi(\mathfrak{m})$. Con esto ya tenemos la finitud de $h_{\mathfrak{m}}$.

Para terminar observamos que $(U_1 k_{\mathfrak{m}})/k_{\mathfrak{m}} \cong U_1/(U_1 \cap k_{\mathfrak{m}}) = U_1/U_{\mathfrak{m}}$, lo que nos da

$$|N : P_{\mathfrak{m}}| = \frac{\Phi(\mathfrak{m})}{|U_1 : U_{\mathfrak{m}}|}.$$

■

Una consecuencia inmediata es que si $[\mathfrak{a}]$ es una clase de similitud de ideales módulo un divisor $\mathfrak{m}$ entonces $[\mathfrak{a}]^{-1} = [\mathfrak{a}^r]$, para un cierto natural r, luego el inverso de un ideal es similar a otro ideal. Como toda clase está representada por un cociente de ideales, concluimos que toda clase puede representarse de hecho por un ideal.

Ejemplos Consideremos $k = \mathbb{Q}$ y tomemos como divisor $m = 9$. La congruencia usual módulo 9 en $\mathbb{Z}$ da lugar a seis clases de equivalencia de elementos primos con 9, a saber, [1], [2], [4], [5], [7], [8]. Por otra parte, la similitud módulo el divisor 9 es la relación de congruencia módulo el subgrupo

$$P_9 = \{(m)/(n) \mid m \equiv n \text{ (mód 9)},\ (mn, 9) = 1\},$$

y nos encontramos con que, por ejemplo, $(7) = (-7)$ y $-7 \equiv 2$ (mód 9), luego $(7)/(2)$ está en P_9, y así (7) y (2) son similares módulo 9.

Es claro que si m y n son números naturales primos con 9, entonces los ideales (m) y (n) son similares módulo 9 si y sólo si $m \equiv \pm n$ (mód 9), con lo que las clases de similitud se reducen a la mitad:

$$[(1)] = [(8)], \quad [(2)] = [(7)], \quad [(4)] = [(5)].$$

En general, para $k = \mathbb{Q}$ el grupo de unidades es $U_1 = \{\pm 1\}$ y, si $m \neq 2$, no se cumple $-1 \equiv 1$ (mód m), luego $U_m = \{1\}$ y el teorema 5.8 nos da que $h_m = \phi(m)/2$, es decir, la congruencia módulo m degenera al tomar ideales y se vuelven congruentes ideales que no deberían serlo.

Esta degeneración se corrige añadiendo el primo infinito. En efecto, dos números enteros r y s primos con m cumplen $r \equiv^* s$ (mód $m\,\infty$) si y sólo si $r \equiv s$ (mód m) y $rs > 0$. Por ejemplo, ya no es cierto que $-7 \equiv^* 2$ (mód 9∞), luego $(-7)/(2) \notin P_{9\,\infty}$. Si r y s son números naturales primos con m, los ideales (r) y (s) son similares módulo $9\,\infty$ si y sólo si $r \equiv s$ (mód 9), con lo que sigue habiendo seis clases de equivalencia.

En general, puesto que dos números naturales r y s cumplen que los ideales (r) y (s) son similares módulo $m\,\infty$ si y sólo si $r \equiv s$ (mód m), es claro que $h_{m\,\infty} = \phi(m)$, así como que el grupo de clases $H(m\,\infty)$ es isomorfo al grupo de unidades módulo m en el sentido usual. ∎

Ejemplo Supongamos que K es un cuerpo cuadrático real. Entonces K_∞ consta de los números positivos cuyos conjugados son también positivos. Obviamente, si $\alpha \in K_\infty$ se cumple $\mathrm{N}(\alpha) > 0$. Recíprocamente, si $\mathrm{N}(\alpha) > 0$ entonces los conjugados de α son ambos positivos o ambos negativos, con lo que $\pm\alpha \in K_\infty$. Puesto que $(\alpha) = (-\alpha)$, es claro entonces que

$$P_\infty = \{(\alpha)/(\beta) \mid \mathrm{N}(\alpha),\ \mathrm{N}(\beta) > 0\},$$

y por lo tanto la similitud módulo ∞ coincide con la similitud estricta definida en [6.4].

En general se define la similitud estricta entre los ideales un cuerpo numérico como la similitud módulo ∞. En los cuerpos sin divisores primos reales la similitud estricta coincide con la similitud usual (módulo 1). ∎

Ejemplo Volviendo al caso $k = \mathbb{Q}$, si m es un número natural, un ideal fraccional de $P_{m\,\infty}$ es de la forma $\mathfrak{a} = (r)/(s)$, donde r y s son números naturales $r \equiv s$ (mód $\mathfrak{m}$). Por el teorema 4.5, si K es el cuerpo ciclotómico de orden n, se cumple que

$$\left(\frac{K/\mathbb{Q}}{(r)}\right) = \left(\frac{K/\mathbb{Q}}{(s)}\right),$$

luego

$$\left(\frac{K/\mathbb{Q}}{\mathfrak{a}}\right) = 1.$$

Esto demuestra que $P_{m\,\infty}$ está contenido en el núcleo del homomorfismo de Artin de $K/\mathbb{Q}$. Como ambos grupos tienen el mismo índice respecto a $I(\mathfrak{m}\,\infty)$, han de coincidir. Por lo tanto el homomorfismo de Artin induce un isomorfismo $\omega : I(m\,\infty)/P_{m\,\infty} \longrightarrow G(K/\mathbb{Q})$.

Así tenemos una representación del grupo de Galois de la extensión $K/\mathbb{Q}$ en términos de un grupo de clases de ideales del cuerpo base. ∎

En el caso general el núcleo del homomorfismo de Artin no es tan sencillo. Aún estamos muy lejos de probarlo, pero lo que sucede es que si K/k es una extensión abeliana de discriminante Δ, entonces existe un divisor $\mathfrak{m}$ de k divisible sólo entre los primos ramificados de k (con lo que $I(\mathfrak{m}) = I(\Delta)$) de manera que el núcleo del homomorfismo de Artin es exactamente $P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$, donde $\mathrm{N}(\mathfrak{m})$ es el grupo de normas definido en 4.9 (entendiendo que depende sólo de la parte finita de $\mathfrak{m}$).

Observemos que el hecho de que el núcleo del homomorfismo de Artin contenga un subgrupo de la forma $P_{\mathfrak{m}}$ significa que el símbolo de Artin de un ideal fraccional $\mathfrak{a}$ depende sólo de la clase de $\mathfrak{a}$ módulo $\mathfrak{m}$, lo cual es de por sí una conexión notable entre el homomorfismo de Artin y la aritmética de k.

5.3 Densidad de ideales

Terminamos generalizando el teorema [11.7], que nos da la densidad de los ideales de un cuerpo numérico en las distintas clases de similitud. Ahora necesitamos un resultado análogo para la similitud módulo un divisor arbitrario, con el cual probaremos en el capítulo IX la convergencia de las funciones dseta generalizadas.

En la fórmula explícita de la densidad de ideales en una clase de similitud aparece el regulador del cuerpo. Aquí hemos de definir el regulador asociado a un divisor.

Sea K un cuerpo numérico con s primos arquimedianos reales y t complejos. Sean $\sigma_1, \ldots, \sigma_s$ los monomorfismos reales de K y $\sigma_{s+1}, \ldots, \sigma_{s+t}$ los monomorfismos complejos (salvo conjugación). Recordemos de [4.20] que la *representación logarítmica* de K es la aplicación $l : K \setminus \{0\} \longrightarrow \mathbb{R}^{s+t}$ dada por

$$l_k(\alpha) = \begin{cases} \log|\sigma_k(\alpha)| & \text{para } k = 1, \ldots, s, \\ \log|\sigma_k(\alpha)|^2 & \text{para } k = s+1, \ldots, s+t. \end{cases}$$

Sabemos [4.22] que la imagen $l[U_1]$ del grupo de unidades de K es un retículo en $\mathbb{R}^{s+t}$ de dimensión $r = s + t - 1$. La aplicación l es un monomorfismo de grupos. Su núcleo es el grupo de las raíces de la unidad de U_1, que es un grupo cíclico finito [4.21] y U_1 se descompone en la suma directa de este grupo finito y un grupo libre de rango r. Una base cualquiera $\epsilon_1, \ldots, \epsilon_r$ de este grupo libre recibe el nombre [4.24] de *sistema fundamental de unidades* de K, y entonces los vectores $l(\epsilon_1), \ldots, l(\epsilon_r)$ forman una base del retículo $l[U_1]$.

Si $\mathfrak{m}$ es un divisor de K, el grupo $U_{\mathfrak{m}} = U_1 \cap K_{\mathfrak{m}}$ tiene índice finito en U_1, lo que implica que $U_{\mathfrak{m}}$ tiene la misma estructura que U_1, es decir, es suma directa

de un grupo cíclico de raíces de la unidad y un grupo libre de rango r. La imagen $l[U_\mathfrak{m}]$ es un retículo de rango r y si $\eta_1, \ldots, \eta_r$ es una base de la parte libre de $U_\mathfrak{m}$, entonces $l(\eta_1), \ldots, l(\eta_r)$ es una base de $l[U_\mathfrak{m}]$.

Definición 5.9 Sea K un cuerpo numérico y $\mathfrak{m}$ un divisor de K. Un *sistema fundamental de unidades* de K módulo $\mathfrak{m}$ será cualquier base de la parte libre de $U_\mathfrak{m}$.

De este modo, si $\eta_1, \ldots, \eta_r$ es un sistema fundamental de unidades módulo $\mathfrak{m}$, toda unidad de $U_\mathfrak{m}$ se expresa de forma única como

$$\zeta\, \eta_1^{a_1} \cdots \eta_r^{a_r},$$

para ciertos enteros $a_1, \ldots, a_r$, donde $\zeta \in U_m$ es una raíz de la unidad.

Notar que los únicos cuerpos donde $r = 0$ (y que por lo tanto no tienen sistemas fundamentales de unidades) son $\mathbb{Q}$ y los cuerpos cuadráticos imaginarios.

Exactamente igual que en [4.24] se razona que el módulo $R_\mathfrak{m}$ de cualquiera de los menores de orden r de la matriz que tiene por filas a $l(\eta_1), \ldots, l(\eta_r)$ es independiente de la elección del sistema fundamental de unidades, y se llama *regulador* de K módulo $\mathfrak{m}$. Si K es el cuerpo racional o un cuerpo cuadrático complejo, definimos $R_\mathfrak{m} = 1$.

Es fácil relacionar los reguladores $R_\mathfrak{m}$ y R_1. Eligiendo adecuadamente los sistemas fundamentales $\epsilon_1, \ldots, \epsilon_r$ módulo 1 y $\eta_1, \ldots, \eta_r$ módulo $\mathfrak{m}$, podemos exigir que $\eta_i = \epsilon_i^{a_i}$, para cierto número natural a_i, de modo que, si llamamos $w_\mathfrak{m}$ al número de raíces de la unidad en $U_\mathfrak{m}$, entonces $|U_1 : U_m| = (w_1/w_\mathfrak{m})a_1 \cdots a_r$. Por otra parte, $l(\eta_i) = a_i\, l(\epsilon_i)$ y al tomar determinantes queda que $R_\mathfrak{m} = a_1 \cdots a_r\, R_1$, es decir,

$$R_\mathfrak{m} = \frac{w_\mathfrak{m}\, |U_1 : U_\mathfrak{m}|}{w_1}\, R_1.$$

Pasemos ya a la cuestión de la densidad de los ideales.

Definición 5.10 Sea K un cuerpo numérico y $\mathfrak{m}$ un divisor de K. Sea C una clase de similitud de ideales módulo $\mathfrak{m}$. Llamaremos *función de distribución de ideales* de la clase C a la función $j_C(r)$ que a cada $r > 0$ le asigna el número de ideales de C de norma menor o igual que r.

Lo que buscamos es una expresión asintótica para la función j.

En primer lugar tomemos un ideal $\mathfrak{b}$ de la clase inversa de C en el grupo de clases módulo $\mathfrak{m}$. Para cada ideal $\mathfrak{a} \in C$ tenemos que $\mathfrak{ab} \in P_\mathfrak{m}$, con lo que $\mathfrak{ab} = (\alpha)$, para un cierto número $\alpha \in K_\mathfrak{m}$ (entero). Además $\mathrm{N}\,\mathfrak{a}\ \mathrm{N}\,\mathfrak{b} = |\,\mathrm{N}(\alpha)|$. Así, la aplicación que a cada $\mathfrak{a}$ le asigna (α) biyecta los ideales de C con los ideales de $P_\mathfrak{m}$ divisibles entre $\mathfrak{b}$, con lo que $j_C(r)$ es igual al número de ideales de $P_\mathfrak{m}$ divisibles entre b y de norma a lo sumo $r\,\mathrm{N}\,\mathfrak{b}$.

La ventaja de este cambio es que ahora manejamos ideales principales. Para pasar a enteros de K hemos de tener en cuenta que enteros asociados generan el

mismo ideal, por lo que habremos de evitar las repeticiones. Para ello usaremos métodos geométricos.

Recordemos que la representación geométrica de K [4.1] es la aplicación $x : K \setminus \{0\} \longrightarrow \mathcal{R}^{st} = \mathbb{R}^s \times \mathbb{C}^t = \mathbb{R}^n$ dada por $x(\alpha) = \big(\sigma_1(\alpha), \dots, \sigma_{s+t}(\alpha)\big)$.

En $\mathcal{R}^{st}$ tenemos definida una norma [4.1]

$$\mathrm{N}(x_1, \dots, x_{s+t}) = x_1 \cdots x_s |x_{s+1}|^2 \cdots |x_{s+t}|^2,$$

de modo que $\mathrm{N}(x(\alpha)) = \mathrm{N}(\alpha)$ para todo $\alpha \in K$.

La *representación logarítmica* [4.20] puede definirse sobre todos los $x \in \mathcal{R}^{st}$ tales que $\mathrm{N}(x) \neq 0$ como $l(x) = \big(l_1(x), \dots, l_{s+t}(x)\big)$, donde

$$l_k(x) = \begin{cases} \log |x_k| & \text{para } k = 1, \dots, s, \\ \log |x_k|^2 & \text{para } k = s+1, \dots, s+t. \end{cases}$$

Así $l\big(x(\alpha)\big) = l(\alpha)$ para todo $\alpha \in K$ no nulo.

Fijemos un sistema fundamental de unidades módulo $\mathfrak{m}$, digamos $\epsilon_1, \dots, \epsilon_r$. Como las unidades tienen norma 1, tomando normas es claro que los vectores $l(\epsilon_1), \dots, l(\epsilon_r)$ (que sabemos que son linealmente independientes) forman una base del espacio vectorial

$$V = \{x \in \mathbb{R}^{s+t} \mid x_1 + \cdots + x_{s+t} = 0\}.$$

Si añadimos el vector $l^* = (1, \overset{s)}{\cdots}, 1, 2, \overset{t)}{\cdots}, 2)$ obtenemos una base de $\mathbb{R}^{s+t}$.

La representación logarítmica de cada vector $x \in \mathcal{R}^{st}$ de norma no nula se expresa de forma única como $l(x) = \xi l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r)$, donde $\xi, \xi_1, \dots, \xi_r$ son números reales.

Definimos el *dominio fundamental* asociado al sistema fundamental de unidades fijado como el conjunto X de todos los vectores $x \in \mathcal{R}^{st}$ tales que:

a) Las coordenadas de x son no nulas, y las correspondientes a divisores arquimedianos reales que dividen a $\mathfrak{m}$ son positivas.

b) $l(x) = \xi l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r)$ con $0 \leq \xi_i < 1$.

El conjunto X es un cono, (o sea, $rx \in X$ cuando $x \in X$ y $r > 0$), pues si $r > 0$ es claro que rx cumple la condición a) y $l(rx) = (\log r) l^* + l(x)$, de donde también cumple la condición b).

El teorema siguiente es esencialmente [11.4], pero lo repetimos para mostrar claramente las pequeñas variantes.

Teorema 5.11 *Si $y \in \mathcal{R}^{st}$ cumple la condición a) de la definición de X, entonces y admite exactamente $w_{\mathfrak{m}}$ representaciones de la forma $y = x\, x(\epsilon)$, donde $x \in X$ y $\epsilon \in U_{\mathfrak{m}}$.*

DEMOSTRACIÓN: Sea $l(y) = \gamma l^* + \gamma_1 l(\epsilon_1) + \cdots + \gamma_r l(\epsilon_r)$ y, para cada $j = 1, \ldots, r$, descompongamos las coordenadas $\gamma_j = k_j + \xi_j$, donde k_j es un entero racional y $0 \le \xi_j < 1$.

Sea $\epsilon = \epsilon_1^{k_1} \cdots \epsilon_r^{k_r}$ y consideremos el punto $x = yx(\epsilon^{-1})$. Entonces $y = x\,x(\epsilon)$ y además

$$l(x) = l(y) + l(\epsilon^{-1}) = \gamma l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r).$$

Como $\epsilon \in U_\mathfrak{m}$, sus conjugados reales correspondientes a divisores de $\mathfrak{m}$ son positivos, y lo mismo sucede con las componentes correspondientes de x. Así pues, $x \in X$.

Recordemos que el núcleo de la representación logarítmica de las unidades está formado por las raíces de la unidad. Sea $\zeta \in U_\mathfrak{m}$ una raíz de la unidad. Entonces $l\big(x\,x(\zeta^{-1})\big) = l(x) + l(\zeta^{-1}) = l(x)$, luego $x\,x(\zeta^{-1})$ está también en X y se cumple $y = \big(x\,x(\zeta^{-1})\big)\,x(\zeta\epsilon)$. Al variar ζ entre las $w_\mathfrak{m}$ raíces posibles obtenemos otras tantas expresiones distintas de la forma buscada. Veamos que no hay más. Sea $y = x\,x(\epsilon) = x'\,x(\epsilon')$. Entonces $l(x) + l(\epsilon) = l(x') + l(\epsilon')$.

Las coordenadas de $l(\epsilon)$ y $l(\epsilon')$ en la base $l(\epsilon_1), \ldots, l(\epsilon_r)$ son enteros racionales y las de $l(x)$ y $l(x')$ están entre 0 y 1. La unicidad de la parte entera de un número real nos da que $l(\epsilon) = l(\epsilon')$. Consecuentemente $\epsilon' = \epsilon\zeta$, donde ζ es una raíz de la unidad y, puesto que $\epsilon, \epsilon' \in U_\mathfrak{m}$, lo mismo le sucede a ζ.

Finalmente, como $x\,x(\epsilon) = x'\,x(\epsilon)\,x(\zeta)$, ha de ser $x' = x\,x(\zeta^{-1})$, luego se trata de una de las $w_\mathfrak{m}$ expresiones que ya habíamos encontrado. ∎

Como consecuencia tenemos el análogo de [11.3]:

Teorema 5.12 *Cada elemento no nulo de $K_\mathfrak{m}$ tiene exactamente $w_\mathfrak{m}$ asociados en $K_\mathfrak{m}$ cuya representación geométrica se encuentra en el dominio fundamental X.*

DEMOSTRACIÓN: Si $\beta \in K_\mathfrak{m}$ es no nulo, por el teorema anterior existen $w_\mathfrak{m}$ representaciones distintas de la forma $x(\beta) = x\,x(\epsilon)$ con $x \in X$ y $\epsilon \in U_\mathfrak{m}$. Para cada una de ellas, el número $\beta\epsilon^{-1}$ es un asociado de β en $K_\mathfrak{m}$ y $x(\beta\epsilon^{-1}) = x \in X$, luego hay $w_\mathfrak{m}$ asociados distintos en estas condiciones. Recíprocamente, cada asociado $\beta\epsilon^{-1}$ de β en $K_\mathfrak{m}$ tal que $x(\beta\epsilon^{-1}) \in X$ da lugar a una representación distinta $x(\beta) = x\,x(\epsilon)$, con $x \in X$ y $\epsilon \in U_\mathfrak{m}$, luego hay exactamente $w_\mathfrak{m}$ asociados que cumplen el teorema. ∎

Con esto tenemos probado que el número de enteros $\alpha \in K_\mathfrak{m}$ divisibles entre $\mathfrak{b}$ y tales que $x(\alpha) \in X$, $|\,\mathrm{N}(\alpha)| \le \mathrm{N}(\mathfrak{b})r$ es igual a $w_\mathfrak{m}\, j_C(r)$. En otras palabras, hemos de contar los enteros $\alpha \in K$ que cumplen:

a) $\alpha \equiv 0$ (mód $\mathfrak{b}$),

b) $\alpha \equiv 1$ (mód $\mathfrak{m}_f$),

c) $x(\alpha) \in X$,

d) $|\,\mathrm{N}(\alpha)| \le \mathrm{N}(\mathfrak{b})r$.

En la condición b) podemos poner $\mathfrak{m}_f$ en lugar de $\mathfrak{m}$ porque las condiciones respecto a los primos infinitos ya están contenidas en c).

Dado que $(\mathfrak{b}, \mathfrak{m}_f) = 1$, el teorema chino del resto nos da que existe un entero ξ tal que $\xi \equiv 0$ (mód $\mathfrak{b}$), $\xi \equiv 1$ (mód $\mathfrak{m}_f$), y las condiciones a) y b) equivalen a que $\alpha - \xi \in \mathfrak{b}\mathfrak{m}_f$, o sea, $\alpha \in \xi + \mathfrak{b}\mathfrak{m}_f$.

De este modo, $w_\mathfrak{m}\, j_C(r)$ es igual al número de elementos $x \in \big(u + x[\mathfrak{b}\mathfrak{m}_f]\big) \cap X$ tales que $|\,\mathrm{N}(x)| \le \mathrm{N}(\mathfrak{b})r$, donde $u = x(\xi)$.

Llamemos $T = \{x \in X \mid |\,\mathrm{N}(x)| \le 1\}$. Teniendo en cuenta que si $r > 0$ es un número real entonces $\mathrm{N}(rx) = r^n\ \mathrm{N}(x)$ (donde n es el grado de K), así como que X es un cono, resulta que

$$\{x \in X \mid |\,\mathrm{N}(x)| \le r\} = \left\{ \sqrt[n]{r}\left(\frac{x}{\sqrt[n]{r}}\right) \in X \mid \left|\mathrm{N}\left(\frac{x}{\sqrt[n]{r}}\right)\right| \le 1 \right\} = \sqrt[n]{r}\,T,$$

luego $w_\mathfrak{m}\, j_C(r)$ es también el número de puntos de

$$\big(u + x[\mathfrak{b}\mathfrak{m}_f]\big) \cap \sqrt[n]{\mathrm{N}(\mathfrak{b})\,r}\,T.$$

Vamos a aplicar el teorema [11.6] tomando $\mathcal{M} = x[\mathfrak{b}\mathfrak{m}_f]$ y $T = \{x \in X \mid |\,\mathrm{N}(x)| \le 1\}$. Entonces la función $n(r)$ que aparece en el teorema está relacionada con j_C por la fórmula

$$j_C(r) = \frac{n(\sqrt[n]{\mathrm{N}(\mathfrak{b})\,r})}{w_\mathfrak{m}}. \tag{5.1}$$

Para poder aplicar el teorema hemos de comprobar que T cumple las hipótesis, es decir, que es medible y su frontera es parametrizable Lipschitz de grado $n-1$. Además necesitaremos explícitamente la medida $\mu(T)$. Los cálculos realizados previos al teorema [11.7] nos aprovechan con los cambios mínimos que vamos a indicar.

Todo $x \in \mathcal{R}^{st}$ de norma no nula cumple

$$l(x) = \xi l^* + \xi_1 l(\epsilon_1) + \cdots + \xi_r l(\epsilon_r),$$

donde $\xi, \xi_1, \ldots, \xi_r$ son números reales.

En nuestro caso el conjunto T está formado por los vectores x que cumplen

a) $0 < \big|\mathrm{N}(x)\big| \le 1$,

b) $0 \le \xi_i < 1$.

c) Las coordenadas correspondientes a primos reales que dividen a $\mathfrak{m}$ son positivas.

Llamamos T' al conjunto de los puntos de T que cumplen las condiciones anteriores pero cuyas coordenadas reales son todas positivas. Éste es exactamente el mismo conjunto considerado en los cálculos previos a [11.7], y la única

diferencia es que ahora T no es la unión de 2^s imágenes de T' por aplicaciones lineales, sino de tan sólo 2^{s-p}, donde p es el número de primos reales que dividen a $\mathfrak{m}$. Concretamente, T se obtiene multiplicando T' por todas las $s+t$-tuplas $(\delta_1,\dots,\delta_s,1,\dots,1)$ tales que cada $\delta_i=\pm1$ pero las p componentes correspondientes a los divisores reales de $\mathfrak{m}$ son positivas.

Por lo demás, todos los cálculos sobre T' valen ahora sin cambio alguno, y así concluimos que T' es medible, acotado, su frontera es parametrizable Lipschitz y

$$\mu(T') = \pi^t R_{\mathfrak{m}}.$$

(Observar que el regulador que aparece es ahora el regulador módulo $\mathfrak{m}$ porque partimos de un sistema fundamental de unidades módulo $\mathfrak{m}$.)

Consecuentemente T cumple las hipótesis de [11.6] y

$$\mu(T) = 2^{s-p}\pi^t R_{\mathfrak{m}}.$$

Por otro lado, la medida del paralelepípedo fundamental del retículo $\mathcal{M} = x[\mathfrak{bm}_f]$ viene dada por [4.5] y resulta ser

$$c = \frac{\sqrt{|\Delta|}}{2^t}\,\mathrm{N}(\mathfrak{bm}_f),$$

donde Δ es el discriminante de K.

Así, ya podemos aplicar [11.6] y concluir que

$$n(r) = \frac{2^s(2\pi)^t\,R_{\mathfrak{m}}}{\sqrt{|\Delta|}\,\mathrm{N}(\mathfrak{b})\,\mathrm{N}(\mathfrak{m})}\,r^n + O(r^{n-1}),$$

donde, por definición $\mathrm{N}(\mathfrak{m}) = 2^p\,\mathrm{N}(\mathfrak{m}_f)$.

Finalmente sustituimos r por $\sqrt[n]{\mathrm{N}(\mathfrak{b})\,r}$, aplicamos 5.1 y tenemos probado el teorema siguiente:

Teorema 5.13 *Sea K un cuerpo numérico de grado n con s primos reales y t complejos. Sea $\mathfrak{m}$ un divisor de K, sea $R_{\mathfrak{m}}$ el regulador de K módulo $\mathfrak{m}$, sea $w_{\mathfrak{m}}$ el número de raíces de la unidad contenidas en $U_{\mathfrak{m}}$, sea Δ el discriminante de K y C una clase de similitud de ideales de K módulo $\mathfrak{m}$. Entonces*

$$j_C(r) = \frac{2^s(2\pi)^t R_{\mathfrak{m}}}{\mathrm{N}(\mathfrak{m})\,w_{\mathfrak{m}}\sqrt{|\Delta|}}\,r + O(r^{1-1/n})$$

Observar que en particular

$$\lim_{r\to+\infty}\frac{j_C(r)}{r} = \frac{2^s(2\pi)^t R_{\mathfrak{m}}}{\mathrm{N}(\mathfrak{m})\,w_{\mathfrak{m}}\sqrt{|\Delta|}},$$

pues

$$\lim_{r\to+\infty}\frac{O(r^{1-1/n})}{r} = \lim_{r\to+\infty}\frac{O(r^{1-1/n})}{r^{1-1/n}}\,\frac{1}{\sqrt[n]{r}} = 0.$$

Capítulo VI

Elementos ideales

En los capítulos anteriores hemos ido introduciendo diversos conceptos de gran utilidad en el estudio de los cuerpos numéricos. Ahora presentamos una poderosísima herramienta que nos permitirá combinarlos de la manera más eficiente y natural para probar los teoremas de la teoría de cuerpos de clases. En el fondo, podemos pensar en los elementos ideales como una generalización de la representación geométrica de un cuerpo numérico. Ésta puede verse como una inmersión del cuerpo en el producto de todas sus compleciones arquimedianas, y lo que haremos ahora es sumergirlo en el producto de todas sus compleciones. En realidad no vamos a considerar todo el producto cartesiano, ni tampoco el producto directo. El grupo de los elementos ideales de un cuerpo k es un grupo intermedio entre ambos definido por una condición de finitud adecuada a su aritmética. La idea básica subyacente es que un elemento de k es una unidad en todas sus compleciones salvo a lo sumo en un número finito de ellas. Veamos los detalles en la primera sección.

6.1 Definiciones y propiedades básicas

Sea K un cuerpo numérico. Para cada divisor primo $\mathfrak{p}$ de K consideramos la compleción $K_\mathfrak{p}$ y el grupo multiplicativo $K_\mathfrak{p}^* = K_\mathfrak{p} \setminus \{0\}$. Definimos

$$U_\mathfrak{p} = \{\alpha \in K_\mathfrak{p}^* \mid |\alpha|_\mathfrak{p} = 1\}.$$

Si $\mathfrak{p}$ no es arquimediano entonces $U_\mathfrak{p}$ es el grupo de las unidades del anillo de enteros de $K_\mathfrak{p}$. Si $\mathfrak{p}$ es arquimediano real entonces $U_\mathfrak{p} = \{\pm 1\}$ y si $\mathfrak{p}$ es arquimediano complejo entonces $U_\mathfrak{p}$ es el grupo de los números complejos de módulo 1.

Sea P el conjunto de todos los divisores primos de K. Sea P_∞ el conjunto de los divisores primos arquimedianos.

Un *elemento ideal* de K es una aplicación α que a cada $\mathfrak{p} \in P$ le asigna un $\alpha_\mathfrak{p} \in K_\mathfrak{p}^*$ con la propiedad de que $\alpha_\mathfrak{p} \in U_\mathfrak{p}$ para todo primo $\mathfrak{p}$ salvo a lo sumo en un número finito de casos.

Llamaremos J al conjunto de todos los elementos ideales de K. Es claro que J es un grupo con el producto definido componente a componente.

Si $E \subset P$ es un conjunto finito llamaremos

$$J_E = \{\alpha \in J \mid \alpha_\mathfrak{p} \in U_\mathfrak{p} \text{ para todo } \mathfrak{p} \in P \setminus E\}.$$

Claramente J_E es un subgrupo de J y J es la unión de todos estos subgrupos. El grupo $U = J_{P_\infty}$ se llama *grupo de unidades* de J.

Si $\alpha \in K^*$ es claro que la función constante igual a α es un elemento ideal de K. Esto nos permite identificar a K^* con un subgrupo de J. Los elementos ideales asociados a elementos de K^* se llaman *elementos ideales principales.*

Si $\alpha \in J$, por definición tenemos que $v_\mathfrak{p}(\alpha_\mathfrak{p}) = 0$ para todos los primos no arquimedianos de K salvo a lo sumo un número finito de ellos. Por lo tanto tiene sentido el producto

$$(\alpha) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} \in I,$$

donde $\mathfrak{p}$ recorre los primos no arquimedianos de K.

De este modo tenemos definido un epimorfismo de grupos $J \longrightarrow I$ sobre el grupo de los ideales fraccionales de K. Su núcleo es obviamente J_{P_∞}, con lo que tenemos un isomorfismo $J/J_{P_\infty} \cong I$.

También es inmediato que si $\alpha \in K^*$ entonces el ideal fraccional (α) en este sentido es simplemente el ideal fraccional generado por α. De aquí deducimos a su vez el isomorfismo $J/K^*J_{P_\infty} \cong I/P$.

Más adelante veremos que todos los grupos de clases de ideales de K pueden representarse de forma similar como cocientes de J. El grupo $C = J/K^*$ se llama *grupo de clases de elementos ideales* de K. De momento tenemos que el grupo de clases I/P es una imagen de C.

Si $\alpha \in J$ llamaremos $\|\alpha\|_\mathfrak{p} = \|\alpha_\mathfrak{p}\|_\mathfrak{p}$ (ver la definición 2.26). Puesto que $\|\alpha\|_\mathfrak{p} = 1$ salvo a lo sumo para una cantidad finita de primos, podemos definir

$$\|\alpha\| = \prod_\mathfrak{p} \|\alpha\|_\mathfrak{p}.$$

Esto da lugar a un homomorfismo de grupos $J \longrightarrow \mathbb{R}^+ =]0, +\infty[$. Para ver que es un epimorfismo conviene definir un monomorfismo $\mathbb{R}^+ \longrightarrow J$ del modo siguiente: a cada número real $r > 0$ le asignamos el elemento ideal α_r tal que si $\mathfrak{p}$ es un primo arquimediano entonces $(\alpha_r)_\mathfrak{p}$ es el único elemento de $K_\mathfrak{p}^*$ tal que $\sigma((\alpha_r)_\mathfrak{p}) = r^{1/n}$, (donde n es el grado de K y $\sigma : K^* \longrightarrow \mathbb{C}$ es un monomorfismo que induzca el valor absoluto de $\mathfrak{p}$). Si $\mathfrak{p}$ no es arquimediano, definimos $(\alpha_r)_\mathfrak{p} = 1$. Es claro que esta aplicación es un monomorfismo de grupos y además $\|\alpha_r\| = r$.

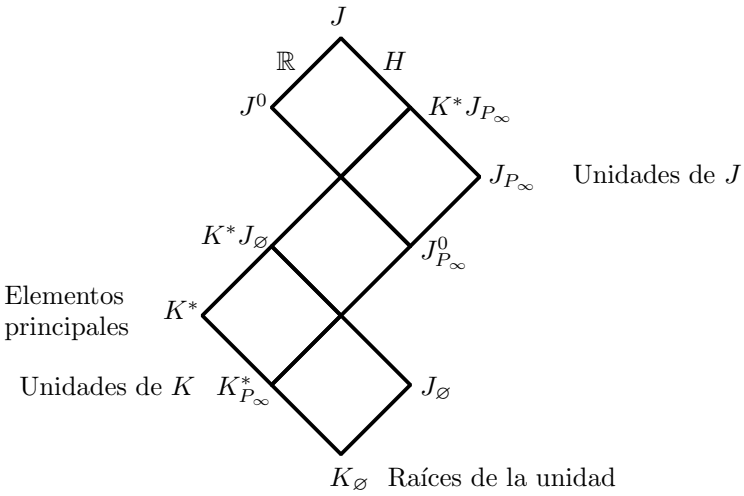
Definimos $J^0 = \{\alpha \in J \mid \|\alpha\| = 1\}$. De este modo $J/J^0 \cong \mathbb{R}^+$. El isomorfismo inverso lo da la aplicación $r \mapsto [\alpha_r]$. En virtud de (2.4) tenemos que $K^* \leq J^0$.

Más aún, es muy fácil comprobar que de hecho $J = \mathbb{R}^+ \times J^0$ (identificando $\mathbb{R}^+$ con el conjunto de los elementos α_r).

Observar que $\mathbb{R}^+ \cong (\mathbb{R}, +)$ (el isomorfismo es la función logaritmo). Por lo que también se cumple que $J/J^0 \cong \mathbb{R}$. Otro hecho obvio es que $J_\varnothing \leq J^0$.

Llamaremos $K_E = K^* \cap J_E$. Claramente K_{P_∞} es el grupo de las unidades del anillo de enteros de K. También es claro que $K_\varnothing$ es el grupo de las raíces de la unidad contenidas en K. En efecto, si $\alpha \in K^*$, la condición $|\alpha|_\mathfrak{p} = 1$ para todos los primos no arquimedianos equivale a que α es una unidad de K, y la condición $|\alpha|_\mathfrak{p} = 1$ para todos los primos arquimedianos implica que α está en el núcleo de la representación logarítmica de K, luego α es una raíz de la unidad ([4.21]).

El esquema siguiente describe la situación en J de los principales subgrupos que hemos definido:



Las líneas ascendentes indican productos, las descendentes intersecciones. Observar que ciertamente $J = J^0 J_{P_\infty}$, pues $J = J^0\mathbb{R}^+$ y $\mathbb{R}^+ \leq J_{P_\infty}$.

Definimos también

$$J^0_E = J_0 \cap J_E, \qquad C^0 = J^0/K^*, \qquad C_E = J_E/K_E, \qquad C^0_E = J^0_E/K_E.$$

Claramente se cumple $C = \mathbb{R}^+ \times C^0$.

Conviene observar una última propiedad de los subgrupos J_E: existe un conjunto finito de primos E tal que $J = K^*J_E$. En efecto, como el cociente J/K^*P_∞ es finito (es el grupo de clases), podemos tomar un conjunto de primos E que contenga a P_∞ y de modo que todos los elementos de un conjunto de representantes de las clases de dicho cociente estén en J_E. Entonces $J = K^*P_\infty J_E = K^*J_E$.

Veamos ahora la relación entre los elementos ideales y los grupos de clases. Sea $\mathfrak{m}$ un divisor de K. Si α, $\beta \in J$, diremos que $\alpha \equiv^* \beta$ (mód $\mathfrak{m}$) si

a) para todo $\mathfrak{p} \mid \mathfrak{m}_f$ se cumple que $\alpha_\mathfrak{p}$, $\beta_\mathfrak{p}$ son enteros en $K_\mathfrak{p}$ y

$$\alpha_\mathfrak{p} \equiv \beta_\mathfrak{p} \text{ (mód } \mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}),$$

b) para todo $\mathfrak{p} \mid \mathfrak{m}$ arquimediano real se cumple que $\sigma(\alpha_\mathfrak{p}/\beta_\mathfrak{p}) > 0$, donde $\sigma : K_\mathfrak{p} \longrightarrow \mathbb{R}$ es el monomorfismo que induce el valor absoluto de $\mathfrak{p}$.

Llamaremos $J_\mathfrak{m} = \{\alpha \in J \mid \alpha \equiv^* 1 \text{ (mód } \mathfrak{m})\}$. Claramente $J_\mathfrak{m} \cap K^* = K_\mathfrak{m}$ (donde $K_\mathfrak{m}$ es el grupo numérico que definimos en el capítulo anterior).

Ahora demostraremos que $J_\mathfrak{m}/K_\mathfrak{m} \cong J/K^*$. Basta probar que toda clase de J/K^* tiene un representante en $J_\mathfrak{m}$.

Sea $\alpha \in J$. Vamos a aplicar el teorema de aproximación a los valores absolutos asociados a los primos $\mathfrak{p}|\mathfrak{m}$. Obtendremos así un $\beta \in K^*$ tal que $|\alpha_\mathfrak{p} - \beta|_\mathfrak{p}$ sea suficientemente pequeño y veremos que esto bastará para garantizar que $\alpha/\beta \in J_\mathfrak{m}$.

Si $\mathfrak{p}$ es no arquimediano observamos en primer lugar que si $|\alpha_\mathfrak{p} - \beta|_\mathfrak{p} < |\alpha_\mathfrak{p}|_\mathfrak{p}$ entonces $|\beta|_\mathfrak{p} = |(\beta - \alpha_\mathfrak{p}) + \alpha_\mathfrak{p}|_\mathfrak{p} = |\alpha_\mathfrak{p}|_\mathfrak{p}$. Si además exigimos $|\alpha_\mathfrak{p} - \beta|_\mathfrak{p} < \epsilon|\alpha_\mathfrak{p}|_\mathfrak{p}$ para un $\epsilon > 0$ prefijado, entonces $|\alpha_\mathfrak{p} - \beta|_\mathfrak{p} < \epsilon|\beta|_\mathfrak{p}$, luego $|\alpha_\mathfrak{p}/\beta - 1|_\mathfrak{p} < \epsilon$.

Esto significa que podemos encontrar un $\beta \in K^*$ tal que $|\alpha_\mathfrak{p}/\beta - 1|_\mathfrak{p} < \epsilon$ para cualquier $\epsilon > 0$ prefijado y todos los divisores primos no arquimedianos $\mathfrak{p} \mid \mathfrak{m}$. Tomando ϵ suficientemente pequeño esto implica que $\alpha_\mathfrak{p}/\beta$ es entero en $K_\mathfrak{p}$ y $\alpha_\mathfrak{p}/\beta \equiv 1$ (mód $\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}$).

Respecto a los posibles divisores arquimedianos (reales), es claro que si exigimos $|\alpha_\mathfrak{p} - \beta|_\mathfrak{p} < |\alpha_\mathfrak{p}|_\mathfrak{p}$, entonces $\sigma(\alpha_\mathfrak{p})$ y $\sigma(\beta)$ tienen el mismo signo (donde σ es el monomorfismo que induce el valor absoluto).

En total obtenemos un $\beta \in K^*$ tal que $\alpha/\beta \equiv^* 1$ (mód $\mathfrak{m}$) y claramente $[\alpha] = [\alpha/\beta]$ (considerando clases módulo K^*).

La aplicación que a cada elemento ideal $\alpha \in J_\mathfrak{m}$ le asigna el ideal $(\alpha) \in I(\mathfrak{m})$ es un epimorfismo de grupos $J_\mathfrak{m} \longrightarrow I(\mathfrak{m})$. Vamos a describir su núcleo:

Para cada divisor primo $\mathfrak{p}$ definimos como sigue un subgrupo abierto $W_\mathfrak{m}(\mathfrak{p})$ de $K_\mathfrak{p}^*$:

a) si $\mathfrak{p} \mid \mathfrak{m}_f$ entonces

$$W_\mathfrak{m}(\mathfrak{p}) = \{\alpha \in K_\mathfrak{p}^* \mid \alpha \equiv 1 \text{ (mód } \mathfrak{p}^{\mathfrak{m}_\mathfrak{p}})\},$$

(donde la congruencia presupone que α es un entero en $K_\mathfrak{p}$). Claramente $W_\mathfrak{m}(\mathfrak{p}) = 1 + \mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}$ es de un disco (abierto y cerrado) de centro 1 en $K_\mathfrak{p}^*$.

b) si $\mathfrak{p} \mid \mathfrak{m}$ es un primo arquimediano real (inducido por el monomorfismo σ) entonces

$$W_\mathfrak{m}(\mathfrak{p}) = \{\alpha \in K_\mathfrak{p}^* \mid \sigma(\alpha) > 0\}.$$

c) Si $\mathfrak{p} \nmid \mathfrak{m}$ es no arquimediano entonces

$$W_\mathfrak{m}(\mathfrak{p}) = U_\mathfrak{p}.$$

d) Si $\mathfrak{p} \nmid \mathfrak{m}$ es arquimediano entonces

$$W_{\mathfrak{m}}(\mathfrak{p}) = K_{\mathfrak{p}}^*.$$

Definimos

$$W_{\mathfrak{m}} = \{\alpha \in J \mid \alpha_{\mathfrak{p}} \in W_{\mathfrak{m}}(\mathfrak{p}) \text{ para cada primo } \mathfrak{p}\} = \prod_{\mathfrak{p}} W_{\mathfrak{m}}(\mathfrak{p}).$$

Es claro que $W_{\mathfrak{m}} \leq J_{\mathfrak{m}}$. Con más precisión, $W_{\mathfrak{m}}$ consta de los elementos $\alpha \in J_{\mathfrak{m}}$ que además cumplen que $\alpha_{\mathfrak{p}}$ es una unidad para cada $\mathfrak{p}$ no arquimediano que no divide a $\mathfrak{m}$. Es claro que $W_{\mathfrak{m}}$ es el núcleo del epimorfismo $J_{\mathfrak{m}} \longrightarrow I(\mathfrak{m})$, luego tenemos el isomorfismo

$$J_{\mathfrak{m}}/W_{\mathfrak{m}} \cong I(\mathfrak{m}),$$

y de aquí

$$J_{\mathfrak{m}}/K_{\mathfrak{m}}W_{\mathfrak{m}} \cong I(\mathfrak{m})/P_{\mathfrak{m}}.$$

Combinando este último isomorfismo con el hecho de que

$$C = J/K^* \cong J_{\mathfrak{m}}/K_{\mathfrak{m}} \tag{6.1}$$

concluimos que los grupos de clases de ideales generalizados $I(\mathfrak{m})/P_{\mathfrak{m}}$ son todos cocientes del grupo de clases de elementos ideales C. Explícitamente,

$$J/K^*W_{\mathfrak{m}} \cong I(\mathfrak{m})/P_{\mathfrak{m}}. \tag{6.2}$$

En efecto, tenemos

$$J/K^*W_{\mathfrak{m}} \cong \frac{J/K^*}{K^*W_{\mathfrak{m}}/K^*}$$

y el isomorfismo (6.1) transforma el denominador en $K_{\mathfrak{m}}W_{\mathfrak{m}}/K_{\mathfrak{m}}$, luego

$$J/K^*W_{\mathfrak{m}} \cong \frac{J_{\mathfrak{m}}/K_{\mathfrak{m}}}{K_{\mathfrak{m}}W_{\mathfrak{m}}/K_{\mathfrak{m}}} \cong J_{\mathfrak{m}}/K_{\mathfrak{m}}W_{\mathfrak{m}} \cong I(\mathfrak{m})/P_{\mathfrak{m}}.$$

6.2 La topología de los elementos ideales

Vamos a definir una topología en el grupo J y en sus grupos asociados, pero antes probaremos unos pocos resultados (los mínimos que necesitaremos) sobre grupos topológicos en general.

Definición 6.1 Un *grupo topológico* G es un grupo dotado de una topología de modo que la aplicación producto $G \times G \longrightarrow G$ y la aplicación $g \mapsto g^{-1}$ son ambas continuas. Es claro que esto equivale a que la aplicación $(g, h) \mapsto g^{-1}h$ sea continua.

Por ejemplo, si K es un cuerpo métrico, los grupos $(K,+)$ y $(K^*,\cdot)$ son grupos topológicos.

Es claro que si G es un grupo topológico y $g \in G$, entonces la aplicación $h \mapsto gh$ es un homeomorfismo. Este hecho tiene muchas consecuencias. Por ejemplo, si H es un subgrupo abierto de G, entonces H es cerrado en G. En efecto, $G \setminus H$ puede expresarse como la unión de las clases gH con $g \in G \setminus H$, y dichas clases son abiertas. Similarmente se prueba que todo subgrupo que contenga un subgrupo abierto es abierto.

Otra consecuencia es que los entornos de un $g \in G$ son de la forma gE, donde E es un entorno de 1, y esto implica que un homomorfismo $f : G \longrightarrow H$ entre grupos topológicos es continuo si y sólo si es continuo en 1.

En general muchas propiedades globales de los grupos topológicos se reducen de este modo a propiedades locales del 1. El teorema siguiente proporciona otro ejemplo.

Teorema 6.2 *Un grupo topológico G es de Hausdorff si y sólo si $\{1\}$ es cerrado.*

Demostración: Una implicación es obvia. Supongamos que $\{1\}$ es cerrado. Por la observación anterior todos los puntos de G son cerrados y basta probar que si $g \in G$ es distinto de 1 existe un entorno E de 1 tal que $E \cap gE = \varnothing$.

Como $\{g\}$ es cerrado tenemos que $V = G \setminus \{g\}$ es un entorno de 1. Consideremos la aplicación $f : G \times G \longrightarrow G$ dada por $f(u,v) = uv^{-1}$. Claramente es continua y $f(1,1) = 1$, luego la antiimagen de V es un entorno de $(1,1)$ en $G \times G$. Consecuentemente existe un entorno E de 1 tal que $EE^{-1} \subset V$. Un punto en $E \cap gE$ sería de la forma $e = ge'$, para ciertos e, $e' \in E$, luego $g = ee'^{-1} \in EE^{-1} \subset V$, contradicción. Así pues, E cumple lo pedido. ∎

Es inmediato que si G es un grupo topológico y H es un subgrupo de G entonces H es un grupo topológico con la topología inducida. Para los grupos cociente tenemos este teorema:

Teorema 6.3 *Sea G un grupo topológico y N un subgrupo normal de G. Entonces existe una única topología sobre G/N con la cual es grupo topológico y de modo que la proyección canónica $p : G \longrightarrow G/N$ es continua y abierta.*

Demostración: Definimos en G/N la topología para la cual un conjunto A es abierto si y sólo si $p^{-1}[A]$ es abierto en G. Es inmediato que los abiertos así definidos forman ciertamente una topología en G/N, para la cual p es continua. Más aún, si A es un abierto en G entonces $p^{-1}[p[A]] = \bigcup_{n\in N} nA$, que es abierto en G, luego $p[A]$ es abierto en N. Por lo tanto p es abierta.

Para probar la continuidad del producto consideremos el diagrama siguiente:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ \downarrow\downarrow & & \downarrow \\ G/N \times G/N & \longrightarrow & G/N \end{array}$$

Las flechas horizontales son los productos respectivos, las verticales son las proyecciones. Si A es un abierto en G/N entonces $p^{-1}[A]$ es un abierto en G. La antiimagen de $p^{-1}[A]$ por el producto de G es un abierto en $G \times G$ y su imagen por la doble proyección es un abierto en $G/N \times G/N$, que no es sino la antiimagen de A por el producto de G/N. Por lo tanto dicho producto es continuo.

Igualmente se prueba que la aplicación $[g] \mapsto [g^{-1}]$ es continua, y en consecuencia G/N es un grupo topológico. La unicidad de la topología es obvia. ∎

En lo sucesivo, siempre que consideremos un cociente G/N de un grupo topológico G lo consideraremos como grupo topológico con la topología que acabamos de definir. Es claro que C es cerrado en un cociente G/N si y sólo si $p^{-1}[C]$ es cerrado en G. En particular G/N es un espacio de Hausdorff si y sólo si N es cerrado en G.

En adelante sólo consideraremos grupos topológicos de Hausdorff, por lo que sólo consideraremos grupos cociente respecto a subgrupos normales cerrados. En particular los subgrupos abiertos son cerrados, y es claro que sus cocientes resultan ser discretos.

Por último estudiamos las componentes conexas de los grupos topológicos. En primer lugar notemos que un grupo topológico conexo G no puede contener un subgrupo abierto distinto de G, pues tal subgrupo sería a la vez cerrado. Otro hecho importante es el siguiente.

Teorema 6.4 *Sea G un grupo topológico y sea C_1 la componente conexa de 1. Entonces C_1 es un subgrupo normal cerrado de G. Sus clases de congruencia son las componentes conexas de G.*

Demostración: Llamemos C_g a la componente conexa de cada $g \in G$. Si $g, h \in C_1$ entonces gC_1 es la componente conexa de g (porque la multiplicación por g es un homeomorfismo), es decir, $C_1 = C_g = gC_1$, luego $h \in gC_1$, y así $g^{-1}h \in C_1$. Esto prueba que C_1 es un subgrupo. Como las conjugaciones son homeomorfismos, de hecho es un subgrupo normal.

Como ya hemos observado, para todo $g \in G$ se cumple $C_g = gC_1$, luego las componentes conexas de G son los elementos de G/C_1. ∎

Pasemos ya a definir la topología de los grupos de elementos ideales.

Definición 6.5 Sea K un cuerpo numérico y E un conjunto finito de primos de K Entonces tenemos que

$$J_E = \prod_{\mathfrak{p}\in E} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\in P\setminus E} U_{\mathfrak{p}}.$$

Esto es un producto de grupos topológicos localmente compactos, luego podemos considerarlo como un grupo topológico localmente compacto con la topología producto.

Si $E \subset E'$, es claro que $J_E \leq J_{E'}$, y la topología de J_E es la inducida por la topología de $J_{E'}$. Más aún, si $\mathfrak{p} \in P \setminus P_\infty$ tenemos que $U_\mathfrak{p}$ es abierto y cerrado en $K_\mathfrak{p}^*$, con lo que si $J_{P_\infty} \leq J_E \leq J_{E'}$, entonces J_E es abierto y cerrado en $J_{E'}$.

Teorema 6.6 *Sea K un cuerpo numérico. Entonces existe una única topología que convierte a J en un grupo topológico de modo que si E es un conjunto finito de primos de K que contenga a todos los primos arquimedianos, entonces J_E (con la topología dada por la definición anterior) es un subgrupo abierto de J.*

Demostración: Consideremos los conjuntos de la forma αA, donde $\alpha \in J$ y A es un entorno abierto de 1 en un subgrupo J_E. Vamos a ver que constituyen la base de una topología en J. Lo único que hay que comprobar es que si $\gamma \in \alpha A \cap \beta B$ entonces existe un C entorno abierto de 1 en algún J_E tal que $\gamma C \subset \alpha A \cap \beta B$.

Existe un E suficientemente grande de modo que α, β, $\gamma \in J_E$ y además J_E contiene a los subgrupos de los cuales A y B son entornos de 1. Como tales subgrupos son abiertos en J_E resulta que A y B también son entornos abiertos de 1 en J_E.

Ahora $\alpha A \cap \beta B$ es un entorno de γ en J_E, luego existe un entorno abierto de 1 en J_E, digamos C, tal que $\gamma C \subset \alpha A \cap \beta B$.

Con esta topología, cada subgrupo J_E es abierto. Más aún, todo abierto de J_E (para su topología) es un abierto de J y, por lo tanto, un abierto para la topología inducida en J_E. Recíprocamente, un abierto básico para la topología inducida es de la forma $\alpha A \cap J_E$, donde $\alpha \in J$ y A es un entorno abierto de 1 en un subgrupo $J_{E'}$. En estas condiciones hemos probado que para todo $\gamma \in \alpha A \cap J_E$ existe un C, entorno abierto de 1 en un subgrupo $J_{E''}$ tal que $E \subset E''$, de manera que $\gamma C \subset \alpha A \cap J_E$. Entonces γC es un abierto en $J_{E''}$ (para su topología), luego en J_E, y consecuentemente $\alpha A \cap J_E$ es un entorno de cada uno de sus puntos en la topología de J_E. Esto prueba que la topología inducida por J en J_E es la dada.

Cada par $(\alpha, \beta) \in J \times J$ está contenido en un entorno $J_E \times J_E$, donde el producto es continuo, luego el producto es continuo en todo J. Igualmente se prueba la continuidad de la aplicación $\alpha \mapsto 1/\alpha$, con lo que J resulta ser un grupo topológico.

La unicidad se debe a que cualquier topología que cumpla estas condiciones tiene como base de entornos de 1 a los entornos de 1 en uno de los subgrupos J_E, y una base de entornos de 1 determina la topología de un grupo topológico. ∎

Observar que si E es cualquier conjunto finito de divisores primos de K (aunque no contenga a los primos arquimedianos), la topología que J induce en J_E es la definida en 6.5, si bien J_E no tiene por qué ser abierto en J.

Si $\mathfrak{p}$ es un divisor primo de K, la proyección $J \longrightarrow K_\mathfrak{p}^*$ es continua al restringirla a J_{P_∞} (pues las proyecciones son continuas para la topología producto), luego es continua en 1, luego es continua en J. Por lo tanto la antiimagen de

$U_\mathfrak{p}$, llamémosla $S_\mathfrak{p}$, es cerrada y

$$J_E = \bigcap_{\mathfrak{p}\in P\setminus E} S_\mathfrak{p}$$

es también un cerrado en J. Resumimos todo esto en el teorema que sigue.

Teorema 6.7 *Sea K un cuerpo numérico y E un conjunto finito de divisores primos de K. Entonces*

a) J es un grupo topológico abeliano localmente compacto.

b) J_E es un subgrupo cerrado de J.

c) Si $P_\infty \subset E$, entonces J_E es un subgrupo abierto de J.

En las condiciones del apartado c) resulta que J_E es abierto y cerrado en J, con lo que $\{1\}$ es abierto y cerrado en J/J_E, luego este grupo es discreto. En particular tenemos que J/J_{P_∞} es discreto, y es isomorfo al grupo I de los ideales fraccionales, por lo que conviene considerar en él la topología discreta.

Observar que $J_\varnothing$ es compacto, pues es el producto de todos los grupos de unidades. Veamos ahora la continuidad de la norma:

Teorema 6.8 *Sea K un cuerpo numérico y E un conjunto finito de primos de K. La aplicación $\alpha \mapsto \|\alpha\|$ es continua en J y el isomorfismo $J \cong \mathbb{R}^+ \times J^0$ es topológico (i.e. es un homeomorfismo). En particular J_E^0 es cerrado en J y si $P_\infty \subset E$, entonces J_E^0 es abierto en J^0.*

Demostración: Basta probar que la norma es continua en 1, para lo cual basta probar que lo es restringida a J_{P_∞}. Ahora bien, si $\alpha \in J_{P_\infty}$ entonces

$$\|\alpha\| = \prod_{\mathfrak{p}\in P_\infty} \|\alpha_\mathfrak{p}\|,$$

y cada una de las aplicaciones $\|\alpha_\mathfrak{p}\|$ es continua (pues es la composición de la proyección $\alpha \mapsto \alpha_\mathfrak{p}$ con la norma en $K_\mathfrak{p}^*$).

Esto significa que la proyección $J \longrightarrow \mathbb{R}^+ \times J^0 \longrightarrow \mathbb{R}^+$ es continua.

La aplicación $\mathbb{R}^+ \longrightarrow J$ dada por $r \mapsto \alpha_r$ también es continua. Para probarlo podemos considerarla como aplicación $\mathbb{R}^+ \longrightarrow J_{P_\infty}$, donde tenemos la topología producto. Entonces basta ver que al componerla con las proyecciones obtenemos funciones continuas. Las proyecciones no arquimedianas son constantes. Si $\mathfrak{p}$ es un primo arquimediano inducido por el monomorfismo $\sigma : K_\mathfrak{p} \longrightarrow \mathbb{C}$, entonces $(\alpha_r)_\mathfrak{p} = \sigma^{-1}(r^{1/n})$, que es una función continua.

Esto significa que el isomorfismo entre $\mathbb{R}^+$ con su topología usual y el subgrupo formado por los elementos ideales α_r es topológico.

En consecuencia, la aplicación que a cada $\alpha \in J$ le asigna $\alpha(\alpha_r)^{-1}$ (donde $r = \|\alpha\|$) es continua, y es la otra proyección $J \longrightarrow \mathbb{R}^+ \times J^0 \longrightarrow J^0$. Concluimos con esto que la aplicación $J \longrightarrow \mathbb{R}^+ \times J^0$ es continua. La inversa es $(r, \alpha) \mapsto \alpha_r\alpha$, que obviamente es continua. ∎

Teorema 6.9 *Sea K un cuerpo numérico. Entonces K^* es cerrado y discreto en J.*

Demostración: Un entorno de 1 en J lo constituye el conjunto V de los elementos ideales α tales que $|\alpha-1|_\mathfrak{p} \le 1$ para los primos no arquimedianos y $|\alpha-1|_\mathfrak{p} \le 1/2$ para los arquimedianos. Si $\alpha \in K^* \cap V$, la fórmula del producto (2.4) implica que $\alpha - 1 = 0$, luego $K^* \cap V = \{1\}$. Esto prueba que K^* es discreto.

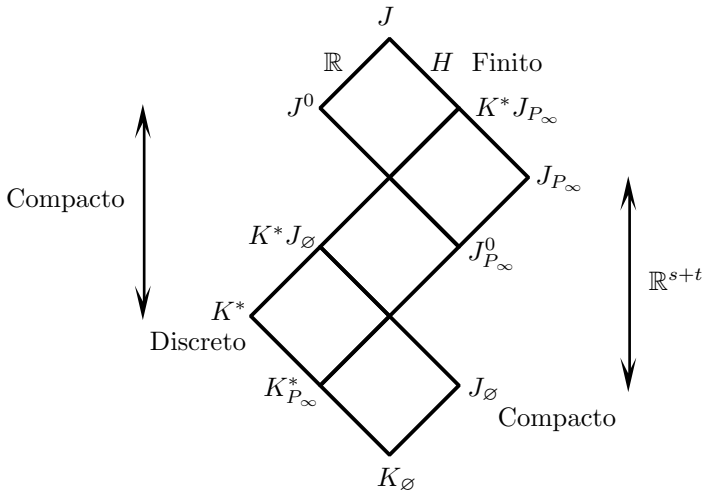
Razonando como en el teorema 6.2 obtenemos un entorno W de 1 tal que $WW^{-1} \subset V$. Para cada $\alpha \in J$, podemos considerar su entorno αW. Si existen u, $v \in K^* \cap \alpha W$, entonces $uv^{-1} \in K^* \cap V = \{1\}$, luego $u = v$. Así pues, αW contiene a lo sumo un punto de K^*. Si $\alpha \notin K^*$ podemos restringir el entorno para obtener otro que no corte a K^*. Así pues, K^* es cerrado. ∎

Como consecuencia podemos considerar como grupos topológicos a los grupos de clases

$$C = J/K^*, \qquad C^0 = J^0/K^*, \qquad C_E = J_E/K_E, \qquad C_E^0 = J_E^0/K_E.$$

Notar que si $P_\infty \subset E$, las inmersiones naturales $C_E \to C$ y $C_E^0 \to C^0$ son homeomorfismos en sus imágenes, por lo que podemos considerar a C_E y C_E^0 como subgrupos abiertos de C y C^0 respectivamente. También tenemos el isomorfismo topológico $C \cong \mathbb{R}^+ \times C^0$.

La figura siguiente resume los principales resultados topológicos que hemos demostrado sobre J junto con algunos que probaremos seguidamente. Todos los subgrupos que aparecen son cerrados.



Ejercicio: Usar que $J_\varnothing$ es compacto para probar que $K^*J_\varnothing$ es cerrado.

Sólo falta probar el isomorfismo topológico $J_{P_\infty}/J_\varnothing \cong \mathbb{R}^{s+t}$ (donde s es el número de primos arquimedianos reales y t el número de primos arquimedianos

complejos) y la compacidad de $C^0 = J^0/K^*$. Respecto a lo primero observamos, más en general, que

$$J_E = \prod_{\mathfrak{p}\in E} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\in P\setminus E} U_\mathfrak{p}, \qquad J_\varnothing = \prod_\mathfrak{p} U_\mathfrak{p},$$

ambos con la topología producto, de donde se sigue inmediatamente el isomorfismo topológico

$$J_E/J\varnothing \cong \prod_{\mathfrak{p}\in E} (K_\mathfrak{p}^*/U_\mathfrak{p}).$$

Ahora, todo número complejo $z \neq 0$ se expresa como $z = |z|(z/|z|)$, lo que da inmediatamente la descomposición $K_\mathfrak{p}^* \cong \mathbb{R}^+ \times U_\mathfrak{p}$ cuando $\mathfrak{p}$ es arquimediano complejo. Lo mismo es válido si $\mathfrak{p}$ es real, pues $R^* \cong \mathbb{R}^+ \times \{\pm 1\}$. Esto implica que $K_\mathfrak{p}^*/U_\mathfrak{p} \cong \mathbb{R}^+ \cong \mathbb{R}$ cuando $\mathfrak{p}$ es arquimediano.

Si $\mathfrak{p}$ es no arquimediano tomamos un primo $\pi \in K_\mathfrak{p}$ y es claro que $K_\mathfrak{p}^* = \langle\pi\rangle \times U_\mathfrak{p}$, con lo que $K_\mathfrak{p}^*/U_\mathfrak{p} \cong \mathbb{Z}$. Como $U_\mathfrak{p}$ es abierto y cerrado el cociente es discreto, luego el isomorfismo es topológico si consideramos en $\mathbb{Z}$ la topología discreta.

Con esto podemos concluir que si E contiene u primos arquimedianos y v primos no arquimedianos entonces $J_E/J_\varnothing$ es topológicamente isomorfo a un producto de u copias de $\mathbb{R}$ y v copias de $\mathbb{Z}$.

Nos ocupamos ahora de la compacidad de C^0. Necesitamos un teorema previo.

Teorema 6.10 *Sea K un cuerpo numérico. Existe una constante $c > 0$ tal que si α es un elemento ideal de K con $\|\alpha\| > c$, entonces existe un $\beta \in K^*$ tal que $|\beta|_\mathfrak{p} \leq |\alpha|_\mathfrak{p}$ para todo divisor primo $\mathfrak{p}$ de K.*

Demostración: Para cada elemento ideal α definimos

$$L(\alpha) = \{\beta \in K \mid |\beta|_\mathfrak{p} \leq |\alpha|_\mathfrak{p} \text{ para todo divisor primo } \mathfrak{p} \text{ de } K\}.$$

Notar que $L(\alpha)$ siempre contiene al cero. Nuestro objetivo es demostrar que si $\|\alpha\|$ es suficientemente grande entonces $L(\alpha)$ contiene más de un elemento.

Llamemos $\lambda(\alpha)$ al número de elementos de $L(\alpha)$. Observar que si $a \in K^*$ entonces la aplicación $\beta \mapsto a\beta$ biyecta $L(\alpha)$ con $L(a\alpha)$, luego $\lambda(a\alpha) = \lambda(\alpha)$.

Sea E el anillo de los enteros de K y sea $v_1, \ldots, v_n$ una base de E como $\mathbb{Z}$-módulo (donde n es el grado de K). Sea c_0 el máximo de los números $n|v_i|_\mathfrak{p}$, donde $i = 1, \ldots, n$ y $\mathfrak{p}$ recorre los primos arquimedianos de K.

Por el teorema de aproximación existe un $u \in K^*$ tal que $c_0 \leq |u\alpha|_\mathfrak{p} \leq 2c_0$ para todo primo arquimediano $\mathfrak{p}$ (basta con que u se aproxime suficientemente a $3c_0/2\alpha_\mathfrak{p}$).

Claramente existe un número natural $m > 0$ tal que $|mu\alpha|_\mathfrak{p} \leq 1$ para todo primo $\mathfrak{p}$ no arquimediano. Llamemos $\alpha' = mu\alpha$. Entonces $\lambda(\alpha') = \lambda(\alpha)$, $\|\alpha'\| = \|\alpha\|$ y además

a) $|\alpha'|_\mathfrak{p} \leq 1$, si $\mathfrak{p}$ es no arquimediano,

b) $c_0|m|_\mathfrak{p} \leq |\alpha'|_\mathfrak{p} \leq 2c_0|m|_\mathfrak{p}$, si $\mathfrak{p}$ es arquimediano.

Queremos probar que si $\|\alpha\|$ es suficientemente grande entonces $\lambda(\alpha) \geq 1$. Lo que acabamos de ver es que podemos suponer que α cumple las propiedades anteriores.

En particular la propiedad a) nos da que el ideal fraccional (α) es de hecho un ideal de E.

Sea L el conjunto de todos los enteros de K de la forma $m_1v_1 + \cdots + m_nv_n$, donde $0 \leq m_i \leq m$.

Entonces L tiene más de m^n elementos. Por lo tanto ha de haber un conjunto $L' \subset L$ con al menos $m^n/\,\mathrm{N}(\alpha)$ elementos con la misma imagen respecto a la proyección canónica $E \longrightarrow E/(\alpha)$. Fijemos uno de ellos x. Si $y \in L'$ y $\mathfrak{p}$ es un divisor no arquimediano de K tenemos que $x - y \in (\alpha)$, luego $|x-y|_\mathfrak{p} \leq |\alpha|_\mathfrak{p}$.

Si $\mathfrak{p}$ es arquimediano las definiciones de L y de c_0 junto con la propiedad b) nos dan que

$$|x-y|_\mathfrak{p} \leq c_0|m|_\mathfrak{p} \leq |\alpha|_\mathfrak{p}.$$

Así pues, $x - y \in L(\alpha)$ y, por lo tanto, $\lambda(\alpha) \geq m^n/\,\mathrm{N}(\alpha)$.

Teniendo en cuenta la propiedad b) es claro que

$$m^n = \prod_{\mathfrak{p}|\infty} m^{n_\mathfrak{p}} = \prod_{\mathfrak{p}|\infty} |m|_\mathfrak{p}^{n_\mathfrak{p}} > c_1 \prod_{\mathfrak{p}|\infty} |\alpha|_\mathfrak{p}^{n_\mathfrak{p}} = c_1 \prod_{\mathfrak{p}|\infty} \|\alpha\|_\mathfrak{p},$$

donde la constante c_1 depende sólo de K (y $n_\mathfrak{p}$ es el grado local de K en $\mathfrak{p}$).

Por otra parte, si $\mathfrak{p}$ es un primo no arquimediano que divide a (α) con multiplicidad k entonces según (2.5) tenemos que $\|\alpha\|_\mathfrak{p} = 1/\,\mathrm{N}\,\mathfrak{p}^k$. Multiplicando para todo primo $\mathfrak{p}$ no arquimediano resulta que $1/\,\mathrm{N}(\alpha) = \prod_{\mathfrak{p}\nmid\infty} \|\alpha\|_\mathfrak{p}$, con lo que concluimos que

$$\lambda(\alpha) > c_1 \prod_{\mathfrak{p}|\infty} \|\alpha\|_\mathfrak{p} \prod_{\mathfrak{p}\nmid\infty} \|\alpha\|_\mathfrak{p} = c_1\|\alpha\|.$$

Así pues, el teorema se cumple con $c = 1/c_1$. ∎

Teorema 6.11 *Sea K un cuerpo numérico y E un conjunto finito de divisores primos de K tal que $P_\infty \subset E$. Entonces los grupos C^0 y C^0_E son compactos.*

Basta probar que $C^0 = J^0/K^*$ es compacto. Puesto que K^* está contenido en el núcleo de la norma, tenemos definido un epimorfismo $f : J/K^* \longrightarrow \mathbb{R}^+$ dado por $f([\alpha]) = \|\alpha\|$.

El núcleo de este epimorfismo es precisamente C^0, y es claro que si $r \in \mathbb{R}^+$ entonces $f^{-1}(r)$ es homeomorfo a C^0, luego basta probar que uno de estos $J_r = f^{-1}(r)$ es compacto. Concretamente tomamos r mayor que la constante c dada por el teorema anterior. Así, si $[\alpha] \in J_r$ se cumple que $\|\alpha\| > c$, luego según dicho teorema existe un $\beta^{-1} \in K^*$ de manera que $|\beta^{-1}|_\mathfrak{p} \leq |\alpha|_\mathfrak{p}$ para todo divisor primo $\mathfrak{p}$ de K o, equivalentemente, $1 \leq \|\beta\alpha\|_\mathfrak{p}$. Por otra parte

$$\|\beta\alpha\|_\mathfrak{p} = \frac{\prod_\mathfrak{q} \|\beta\alpha\|_\mathfrak{q}}{\prod_{\mathfrak{q}\neq\mathfrak{p}} \|\beta\alpha\|_\mathfrak{q}} \leq \frac{r}{1} = r.$$

Así pues, tenemos que $1 \leq \|\beta\alpha\|_\mathfrak{p} \leq r$ para todo divisor primo $\mathfrak{p}$ de K.

Ahora bien, $\|\beta\alpha\|_\mathfrak{p}$ sólo puede ser mayor que 1 para un número finito de primos. Sea E el conjunto formado por estos primos más los primos arquimedianos. Lo que hemos probado es que para cada $[\alpha] \in J_r$ existe un $\beta \in K^*$ tal que $\beta\alpha$ está en el conjunto X formado por todos los $\gamma \in J$ tales que

a) $1 \le \|\gamma\|_\mathfrak{p} \le r$ para todo $\mathfrak{p} \in E$,

b) $\|\gamma\|_\mathfrak{p} = 1$ para todo $\mathfrak{p} \in P \setminus E$.

Puesto que $[\alpha] = [\beta\alpha]$, esto significa que J_r está contenido en la imagen de X a través de la proyección canónica $J \longrightarrow C$. Pero X es compacto, ya que es el producto de un número finito de anillos en ciertos cuerpos $K_\mathfrak{p}$ (compactos) por los grupos de unidades de los cuerpos restantes (compactos también). Como J_r es cerrado concluimos que también es compacto. ∎

Por último nos ocupamos de los grupos $W_\mathfrak{m}$ y $J_\mathfrak{m}$. Notar que cada grupo $W_\mathfrak{m}(\mathfrak{p})$ es abierto y cerrado en $K_\mathfrak{m}^*$, luego si E contiene a los primos arquimedianos y a los divisores de $\mathfrak{m}$, se cumple que $W_\mathfrak{m}$ es abierto y cerrado en J_E (pues J_E tiene la topología producto y casi todos los factores de $W_\mathfrak{m}$ coinciden con los de J_E). Esto implica a su vez que cada $W_\mathfrak{m}$ es abierto y cerrado en J, luego los grupos $J/W_\mathfrak{m}$ son discretos y todo grupo intermedio es abierto y cerrado. Así cada $J_\mathfrak{m}$ es abierto y cerrado en J y los cocientes $J_\mathfrak{m}/W_\mathfrak{m}$ son discretos.

El resultado principal sobre estos grupos es el siguiente:

Teorema 6.12 *Sea K un cuerpo numérico y H un subgrupo del grupo J de los elementos ideales de K. Entonces H es abierto en J si y sólo si existe un divisor $\mathfrak{m}$ de K tal que $W_\mathfrak{m} \le H$.*

Demostración: Una implicación es obvia. Si H es abierto, cambiándolo por $H \cap J_{P_\infty}$ podemos suponer que

$$H \le J_{P_\infty} = \prod_{\mathfrak{p}\in P_\infty} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\in P\setminus P_\infty} U_\mathfrak{p}.$$

Entonces H contiene un entorno básico de 1 para la topología producto. Puesto que si $\mathfrak{p}$ es no arquimediano los grupos $W_\mathfrak{m}(\mathfrak{p})$ forman una base de entornos de 1 en $U_\mathfrak{p}$, es claro que un un entorno básico de 1 para la topología producto es de la forma

$$\prod_{\mathfrak{p}\in P_\infty} A_\mathfrak{p} \times \prod_{\mathfrak{p}\in P\setminus P_\infty} W_\mathfrak{m}(\mathfrak{p}) \le H,$$

para cierto divisor $\mathfrak{m}$ de K y ciertos entornos de 1 (abiertos) $A_\mathfrak{p}$ en cada grupo $K_\mathfrak{p}^*$. No supone ninguna alteración suponer que $\mathfrak{m}$ es divisible entre todos los primos infinitos de K. Sea C_1 la componente conexa de 1 en J. Entonces $C_1 \cap H$ es un subgrupo abierto de C_1 y, por conexión, ha de ser $C_1 \cap H = C_1$, o sea, $C_1 \le H$.

Pero $\prod_{\mathfrak{p}\in P_\infty} W_\mathfrak{m}(\mathfrak{p}) \times 1$ es un subgrupo conexo de J, luego está contenido en H, como también lo está el subgrupo $1 \times \prod_{\mathfrak{p}\in P\setminus P_\infty} W_\mathfrak{m}(\mathfrak{p})$. El producto de ambos subgrupos es $W_\mathfrak{m} \le H$. ∎

Más aún, es fácil ver que $W_{\mathfrak{m}}W_{\mathfrak{n}} = W_{(\mathfrak{m},\mathfrak{n})}$ (cada elemento del grupo de la derecha se descompone en producto de elementos de los grupos de la izquierda dejando su componente en el factor apropiado y haciendo la componente del otro factor igual a 1), luego existe un mínimo divisor $\mathfrak{f}$ tal que $W_{\mathfrak{f}} \leq H$.

Definición 6.13 Sea K un cuerpo numérico y sea H un subgrupo abierto del grupo J de los elementos ideales de K. Diremos que un divisor $\mathfrak{m}$ de K es *admisible* para H si $W_{\mathfrak{m}} \leq H$. Llamaremos *conductor* de H al menor divisor admisible. La f proviene del alemán *Fürer*.

6.3 Extensiones de elementos ideales

En esta sección consideraremos una extensión de cuerpos numéricos K/k y estudiaremos la relación entre los elementos ideales de K y los de k. Usaremos subíndices o superíndices, según convenga, para distinguir los grupos asociados a cada cuerpo. En primer lugar veamos que J_k puede identificarse con un subgrupo de J_K. En efecto.

Teorema 6.14 *Sea K/k una extensión finita de cuerpos numéricos. Entonces la aplicación $f : J_k \longrightarrow J_K$ dada por*

$$f(\alpha)_{\mathfrak{P}} = \alpha_{\mathfrak{p}}, \qquad \text{donde } \mathfrak{P} \mid \mathfrak{p},$$

es un isomorfismo topológico entre J_k y un subgrupo cerrado de J_K.

Demostración: Claramente f es un monomorfismo. Si E es un conjunto finito de primos de k que contiene a los primos arquimedianos y E' es el conjunto de sus divisores en K, es fácil ver que la restricción de f a J_E es un isomorfismo topológico en su imagen y que ésta es un subgrupo cerrado de $J_{E'}$ (tener en cuenta que J_E y $J_{E'}$ tienen la topología producto). En otras palabras, si identificamos a J_k con su imagen por f, cada grupo J_E recibe la misma topología de J_k que de J_K. Por consiguiente la topología de J_k coincide con la inducida desde J_K. Un punto de J_K en la clausura de J_k estaría en la clausura de algún J_E, pero estos grupos son cerrados, luego J_k también lo es. ∎

Observar que la identificación del teorema anterior es consistente con la identificación de k^* con un subgrupo de J_k, es decir, el diagrama siguiente es conmutativo:

$$\begin{array}{ccc} J_k & \longrightarrow & J_K \\ \uparrow & & \uparrow \\ k^* & \longrightarrow & K^* \end{array}$$

En particular $K^* \cap J_k = k^*$, lo que nos permite identificar a C_k con un subgrupo cerrado de C_K.

Nos ocupamos ahora de las normas:

Definición 6.15 Sea K/k una extensión de cuerpos numéricos. Definimos la *norma* $\mathrm{N} : J_K \longrightarrow J_k$ como la dada por

$$\mathrm{N}(\alpha)_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P}),$$

donde $\mathrm{N}_\mathfrak{P} : K_\mathfrak{P} \longrightarrow k_\mathfrak{p}$ es la norma local de la extensión $K_\mathfrak{P}/k_\mathfrak{p}$.

Es claro que si $\mathfrak{P}$ es no arquimediano y $\alpha_\mathfrak{P}$ es una unidad de $K_\mathfrak{P}$ entonces $\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P})$ es una unidad de $k_\mathfrak{p}$, por lo que $\mathrm{N}(\alpha)$ es ciertamente un elemento ideal de k. Obviamente la norma es un homomorfismo de grupos.

La fórmula (2.1) implica que la norma que acabamos de definir extiende a la norma de la extensión K/k cuando consideramos $K^* \le J_K$ y $k^* \le J_k$.

También es inmediato que las normas locales son continuas, de donde se sigue fácilmente que la restricción de la norma en J_K a cualquier subgrupo J_E^K es continua, y a su vez esto implica la continuidad de la norma en J_K.

El teorema siguiente prueba que la norma en J_K es consistente también con la norma entre ideales fraccionales.

Teorema 6.16 *Sea K/k una extensión de cuerpos numéricos. Entonces para todo $\alpha \in J_K$ se cumple $\big(\mathrm{N}(\alpha)\big) = \mathrm{N}\big((\alpha)\big)$. Es decir, el diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} J_K & \longrightarrow & I_K \\ {\scriptstyle \mathrm{N}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}} \\ J_k & \longrightarrow & I_k \end{array}$$

Demostración: Sea $\alpha \in J_K$. Si $\mathfrak{p}$ es un primo no arquimediano en k, entonces el exponente de $\mathfrak{p}$ en $\big(\mathrm{N}(\alpha)\big)$ es

$$v_\mathfrak{p}(\mathrm{N}(\alpha)_\mathfrak{p}) = \sum_{\mathfrak{P}|\mathfrak{p}} v_\mathfrak{p}(\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P})) = \sum_{\mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}/\mathfrak{p}) v_\mathfrak{P}(\alpha_\mathfrak{P}),$$

pero $v_\mathfrak{P}(\alpha_\mathfrak{P})$ es el exponente de $\mathfrak{P}$ en (α), luego el término izquierdo de la igualdad anterior es el exponente de $\mathfrak{p}$ en $\mathrm{N}\big((\alpha)\big)$, y esto prueba la igualdad $\big(\mathrm{N}(\alpha)\big) = \mathrm{N}\big((\alpha)\big)$. ∎

La norma induce un homomorfismo entre los grupos de clases $\mathrm{N} : C_K \longrightarrow C_k$, pues si $[\alpha] = [\beta] \in C_K$, entonces $\alpha = \beta\gamma$, para un cierto $\gamma \in K^*$, luego tenemos $\mathrm{N}(\alpha) = \mathrm{N}(\beta)\,\mathrm{N}(\gamma)$ con $\mathrm{N}(\gamma) \in k^*$, por lo que $[\mathrm{N}(\alpha)] = [\mathrm{N}(\beta)]$.

Un hecho crucial en la teoría de cuerpos de clases es que el grupo de normas $\mathrm{N}[J_k]$ es abierto (y por tanto cerrado) en J_k. Esto no es trivial, sino que se desprende de los dos teoremas siguientes:

Teorema 6.17 *Sea K/k una extensión finita separable de cuerpos métricos completos. Entonces el grupo de normas $\mathrm{N}[K^*]$ es abierto en k^*.*

DEMOSTRACIÓN: Si $\alpha = \mathrm{N}(\beta)$, para un $\beta \in K^*$ y f es su polinomio mínimo, entonces el término independiente de f es $(-1)^n\alpha$, donde n es el grado de f. El teorema 2.18 implica que existe un $\delta > 0$ de modo que si $|\alpha - \alpha'| < \delta$ entonces el polinomio que resulta de cambiar el término independiente de f por $(-1)^n\alpha'$ es irreducible en $k[x]$ y tiene una raíz β' tal que $k(\beta') = k(\beta)$. En particular $\beta' \in K$ y $\mathrm{N}(\beta') = \alpha'$. Por consiguiente la bola de centro α y radio δ está contenida en $\mathrm{N}[K^*]$, lo que prueba que éste es abierto. ∎

Teorema 6.18 *Sea K/k una extensión no ramificada de cuerpos métricos discretos localmente compactos. Entonces toda unidad de k es la norma de una unidad de K.*

DEMOSTRACIÓN: Sean D y E los anillos de enteros de K y k respectivamente. Sea $\mathfrak{p}$ el único primo de D y $\mathfrak{P}$ el único primo de E. Por la compacidad local ([7.15]), los cuerpos de restos $\overline{K} = E/\mathfrak{P}$ y $\overline{k} = D/\mathfrak{p}$ son finitos.

Según el teorema 2.37, la extensión K/k es finita de Galois con grupo de Galois cíclico. Más aún, según 2.36 el grupo de Galois es isomorfo al de la extensión de los cuerpos de restos. Además es claro que la norma de esta extensión de cuerpos de restos viene inducida por la norma de K/k, es decir, $\mathrm{N}([\alpha]) = [\mathrm{N}(\alpha)]$, para todo $\alpha \in E$.

Ahora bien, la norma y la traza son suprayectivas en el caso de extensiones finitas de cuerpos finitos, luego, dada una unidad u de k, existe una unidad $a_0 \in K$ tal que $u \equiv \mathrm{N}(\alpha_0) \pmod{\mathfrak{p}}$. Por lo tanto $u\,\mathrm{N}(\alpha_0)^{-1} = 1 + c_1\pi$, donde π es un primo en k y $c_1 \in D$.

Consideremos un elemento de la forma $\alpha_1 = 1 + x_1\pi$, donde $x_1 \in E$. Es claro que $\mathrm{N}(\alpha_1) \equiv 1 + \mathrm{Tr}(x_1)\pi \pmod{\mathfrak{p}^2}$. Por la suprayectividad de la traza podemos tomar x_1 de modo que $\mathrm{Tr}(x_1) \equiv c_1 \pmod{\mathfrak{p}}$, y así $u\,\mathrm{N}(\alpha_0)^{-1} \equiv \mathrm{N}(\alpha_1) \pmod{\mathfrak{p}^2}$. De aquí se concluye que

$$u\,\mathrm{N}(\alpha_0\alpha_1)^{-1} = 1 + c_2\pi^2, \qquad \text{con } c_2 \in D.$$

Inductivamente obtenemos elementos $\alpha_0, \alpha_1, \ldots, \alpha_n \in E$ tales que

$$\alpha_n \equiv 1 \pmod{\mathfrak{p}^n} \quad \text{y} \quad u\,\mathrm{N}(\alpha_0\alpha_1\cdots\alpha_n)^{-1} \equiv 1 \pmod{\mathfrak{p}^{n+1}}.$$

Basta probar que la sucesión de productos $\alpha_0\alpha_1\cdots\alpha_n$ es de Cauchy, pues entonces convergerá a un $\alpha \in E$ que cumplirá $\mathrm{N}(\alpha) = u$. Obviamente α es una unidad. Ahora bien, para cada natural n tenemos

$$\left|\prod_{k=1}^{n}\alpha_k - \prod_{k=1}^{n-1}\alpha_k\right| = \left|\prod_{k=1}^{n-1}\alpha_k\right| |1 - a_n| \le |1 - \alpha_n| \longrightarrow 0,$$

y basta aplicar [7.6] ∎

Como consecuencia:

Teorema 6.19 *Sea K/k una extensión de cuerpos numéricos. Entonces el grupo de normas $\mathrm{N}[J_K]$ es abierto y cerrado en J_k, e igualmente, el grupo de normas $\mathrm{N}[C_K] = \mathrm{N}[J_K]k^*/k^*$ es abierto y cerrado en C_k.*

DEMOSTRACIÓN: La segunda afirmación es consecuencia inmediata de la primera. Para probar ésta consideramos un conjunto finito E de primos de k que contenga a todos los primos arquimedianos y a los que se ramifican en K.

Sea S un conjunto de primos de K formado por un único divisor de cada primo de k. Para cada primo $\mathfrak{p}$ de k, sea $\mathfrak{P} \in S$ el primo que lo divide. Si $\mathfrak{p} \in E$ escogemos un $\alpha_\mathfrak{P} \in K_\mathfrak{P}^*$ y en caso contrario tomamos $\alpha_\mathfrak{P} \in U_\mathfrak{P}$. Completando con unos en los primos de K que no están en S obtenemos un elemento ideal $\alpha \in J_K$ cuya norma es un elemento arbitrario del producto

$$\prod_{\mathfrak{P}\in S_E} \mathrm{N}_\mathfrak{P}[K_\mathfrak{P}^*] \times \prod_{\mathfrak{P}\in P\setminus S_E} \mathrm{N}_\mathfrak{P}[U_\mathfrak{P}],$$

donde S_E es el conjunto de primos de S que dividen a primos de E.

Según el teorema anterior, si $\mathfrak{P} \in P \setminus S_E$, se cumple $\mathrm{N}_\mathfrak{P}[U_\mathfrak{P}] = U_\mathfrak{p}$. Por el teorema 6.17 el grupo de normas locales $\mathrm{N}_\mathfrak{P}[K_\mathfrak{P}^*]$ es abierto en $k_\mathfrak{p}^*$. Por consiguiente, el producto anterior es abierto en J_E, y está contenido en $\mathrm{N}[J_K]$, luego el grupo de normas es abierto. ∎

En el capítulo anterior anticipamos que el núcleo del homomorfismo de Artin $\omega : I(\Delta) \longrightarrow G(K/k)$ de una extensión abeliana de cuerpos numéricos, es de la forma $P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$, para un cierto divisor $\mathfrak{m}$ de k. Ahora ya podemos decir quién es este divisor: se trata del conductor del grupo de normas. No obstante todavía no estamos en condiciones de relacionarlo con el homomorfismo de Artin. Nos limitaremos a definirlo y obtener algunos resultados de interés.

Definición 6.20 Sea K/k una extensión de cuerpos numéricos. Diremos que un divisor $\mathfrak{m}$ de k es *admisible* para K/k si lo es para el grupo de normas $\mathrm{N}[J_K]$, es decir, si $W_\mathfrak{m} \leq \mathrm{N}[J_K]$. El *conductor* de la extensión es el conductor $\mathfrak{f}$ del grupo de normas, es decir, el mínimo divisor admisible para la extensión.

De este modo, el conductor es el menor divisor admisible. En el teorema anterior hemos probado que el grupo de normas $\mathrm{N}[J_K]$ contiene un subgrupo abierto de la forma

$$\prod_{\mathfrak{P}\in S_E} \mathrm{N}_\mathfrak{P}[K_\mathfrak{P}^*] \times \prod_{\mathfrak{p}\in P\setminus E} U_\mathfrak{p},$$

donde E está formado por los primos arquimedianos de k y los que se ramifican en K y S_E contiene un divisor en K de cada primo de E.

Ahora observamos que si $\mathfrak{p}$ es un primo arquimediano en k no ramificado en K, entonces $K_\mathfrak{P} = k_\mathfrak{p}$, luego $\mathrm{N}_\mathfrak{P}[K_\mathfrak{P}^*] = k_\mathfrak{p}^*$. Por otra parte, si $\mathfrak{p}$ es ramificado (y por consiguiente real), la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ es isomorfa a $\mathbb{C}/\mathbb{R}$, y el grupo de normas de esta última es $\mathbb{R}^+$, luego

$$\mathrm{N}[K_\mathfrak{P}^*] = \{\alpha \in k^* \mid \sigma(\alpha) > 0\},$$

donde $\sigma : k_\mathfrak{p} \longrightarrow \mathbb{R}$ es el monomorfismo que induce a $\mathfrak{p}$.

De todo esto se sigue claramente que podemos construir un divisor $\mathfrak{m}$ divisible únicamente entre los primos de k ramificados en K tal que $W_\mathfrak{m}$ esté contenido en el producto anterior. Dicho divisor será admisible, luego concluimos que

el conductor de la extensión K/k sólo es divisible entre primos ramificados en K. Más adelante veremos que, de hecho, es divisible entre todos los primos ramificados, lo que implicará que $I(\mathfrak{f}) = I(\Delta)$.

Según esto, el homomorfismo de Artin de una extensión abeliana de cuerpos numéricos permite representar su grupo de Galois como el grupo de clases de ideales $I(\mathfrak{f})/P_\mathfrak{f}\,\mathrm{N}(\mathfrak{f})$. Ahora probamos que este grupo de clases puede representarse también en términos de elementos ideales.

Teorema 6.21 *Sea K/k una extensión de cuerpos numéricos y sea $\mathfrak{m}$ un divisor admisible. Entonces*

$$C_k/\,\mathrm{N}[C_K] \cong J_k/k^*\,\mathrm{N}[J_K] \cong I(\mathfrak{m})/P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}).$$

El segundo isomorfismo viene inducido por el isomorfismo $J_k/k^* \cong J_\mathfrak{m}/k_\mathfrak{m}$ seguido del epimorfismo $J_\mathfrak{m}/k_\mathfrak{m} \longrightarrow I(\mathfrak{m})$.

Demostración: Consideremos el epimorfismo $J_\mathfrak{m} \longrightarrow I(\mathfrak{m})$ y calculemos la antiimagen de $P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$. Llamemos H al conjunto de los elementos ideales de J_K cuyas componentes en los primos que dividen a $\mathfrak{m}$ sean iguales a 1. Claramente H es un subgrupo de $J_\mathfrak{m}^K$ y vamos a probar que la antiimagen de $P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$ es $k_\mathfrak{m}W_\mathfrak{m}\,\mathrm{N}[H]$.

Sea, pues, $\alpha \in J_\mathfrak{m}$ tal que $(\alpha) = (\beta)\,\mathrm{N}(\mathfrak{a})$, donde $\beta \in k_\mathfrak{m}$ y $\mathfrak{a}$ es un ideal fraccional de K primo con $\mathfrak{m}$.

Definimos $\gamma \in J_K$ del modo siguiente:

Si $\mathfrak{P}$ es arquimediano o $\mathfrak{P} \mid \mathfrak{m}$ o $\mathfrak{P}$ es primo con $\mathfrak{a}$ entonces $\gamma_\mathfrak{P} = 1$ (así $\gamma \in H$).

Si $\mathfrak{P}$ es no arquimediano y divide a $\mathfrak{a}$ (con exponente positivo o negativo) entonces tomamos $\gamma_\mathfrak{P}$ de modo que $v_\mathfrak{P}(\gamma_\mathfrak{P})$ sea el exponente de $\mathfrak{P}$ en $\mathfrak{a}$.

Claramente $(\gamma) = \mathfrak{a}$ y por el teorema 6.16 sabemos que $\big(\mathrm{N}(\gamma)\big) = \mathrm{N}(\mathfrak{a})$, luego $(\alpha) = \big(\beta\,\mathrm{N}(\gamma)\big)$. Como el núcleo del epimorfismo $J_\mathfrak{m}, \longrightarrow I(\mathfrak{m})$ es $W_\mathfrak{m}$ resulta que α y $\beta\,\mathrm{N}(\gamma)$ se diferencian en un elemento de este subgrupo, y así concluimos que $\alpha \in k_\mathfrak{m}W_\mathfrak{m}\,\mathrm{N}[H]$.

Recíprocamente, la imagen de $W_\mathfrak{m}$ es el subgrupo trivial, la imagen de $k_\mathfrak{m}$ es $P_\mathfrak{m}$ y la imagen de $\mathrm{N}[H]$ está contenida en $\mathrm{N}(\mathfrak{m})$, pues si $\alpha \in H$ entonces $\big(\mathrm{N}(\alpha)\big) = \mathrm{N}\big((\alpha)\big)$ y (α) es un ideal de K primo con $\mathfrak{m}$.

Con esto tenemos probado que

$$J_\mathfrak{m}/k_\mathfrak{m}W_\mathfrak{m}\,\mathrm{N}[H] \cong I(\mathfrak{m})/P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}).$$

Ahora consideramos el isomorfismo $J_k/k^* \cong J_\mathfrak{m}/k_\mathfrak{m}$ y hemos de probar que la antiimagen de $k_\mathfrak{m}W_\mathfrak{m}\,\mathrm{N}[H]/k_\mathfrak{m}$ es precisamente $k^*\,\mathrm{N}[J_K]/k^*$. Es fácil ver que esto es equivalente a que $k_\mathfrak{m}W_\mathfrak{m}\,\mathrm{N}[H] = J_\mathfrak{m} \cap k^*\,\mathrm{N}[J_K]$.

Una inclusión es clara: $k_\mathfrak{m} \le J_\mathfrak{m} \cap k^*$, $\mathrm{N}[H] \le J_\mathfrak{m} \cap \mathrm{N}[J_K]$ y, como $\mathfrak{m}$ es admisible, $W_\mathfrak{m} \le J_\mathfrak{m} \cap \mathrm{N}[J_K]$.

Para probar la otra inclusión tomamos $\alpha = \beta\,\mathrm{N}(\gamma)$, donde $\beta \in k^*$, $\gamma \in J_K$ y suponemos que $\alpha \in J_\mathfrak{m}$. Mediante el teorema de aproximación y la continuidad

de las normas locales y el producto en k es fácil probar la existencia de un $\delta \in K^*$ de modo que

$$|\,\mathrm{N}(\delta)_\mathfrak{p} - \mathrm{N}(\gamma^{-1})_\mathfrak{p}|_\mathfrak{p} < |\,\mathrm{N}(\gamma^{-1})_\mathfrak{p}|_\mathfrak{p}\epsilon$$

para un número real $\epsilon > 0$ prefijado y todo $\mathfrak{p} \mid \mathfrak{m}$. De aquí llegamos a que $|\,\mathrm{N}(\delta\gamma)_\mathfrak{p} - 1|_\mathfrak{p} < \epsilon$ y, si ϵ es suficientemente pequeño, esto implica que $\mathrm{N}(\delta\gamma) \in J_\mathfrak{m}$.

Así, $\alpha = (\beta\,\mathrm{N}(\delta^{-1}))\,\mathrm{N}(\delta\gamma)$ y, como α y $\mathrm{N}(\delta\gamma)$ están en $J_\mathfrak{m}$, concluimos que $\beta\,\mathrm{N}(\delta^{-1})$ está, en $J_\mathfrak{m} \cap k^* = k_\mathfrak{m}$.

Por último podemos descomponer $\mathrm{N}(\delta\gamma) = \mathrm{N}(\gamma_1)\,\mathrm{N}(\gamma_2)$, donde γ_1 tiene iguales a 1 las componentes correspondientes a los divisores de $\mathfrak{m}$ y γ_2 tiene iguales a 1 las componentes correspondientes a primos que no dividen a $\mathfrak{m}$.

Así, $\mathrm{N}(\gamma_1) \in \mathrm{N}[H]$ y (si ϵ es suficientemente pequeño) $\mathrm{N}(\gamma_2) \in W_\mathfrak{m}$. En consecuencia,

$$\alpha = (\beta\,\mathrm{N}(\delta^{-1}))\,\mathrm{N}(\gamma_1)\,\mathrm{N}(\gamma_2) \in k_\mathfrak{m} W_\mathfrak{m}\,\mathrm{N}[H],$$

como queríamos probar. ∎

Del teorema anterior se desprende en particular que los grupos $I(\mathfrak{m})/P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$ son todos isomorfos, cuando $\mathfrak{m}$ varía entre los ideales admisibles para la extensión K/k. Más precisamente, si $\mathfrak{m} \mid \mathfrak{n}$ son dos divisores admisibles, la inclusión $I(\mathfrak{n}) \longrightarrow I(\mathfrak{m})$ induce un isomorfismo

$$I(\mathfrak{n})/P_\mathfrak{n}\,\mathrm{N}(\mathfrak{n}) \cong I(\mathfrak{m})/P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}).$$

En efecto, dada una clase $[\mathfrak{a}]$ en el primer grupo, tomamos $\alpha \in J_\mathfrak{n}$ tal que $(\alpha) = \mathfrak{a}$. Entonces la antiimagen en $C/\,\mathrm{N}[C]$ de $[\mathfrak{a}]$ por el isomorfismo del teorema anterior es $[\alpha]$, y la imagen de ésta en $I(\mathfrak{m})/P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$ por el isomorfismo correspondiente es $[\mathfrak{a}]$. Así pues, la composición de los dos isomorfismos es el homomorfismo inducido por la inclusión. Del hecho de que sea inyectivo se sigue en particular que

$$P_\mathfrak{n}\,\mathrm{N}(\mathfrak{n}) = I(\mathfrak{n}) \cap P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}). \tag{6.3}$$

6.4 Extensiones de Galois

Consideremos ahora el caso de una extensión de Galois K/k de cuerpos numéricos.

En primer lugar observamos que los k-automorfismos de K inducen automorfismos del grupo de elementos ideales J_K. Más en general, supongamos que $\sigma : K \longrightarrow L$ es un isomorfismo entre cuerpos numéricos. Si $\mathfrak{P}$ es un primo de K, asociado al valor absoluto $|\ |_\mathfrak{P}$, entonces σ se extiende a una isometría $\sigma : K_\mathfrak{P} \longrightarrow L_{\sigma(\mathfrak{P})}$. De aquí podemos definir $\sigma : J_K \longrightarrow J_L$ mediante $\sigma(\alpha)_{\sigma(\mathfrak{P})} = \sigma(\alpha_\mathfrak{P})$, lo que claramente es un isomorfismo topológico que restringido a K^* coincide con el isomorfismo de partida.

En particular, cada $\sigma \in G(K/k)$ puede verse también como un automorfismo continuo de J_K. Si $\alpha \in J_K$ y $\mathfrak{P}$ es un primo en K, entonces $\sigma(\alpha)_\mathfrak{P} = \sigma(\alpha_{\sigma^{-1}(\mathfrak{P})})$.

Teorema 6.22 *Sea K/k una extensión de Galois de cuerpos numéricos. Entonces los elementos ideales de J_K fijados por todos los k-automorfismos de K son exactamente los de J_k.*

DEMOSTRACIÓN: Si $\alpha \in J_k$, entonces, para cada primo $\mathfrak{P}$ de k, se cumple $\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{p}}$, donde $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$. Entonces, si $\sigma \in G(K/k)$, tenemos

$$\sigma(\alpha)_{\mathfrak{P}} = \sigma(\alpha_{\sigma^{-1}(\mathfrak{P})}) = \sigma(\alpha_{\mathfrak{p}}) = \alpha_{\mathfrak{p}} = \alpha_{\mathfrak{P}},$$

luego $\sigma(\alpha) = \alpha$.

Recíprocamente, si $\alpha \in J_K$ es fijado por todos los k-automorfismos, sea $\mathfrak{P}$ un primo en K y sea $\sigma \in G(K/k)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}$. Entonces

$$\sigma(\alpha_{\mathfrak{P}}) = \sigma(\alpha)_{\mathfrak{P}} = \alpha_{\mathfrak{P}}.$$

Si $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$, hemos probado que $\alpha_{\mathfrak{P}}$ es fijado por todos los automorfismos de $G(K_{\mathfrak{P}}/k_{\mathfrak{p}})$, luego $\alpha_{\mathfrak{P}} \in k_{\mathfrak{p}}$.

Por otra parte, si $\mathfrak{P}'$ es otro divisor de $\mathfrak{p}$ en K, existe un $\sigma \in G(K/k)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Entonces

$$\alpha_{\mathfrak{P}} = \sigma(\alpha_{\mathfrak{P}}) = \sigma(\alpha)_{\mathfrak{P}'} = \alpha_{\mathfrak{P}'}.$$

Así pues, podemos definir $\alpha_{\mathfrak{p}} = \alpha_{\mathfrak{P}} \in k_{\mathfrak{p}}^*$, para cualquier divisor $\mathfrak{P}$ de $\mathfrak{p}$ en K, y la definición no depende de la elección de éste. Claramente entonces, $\alpha \in J_k$. ∎

Teorema 6.23 *Sea K/k una extensión de Galois de cuerpos numéricos, sea G su grupo de Galois y $\alpha \in J_K$. Entonces*

$$\mathrm{N}(\alpha) = \prod_{\sigma\in G} \sigma(\alpha).$$

DEMOSTRACIÓN: Sea $\mathfrak{P}$ un primo en K y sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ sus conjugados, digamos $\mathfrak{P} = \mathfrak{P}_1$. Fijemos un $\sigma_i \in G$ tal que $\sigma_i(\mathfrak{P}_i) = \mathfrak{P}$. Observemos que los automorfismos que cumplen $\sigma(\mathfrak{P}_i) = \mathfrak{P}$ son los de la forma $\sigma = \tau\sigma_i$, donde $\tau \in G_{\mathfrak{P}_i}$. Así pues,

$$\prod_{\sigma\in G} \sigma(\alpha)_{\mathfrak{P}} = \prod_{\sigma\in G} \sigma(\alpha_{\sigma^{-1}(\mathfrak{P})}) = \prod_{i=1}^{r} \prod_{\sigma(\mathfrak{P}_i)=\mathfrak{P}} \sigma(\alpha_{\mathfrak{P}_i}) = \prod_{i=1}^{r} \prod_{\tau\in G_{\mathfrak{P}_i}} \sigma_i(\tau(\alpha_{\mathfrak{P}_i}))$$

$$= \prod_{i=1}^{r} \sigma_i\big(\mathrm{N}_{\mathfrak{P}_i}(\alpha_{\mathfrak{P}_i})\big) = \prod_{i=1}^{r} \mathrm{N}_{\mathfrak{P}_i}(\alpha_{\mathfrak{P}_i}) = \mathrm{N}(\alpha)_{\mathfrak{P}}.$$

(Observar que $\sigma_i\big(\mathrm{N}_{\mathfrak{P}_i}(\alpha_{\mathfrak{P}_i})\big) = \mathrm{N}_{\mathfrak{P}_i}(\alpha_{\mathfrak{P}_i})$ porque la norma está en $k_{\mathfrak{p}}$.) ∎

Si dos elementos ideales de K se diferencian en un elemento de K^* es claro que sus imágenes por k-automorfismo σ se diferencian en un elemento de k^*, luego σ induce a su vez un automorfismo (continuo) de C_K. Es inmediato que el teorema anterior vale también para clases de elementos ideales, así como que los k-automorfismos de K fijan a C_k. Sin embargo, el el análogo al teorema 6.22, aunque es cierto en general, no es evidente. Lo probaremos únicamente para el caso que vamos a necesitar: el de extensiones cíclicas.

Teorema 6.24 *Sea K/k una extensión cíclica de cuerpos numéricos. El conjunto de las clases de C_K fijadas por todos los k-automorfismos de K es C_k.*

DEMOSTRACIÓN: Como ya hemos comentado, es claro que los elementos de C_k son fijados. Sea $G(K/k) = \langle\sigma\rangle$ y tomemos un $[\alpha] \in C_K$ tal que $\sigma([\alpha]) = [\alpha]$. Entonces $\sigma(\alpha) = u\alpha$, para un cierto $u \in K^*$. Entonces $\sigma^2(\alpha) = \sigma(u)u\alpha$, $\sigma^3(\alpha) = \sigma^2(u)\sigma(u)u\alpha$ y, si la extensión tiene grado n, podemos llegar hasta

$$\alpha = \sigma^n(\alpha) = \mathrm{N}(u)\alpha,$$

luego $\mathrm{N}(u) = 1$. Por el teorema 90 de Hilbert tenemos que $u = v/\sigma(v)$, para un cierto $v \in K^*$, luego $\sigma(v\alpha) = v\alpha$. Por el teorema 6.22 concluimos que $v\alpha \in J_k$, luego $[\alpha] = [v\alpha] \in C_k$. ∎

Capítulo VII

El isomorfismo de Artin

En este capítulo probaremos uno de los resultados fundamentales de la teoría de cuerpos de clases: veremos que si K/k es una extensión abeliana de cuerpos numéricos y $\mathfrak{m}$ es un divisor admisible, entonces el homomorfismo de Artin induce un isomorfismo

$$\omega : I(\mathfrak{m})/P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m}) \longrightarrow G(K/k).$$

Para ello seguiremos los pasos siguientes: En primer lugar probaremos la igualdad de índices

$$|I(\mathfrak{m}) : P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})| = |K : k|.$$

De hecho probaremos la fórmula equivalente en términos de clases de elementos ideales

$$|C_k : \mathrm{N}[C_K]| = |K : k|.$$

Para ello probaremos por separado y con técnicas muy diferentes las dos desigualdades. Primero probaremos la llamada *primera desigualdad fundamental:*

$$|K : k| \leq |C_k : \mathrm{N}[C_K]|.$$

De hecho probaremos que el grado de la extensión divide al índice del grupo de normas. Esto basta para probar que el homomorfismo de Artin es suprayectivo. Después probaremos la *segunda desigualdad fundamental:*

$$|C_k : \mathrm{N}[C_K]| \leq |K : k|.$$

Finalmente probaremos que existe un divisor admisible $\mathfrak{m}$ (divisible sólo entre los primos ramificados) tal que $P_{\mathfrak{m}}$ está contenido en el núcleo N del homomorfismo de Artin. Puesto ya sabemos que el grupo de normas $\mathrm{N}(\mathfrak{m})$ está contenido en dicho núcleo, tendremos que $P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m}) \leq N \leq I(\mathfrak{m})$, y la igualdad de índices probará que el núcleo es exactamente $P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$. A partir de aquí será fácil probar que esto vale para cualquier divisor admisible.

7.1 Cocientes de Herbrand y grupos de cohomología

Las técnicas que usaremos para probar la primera desigualdad fundamental provienen de la cohomología de grupos. En esta sección demostraremos los resultados de cohomología que vamos a necesitar sin presuponer ningún conocimiento al respecto. En realidad lo que haremos será llegar a ellos evitando la cohomología propiamente dicha, si bien conservaremos la notación. Esencialmente daremos algunos resultados útiles para calcular índices de subgrupos.

Definición 7.1 Si f es un homomorfismo definido sobre un grupo A, representaremos por A_f y A^f respectivamente a su núcleo y su imagen. Similarmente, si B es un subgrupo de A, llamaremos B_f y B^f al núcleo y la imagen de la restricción de f a B.

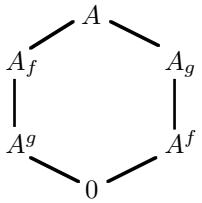
Sean f y g dos homomorfismos de un grupo abeliano A en sí mismo tales que $f \circ g = g \circ f = 0$. Llamaremos *cociente de Herbrand* a

$$C(A) = C_{fg}(A) = \frac{|A_f : A^g|}{|A_g : A^f|}.$$

El cociente $C(A)$ está definido únicamente cuando los dos índices son finitos. Esto sucede, por supuesto, cuando A es finito, pero este caso es trivial:

Teorema 7.2 *Sea A un grupo abeliano finito y sean f y g homomorfismos de A en sí mismo tales que $f \circ g = g \circ f = 0$. Entonces $C(A) = 1$.*

Demostración: Consideramos la red de subgrupos



El teorema de isomorfía implica que los cocientes correspondientes a lados paralelos no verticales tienen el mismo número de elementos, luego por la transitividad de los índices lo mismo vale para los lados verticales, pero esto es precisamente $C(A) = 1$. ∎

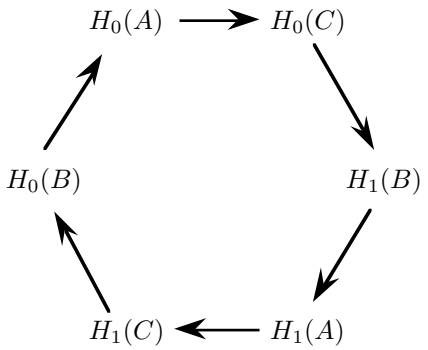
La utilidad de los cocientes de Herbrand se debe al teorema siguiente:

Teorema 7.3 *Sea A un grupo abeliano, sean f y g homomorfismos de A en sí mismo tales que $f \circ g = g \circ f = 0$, sea B un subgrupo de A tal que $B^f \leq B$, $B^g \leq B$, de modo que f y g inducen homomorfismos en $C = A/B$. Entonces*

$$C(A) = C(B)C(A/B),$$

en el sentido de que si dos de ellos están definidos también lo está el tercero y se da la igualdad.

DEMOSTRACIÓN: Definimos $H_0(A) = A_f/A^g$, $H_1(A) = A_g/A^f$, y análogamente para B y C. Vamos a construir homomorfismos



de modo que la sucesión es exacta, es decir, que la imagen de cada aplicación coincide con el núcleo de la siguiente.

Las aplicaciones de B a A y de A a C son las inducidas de forma natural por la inclusión de B en A y la proyección de A en C. Dejamos al lector la comprobación de que están bien definidas, junto con la exactitud en $H_0(A)$ y $H_1(A)$.

Para pasar de $H_0(C) = C_f/C^g$ hasta $H_1(B) = B_g/B^f$ tomamos un elemento $c = [a] \in C_f$. Entonces $f(c) = [f(a)] = 0$, luego $f(a) \in B$ y, como $g(f(a)) = 0$, de hecho $f(a) \in B_g$.

Es inmediato comprobar que la aplicación $[a] \mapsto [f(a)]$ está bien definida y es un homomorfismo $C_f \longrightarrow B_g/B^f$, que a su vez induce el homomorfismo que buscamos. La aplicación entre $H_1(C)$ y $H_0(B)$ se define análogamente y es una simple rutina comprobar la exactitud.

Dicha exactitud demuestra que si dos de los cocientes $C(A)$, $C(B)$ o $C(A/B)$ están definidos también lo está el tercero. Por ejemplo, si están definidos $C(B)$ y $C(A/B)$ entonces son finitos los grupos del hexágono correspondientes a B y C, luego el cociente de $H_0(A)$ sobre la imagen de $H_0(B)$ (que es finita) es isomorfo a un subgrupo de $H_0(C)$ (que es finito), luego $H_0(A)$ también es finito, e igual le sucede a $H_1(A)$.

Así pues, podemos suponer que los seis grupos son finitos. Para simplificar la notación numeramos los grupos cíclicamente M_1, M_2, ... de manera que $M_i = M_{i+6}$.

Sea m_i el número de elementos del núcleo del homomorfismo que parte de M_i, que coincide con la imagen del homomorfismo que llega a M_i.

Igual que hemos razonado antes, el cociente de M_i entre el núcleo del homomorfismo que parte de M_i es isomorfo a la imagen de dicho homomorfismo, de donde el número de elementos de M_i es $m_i\, m_{i+1}$.

Si comenzamos la numeración por ejemplo en $M_1 = H_0(A)$, entonces la fórmula que hemos de probar es

$$\frac{m_1 m_2}{m_4 m_5} = \frac{m_6 m_1}{m_3 m_4}\,\frac{m_2 m_3}{m_5 m_6},$$

que es cierta trivialmente. ∎

Definición 7.4 Una *acción* de un grupo G sobre un grupo A es un homomorfismo de G en el grupo de los automorfismos de A. Se dice que G *actúa* sobre A cuando hay definida una acción de G sobre A.

En tal caso, identificaremos cada $\sigma \in G$ con su automorfismo asociado, con la única precaución de que dos elementos distintos de G pueden coincidir como automorfismos de A.

El caso más frecuente se da cuando los elementos de G son ya automorfismos de A. Por ejemplo, el grupo de Galois de una extensión K/k actúa sobre los grupos K (con la suma) y K^* (con el producto).

Supongamos que G es un grupo cíclico de orden n que actúa sobre un grupo abeliano A. Sea σ un generador de G. Definimos la *traza* de G como

$$\mathrm{Tr}_G = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1},$$

donde la suma es la operación definida puntualmente en el conjunto de los homomorfismos de A. Si en A usamos notación multiplicativa hablaremos de la *norma* de G y la representaremos por N_G.

Observar que si G es el grupo de Galois de una extensión K/k y $A = K$ entonces la traza que hemos definido es la traza usual de la extensión, y si $A = K^*$ obtenemos la norma usual.

En general sea $f = 1 - \sigma$ y $g = \mathrm{Tr}_G$. Es inmediato comprobar que los homomorfismos f y g cumplen $f \circ g = g \circ f = 0$, luego podemos considerar el cociente de Herbrand (que, no obstante, puede no estar definido si algún índice no es finito)

$$C(G, A) = C_{fg}(A) = \frac{|A^G : \mathrm{Tr}[A]|}{|A_{\mathrm{Tr}} : A_G|},$$

donde $A^G = A_{1-\sigma}$ es el subgrupo de A formado por los elementos fijados por todos los elementos de G y $A_G = (1-\sigma)[A]$ cumple que

$$A_G = \{(1-\tau)(a) \mid a \in A,\ \tau \in G\},$$

pues una inclusión es obvia y si $\tau = \sigma^i$ es cualquier elemento de G resulta que

$$(1-\sigma^i)(a) = (1-\sigma)(a + \sigma(a) + \cdots + \sigma^{i-1}(a)) \in (1-\sigma)[A].$$

Por lo tanto el número $C(G, A)$, si está definido, depende de G y de A, pero no del generador de G que usemos para calcularlo.

Ejemplo Supongamos que un grupo cíclico G de orden n actúa trivialmente sobre $\mathbb{Z}$ (o sea, mediante la acción trivial dada por $g(n) = n$ para todo $n \in \mathbb{Z}$ y todo $g \in G$). Entonces $C(G, \mathbb{Z}) = |G|$.

En efecto, tenemos que $\mathbb{Z}^G = \mathbb{Z}$, $\mathrm{Tr}[\mathbb{Z}] = n\mathbb{Z}$, $\mathbb{Z}_{\mathrm{Tr}} = 0$ y $\mathbb{Z}_G = 0$. ∎

Observar que si un grupo cíclico G actúa sobre un grupo abeliano A y B es un subgrupo de A tal que $\sigma[B] = B$ para todo $\sigma \in G$, entonces G actúa sobre B y sobre A/B (en el caso del cociente la acción es $\sigma([a]) = [\sigma(a)]$). Es obvio que los homomorfismos f y g inducidos por esta acción sobre B y A/B son los inducidos por los homomorfismos correspondientes a la acción sobre A, de modo que podemos aplicar el teorema 7.3 y concluir que

$$C(G, A) = C(G, B)C(G, A/B), \tag{7.1}$$

entendiendo que si dos cocientes están definidos también lo está el tercero.

Ahora definimos los grupos

$$H^0(G, A) = A^G/\operatorname{Tr}[A] \qquad \text{y} \qquad H^{-1}(G, A) = A_{\mathrm{Tr}}/A_G. \tag{7.2}$$

Estos grupos pueden definirse en un contexto mucho más general y se llaman grupos de cohomología. Vemos que el cociente $C(G, A)$ está definido exactamente cuando los dos grupos de cohomología son finitos, y entonces es igual al cociente de sus órdenes.

Por ejemplo si G es el grupo de Galois de una extensión cíclica K/k, es claro que

$$H^0(G, K) = k/\operatorname{Tr}[K], \qquad H^0(G, K^*) = k^*/\operatorname{N}[K^*].$$

El teorema 90 de Hilbert equivale a que $H^{-1}(G, K) = 0$, $H^{-1}(G, K^*) = 1$.

Ahora vamos a dar varios criterios para calcular grupos de cohomología y cocientes de Herbrand. El primero es una observación elemental, y es que todos estos conceptos se conservan por isomorfismos en el sentido siguiente:

Definición 7.5 Si G_1 y G_2 son grupos que actúan sobre otros grupos A_1 y A_2, diremos que las acciones son *equivalentes* si existen isomorfismos $u : G_1 \longrightarrow G_2$ y $v : A_1 \longrightarrow A_2$ de modo que, para todo $g \in G_1$ y todo $a \in A_1$ se cumple $u(g)\big(u(a)\big) = g(a)$.

Es claro que en esta situación (si los grupos G_1 y G_2 son cíclicos)

$$H^0(G_1, A_1) \cong H^0(G_2, A_2), \qquad H^{-1}(G_1, A_1) \cong H^{-1}(G_2, A_2)$$

$$\text{y} \qquad C(G_1, A_1) \cong C(G_2, A_2),$$

donde en la última igualdad se entiende que un cociente está definido si y sólo si lo está el otro, y en tal caso coinciden. La prueba es comprobar rutinariamente que los isomorfismos dados por la hipótesis de equivalencia inducen isomorfismos entre todos los grupos construidos a partir de las acciones (grupos de trazas, grupos fijados, etc.) Otro caso sencillo es el siguiente:

Teorema 7.6 *Sea G un grupo cíclico que actúa sobre una familia de subgrupos $\{A_i\}_{i\in I}$. Entonces G actúa sobre $\prod_{i\in I} A_i$ mediante $\sigma((a_i)_{i\in I}) = (\sigma(a_i))_{i\in I}$. Además*

$$H^0\Big(G, \prod_{i\in I} A_i\Big) \cong \prod_{i\in I} H^0(G, A_i), \qquad H^{-1}\Big(G, \prod_{i\in I} A_i\Big) \cong \prod_{i\in I} H^{-1}(G, A_i).$$

Si el número de factores es finito, entonces

$$C\Big(G, \prod_{i\in I} A_i\Big) = \prod_{i\in I} C(G, A_i),$$

entendiendo que el miembro izquierdo está definido si y sólo si lo están todos los factores del miembro izquierdo.

DEMOSTRACIÓN: La prueba consiste en comprobar rutinariamente que el grupo de trazas del producto es el producto de los grupos de trazas de los factores, el grupo fijado por el producto es el producto de los grupos fijados por los factores, etc. ∎

Veamos ahora un resultado más profundo:

Teorema 7.7 *Sea $A = \prod_{i=1}^{s} A_i$ un producto de grupos abelianos. Sea G un grupo cíclico finito que actúe sobre A de modo que permute los subgrupos A_i, es decir, para todo $\sigma \in G$ y todo índice i existe un índice j tal que $\sigma[A_i] = A_j$. Supongamos también que, dados i, j, existe un $\sigma \in G$ tal que $\sigma[A_i] = A_j$. Sea $G_1 = \{\sigma \in G \mid \sigma[A_1] = A_1\}$. Entonces*

$$H^0(G, A) \cong H^0(G_1, A_1), \qquad H^{-1}(G, A) \cong H^{-1}(G_1, A_1).$$

DEMOSTRACIÓN: Observar que $\sigma[A_1] = \tau[A_1]$ si y sólo si $\sigma\tau^{-1}[A_1] = A_1$, o sea, si y sólo si $\sigma\tau^{-1} \in G_1$. De aquí que la aplicación $G/G_1 \longrightarrow \{A_1, \dots, A_s\}$ dada por $[\sigma] \mapsto \sigma[A_1]$ es inyectiva y por hipótesis suprayectiva, lo que nos da la igualdad $|G : G_1| = s$.

Sea $G/G_1 = \{[\sigma_1], \dots, [\sigma_s]\}$. Podemos exigir que $\sigma_i[A_1] = A_i$ y que $\sigma_1 = 1$.

Entonces cada elemento de A_i se expresa de forma única como $\sigma_i(a)$, con $a \in A_1$ y cada elemento de A se expresa de forma única como

$$\sum_{i=1}^{s} \sigma_i(a_i) \qquad \text{con } a_1, \dots, a_s \in A_1.$$

Los elementos de A^G son los de la forma

$$\sum_{i=1}^{s} \sigma_i(a_1), \qquad \text{con } a_1 \in (A_1)^{G_1}.$$

En efecto, dado $\sigma \in G$, es claro que las clases $[\sigma_1\sigma], \dots, [\sigma_s\sigma]$ son las mismas que $[\sigma_1], \dots, [\sigma_s]$, aunque en otro orden. Notar que $[\sigma] = [\tau]$ implica $\sigma\tau^{-1} \in G_1$, luego $(\sigma\tau^{-1})(a_1) = a_1$ y por tanto $\sigma(a_1) = \tau(a_1)$. De todo esto concluimos que

$$\sigma\Big(\sum_{i=1}^{s} \sigma_i(a_1)\Big) = \sum_{i=1}^{s} \sigma_i\sigma(a_1) = \sum_{i=1}^{s} \sigma_i(a_1).$$

Recíprocamente, si $a = \sum_{i=1}^{s} \sigma_i(a_i) \in A^G$, aplicamos σ_j^{-1} y así vemos que la componente en A_1 de $a = \sigma_j^{-1}(a)$ es $a_1 = a_j$. Por lo tanto $a = \sum_{i=1}^{s} \sigma_i(a_1)$.

Aplicando ahora $\sigma \in G_1$ vemos que $a = \sigma(a) = \sum_{i=1}^{s} \sigma_i(\sigma(a_1))$, de donde $\sigma(a_1) = a_1$.

Así pues, cada elemento de A^G está determinado por su primera componente, luego la proyección $\pi : A^G \longrightarrow (A_1)^{G_1}$ es un isomorfismo.

Por otra parte, si $a = \sum_{i=1}^{s} \sigma_i(a_i)$ es un elemento arbitrario de A, se cumple que

$$\mathrm{Tr}_G(\sigma_j(a_j)) = \sum_{\sigma\in G} \sigma(\sigma_j(a_j)) = \sum_{\sigma\in G} \sigma(a_j)$$

$$= \sum_{i=1}^{s} \sum_{\sigma\in G_1} \sigma_i(\sigma(a_j)) = \sum_{i=1}^{s} \sigma_i(\mathrm{Tr}_{G_1}(a_j)),$$

y sumando en j queda

$$\mathrm{Tr}_G(a) = \sum_{j=1}^{s} \sigma_j(\mathrm{Tr}_{G_1}(a_1 + \cdots + a_s)). \tag{7.3}$$

Así pues, $\mathrm{Tr}_G[A]$ está formado por los elementos de la forma

$$\sum_{i=1}^{s} \sigma_i(\mathrm{Tr}_{G_1}(a_1)), \qquad \text{con } a_1 \in G_1.$$

Por lo tanto $\pi[\mathrm{Tr}_G[A]] = \mathrm{Tr}_{G_1}[G_1]$ y, en consecuencia,

$$A^G/\,\mathrm{Tr}_G[A] \cong (A_1)^{G_1}/\,\mathrm{Tr}_{G_1}[G_1],$$

que es uno de los isomorfismos buscados.

La fórmula (7.3) implica que

$$\mathrm{Tr}_G(a) = 0 \Leftrightarrow \mathrm{Tr}_{G_1}(a_1 + \cdots + a_s) = 0.$$

Sea $\lambda : A_{\mathrm{Tr}_G} \longrightarrow (A_1)^{\mathrm{Tr}_{G_1}}$ la aplicación dada por $\lambda(a) = a_1 + \cdots + a_s$. Claramente es un epimorfismo (si $a_1 \in (A_1)^{\mathrm{Tr}_{G_1}}$ entonces $\lambda(a_1) = a_1$).

Sea $\sigma \in G$. Existe una permutación p de los índices de modo que $\sigma_i\sigma = \tau_{p(i)}\sigma_{p(i)}$, para ciertos $\tau_{p(i)} \in G_1$.

Entonces, dado un $a = \sum_{i=1}^{s} \sigma_i(a_i) \in A$, tenemos

$$\lambda\big((1-\sigma)(a)\big) = \lambda\Big(\sum_{i=1}^{s}\big(\sigma_i(a_i) - \sigma_{p(i)}(\tau_{p(i)}(a_i))\big)\Big)$$

$$= \lambda\Big(\sum_{i=1}^{s}\big(\sigma_i(a_i) - \sigma_i(\tau_i(a_i))\big)\Big) = \sum_{i=1}^{s}(1-\tau_i)(a_i) \in (A_1)_{G_1}.$$

Esto prueba que $\lambda[A_G] \le (A_1)_{G_1}$. Para probar la inclusión contraria vemos primero que si $\lambda(a) = 0$, es decir, si $\sum_{i=1}^{s} a_i = 0$, claramente

$$a = \sum_{i=1}^{s} \sigma_i(a_i) = \sum_{i=1}^{s} (\sigma_i(a_i) - a_i) \in A_G.$$

En general, si $\lambda(a) \in (A_1)_{G_1}$, o sea, si $\lambda(a) = (1-\tau)(b)$, con $b \in A_1$ y $\tau \in G_1$, entonces $\lambda(a - (1-\tau)(b)) = 0$, luego $a - (1-\tau)(b) \in A_G$ y también $a \in A_G$. Consecuentemente $A_{\mathrm{Tr}_G}/A_G \cong (A_1)_{\mathrm{Tr}_{G_1}}/(A_1)_{G_1}$. ∎

Notar que si en el teorema anterior se cumple $G_1 = 1$ la conclusión es $H^0(G, A) = 0$, $H^{-1}(G, A) = 0$.

En particular, si G es el grupo de Galois de una extensión cíclica K/k, el teorema de la base normal afirma que K tiene una base de la forma

$$\{\sigma(\alpha) \mid \sigma \in G\},$$

para un $\alpha \in K$, y entonces K es la suma directa de los subespacios $\langle \sigma(\alpha) \rangle$, que están en las hipótesis del teorema anterior con $G_1 = 1$. Por lo tanto concluimos que $H^0(G, K) = 0$, $H^{-1}(G, K) = 0$. La última igualdad nos la daba ya el teorema 90 de Hilbert junto con $H^{-1}(G, K^*) = 1$.

Por el contrario, $H^0(G, K^*) = k^*/\,\mathrm{N}[K^*]$ no es trivial en general. Lo es en el caso de las extensiones de cuerpos finitos (ver la prueba del teorema 2.37, nota al pie). Las técnicas que hemos expuesto nos permiten calcularlo en el caso de cuerpos p-ádicos. Para ello necesitamos un sencillo resultado técnico:

Teorema 7.8 *Sea f un homomorfismo de grupos definido sobre un grupo abeliano A y sea B un subgrupo de A. Entonces*

$$|A : B| = |A^f : B^f|\,|A_f : B_f|.$$

Demostración: Consideremos el epimorfismo $A \longrightarrow A^f/B^f$. Su núcleo es $B + A_f$, luego tenemos que $A/(B + A_f) \cong A^f/B^f$.

Por otra parte, $(B + A_f)/B \cong A_f/(A_f \cap B) = A_f/B_f$. El resultado es ahora inmediato. ∎

Teorema 7.9 *Sea K/k una extensión cíclica de grado n de cuerpos p-ádicos. Sea $G = \langle \sigma \rangle$ su grupo de Galois. Sean U_K y U_k los grupos de unidades respectivos y sea e el índice de ramificación. Entonces:*

$$C(G, K^*) = |k^* : \mathrm{N}[K^*]| = |K : k|, \qquad |U_k : \mathrm{N}[U_K]| = e, \qquad C(G, U_K) = 1.$$

Demostración: Por el teorema 90 de Hilbert $H^{-1}(G, K^*) = 1$, con lo que ciertamente $C(G, K^*) = |k^* : \mathrm{N}[K^*]|$ (supuesto que este índice sea finito).

El grupo G actúa sobre K^* y U_K, luego también sobre $K^*/U_K \cong \mathbb{Z}$. La última acción es trivial, pues si $\alpha \in K^*$ entonces $|\sigma(\alpha)| = |\alpha|$, lo que implica

que $\sigma(\alpha)/\alpha \in U_K$, y así $[\sigma(\alpha)] = [\alpha]$. Por consiguiente al aplicar el teorema 7.3 obtenemos que

$$|K : k| = |G| = C(G, \mathbb{Z}) = C(G, K^*)/C(G, U_K).$$

Si probamos que $C(G, U_K)$ está definido y vale 1 tendremos la primera afirmación del teorema.

Consideremos una base normal de K/k, es decir, una base de la forma $v_1, \ldots, v_n$ donde cada v_i es la imagen de v_1 por un elemento de G. Sea D el anillo de enteros de k y sea

$$M = \sum_{i=1}^{n} Dv_i.$$

Es claro que G actúa sobre M, y estamos en las hipótesis del teorema 7.7 con $G_1 = 1$, luego $C(G, M) = 1$.Es claro que si multiplicamos la base normal por un elemento de k sigue siendo una base normal, y si la multiplicamos por una potencia del primo de k suficientemente grande podemos exigir que los valores absolutos de los v_i sean menores que un número real $\epsilon > 0$ arbitrario.

Teniendo en cuenta que los elementos de D tienen todos valor absoluto menor o igual que 1, concluimos que todos los elementos de M tienen valor absoluto menor que ϵ.

Por otra parte M es un subgrupo abierto de K, pues las funciones coordenadas son continuas (esto es consecuencia de que todas las normas en K son equivalentes, y así el valor absoluto en K induce la misma topología que la norma dada por el supremo de los valores absolutos de las coordenadas)

Ahora recordamos que, según [7.26], la función exponencial es un isomorfismo de grupos entre una bola abierta suficientemente pequeña de centro 0 en K y una bola abierta suficientemente pequeña de centro 1 en U_K. Más aún, tanto la función exp como su inversa log son continuas en sus dominios (como toda serie de potencias). En consecuencia $V = \exp[M]$ es un subgrupo abierto de U_K topológicamente isomorfo a M. La continuidad de los automorfismos hace que conmuten con las series de potencias, y entonces es claro que $\sigma\big(\exp(\alpha)\big) = \exp\big(\sigma(\alpha)\big)$, para todo $\sigma \in G$ y todo $\alpha \in M$.

Esto significa que las acciones de G sobre M y V son equivalentes, luego $C(G, V) = 1$. Pero V es un subgrupo abierto en U_K, que es compacto, por lo que el índice $|U_K : V|$ ha de ser finito, y así el teorema 7.2 nos da que $C(G, U_k/V) = 1$. Por consiguiente $C(G, U_K) = C(G, V) = 1$, como había que probar.

Por definición

$$C(G, U_K) = \frac{|U_k : \mathrm{N}[U_K]|}{|(U_K)_\mathrm{N} : (1-\sigma)[U_K]|},$$

y por el teorema 90 de Hilbert sabemos que $(U_K)_\mathrm{N} = (1-\sigma)[K^*]$. Así, usando el teorema anterior,

$$|U_k : \mathrm{N}[U_K]| = |(1-\sigma)[K^*] : (1-\sigma)[U_K]| = |(1-\sigma)[K^*] : (1-\sigma)[k^* U_K]|$$

$$= \frac{|K^* : k^*U_K|}{|K^*_{1-\sigma} : (k^*U_K)_{1-\sigma}|} = \frac{|K^* : k^*U_K|}{|k^* : k^*|} = e,$$

pues es fácil ver que el grupo K^*/k^*U_K es cíclico de orden e. ∎

Observar que el teorema anterior es cierto trivialmente cuando los cuerpos K y k son $\mathbb{R}$ o $\mathbb{C}$, entendiendo que los grupos de unidades son todo el grupo multiplicativo.

Este resultado generaliza al teorema 6.18 para cuerpos p-ádicos, pues las extensiones no ramificadas son cíclicas y $e = 1$. Además nos permite demostrar un recíproco.

Teorema 7.10 *Sea K/k una extensión abeliana de cuerpos numéricos. Sea $\mathfrak{P}$ un primo en K y $\mathfrak{p}$ el primo de k divisible entre $\mathfrak{P}$. Entonces $e(\mathfrak{P}/\mathfrak{p}) = 1$ si y sólo $U_\mathfrak{p} = \mathrm{N}[U_\mathfrak{P}]$. En consecuencia los divisores admisibles de la extensión son divisibles entre todos los primos ramificados.*

Demostración: Una implicación es el teorema 6.18. Para probar la inversa consideramos el grupo $G(K/k)$, que se puede descomponer como producto directo de grupos cíclicos. Para cada uno de estos subgrupos consideramos el cuerpo fijado por el producto de todos los demás, con lo que tenemos una familia $K_1, \ldots, K_r$ de extensiones cíclicas de k cuyo producto coincide con K (su grupo de automorfismos es trivial). Sea $\mathfrak{P}_i$ el primo de K_i divisible entre $\mathfrak{P}$. Es claro que $U_\mathfrak{p} = \mathrm{N}[U_{\mathfrak{P}_i}]$ (por la transitividad de las normas), luego el teorema anterior nos da que $\mathfrak{p}$ es no ramificado en cada K_i.

Por otra parte, aplicando 2.15 tenemos que $K_\mathfrak{P} = (K_1)_{\mathfrak{P}_1} \cdots (K_r)_{\mathfrak{P}_r}$, y entonces el teorema 2.35 nos da que $\mathfrak{P}$ es no ramificado sobre $\mathfrak{p}$. ∎

7.2 La primera desigualdad fundamental

En esta sección probaremos la desigualdad

$$|K : k| \le |C_k : \mathrm{N}[C_K]|.$$

Por conveniencia la probaremos únicamente para extensiones cíclicas, pues esto será suficiente para probar la suprayectividad del homomorfismo de Artin y el caso general se deducirá trivialmente de resultados posteriores.

Al final del capítulo anterior vimos que el grupo de Galois $G = G(K/k)$ actúa sobre el grupo C_K. El teorema 6.23 (en su versión para clases de elementos ideales) muestra que la norma de la acción coincide con la norma usual en C_K y el teorema 6.24 prueba que $C_K^G = C_k$, con lo que $H^0(G, C_K) = C_k/\mathrm{N}[C_K]$. Así pues, queremos estimar el orden de $H^0(G, C_K)$.

Vamos a aplicar las técnicas de la sección precedente. En el capítulo anterior vimos que existe un conjunto finito E de primos de K tal que $J_K = K^* J_E^K$. Podemos ampliarlo de modo que esté formado por todos los primos de K que

dividen a los de un conjunto finito de primos de k, y de modo que E contenga, además de los primos infinitos, a los primos ramificados. Entonces

$$C(G, C_K) = C(G, J_K/K^*) = C(G, K^*J_E/K^*) = C(G, J_E/K_E),$$

donde hemos usado que las acciones de G sobre los grupos K^*J_E/K^* y J_E/K_E son equivalentes. Ahora el teorema 7.3 nos da

$$C(G, C_K) = C(G, J_E)/C(G, K_E), \tag{7.4}$$

supuesto que estos dos cocientes estén definidos. Nos ocupamos primero de $C(G, J_E)$. Para ello sea E_k el conjunto de los primos de k divisibles por los primos de E. Podemos descomponer

$$J_E = \prod_{\mathfrak{p}\in E_k} \Big(\prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*\Big) \times \prod_{\mathfrak{p}\notin E_k} \Big(\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}\Big).$$

Si $\mathfrak{P}$ no está en E_k, entonces es no ramificado. La extensión local $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ es cíclica y su grupo de Galois es isomorfo a $G_{\mathfrak{P}}$, el grupo de los automorfismos de K que fijan a $\mathfrak{P}$. Esta acción de $G_{\mathfrak{P}}$ sobre $K_{\mathfrak{P}}$ es la misma que la que induce la acción de G sobre J_E (por definición de ésta última). Por el teorema 7.9 tenemos $H^0(G_{\mathfrak{P}}, U_{\mathfrak{P}}) = H^{-1}(G_{\mathfrak{P}}, U_{\mathfrak{P}}) = 1$.

Ahora consideramos la acción de G sobre cada producto $\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}$. Podemos aplicar el teorema 7.7 y concluir que

$$H^0\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}\Big) = H^{-1}\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}\Big) = 1.$$

Si llamamos $V = \prod_{\mathfrak{p}\notin E_k} \Big(\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}\Big)$, el teorema 7.6 nos da que

$$H^0(G, V) = H^{-1}(G, V) = 1$$

y, en consecuencia, $C(G, V) = 1$. Por los teoremas 7.3, 7.6, 7.7 y 7.9 llegamos a que

$$C(G, J_E) = \prod_{\mathfrak{p}\in E_k} C\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^*\Big) = \prod_{\mathfrak{p}\in E_k} C(G_{\mathfrak{P}}, K_{\mathfrak{P}}^*) = \prod_{\mathfrak{p}\in E_k} n_{\mathfrak{p}}, \tag{7.5}$$

donde en el penúltimo producto se entiende que $\mathfrak{P}$ es un divisor (cualquiera) de $\mathfrak{p}$ y en el último $n_{\mathfrak{p}}$ es el orden de $G_{\mathfrak{p}}$, es decir, el grado local $K_{\mathfrak{P}}/k_{\mathfrak{p}}$.

Si probamos que

$$C(G, K_E) = \frac{1}{|K : k|} \prod_{\mathfrak{p}\in E_k} n_{\mathfrak{p}}, \tag{7.6}$$

recordando (7.4) podremos concluir que

$$C(G, C_K) = |K : k|,$$

luego tendremos que

$$|C_k : \mathrm{N}[C_K]| = h_{-1}\,|K : k|, \tag{7.7}$$

donde h_{-1} es el orden de $H^{-1}(G, C_K)$. Así quedará probada la primera desigualdad fundamental.

Para investigar la acción de G sobre K_E usaremos una representación logarítmica que incidentalmente nos dará una generalización del teorema de Dirichlet sobre las unidades de un cuerpo numérico. Daremos una prueba basada en la compacidad del grupo C^0 de clases de elementos ideales.

Teorema 7.11 *Sea K un cuerpo numérico y E un conjunto finito de divisores primos de K que contenga a todos los primos arquimedianos. Sea s el número de elementos de E. Sea $\log : J_E \longrightarrow \mathbb{R}^s$ la aplicación dada por $\log \alpha = (\log \|\alpha\|_{\mathfrak{p}})_{\mathfrak{p}\in E}$. Entonces $\log[K_E]$ es un retículo de rango $s-1$ contenido en el hiperplano*

$$H = \{(x_1, \dots, x_s) \in \mathbb{R}^s \mid x_1 + \cdots + x_s = 0\}.$$

Demostración: Es claro que la aplicación log es un homomorfismo, luego $\log[K_E]$ es un subgrupo de $\mathbb{R}^s$ y obviamente $\log[K_E] \subset \log[J_E^0] \subset H$.

Se cumple que $\log[K_E]$ es discreto, pues si tomamos un conjunto

$$M = \{\alpha \in K_E \mid \|\log \alpha\| \le C\},$$

podemos tomar un entero $\alpha_0 \in K$ tal que $\alpha_0^{-1}M$ está contenido en el anillo de enteros de K, luego M está contenido en un $\mathbb{Z}$-módulo finitamente generado y por consiguiente la representación geométrica usual de los puntos de M ha de ser discreta. Pero dicha representación está acotada, luego M es finito.

Para probar que el rango es exactamente $s-1$ notamos en primer lugar que H está generado (como espacio vectorial) por $\log[J_E^0]$ pues, por ejemplo, fijando una componente arquimediana, es fácil construir elementos de J_E^0 cuyas imágenes tengan ceros en $s-2$ posiciones a elegir entre las restantes (ajustando la componente reservada para que la norma del elemento sea 1). Así obtenemos $s-1$ vectores independientes.

Sea W el subespacio generado por $\log[K_E]$. Entonces tenemos un homomorfismo de grupos $J_E^0/K_E \longrightarrow H/W$ tal que la imagen genera H/W como espacio vectorial. Pero la aplicación es continua, luego la imagen es un subgrupo compacto, luego es trivial (si contiene a un elemento no nulo contiene a sus múltiplos, luego no es acotado). Por lo tanto $W = H$, como había que probar. ∎

Observar que el núcleo de la aplicación log descrita en el teorema anterior es exactamente $K_\varnothing$, o sea, el grupo (finito) de las raíces de la unidad en K. De aquí se deduce obviamente un teorema de estructura para K_E que coincide con el teorema de Dirichlet en el caso en que $E = P_\infty$.

Teorema 7.12 (Teorema de las unidades de Hasse) *Sea K un cuerpo numérico y E un conjunto de primos de K que contenga a todos los primos arquimedianos. Entonces el grupo K_E es un grupo abeliano finitamente generado cuya parte de torsión es el grupo (finito) de las raíces de la unidad contenidas en K y cuya parte libre tiene rango $s-1$, donde s es el número de elementos de E.*

Para nuestros objetivos inmediatos nos es suficiente el teorema 7.11. Llamemos $N = \log[K_E]$, que es un retículo de rango $s-1$ en $\mathbb{R}^s$ y $K_E/K_\varnothing \cong N$.

Observemos que el grupo de Galois G actúa sobre $K_\varnothing$ y, por tanto, sobre $K_E/K_\varnothing$. Como el denominador es finito, los teoremas 7.3 y 7.2 nos dan que $C(G, K_E) = C(G, K_E/K_\varnothing)$, entendiendo que basta probar que $C(G, K_E/K_\varnothing)$ esté definido para que lo esté $C(G, K_E)$ y en tal caso coincidirán.

El isomorfismo nos permite definir una acción de G sobre N equivalente a su acción en $K_E/K_\varnothing$. De este modo

$$C(G, K_E) = C(G, K_E/K_\varnothing) = C(G, N), \tag{7.8}$$

entendiendo, como siempre, que hemos de justificar que el último cociente está definido.

Vamos a describir explícitamente la acción de G sobre N. Está caracterizada por que

$$\sigma(\log \alpha) = \log \sigma(\alpha), \qquad \sigma \in G, \quad \alpha \in K_E. \tag{7.9}$$

Si representamos la base canónica de $\mathbb{R}^s$ mediante $\{X_\mathfrak{P}\}_{\mathfrak{P}\in E}$, la aplicación $\log : K_E \longrightarrow \mathbb{R}^s$ se expresa en la forma

$$\log \alpha = \sum_{\mathfrak{P}\in E} \log \|\alpha_\mathfrak{P}\|\, X_\mathfrak{P}.$$

Claramente $\|\sigma(\alpha)\|_{\sigma(\mathfrak{P})} = \|\alpha\|_\mathfrak{P}$, de donde (7.9) equivale a

$$\sigma\Big(\sum_{\mathfrak{P}\in E} \log \|\alpha_\mathfrak{P}\|\, X_\mathfrak{P}\Big) = \sum_{\mathfrak{P}\in E} \log \|\alpha_\mathfrak{P}\|\, X_{\sigma(\mathfrak{P})}.$$

Podemos definir una acción de G sobre todo $\mathbb{R}^s$ asociando a cada $\sigma \in G$ la aplicación lineal en $\mathbb{R}^s$ determinada por $\sigma(X_\mathfrak{P}) = X_{\sigma(\mathfrak{P})}$. Lo que hemos visto es que la acción de G sobre N es simplemente la restricción a N de esta acción de G sobre $\mathbb{R}^s$.

Sea $X_0 = \sum_{\mathfrak{P}\in E} X_\mathfrak{P}$. Entonces el subgrupo $\langle X_0\rangle$ generado por X_0 es isomorfo a $\mathbb{Z}$ y G actúa trivialmente sobre él, pues todos los elementos de G dejan fijo a X_0. El teorema 7.3 nos da que

$$C(G, N + \langle X_0\rangle) = C(G, N)\, C(G, \mathbb{Z}) = C(G, N)\, |K : k|, \tag{7.10}$$

entendiendo, una vez más, que basta probar que está definido el miembro izquierdo para que podamos asegurar que lo está $C(G, N)$. Con este cambio hemos ganado que $M = N + \langle X_0\rangle$ es un retículo completo en $\mathbb{R}^s$. Los teoremas siguientes nos calcularán el cociente $C(G, M)$.

Teorema 7.13 *En las condiciones anteriores, si M es un retículo completo en $\mathbb{R}^s$ que es invariante por G (es decir, que cumple $\sigma[M] \subset M$ para todo $\sigma \in G$) entonces existe un subretículo M' de índice finito en M invariante por G y que tiene una base $\{Y_\mathfrak{P}\}_{\mathfrak{P}\in E}$ tal que $\sigma(Y_\mathfrak{P}) = Y_{\sigma(\mathfrak{P})}$ para todo $\sigma \in G$.*

DEMOSTRACIÓN: Consideramos en $\mathbb{R}^s$ la norma supremo. Es claro que existe un número $b > 0$ tal que para todo $X \in \mathbb{R}^s$ existe un $Z \in M$ de modo que $\|X - Z\| < b$. Para cada $\mathfrak{p} \in E_k$ sea $\mathfrak{P}_\mathfrak{p} \in E$ tal que $\mathfrak{P}_\mathfrak{p} \mid \mathfrak{p}$. Sea $t > 0$ arbitrario. Sea $Z_\mathfrak{p} \in M$ tal que $\|tX_{\mathfrak{P}_\mathfrak{p}} - Z_\mathfrak{p}\| < b$. Para cada $\mathfrak{P} \mid \mathfrak{p}$ sea

$$Y_\mathfrak{P} = \sum_{\sigma(\mathfrak{P}_\mathfrak{p})=\mathfrak{P}} \sigma(Z_\mathfrak{p}).$$

Veamos que estos vectores cumplen lo pedido. Claramente, si $\tau \in G$, tenemos

$$\tau(Y_\mathfrak{P}) = \sum_{\sigma(\mathfrak{P}_\mathfrak{p})=\mathfrak{P}} \sigma\tau(Z_\mathfrak{p}) = \sum_{\rho(\mathfrak{P}_\mathfrak{p})=\tau(\mathfrak{P})} \rho(Z_\mathfrak{p}) = Y_{\tau(\mathfrak{P})}.$$

Esto implica que el retículo generado por estos vectores es invariante por G. Falta ver que son linealmente independientes, lo que a su vez ya implica que el índice del retículo que generan es finito.

Supongamos que $\sum_\mathfrak{P} c_\mathfrak{P} Y_\mathfrak{P} = 0$. Si no todos los coeficientes son nulos, dividiendo entre el mayor podemos suponer que $|c_\mathfrak{P}| \le 1$ para todo $\mathfrak{P}$ y que $c_\mathfrak{P} = 1$ para un $\mathfrak{P}$. Sea $Z_\mathfrak{p} = tX_{\mathfrak{P}_\mathfrak{p}} + B_\mathfrak{p}$, donde por construcción $\|B_\mathfrak{p}\| < b$. Entonces

$$Y_\mathfrak{P} = \sum_{\sigma(\mathfrak{P}_\mathfrak{p})=\mathfrak{P}} \sigma(Z_\mathfrak{p}) = t \sum_{\sigma(\mathfrak{P}_\mathfrak{p})=\mathfrak{P}} \sigma(X_{\mathfrak{P}_\mathfrak{p}}) + C_\mathfrak{P},$$

donde $\|C_\mathfrak{P}\| \le nb$.

Queda, pues, que $Y_\mathfrak{P} = tm_\mathfrak{P} X_\mathfrak{P} + C_\mathfrak{P}$, donde $m_\mathfrak{P}$ es el número de automorfismos $\sigma \in G$ tales que $\sigma(\mathfrak{P}_\mathfrak{P}) = \mathfrak{P}$. Al sustituir en la combinación lineal llegamos a que

$$0 = \sum_\mathfrak{P} c_\mathfrak{p} Y_\mathfrak{P} = t \sum_\mathfrak{P} c_\mathfrak{P} m_\mathfrak{P} X_\mathfrak{P} + C,$$

donde $\|C\| \le snb$.

Teniendo en cuenta que la norma es la norma supremo, si consideramos la componente que cumple $c_\mathfrak{P} = 1$ resulta que $tm_\mathfrak{P} \le snb$ y, si se escoge t suficientemente grande, esto es una contradicción. ∎

Para terminar:

Teorema 7.14 *En las hipótesis del teorema anterior, si G es cíclico se cumple*

$$C(G, M) = C(G, M') = \prod_{\mathfrak{p} \in E_k} n_\mathfrak{p},$$

donde $n_\mathfrak{p}$ es grado local en $\mathfrak{p}$.

DEMOSTRACIÓN: Ante todo observamos que por 2.28 el grupo $G_\mathfrak{P}$ depende sólo de $\mathfrak{p}$. Se cumple $C(G, M) = C(G, M')$ porque el cociente M/M' es finito. Ahora expresamos

$$M' = \prod_{\mathfrak{p} \in E_k} \prod_{\mathfrak{P} \mid \mathfrak{p}} \langle Y_\mathfrak{P} \rangle$$

y vemos que G actúa en cada uno de los factores del primer producto.

Podemos aplicar el teorema 7.3 varias veces, lo que nos da

$$C(G, M') = \prod_{\mathfrak{p}\in E_k} C\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} \langle Y_{\mathfrak{P}}\rangle\Big).$$

Ahora vemos que la acción de G sobre cada uno de estos factores está en las hipótesis del teorema 7.7, con lo que tenemos

$$C\Big(G, \prod_{\mathfrak{P}|\mathfrak{p}} \langle Y_{\mathfrak{P}}\rangle\Big) = C(G_{\mathfrak{P}}, \langle Y_{\mathfrak{P}}\rangle).$$

Por último, cada grupo $\langle Y_{\mathfrak{P}}\rangle$ es isomorfo a $\mathbb{Z}$ y la acción de G sobre él es trivial (porque es lineal). Esto implica que $C(G_{\mathfrak{P}}, \langle Y_{\mathfrak{P}}\rangle) = |G_{\mathfrak{P}}| = n_{\mathfrak{p}}$. ∎

Con esto tenemos calculado el miembro izquierdo de (7.10), lo que unido a (7.8) nos da (7.6). Así queda probada la primera desigualdad fundamental.

Como consecuencia de la primera desigualdad fundamental obtenemos la suprayectividad del homomorfismo de Artin. Para probarla nos basaremos en el teorema siguiente:

Teorema 7.15 *Sea K/k una extensión abeliana de cuerpos numéricos (de grado mayor que 1). Entonces hay infinitos primos en k que no se escinden completamente en K.*

Demostración: Claramente podemos suponer que la extensión es cíclica. Sea E el conjunto de los primos de k que no se escinden completamente en K. Supongamos que es finito. Así, si $\mathfrak{p}$ es un primo que no está en E y $\mathfrak{P} \mid \mathfrak{p}$, tenemos $K_{\mathfrak{P}} = k_{\mathfrak{p}}$.

Vamos a probar que $J_k = k^* \,\mathrm{N}[J_K]$, lo que equivale a que $C_k = \mathrm{N}[C_K]$, en contradicción con la primera desigualdad fundamental.

Tomamos $\alpha \in J_k$. Por el teorema de aproximación existe un $\beta \in k^*$ tal que $|\alpha_{\mathfrak{P}}\beta - 1|_{\mathfrak{P}} < \epsilon$ para un número real $\epsilon > 0$ arbitrario y todo $\mathfrak{P}$ en E.

Como los grupos de normas locales son abiertos (por 6.17), tomando ϵ suficientemente pequeño podemos asegurar que $\alpha_{\mathfrak{P}}\beta$ es una norma local para todo $\mathfrak{P} \in E$, y trivialmente es una norma local para los primos restantes, pues las extensiones locales correspondientes son triviales. Así pues, $\alpha\beta \in \mathrm{N}[J_K]$ y $\alpha \in k^* \,\mathrm{N}[J_K]$. ∎

Teorema 7.16 *Sea K/k una extensión abeliana de cuerpos numéricos y $\mathfrak{m}$ un divisor de k divisible entre todos los primos ramificados de la extensión. Entonces el homomorfismo de Artin $\omega : I(\mathfrak{m}) \longrightarrow G(K/k)$ es suprayectivo.*

Demostración: Sea H la imagen de ω y sea F su cuerpo fijado. Hemos de probar que $F = k$. Si $\mathfrak{p} \in I(\mathfrak{m})$ entonces

$$\left(\frac{F/k}{\mathfrak{p}}\right) = \left(\frac{K/k}{\mathfrak{p}}\right)\Big|_F = 1,$$

donde usamos 4.4 y el hecho de que F es el cuerpo fijado por todos los símbolos de Artin.

Ahora bien, por el teorema 4.4 el orden del símbolo de Artin de $\mathfrak{p}$ es igual al grado de inercia de $\mathfrak{p}$ en F. Así pues, éste es igual a 1, lo que significa que todos los primos de k se escinden completamente en F excepto a lo sumo los que dividen a $\mathfrak{m}$, que son un número finito.

No podemos aplicar directamente el teorema anterior porque F/k no tiene por qué ser cíclica. Ahora bien, si $F \neq k$ el grupo $G(F/k)$, que es abeliano, contiene un subgrupo con cociente cíclico no trivial, cuyo cuerpo fijado F_0 es una extensión cíclica de k. Obviamente todos los primos de k que se escinden completamente en F se escinden completamente en F_0, lo cual sí contradice al teorema anterior. ∎

7.3 Preliminares a la segunda desigualdad

Para probar la segunda desigualdad fundamental necesitamos varios resultados de índole diversa que recogemos aquí en tres apartados.

Consecuencias de la primera desigualdad El teorema siguiente es un refinamiento de 7.15 para extensiones de grado potencia de primo.

Teorema 7.17 *Sea K/k una extensión cíclica de cuerpos numéricos de grado p^n, donde p es un primo. Entonces existen infinitos primos de k que se conservan primos en K.*

Demostración: Claramente K contiene un único subcuerpo F de grado p sobre k. Sea $\mathfrak{p}$ un primo en k no ramificado sobre K que no se conserve primo en K. Sea $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en K. Que $\mathfrak{p}$ no se conserve primo equivale a que $f(\mathfrak{P}/\mathfrak{p}) \neq p^n$. Este grado de inercia es el grado

$$|K_{\mathfrak{P}} : k_{\mathfrak{p}}| = |Kk_{\mathfrak{p}} : k_{\mathfrak{p}}| = |K : K \cap k_{\mathfrak{p}}| = \frac{|K : k|}{|K \cap k_{\mathfrak{p}} : k|},$$

luego $p \mid |K \cap k_{\mathfrak{p}} : k|$ y, por consiguiente, $F \subset K \cap k_{\mathfrak{p}}$. De aquí se sigue que el grado de inercia de $\mathfrak{p}$ en F es 1, es decir, $\mathfrak{p}$ se escinde completamente en F.

Así pues, si hay sólo un número finito de primos de k que se conservan primos en k, hay a lo sumo un número finito de primos en k que no se escinden completamente en F, en contradicción con el teorema 7.15. ∎

De aquí deducimos:

Teorema 7.18 *Sea k un cuerpo numérico y sean $K_1, \ldots, K_r$ extensiones cíclicas de k de grado primo p mutuamente disjuntas sobre k (es decir, la intersección entre una de ellas y el producto de las demás es k). Entonces existen infinitos primos en k que se conservan primos en K_1 y se escinden completamente en K_i, para $i = 2, \ldots, r$.*

DEMOSTRACIÓN: Sea $K = K_1 \cdots K_r$. Entonces $K/K_2 \cdots K_r$ es cíclica de grado p. Por el teorema anterior existen infinitos primos $\mathfrak{P}$ en $K_2 \cdots K_r$ que se conservan primos en K. Fijado uno de ellos, sea $\mathfrak{p}$ el primo de k divisible entre $\mathfrak{P}$. Supongamos que $\mathfrak{p}$ no se ramifica en K (tenemos infinitos primos $\mathfrak{p}$ en estas condiciones).

Claramente, el grupo de Galois $G(K/k)$ es producto directo de grupos cíclicos de orden p (es isomorfo al producto de los $G(K_i/k)$) y contiene como subgrupo a $G(K_\mathfrak{P}/k_\mathfrak{p})$, que es cíclico porque la extensión es no ramificada. Esto implica que $|K_\mathfrak{P}/k_\mathfrak{p}| \leq p$.

Por otra parte $|K_\mathfrak{P} : (K_2 \cdots K_r)_\mathfrak{P}| = p$, luego ha de ser $(K_2 \cdots K_r)_\mathfrak{P} = k_\mathfrak{p}$. Esto significa que $\mathfrak{p}$ se escinde completamente en $K_2 \cdots K_r$, luego también en cada K_i (con $i > 1$). Por otra parte, $\mathfrak{p}$ se conserva primo en K_1, o de lo contrario se escindiría completamente en K, y lo mismo le pasaría a $\mathfrak{P}$. ∎

Índices de grupos de potencias Nos ocupamos ahora del cálculo de los índices de ciertos grupos de potencias en cuerpos localmente compactos.

Definición 7.19 Sea K un cuerpo métrico discreto localmente compacto. Sea $\mathfrak{p}$ su único primo. La compacidad local equivale a que el cuerpo de restos es finito. De acuerdo con 1.44, llamaremos $\mathrm{N}\,\mathfrak{p}$ a su número de elementos. Sea U el grupo de unidades de K. Llamaremos $U_m = 1 + \mathfrak{p}^m$. Claramente estos conjuntos son bolas abiertas de centro 1 y constituyen una base de entornos de 1 en U (o en K). Definimos $U_0 = U$.

Llamaremos U^m al subgrupo de U formado por las potencias m-simas.

Los índices que nos interesan son los de los grupos U^m, pero calcularemos primero los de los grupos U_m.

Teorema 7.20 *Si K es un cuerpo métrico discreto localmente compacto, los conjuntos U_m son subgrupos abiertos y cerrados del grupo U de las unidades de K. Si $\mathfrak{p}$ es el primo de K se cumple*

$$|U : U_1| = \mathrm{N}\,\mathfrak{p} - 1 \quad \textit{y para } i \geq 1 \quad |U_m : U_{m+1}| = \mathrm{N}\,\mathfrak{p}.$$

DEMOSTRACIÓN: Del hecho de que $\mathfrak{p}^m$ es un ideal se sigue inmediatamente que el producto de elementos de U_m está en U_m. Por otra parte, si $1 + x \in U_m$, entonces

$$(1+x)^{-1} = 1 - x + x^2 - x^3 + \cdots = 1 + x(-1 + x - x^2 + x^3 + \cdots) \in U_m,$$

Sea E el anillo de los enteros de K. Si π es un primo en E, entonces cada elemento no nulo de E se expresa de forma única como $u\pi^n$, con $u \in U$, de donde la restricción a U de la proyección $E \longrightarrow E/\mathfrak{p}$ es un epimorfismo de grupos $U \longrightarrow (E/\mathfrak{p})^*$ cuyo núcleo es precisamente U_1. Tenemos que $|E/\mathfrak{p}| = \mathrm{N}\,\mathfrak{p}$, luego $|U : U_1| = \mathrm{N}\,\mathfrak{p} - 1$.

Si $m \geq 1$ la aplicación $\mathfrak{p}^m \longrightarrow U_m/U_{m+1}$ dada por $x \mapsto [1+x]$ es un epimorfismo de grupos, pues $[1+x][1+y] = [1+x+y+xy]$ y

$$\frac{1+x+y+xy}{1+x+y} = 1 + \frac{xy}{1+x+y},$$

con $v_\mathfrak{p}(xy/(1+x+y)) \geq 2m \geq m+1$, luego $[1+x][1+y] = [1+x+y]$.

El núcleo es $\mathfrak{p}^{m+1}$, luego

$$|U_m : U_{m+1}| = |\mathfrak{p}^m : \mathfrak{p}^{m+1}| = \frac{|E : \mathfrak{p}^m|}{|E : \mathfrak{p}^{m+1}|} = \mathrm{N}\,\mathfrak{p}.$$

■

Teorema 7.21 *Sea K un cuerpo métrico discreto localmente compacto y sea m un natural no divisible entre la característica de K. Entonces el grupo U^m es abierto y cerrado en U y además*

$$|U : U^m| = \frac{K_m^*}{\|m\|_\mathfrak{p}},$$

donde K_m^* es el grupo de las raíces m-simas de la unidad contenidas en K y

$$\|m\|_\mathfrak{p} = \frac{1}{(\mathrm{N}\,\mathfrak{p})^{v_\mathfrak{p}(m)}}.$$

Demostración: Sea π un primo en K. Tomemos r suficientemente grande para que $|m\pi^{r+1}| \geq |\pi^{2r}|$. Entonces, para cualquier x entero en K se cumple

$$(1+x\pi^r)^m \equiv 1 + mx\pi^r \ (\text{mód } m\pi^{r+1}).$$

En consecuencia $U_r^m \leq U_{r+s}$, donde $s = v_\mathfrak{p}(m)$. Para probar la inclusión opuesta tomamos un elemento arbitrario de U_{r+s}, que podemos expresar como $1 + my\pi^r$ para cierto entero y de K. Queremos encontrar un entero x de K tal que $(1+x\pi^r)^m = 1 + my\pi^r$. Operando, esto equivale a que el polinomio

$$F(x) = \frac{\pi^{(m-1)r}}{m}\, x^m + \cdots + \binom{m}{2}\frac{\pi^r}{m}\, x^2 + x - y$$

tenga una raíz entera en K. Observar que si exigimos $s < r$ entonces todos los coeficientes son enteros. Podemos aplicar el teorema [7.18]. Para ello observamos que $F(y) \equiv 0 \ (\text{mód } \pi)$ pero $F'(y) \equiv 1 \ (\text{mód } \pi)$, luego existe la raíz buscada, y así $U_r^m = U_{r+s}$.

En particular $U_{r+s} \leq U^m$, lo que prueba que el grupo U^m es abierto, luego también cerrado. Del hecho de que U^m sea abierto se deduce que el índice $|U : U^m|$ es finito (pues U es compacto).

Podemos tomar r suficientemente grande como para que U_r no contenga ninguna raíz m-sima de la unidad distinta de 1. Aplicamos el teorema 7.8 al homomorfismo $f : U \longrightarrow U^m$ dado por $f(u) = u^m$. Con ello obtenemos que

$$|U : U_r| = |U^m : U_{r+s}|\,|K_m^* : 1| = \frac{|U : U_{r+s}|}{|U : U^m|}\,|K_m^*|,$$

de donde, usando el teorema anterior

$$|U : U^m| = |U_r : U_{r+s}|\,|K_m^*| = (\mathrm{N}\,\mathfrak{p})^s|K_m^*| = \frac{|K_m^*|}{\|m\|_{\mathfrak{p}}}.$$

■

El último índice que necesitamos calcular es el siguiente:

Teorema 7.22 *Sea K un cuerpo métrico discreto localmente compacto, sea m un natural no divisible entre la característica de K, sea K^{*m} el grupo de las potencias m-simas de K y sea K_m^* el grupo de las raíces m-simas de la unidad en K. Entonces*

$$|K^* : K^{*m}| = \frac{m\,|K_m^*|}{\|m\|_{\mathfrak{p}}}.$$

Demostración: Sea π un primo en K. Claramente $K^* = U \times \langle\pi\rangle$, luego $K^{*m} = U^m \times \langle\pi^m\rangle$ y, en consecuencia,

$$|K^* : K^{*m}| = |U : U^m|\,|\,\langle\pi\rangle : \langle\pi^m\rangle\,| = m\,|U : U^m|.$$

■

La teoría de Kummer La teoría de Kummer es una especie de teoría de cuerpos de clases rudimentaria que pone en correspondencia ciertas extensiones abelianas de un cuerpo numérico k y ciertos subgrupos de k^*. Veamos las definiciones precisas.

Definición 7.23 Diremos que una extensión de cuerpos K/k es una *extensión de Kummer* (o que K es un *cuerpo de Kummer* sobre k) si la extensión K/k es abeliana y existe un número natural n tal que el grupo $G(K/k)$ tiene exponente[1] n y k contiene una raíz n-sima primitiva de la unidad (en particular n no es divisible entre la característica de k).

Sea k un cuerpo que contenga una raíz n-sima primitiva de la unidad. Llamaremos k^{*n} al grupo de las potencias n-simas de k^*. Sea Δ un grupo tal que $k^{*n} \le \Delta \le k^*$ y el índice $|\Delta : k^{*n}|$ sea finito. Sea $\Delta^{1/n}$ el conjunto de las raíces n-simas de los elementos de Δ. Sea $k_\Delta = k(\Delta^{1/n})$.

Es claro que si $\Delta/k^{*n} = \{[\alpha_1], \ldots, [\alpha_m]\}$ y $\sqrt[n]{\alpha_i}$ es una raíz n-sima de cada α_i, entonces $k_\Delta = k\big(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_m}\big)$, luego la extensión k_Δ/k es finita.

Es un hecho conocido de la teoría de cuerpos que cada una de las extensiones $k\big(\sqrt[n]{\alpha_i}\big)/k$ es cíclica de grado divisor de n, luego k_Δ/k es abeliana de exponente n, pues hay un monomorfismo de $G(k_\Delta/k)$ en el producto de los grupos $G\big(k\big(\sqrt[n]{\alpha_i}\big)/k\big)$.

[1]Un grupo tiene exponente n si el orden de todos sus elementos divide a n. Diremos que una extensión de cuerpos tiene exponente n si es de Galois y su grupo de automorfismos tiene exponente n.

Recíprocamente, si K/k es una extensión abeliana de exponente n, entonces K puede expresarse como producto $K = K_1 \cdots K_m$, donde cada K_i/k es cíclica, y es conocido que cada K_i es de la forma $k\big(\sqrt[n]{\alpha_i}\big)$ para un $\alpha_i \in k$. Concluimos que $K = k_\Delta$, donde Δ es el subgrupo generado por $\alpha_1, \ldots, \alpha_m$ y por k^{*n}.

Recogemos lo que hemos probado en un teorema junto con un importante hecho adicional.

Teorema 7.24 *Sea k un cuerpo que contenga a las raíces n-simas de la unidad. Entonces la aplicación $\Delta \mapsto k_\Delta = k(\Delta^{1/n})$ biyecta los grupos $k^{*n} \le \Delta \le k^*$ tales que el índice $|\Delta : k^{*n}|$ es finito con las extensiones de Kummer de k de exponente n. Además se cumple que $|k_\Delta : k| = |\Delta : k^{*n}|$.*

Demostración: Sólo queda probar la última afirmación. Sea $\zeta \in k$ una raíz n-sima primitiva de la unidad, sea $G = G(k_\Delta/k)$ y sea $C = \langle\zeta\rangle$. Para cada $\alpha \in \Delta$ consideremos un $\beta \in k_\Delta$ tal que $\beta^n = \alpha$. Los demás elementos que cumplen esto son $\beta,\ \beta\zeta,\ \cdots,\ \beta\zeta^{n-1}$. Sea ahora $\sigma \in G$. Entonces $\sigma(\beta) = \beta\zeta^s$ para cierto s, luego $\sigma(\beta\zeta^i)/\beta\zeta^i = \zeta^s$ es independiente de i o, en otras palabras, el número $\sigma(\beta)/\beta$ es una raíz de la unidad que depende de α y de σ, pero no de la elección de β.

Podemos definir $(\ ,\ ) : G \times \Delta \longrightarrow C$ mediante $(\sigma, \alpha) = \sigma(\beta)/\beta$, y es inmediato comprobar que las aplicaciones $(\sigma,\ ) : \Delta \longrightarrow C$ y $(\ , \alpha) : G \longrightarrow C$ son homomorfismos de grupos. Veámoslo para las segundas:

$$(\sigma\tau, \alpha) = \frac{\tau(\sigma(\beta))}{\beta} = \frac{\sigma(\beta)}{\beta}\,\frac{\tau(\sigma(\beta))}{\sigma(\beta)} = (\sigma, \alpha)(\tau, \alpha).$$

También es claro que el núcleo de $(\sigma,\ ) : \Delta \longrightarrow C$ contiene a k^{*n}, pues para todo $\beta \in k^*$ se cumple $(\sigma, \beta^n) = \sigma(\beta)/\beta = 1$. Por lo tanto este par induce a su vez otro par

$$(\ ,\ ) : G \times (\Delta/k^{*n}) \longrightarrow C.$$

Este par induce dos homomorfismos $G \longrightarrow (\Delta/k^{*n})^*$ y $(\Delta/k^{*n}) \longrightarrow G^*$, donde el asterisco denota el grupo de caracteres de un grupo abeliano (notar que podemos identificar a C con un subgrupo de $\mathbb{C}$). Ambos homomorfismos son de hecho inyectivos, pues si $(\sigma, \alpha) = 1$ para todo $\alpha \in \Delta$, entonces $\sigma(\beta)/\beta = 1$ para todo $\beta \in k_\Delta$, luego $\sigma = 1$, y si $\sigma(\beta)/\beta = 1$ para todo $\sigma \in G$, entonces $\beta \in k$, con lo que $\alpha \in k^{*n}$.

Teniendo en cuenta que el grupo dual de un grupo abeliano finito G tiene el mismo orden que G, los monomorfismos anteriores prueban que

$$|k_\Delta : k| = |G| = |\Delta : k^{*n}|.$$

∎

El claro que la biyección $\Delta \leftrightarrow k_\Delta$ conserva las inclusiones, de donde se siguen inmediatamente las relaciones

$$\begin{array}{ccc} \Delta_1\Delta_2 & \leftrightarrow & k_{\Delta_1} k_{\Delta_2} \\ \Delta_1 \cap \Delta_2 & \leftrightarrow & k_{\Delta_1} \cap k_{\Delta_2}. \end{array}$$

En la práctica, si Δ es un subgrupo de k^*, que no contenga necesariamente a k^{*n}, podemos considerar el subgrupo $k^{*n}\Delta$. Se cumple

$$|k^{*n}\Delta : k^{*n}| = |\Delta : \Delta \cap k^{*n}|,$$

luego si este índice es finito podemos definir $k_\Delta = k_{k^{*n}\Delta} = k(\Delta^{1/n})$. Entonces se cumple

$$|k_\Delta : k| = |\Delta : \Delta \cap k^{*n}|.$$

También es claro que k_Δ es cíclico si y sólo si Δ/k^{*n} es cíclico y, en tal caso, si α genera el cociente Δ/k^{*n}, se cumple $k_\Delta = k\big(\sqrt[n]{\alpha}\big)$.

Veamos por último un resultado sobre la aritmética en extensiones de Kummer de cuerpos numéricos:

Teorema 7.25 *Sea k un cuerpo numérico que contenga las raíces n-simas de la unidad. Sea $K = k_\Delta$ una extensión de Kummer de exponente n y $\mathfrak{p}$ un primo en k.*

a) $\mathfrak{p}$ se escinde completamente en K si y sólo si $\Delta \subset k_\mathfrak{p}^{*n}$.

b) Si $\mathfrak{p}$ es finito y $\mathfrak{p} \nmid n$, entonces $\mathfrak{p}$ es no ramificado en K si y sólo si $\Delta \subset U_\mathfrak{p} k^{*n}$.

Demostración: a) Sea $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en K. Entonces $\mathfrak{p}$ se escinde completamente en K si y sólo si $K_\mathfrak{P} = k_\mathfrak{p}(\Delta^{1/n}) = k_\mathfrak{p}$, si y sólo si $\Delta \subset k_\mathfrak{p}^{*n}$.

b) Supongamos que $\mathfrak{p}$ no se ramifica y sea $\alpha \in \Delta$. Entonces α es una potencia n-sima en $K_\mathfrak{P}$, luego $n \mid v_\mathfrak{P}(\alpha) = v_\mathfrak{p}(\alpha)$. Por lo tanto, si $\pi \in \mathfrak{p}\setminus\mathfrak{p}^2$ (en particular $\pi \in k$), podemos descomponer $\alpha = \epsilon\beta^n$, donde $\epsilon \in U_\mathfrak{p}$ y $\beta \in k$ es una potencia de π. Así pues, $\alpha \in U_\mathfrak{p} k^{*n}$.

Recíprocamente, supongamos que $\Delta \subset U_\mathfrak{p} k^{*n}$. Sabemos que K se obtiene adjuntando a k un número finito de raíces $\sqrt[n]{\alpha}$, con $\alpha \in \Delta$, luego por las propiedades de las extensiones no ramificadas basta ver que $\mathfrak{p}$ es no ramificado en cada $k\big(\sqrt[n]{\alpha}\big)$. Por la hipótesis podemos suponer que $\alpha \in U_\mathfrak{p}$. Entonces $\alpha = u/v$, donde u y v son enteros en k y $\mathfrak{p} \nmid v$. Multiplicando por v^n podemos suponer que α es entero en k.

Probemos que $\mathfrak{p}$ no divide al diferente de la extensión. Sea $p(x)$ el polinomio mínimo de $\sqrt[n]{\alpha}$. Claramente $p(x) \mid f(x) = x^n - \alpha$, luego $p'\big(\sqrt[n]{\alpha}\big) \mid n\big(\sqrt[n]{\alpha}\big)^{n-1}$. Por el teorema 3.13 tenemos que el diferente divide a $n\big(\sqrt[n]{\alpha}\big)^{n-1}$, y por hipótesis $\mathfrak{p} \nmid n\big(\sqrt[n]{\alpha}\big)^{n-1}$. ∎

7.4 La segunda desigualdad fundamental

En esta sección demostramos la segunda desigualdad fundamental:

$$|C_k : \mathrm{N}[C_K]| \le |K : k|,$$

para toda extensión abeliana K/k de cuerpos numéricos.

Empezamos con varios resultados sencillos que nos reducen el problema al caso de extensiones de Kummer de grado primo.

Teorema 7.26 *Sea $k \subset K \subset L$ una cadena de cuerpos numéricos tal que L/k es abeliana. Entonces*

a) $|C_k : \mathrm{N}[C_K]| \,\big|\, |C_k : \mathrm{N}[C_L]|$,

b) $|C_k : \mathrm{N}[C_L]| \,\big|\, |C_k : \mathrm{N}[C_K]|\,|C_K : \mathrm{N}[C_L]|$.

En ambos casos suponemos (únicamente) que el miembro derecho es finito. En particular, si K/k y L/K cumplen la segunda desigualdad, también la cumple L/k.

Demostración: Es fácil ver que $\mathrm{N}_K^L \circ \mathrm{N}_k^K = \mathrm{N}_k^L$, con lo que tenemos las inclusiones $\mathrm{N}[C_L] \le \mathrm{N}[C_K] \le C_k$. Por consiguiente

$$|C_k : \mathrm{N}[C_L]| = |\,\mathrm{N}[C_K] : \mathrm{N}[C_L]|\,|C_k : \mathrm{N}[C_K]|.$$

Esto prueba a).

Más aún la norma induce un epimorfismo $C_K/\,\mathrm{N}[C_L] \longrightarrow \mathrm{N}[C_K]/\,\mathrm{N}[C_L]$, con lo que $|\,\mathrm{N}[C_K] : \mathrm{N}[C_L]| \,\big|\, |C_K : \mathrm{N}[C_L]|$, y tenemos b). ∎

Como toda extensión abeliana puede descomponerse en una cadena de extensiones cíclicas de grado primo, basta probar la segunda desigualdad para estas extensiones.

Teorema 7.27 *Si K/k es una extensión abeliana, entonces el índice del grupo de normas $|C_k : \mathrm{N}[C_K]|$ es finito y divide a una potencia de $|K : k|$.*

Demostración: Por el teorema anterior basta probarla finitud para extensiones cíclicas de orden primo. Sea E_k un conjunto finito de primos en k y E el conjunto de sus divisores primos en K. Podemos escogerlos de modo que E_k contenga a todos los primos arquimedianos, a todos los primos que se ramifican en K y además

$$J_k = k^* J_{E_k}, \qquad J_K = K^* J_E.$$

Entonces $k^*\,\mathrm{N}[J_K] = k^*\,\mathrm{N}[K^*]\,\mathrm{N}[J_E] = k^*\,\mathrm{N}[J_E]$, de donde

$$|C_k : \mathrm{N}[C_K]| = |J_k : k^*\,\mathrm{N}[J_K]| = |k^* J_{E_k} : k^*\,\mathrm{N}[J_E]| \le |J_{E_k} : \mathrm{N}[J_E]|$$

(notar que hay un epimorfismo del último cociente en el penúltimo.)

El último índice es el orden de $H^0(G, J_E)$, y su finitud está contenida en la fórmula (7.5).

Si K/k es una extensión abeliana arbitraria de grado n y $\alpha \in C_k$, es claro que $\alpha^n = \mathrm{N}(\alpha)$, por lo que todos los elementos del grupo $C_k/\,\mathrm{N}[C_K]$ tienen orden divisor de n. Necesariamente entonces el orden del grupo divide a una potencia de n. ∎

Teorema 7.28 *Si la segunda desigualdad fundamental se cumple en todas las extensiones K/k cíclicas de grado primo p tales que k contiene una raíz p-ésima primitiva de la unidad, entonces se cumple en toda extensión abeliana.*

DEMOSTRACIÓN: Según hemos comentado, basta probar que se cumple en toda extensión cíclica K/k de grado primo p. Sea ζ una raíz p-ésima primitiva de la unidad. Por el teorema 7.26, el índice del grupo de normas de K/k divide al de $K(\zeta)/k$, que a su vez divide al producto de los índices de $K(\zeta)/k(\zeta)$ y $k(\zeta)/k$.

Ahora bien, el índice de K/k es potencia de p, y el índice de $k(\zeta)/k$ divide al grado, que a su vez divide a $p-1$, luego el índice de K/k divide al de $K(\zeta)/k(\zeta)$, que por hipótesis divide a p. ∎

Fijemos ahora un cuerpo numérico k que contenga las raíces n-simas de la unidad. De momento no suponemos que n sea primo. Vamos a realizar una construcción general de la que deduciremos la segunda desigualdad, pero que más adelante nos aprovechará para otros fines. Consideremos un conjunto finito E de primos de k que contenga a todos los primos arquimedianos y a los divisores de n. Dividamos $E = E_1 \cup E_2$ en dos conjuntos disjuntos, uno de los cuales puede ser vacío. Sea i uno de los índices 1 o 2 y sea j el otro. Definimos

$$D_i = \prod_{\mathfrak{p}\in E_j} k_{\mathfrak{p}}^{*n} \times \prod_{\mathfrak{p}\in E_i} k_{\mathfrak{p}}^{*} \times \prod_{\mathfrak{p}\in P\setminus E} U_{\mathfrak{p}}. \tag{7.11}$$

Claramente $D_i \le J_E$. Todo $\alpha \in D_i$ puede escribirse como $\alpha = \beta^n\gamma$, donde

$$\beta \in \prod_{\mathfrak{p}\in E_j} k_{\mathfrak{p}}, \qquad \gamma \in \prod_{\mathfrak{p}\in E_i} k_{\mathfrak{p}}^{*} \times \prod_{\mathfrak{p}\in P\setminus E} U_{\mathfrak{p}}. \tag{7.12}$$

Sea $\Delta_i = D_i \cap k^*$. Claramente $k_E^n \le \Delta_i \le k_E$. Si llamamos s al número de elementos de E, el teorema 7.12 implica que

$$|k_E : k_E^n| = n^s. \tag{7.13}$$

En efecto, k_E es producto de un grupo cíclico de raíces de la unidad (de orden múltiplo de n) por un grupo abeliano libre de rango $s-1$. Al elevar a n, el primer factor da cociente de orden n y el segundo de orden n^{s-1}.

Consideremos la extensión de Kummer $K_i = k(\Delta_i^{1/n})$, correspondiente al grupo $\Delta_i k^{*n}$. Es claro que $\Delta_i \cap k^{*n} = k_E^n$, luego

$$|K_i : k| = |\Delta_i k^{*n} : k^{*n}| = |\Delta_i : k_E^n|. \tag{7.14}$$

Por el teorema 7.25 tenemos:

a) Si $\mathfrak{p} \in P \setminus E$ entonces $\mathfrak{p}$ es no ramificado en K_i.

b) Si $\mathfrak{p} \in E_j$ entonces $\mathfrak{p}$ se escinde completamente en K_i.

Igualmente tenemos definido el cuerpo K_j. Llamaremos J_i y J_j a los grupos de elementos ideales de K_i y K_j, y N_i, N_j a las normas correspondientes. Veamos ahora un resultado auxiliar:

Teorema 7.29 *Sea K/k una extensión abeliana de cuerpos numéricos de exponente n. Si $\alpha \in J_k$, entonces $\alpha^n \in k^* \,\mathrm{N}[J_K]$.*

Demostración: Por el teorema de aproximación existe un $\beta \in k^*$ tal que $\beta\alpha_\mathfrak{p}$ esté lo suficientemente cerca de 1 en los primos ramificados como para que $(\beta\alpha_\mathfrak{p})^n \in \mathrm{N}[K_\mathfrak{P}]$, para cualquier $\mathfrak{P} \mid \mathfrak{p}$ en K. (Esto es posible porque los grupos de normas locales son abiertos).

Si $\mathfrak{p}$ es no ramificado, entonces las extensiones $K_\mathfrak{p}/k_\mathfrak{p}$ son cíclicas y tienen también exponente n, luego su grado divide a n y $(\beta\alpha_\mathfrak{p})^n$ es la norma de una potencia de $\beta\alpha_\mathfrak{p}$. Claramente entonces $\beta\alpha \in \mathrm{N}[J_K]$. ∎

El resultado principal es el siguiente:

Teorema 7.30 *Sea k un cuerpo numérico que contenga las raíces n-simas de la unidad. Sea E un conjunto finito de primos de k que contenga todos los primos arquimedianos, todos los divisores de n y tal que $J_k = k^* J_E$. Sea $E = E_1 \cup E_2$ en las condiciones anteriores. Entonces*

a) $k^* D_i \le k^* \,\mathrm{N}_j[J_j]$,

b) $|J_k : k^* D_1|\,|J_k : k^* D_2| = |K_1 : k|\,|K_2 : k|$.

En particular

$$|J_k : k^* \,\mathrm{N}_1[J_1]|\,|J_k : k^* \,\mathrm{N}_2[J_2]| \le |K_1 : k|\,|K_2 : k|.$$

Demostración: a) Sea $\alpha \in D_i$. Podemos descomponerlo como $\alpha = \beta^n\gamma$, en las condiciones (7.12). Por el teorema anterior $\beta^n \in k^* \,\mathrm{N}_j[J_j]$. Basta probar que todas las componentes de γ son normas. Si $\mathfrak{p} \in E_j$ entonces $\gamma_\mathfrak{p} = 1$. Si $\mathfrak{p} \in S_i$ entonces $\mathfrak{p}$ se escinde completamente en K_j, luego las extensiones locales correspondientes son triviales, luego $\gamma_\mathfrak{p}$ también es una norma. Finalmente, si $\mathfrak{p} \in P \setminus E$, entonces $\gamma_\mathfrak{p} \in U_\mathfrak{p}$ y las extensiones locales son no ramificadas, luego $\gamma_\mathfrak{p}$ es una norma por el teorema 7.9.

b) Calculemos:

$$|J_k : k^* D_i| = |k^* J_E : k^* D_i| = |k^* J_E/k^* : k^* D_i/k^*|.$$

El isomorfismo canónico $k^* J_E/k^* \cong J_E/k_E$ transforma el subgrupo $k^* D_i/k^*$ en $D_i k_E/k_E$, luego

$$|J_k : k^* D_i| = |J_E/k_E : D_i k_E/k_E| = |J_E : D_i k_E| = |J_E/D_i : D_i k_E/D_i|$$

$$= \frac{|J_E : D_i|}{|k_E : k_E \cap D_i|} = \frac{|J_E : D_i|}{|k_E : \Delta_i|} = \frac{|J_E : D_i|}{|k_E : k_E^n|}\,|\Delta_i : k_E^n| = \frac{|J_E : D_i|}{n^s}\,|K_i : k|,$$

donde hemos usado (7.13). De la propia definición de D_i se sigue que

$$|J_E : D_i| = \prod_{\mathfrak{p} \in E_j} |k_\mathfrak{p}^* : k_\mathfrak{p}^{*n}|.$$

Multiplicando esta fórmula por la correspondiente para j queda

$$|J_k : k^*D_1|\,|J_k : k^*D_2| = \frac{\prod_{\mathfrak{p}\in E} |k_\mathfrak{p}^* : k_\mathfrak{p}^{*n}|}{n^{2s}}\,|K_1 : k|\,|K_2 : k|.$$

Teniendo en cuenta que k contiene las n raíces de la unidad, el teorema 7.22 afirma que

$$|k_\mathfrak{p}^* : k_\mathfrak{p}^{*n}| = \frac{n^2}{\|n\|_\mathfrak{p}}.$$

Por otra parte, si $\mathfrak{p} \in P\setminus E$ entonces $\|n\|_\mathfrak{p} = 1$, luego la fórmula del producto implica que

$$\prod_{\mathfrak{p}\in E} \|n\|_\mathfrak{p} = \prod_{\mathfrak{p}} \|n\|_\mathfrak{p} = 1,$$

luego

$$\prod_{\mathfrak{p}\in E} |k_\mathfrak{p}^* : k_\mathfrak{p}^{*n}| = n^{2s},$$

lo que nos da la igualdad buscada. ∎

La segunda desigualdad fundamental se deduce inmediatamente del teorema siguiente:

Teorema 7.31 *Sea p un primo y $K = k\big(\sqrt[p]{\alpha}\big)$ una extensión de Kummer de grado p. Entonces existen dos conjuntos disjuntos E_1 y E_2 de primos de k en las condiciones del teorema anterior y tales que $J_k = k^*D_1$ y $K_1 = K$.*

Antes de probar esto, veamos cómo se sigue de aquí la segunda desigualdad.

Puesto que $J_k = k^*D_1 \le k^*\,\mathrm{N}_2[J_2]$, tenemos que $|J_k : k^*\,\mathrm{N}_2[J_2]| = 1$. La primera desigualdad implica que $K_2 = k$. Observar que no podemos aplicarla directamente, pues sólo la tenemos probada para extensiones cíclicas y no sabemos si K_2/k lo es. Sin embargo, si $K_2 \ne k$ entonces K_2 contiene una extensión cíclica L de k no trivial, y como $\mathrm{N}[C_{K_2}] \le \mathrm{N}[C_L] \le C_k$, llegamos a que el grupo de normas de L/k es trivial, y esto sí es una contradicción.

Así pues, la última desigualdad del teorema anterior es la segunda desigualdad fundamental. ∎

Demostración (de 7.31): Multiplicando α por una potencia n-sima, podemos suponer que es un entero en k.

Sea E_1 un conjunto finito de primos de k que contenga a todos los primos arquimedianos, a los divisores de n, a los de α y tal que $J_k = k^*J_{E_1}$. Sea s_1 el número de elementos de E_1.

El grupo $k_{E_1}/k_{E_1}^p$ tiene p^{s_1} elementos, todos de orden p, luego es producto de grupos cíclicos de orden p. Podemos verlo como espacio vectorial sobre el cuerpo de p elementos. La clase de α no es nula (o la extensión K/k sería trivial), luego puede extenderse hasta una base del cociente, digamos $[\alpha_1], \dots [\alpha_{s_1}]$, con $\alpha = \alpha_1$.

Sea $K_i = k\big(\sqrt[p]{\alpha_i}\big)$. Entonces $K = K_1$ y $|K_i : k| = p$. El cuerpo $K_1 \cdots K_{s_1}$ es la extensión de Kummer asociada a $k^{*p}\langle \alpha_1, \ldots, \alpha_{s_1}\rangle$. La inclusión induce un homomorfismo

$$\langle \alpha_1, \ldots, \alpha_{s_1}\rangle \longrightarrow k_{E_1}/k_{E_1}^p$$

que claramente es suprayectivo y su núcleo es $\langle \alpha_1, \ldots, \alpha_{s_1}\rangle \cap k^{*p}$, luego

$$|K_1 \cdots K_{s_1} : k| = |\langle \alpha_1, \ldots, \alpha_{s_1}\rangle : \langle \alpha_1, \ldots, \alpha_{s_1}\rangle \cap k^{*p}| = p^{s_1}.$$

El grado del producto de todos los cuerpos menos uno es p^{s_1-1} (pues ahora el homomorfismo ya no es suprayectivo, sino que su imagen es un subespacio de dimensión $s_1 - 1$). Esto implica que los cuerpos K_i son mutuamente disjuntas sobre k, con lo que estamos en las hipótesis del teorema 7.18, que nos permite escoger primos $\mathfrak{p}_i$ fuera de E_1 tales que p_i se conserva primo en K_i y se escinde completamente en los otros cuerpos. Tomamos $E_2 = \{\mathfrak{p}_2, \ldots, \mathfrak{p}_{s_1}\}$.

Por el teorema 7.25, $\alpha_i \in k_{\mathfrak{p}_j}^{*p}$ para $i \neq j$, pero no para $i = j$. Observemos los grupos J_{E_1}, D_1 y $J_{E_1} \cap D_1$:

$$\begin{aligned}
J_{E_1} &= \prod_{\mathfrak{p}\in E_1} k_{\mathfrak{p}}^* \times \prod_{i=2}^{s_1} U_{\mathfrak{p}_i} \times \prod_{\mathfrak{p}\in P\setminus E} U_{\mathfrak{p}},\\
D_1 &= \prod_{\mathfrak{p}\in E_1} k_{\mathfrak{p}}^* \times \prod_{i=2}^{s_1} k_{\mathfrak{p}_i}^{*p} \times \prod_{\mathfrak{p}\in P\setminus E} U_{\mathfrak{p}},\\
J_{E_1}\cap D_1 &= \prod_{\mathfrak{p}\in E_1} k_{\mathfrak{p}}^* \times \prod_{i=2}^{s_1} U_{\mathfrak{p}_i}^{p} \times \prod_{\mathfrak{p}\in P\setminus E} U_{\mathfrak{p}}.
\end{aligned}$$

Por el teorema 7.21, sabemos que $|U_{\mathfrak{p}_i} : U_{\mathfrak{p}_i}^p| = p/\|p\|_{\mathfrak{p}_i} = p$, ya que los primos que dividen a p están en E_1. Por lo tanto el cociente $U_{\mathfrak{p}_i} : U_{\mathfrak{p}_i}^p$ es cíclico de orden p. El cociente $J_{E_1}/J_{E_1}\cap D_1$ es producto de $s_1 - 1$ grupos cíclicos de orden p, luego podemos considerarlo como un espacio vectorial sobre el cuerpo de p elementos, y es claro que las clases de $\alpha_2, \ldots, \alpha_{s_1}$ constituyen una base. Puesto que están en k^*, concluimos que $J_{E_1} \leq k^*(J_{E_1}\cap D_1) \leq k^* D_1$, luego $J_k = k^* J_{E_1} = k^* D_1$, que es una parte de lo que teníamos que probar.

Falta ver que $K = k(\Delta_1^{1/p})$. La expresión de D_1 muestra que $D_1 \leq J_{E_1} J_k^p = J_{E_1}(k^* J_{E_1})^p = k^{*p} J_{E_1}$, luego $\Delta_1 = D_1 \cap k^* \leq k^{*p} k_{E_1}$. Por lo tanto, toda clase del cociente $\Delta_1 k^{*p}/k^{*p}$ tiene un representante en k_{E_1}. Más aún, podemos tomarlo de la forma

$$\delta = \alpha_1^{e_1} \cdots \alpha_{s_1}^{e_{s_1}}.$$

Como $\delta \in D_1$, ha de cumplir $\delta \in k_{\mathfrak{p}_i}^{*p}$, para $i = 2, \ldots s_1$. Si $j \neq i$ entonces $\alpha_j \in k_{\mathfrak{p}_i}^{*p}$, luego también $\alpha_i^{e_i} \in k_{\mathfrak{p}_i}^{*p}$. Como $\alpha_i \notin k_{\mathfrak{p}_i}^{*p}$, necesariamente $p \mid e_i$, para $i = 2, \ldots, s_1$. Esto significa que toda clase de $\Delta_1 k^{*p}/k^{*p}$ tiene, de hecho, un representante de la forma $\alpha_1^{e_1}$. Por otra parte $\alpha = \alpha_1 \in \Delta_1$, ya que $\alpha \in k_{\mathfrak{p}_1}^{*p}$ para $i = 2, \ldots, s_1$, luego en definitiva $\Delta_1 k^{*p}/k^{*p}$ está generado por α, con lo que el cuerpo de Kummer asociado es $K_1 = k\big(\sqrt[p]{\alpha}\big)$. ∎

7.5 El núcleo del homomorfismo de Artin

El último trabajo que nos queda por realizar es demostrar que si K/k es una extensión abeliana de cuerpos numéricos, existe un divisor admisible $\mathfrak{m}$, divisible sólo entre los primos ramificados de la extensión, tal que $P_\mathfrak{m}$ está contenido en el núcleo del homomorfismo de Artin.

De aquí se sigue fácilmente el resultado que anticipábamos al comienzo del capítulo. En efecto, tenemos el homomorfismo de Artin $\omega : I(\mathfrak{m}) \longrightarrow G(K/k)$. Llamamos N a su núcleo. Por 7.10 sabemos que $\mathfrak{m}$ es divisible entre todos los primos ramificados de la extensión, por 7.16 sabemos que ω es suprayectivo y por 4.10 sabemos que el grupo $\mathrm{N}(\mathfrak{m}) = \mathrm{N}(\Delta)$ está contenido en N. Así pues, $P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}) \le N \le I(\mathfrak{m})$. El teorema de isomorfía implica que $|I(\mathfrak{m}) : N| = |K : k|$, y la segunda desigualdad fundamental (junto con 6.21) es

$$|I(\mathfrak{m}) : P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})| = |C_k : \mathrm{N}[C_K]| \le |K : k|.$$

Esto implica que $N = P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$. Por consiguiente ω induce un isomorfismo

$$I(\mathfrak{m})/P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}) \cong G(K/k).$$

Si $\mathfrak{f}$ es el conductor de la extensión, es decir, el menor divisor admisible, entonces $I(\mathfrak{f}) = I(\mathfrak{m})$ (pues $\mathfrak{f}$ y $\mathfrak{m}$ son ambos divisibles entre los primos ramificados y sólo entre ellos), y la relación (6.3) nos da que $P_\mathfrak{f}\,\mathrm{N}(\mathfrak{f}) = P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$, luego trivialmente

$$I(\mathfrak{f})/P_\mathfrak{f}\,\mathrm{N}(\mathfrak{f}) \cong G(K/k).$$

Finalmente, si $\mathfrak{m}$ es cualquier divisor admisible para la extensión, la fórmula (6.3) nos da que $P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}) = P_\mathfrak{f}\,\mathrm{N}(\mathfrak{f}) \cap I(\mathfrak{m})$, de donde se sigue que la restricción de ω a $I(\mathfrak{m})$ tiene núcleo $P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$, y sigue siendo suprayectiva por 7.16. En definitiva tenemos:

Teorema 7.32 *Sea K/k una extensión abeliana de cuerpos numéricos y $\mathfrak{m}$ un divisor admisible. Entonces el símbolo de Artin induce un isomorfismo*

$$\omega : I(\mathfrak{m})/P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}) \longrightarrow G(K/k),$$

al que llamaremos isomorfismo de Artin *de la extensión.*

Probemos, pues, que el núcleo del homomorfismo de Artin contiene un subgrupo $P_\mathfrak{m}$. Lo probaremos primero para extensiones ciclotómicas, luego para extensiones cíclicas y luego para extensiones abelianas. En primer lugar necesitamos varios resultados técnicos sobre extensiones ciclotómicas. En el primer teorema recogemos algunos hechos elementales.

Teorema 7.33 *Se cumple:*

a) Para cada número natural n sea ζ_n una raíz n-sima primitiva de la unidad. Sean a y b dos números naturales, sea $d = \mathrm{mcd}(a,b)$ y sea $m = \mathrm{mcm}(a,b)$. Entonces

$$\mathbb{Q}(\zeta_a)\mathbb{Q}(\zeta_b) = \mathbb{Q}(\zeta_m) \qquad y \qquad \mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) = \mathbb{Q}(\zeta_d).$$

b) Si K es un cuerpo numérico, existe un número natural s de manera que si m es un número natural primo con s y ζ es una raíz de la unidad de orden m, entonces

$$K \cap \mathbb{Q}(\zeta) = \mathbb{Q},$$

y para todo subcuerpo $k \subset K$ se cumple $K \cap k(\zeta) = k$.

Demostración: a) Es claro que $\mathbb{Q}(\zeta_a)\mathbb{Q}(\zeta_b) \subset \mathbb{Q}(\zeta_m)$. Un automorfismo $\sigma \in G(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ actúa sobre las raíces de la unidad elevándolas a un cierto i primo con m. Si cumple $\sigma(\zeta_a) = \zeta_a$ y $\sigma(\zeta_b) = \zeta_b$, entonces $i \equiv 1$ (mód a) e $i \equiv 1$ (mód b). Esto prueba que los grupos de automorfismos que fijan a $\mathbb{Q}(\zeta_a)$ y $\mathbb{Q}(\zeta_b)$ tienen intersección trivial, luego $\mathbb{Q}(\zeta_a)\mathbb{Q}(\zeta_b) = \mathbb{Q}(\zeta_m)$.

También es evidente que $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b)$. Para tener la igualdad basta probar que $|\mathbb{Q}(\zeta_a) \cap \mathbb{Q}(\zeta_b) : \mathbb{Q}| = \phi(d)$, o también que el grupo de automorfismos asociado a esta intersección tiene orden $\phi(m)/\phi(d)$. Pero dicho grupo es el producto de los grupos $G(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_a))$ y $G(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_b))$ y, como tienen intersección trivial, el orden del producto es $(\phi(m)/\phi(a))(\phi(m)/\phi(b)) = \phi(m)/\phi(d)$.

Para probar b) observamos que K tiene un número finito de subcuerpos. Para cada uno de ellos tomamos (si existe) una extensión ciclotómica de $\mathbb{Q}$ que lo contenga. Multiplicando todas estas extensiones ciclotómicas obtenemos una extensión ciclotómica $\mathbb{Q}(\omega)$ (digamos de grado s) que contiene a todos los subcuerpos de K contenidos en alguna extensión ciclotómica de $\mathbb{Q}$. Si m es primo con s y ζ es una raíz m-sima primitiva de la unidad, entonces por a) tenemos $\mathbb{Q}(\omega) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$, y de aquí es claro que $K \cap \mathbb{Q}(\zeta) = \mathbb{Q}$.

A su vez esto implica que $G(K(\zeta)/K) \cong G(\mathbb{Q}(\zeta)/\mathbb{Q})$. Comparando grados se ve que el polinomio mínimo de ζ sobre K tiene sus coeficientes en $\mathbb{Q}$. Consideremos una extensión de Galois de k que contenga a K y sea σ uno de sus k-automorfismos. Como σ deja fijo al polinomio de ζ, es claro que $\sigma|_K$ admite una extensión a $K(\zeta)$ que deja fijo a ζ, luego su restricción a $K \cap k(\zeta)$ (que es también la restricción de σ) es la identidad. Esto prueba que $K \cap k(\zeta) = k$. ∎

Los próximos teoremas pertenecen a la aritmética elemental. Después los traduciremos a resultados sobre extensiones ciclotómicas. Cuando hablemos del orden de un entero a módulo otro entero m (en signos $\mathrm{o}_m(a)$) nos referiremos al orden de la clase de a en el grupo de unidades módulo m.

Teorema 7.34 *Sean a, $r > 1$ números naturales y q un número primo. Entonces existe un primo p tal que $\mathrm{o}_p(a) = q^r$.*

Demostración: Desarrollamos por la fórmula de Newton

$$a^{q^r} = (a^{q^{r-1}})^q = (a^{q^{r-1}} - 1 + 1)^q = \sum_{n=0}^{q} \binom{q}{n} (a^{q^{r-1}} - 1)^n.$$

De aquí se sigue obviamente que

$$T = \frac{a^{q^r} - 1}{a^{q^{r-1}} - 1} = \sum_{n=0}^{q-1} \binom{q}{n+1} (a^{q^{r-1}} - 1)^n. \tag{7.15}$$

Sea p un primo que divida a T. Es claro que si $p \nmid a^{q^{r-1}} - 1$ entonces p cumple lo pedido. Examinemos la otra posibilidad. Si $p \mid a^{q^{r-1}} - 1$ entonces p divide al sumando $n = 0$ de (7.15), o sea, $p \mid q$ y, por lo tanto, $p = q$. Se trata de probar que q no es el único primo que divide a T. Suponemos, pues, que $q \mid T$ (ya que en caso contrario hemos terminado).

Tenemos que $a \equiv 1 \pmod q$, luego $q \mid a^{q^{r-1}} - 1$. Si $q > 2$ entonces q^2 divide a todos los sumandos del miembro derecho de (7.15) menos al primero (que es igual a q). Esto implica que $q^2 \nmid T$, y por otra parte $T > q$, luego ha de existir otro primo $p \mid T$.

Si $q = 2$ queda $T = 2 + (a^{2^{r-1}} - 1)$, y de nuevo concluimos que T no es divisible entre 4 (pues $a^{2^{r-1}} \equiv 0, 1 \pmod 4$). ∎

Diremos que dos enteros son *independientes* módulo m si los subgrupos que generan en el grupo de unidades módulo m tienen intersección trivial.

Teorema 7.35 *Sea $n = q_1^{r_1} \cdots q_s^{r_s}$ la descomposición en primos de un número natural y sea $a > 1$ otro número natural. Entonces existe un número natural*

$$m = p_1 \cdots p_s p'_1 \cdots p'_s,$$

donde los primos p_i, p'_i son distintos entre sí, de modo que $n \mid \mathrm{o}_m(a)$, existe un número natural b tal que $n \mid \mathrm{o}_m(b)$ y a y b son independientes módulo m. Además los primos p_i, p'_i pueden elegirse arbitrariamente grandes.

Demostración: Ante todo notemos que, si en el lema anterior tomamos r suficientemente grande, podemos garantizar que p es arbitrariamente grande (pues $\mathrm{o}_p(a) \le p$).

Sean $p_1, \ldots, p_s$ primos distintos de modo que $\mathrm{o}_{p_i}(a) = q_i^{r_i^*}$, para cierto $r_i^* > r_i$ (cada r_i^* se elige suficientemente grande para que el correspondiente p_i sea mayor que los anteriores). Es claro que estos primos pueden ser elegidos arbitrariamente grandes.

Repetimos el proceso para obtener primos distintos $p'_1, \ldots, p'_s$ mayores aún que los anteriores y de modo que $\mathrm{o}_{p'_i}(a) = q_i^{r'_i}$, con $r'_i > r_i^*$.

Si u y v son enteros primos entre sí, entonces la aplicación $[a] \mapsto ([a], [a])$ es un isomorfismo entre el grupo de unidades módulo uv y el producto de los grupos de unidades módulo u y módulo v. En particular, si $\mathrm{o}_u(a)$ y $\mathrm{o}_v(a)$ son primos entre sí se cumple $\mathrm{o}_{uv}(a) = \mathrm{o}_u(a)\mathrm{o}_v(a)$. Teniendo esto en cuenta concluimos que $n \mid \mathrm{o}_m(a)$.

Por el teorema chino del resto existe un número natural b tal que

$$b \equiv a \pmod{p_1 \cdots p_s}, \qquad b \equiv 1 \pmod{p'_1 \cdots p'_s}.$$

Igual que antes tenemos que n divide al orden de a módulo $p_1 \cdots p_s$, que es el orden de b módulo m.

Sólo queda probar que a y b son independientes módulo m. Un elemento de la intersección de los grupos que generan sería de la forma $a^u \equiv b^v \pmod m$.

Entonces $a^u \equiv 1 \pmod{p'_1 \cdots p'_s}$ y, para cada i, tenemos $a^u \equiv 1 \pmod{p'_i}$. Por lo tanto $q_i^{r_i^*} \mid q_i^{r'_i} \mid u$, y así $a^u \equiv 1 \pmod{p_1 \cdots p_s}$.

Concluimos que $a^u \equiv 1 \pmod{m}$, luego la intersección es trivial. ∎

Veamos ahora la repercusión de estos hechos sobre las extensiones ciclotómicas. Observemos que si k es un cuerpo numérico y ζ una raíz de la unidad de orden m, entonces (por 3.13) el diferente de la extensión $k(\zeta)/k$ divide al ideal $(f'(\zeta))$, donde $f(x)$ es el polinomio mínimo de ζ sobre k y, como $f(x) \mid x^m - 1$, es claro que $(f'(\zeta)) \mid (m)$. La conclusión es que los primos ramificados de la extensión dividen a m, luego el homomorfismo de Artin de $k(\zeta)/k$ está definido sobre cualquier ideal primo con m. Equivalentemente, está definido sobre todo grupo $I(\mathfrak{m})$ con tal de que m contenga a los divisores primos de m. Lo mismo es válido para cualquier extensión K/k con $K \subset k(\zeta)$.

Diremos que dos automorfismos de un cuerpo son *independientes* si la intersección de los grupos cíclicos que generan es trivial.

Teorema 7.36 *Sea K/k una extensión abeliana de grado n de cuerpos numéricos. Sea S un conjunto finito de primos racionales. Sea $\mathfrak{p}$ un primo en k no ramificado en K. Entonces existe un número natural $m > 1$ que no es divisible entre ningún primo de S ni entre $\mathfrak{p}$ y de modo que si ζ es una raíz m-sima primitiva de la unidad se cumple:*

a) $K \cap k(\zeta) = k$.

b) El orden de $\left(\frac{k(\zeta)/k}{\mathfrak{p}}\right)$ es múltiplo de n.

c) Existe un k-automorfismo τ de K independiente de $\left(\frac{k(\zeta)/k}{\mathfrak{p}}\right)$ y cuyo orden es múltiplo de n.

Demostración: Aplicamos el teorema anterior tomando $a = \mathrm{N}\,\mathfrak{p}$ (la norma sobre $\mathbb{Q}$). Tomando suficientemente grandes los primos que dividen a m podemos garantizar que m no es divisible entre los primos de S ni entre $\mathfrak{p}$ y, por el teorema 7.33, que $K \cap \mathbb{Q}(\zeta) = \mathbb{Q}$, $K \cap k(\zeta) = k$.

Observar que $G(k(\zeta)/k) \cong G(\mathbb{Q}(\zeta)/\mathbb{Q})$, y a su vez este grupo es isomorfo al grupo de las unidades módulo m. Concretamente, un k-automorfismo de $k(\zeta)$ cumple $\sigma(\zeta) = \zeta^s$, para cierto s primo con m, y entonces el orden de σ es el orden de s módulo m.

Sea ahora

$$\sigma = \left(\frac{k(\zeta)/k}{\mathfrak{p}}\right).$$

Notemos que σ está bien definido por la observación previa al teorema. Por 4.4 se cumple que

$$\sigma|_{\mathbb{Q}(\zeta)} = \left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\mathrm{N}\mathfrak{p}}\right),$$

luego por 4.5 tenemos que $\sigma(\zeta) = \zeta^a$, lo que implica la propiedad b).

Para demostrar c) tomamos b según el teorema anterior (primo con m) y consideramos el k-automorfismo dado por $\tau(\zeta) = \zeta^b$ (que existe por el isomorfismo entre $G(k(\zeta)/k)$ y el grupo de unidades módulo m). Entonces n divide al orden de τ y (de nuevo por el isomorfismo) del hecho de que a y b sean independientes módulo m se sigue que σ y τ lo son también. ∎

Teorema 7.37 *Sea K/k una extensión cíclica de grado n de cuerpos numéricos, sea S un conjunto finito de primos racionales y sea $\mathfrak{p}$ un ideal primo de k no ramificado en K. Entonces existe un número natural m no divisible entre ninguno de los primos de S ni entre $\mathfrak{p}$ y un cuerpo numérico E que contiene a k, de modo que si ζ es una raíz m-sima primitiva de la unidad se cumple:*

a) $K \cap E = k$.

b) $K(\zeta) = E(\zeta), \qquad K \cap k(\zeta) = k$.

c) El primo $\mathfrak{p}$ se escinde completamente en E.

Demostración: Tomamos el número m dado por el teorema anterior. En particular tenemos que $K \cap k(\zeta) = k$ y que $\mathfrak{p}$ es no ramificado en $k(\zeta)$, luego también en $K(\zeta)$. Claramente

$$G(K(\zeta)/k) \cong G(K/k) \times G(k(\zeta)/k).$$

(El isomorfismo asigna a cada automorfismo sus restricciones a K y a $k(\zeta)$).

Sea σ un generador de $G(K/k)$ y sea $\tau \in G(k(\zeta)/k)$ según el teorema anterior. Sea H el subgrupo de $G(K(\zeta)/k)$ generado por (σ, τ) y por

$$\left(\frac{K(\zeta)/k}{\mathfrak{p}}\right) = \left(\left(\frac{K/k}{\mathfrak{p}}\right), \left(\frac{k(\zeta)/k}{\mathfrak{p}}\right)\right).$$

Entonces, por la propia definición del símbolo de Artin, H contiene al grupo de descomposición de $\mathfrak{p}$ en $K(\zeta)$. Sea E el cuerpo fijado por H. Según el teorema 1.38 el primo $\mathfrak{p}$ tiene grado de inercia 1 sobre su cuerpo de descomposición, luego también sobre E, que es un subcuerpo. Esto significa que $\mathfrak{p}$ se escinde completamente en E.

Ahora, como los grupos de Galois son todos abelianos, un elemento cualquiera de H es de la forma

$$(\sigma, \tau)^u \left(\left(\frac{K/k}{\mathfrak{p}}\right), \left(\frac{k(\zeta)/k}{\mathfrak{p}}\right)\right)^v,$$

para ciertos números naturales u y v.

Si la segunda componente es 1, como τ y $\left(\frac{k(\zeta)/k}{\mathfrak{p}}\right)$ son independientes, ha de ser

$$\tau^u = 1 \qquad \text{y} \qquad \left(\frac{k(\zeta)/k}{\mathfrak{p}}\right)^v = 1,$$

luego $n \mid u$ y $n \mid v$, luego la primera componente también es 1.

Esto prueba que $H \cap (G(K/k) \times 1) = 1$, luego, por el teorema de Galois, se ha de cumplir $E(\zeta) = Ek(\zeta) = K(\zeta)$.

Por otra parte todo automorfismo de $G(K(\zeta)/k)$ se puede expresar como una potencia de (σ, τ) por un elemento de $1 \times G(k(\zeta)/k)$, luego

$$G(K(\zeta)/k) = H(1 \times G(k(\zeta)/k)),$$

y, considerando los cuerpos fijados, esto equivale a que $k = E \cap K$. ∎

Ahora aplicamos varias veces el teorema anterior para trabajar simultáneamente con varios ideales primos.

Teorema 7.38 *Sea K/k una extensión cíclica de cuerpos numéricos y $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ideales primos de k no ramificados en K. Entonces existen números naturales $m_1, \dots, m_r$ primos entre sí dos a dos y primos con $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ y existen extensiones finitas $E_1, \dots, E_r$ tales que si ζ_i es una raíz de la unidad de orden m_i se cumple:*

a) $K \cap E_i = k, \qquad K(\zeta_i) = E_i(\zeta_i)$.

b) $\mathfrak{p}_i$ *se escinde completamente en* E_i.

c) Si $E = E_1 \cdots E_r$ *entonces* $K \cap E = k$.

Demostración: Aplicamos r veces el teorema anterior de modo que cada m_{i+1} se escoge divisible entre primos suficientemente grandes como para que según el teorema 7.33 se cumpla

$$K(\zeta_1, \dots, \zeta_i) \cap k(\zeta_{i+1}) = k, \qquad k \cap \mathbb{Q}(\zeta_{i+1}) = \mathbb{Q}.$$

Sólo falta probar la parte c). Las condiciones anteriores garantizan que

$$G\big(K(\zeta_1, \dots, \zeta_i, \zeta_{i+1})/k\big) \cong G\big(K(\zeta_1, \dots, \zeta_i)/k\big) \times G\big(k(\zeta_{i+1})/k\big).$$

En total (y teniendo en cuenta la prueba del teorema anterior para el primer paso) concluimos que

$$G\big(K(\zeta_1, \dots, \zeta_r)/k\big) \cong G\big(K/k\big) \times G\big(k(\zeta_1)/k\big) \times \cdots \times G\big(k(\zeta_r)/k\big).$$

Por supuesto, la imagen de un automorfismo de la extensión por este isomorfismo de grupos está formada por sus restricciones a las extensiones correspondientes.

Sea σ un generador de $G(K/k)$ y τ_i el automorfismo de $k(\zeta_i)/k$ considerado en el teorema anterior. Vimos allí que (σ, τ_i) es un automorfismo de $K(\zeta_i)/k$ que fija a E_i, luego $(\sigma, \tau_1, \dots, \tau_r)$ es un automorfismo de $K(\zeta_1, \dots, \zeta_r)/k$ que fija a todos los cuerpos E_i, luego a E. Por otra parte $(1, \tau_1, \dots, \tau_r)$ fija a K, luego $(\sigma, 1, \dots, 1)$ fija a $K \cap E$.

En otras palabras, $K \cap E$ es fijado por todo el grupo $G(K/k)$ y, por lo tanto, $K \cap E = k$. ∎

Con esto estamos en condiciones de determinar el núcleo del homomorfismo de Artin.

Teorema 7.39 *Sea k un cuerpo numérico, m un número natural, ζ una raíz de la unidad de orden m y K un subcuerpo de $k(\zeta)$. Entonces existe un divisor $\mathfrak{m}$ de k divisible sólo entre los primos de k que dividen a m y los primos arquimedianos y tal que el núcleo del homomorfismo de Artin de K/k restringido a $I(\mathfrak{m})$ es $P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$. Cualquier otro divisor múltiplo de $\mathfrak{m}$ tiene la misma propiedad.*

DEMOSTRACIÓN: Veamos primero que existe un divisor $\mathfrak{m}$ en las condiciones indicadas tal que $P_{\mathfrak{m}}$ está contenido en el homomorfismo de Artin (es obvio que cualquier múltiplo tendrá la misma propiedad). Basta probarlo en el caso en que $K = k(\zeta)$, pues el divisor $\mathfrak{m}$ que sirve en este caso sirve también para cualquier subcuerpo K (porque un símbolo de Artin para K es la restricción del mismo símbolo para $k(\zeta)$).

Por la continuidad de las normas locales $\mathrm{N}_{\mathfrak{p}} : k_{\mathfrak{p}} \longrightarrow \mathbb{Q}_p$, la relación (2.1) y la continuidad del producto en $\mathbb{Q}_p$, dado $\epsilon > 0$ existe un $\delta > 0$ tal que para todo primo $p \mid m$, si $\alpha \in k^*$ y $|\alpha - 1|_{\mathfrak{p}} < \delta$ para todo primo $\mathfrak{p} \mid p$ en k, entonces $|\,\mathrm{N}(\alpha) - 1|_p < \epsilon$.

Esto implica que existe un divisor $\mathfrak{m}$ de k (divisible sólo entre los primos que dividen a m) tal que si $\alpha \in k^*$ y $\alpha \equiv^* 1$ (mód $\mathfrak{m}$) entonces $\mathrm{N}(\alpha) \equiv^* 1$ (mód m).

Si exigimos además que $\infty \mid m$ entonces los conjugados reales de α son positivos, luego $\mathrm{N}(\alpha) > 0$, es decir, $\mathrm{N}(\alpha) \equiv^* 1$ (mód $m\,\infty$).

Por lo tanto $\mathrm{N}[P_{\mathfrak{m}}] \subset P_{m\,\infty}$ y así si $(\alpha) \in P_{\mathfrak{m}}$ se cumple que

$$\left(\frac{K/k}{\alpha}\right)\Bigg|_{\mathbb{Q}(\zeta)} = \left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\mathrm{N}(\alpha)}\right) = 1,$$

ya que, según vimos en el capítulo V, el núcleo del homomorfismo de Artin para la extensión ciclotómica de orden m sobre $\mathbb{Q}$ es precisamente $P_{m\,\infty}$.

Como el comportamiento de un automorfismo de K/k está determinado por su acción sobre ζ, concluimos que

$$\left(\frac{K/k}{\alpha}\right) = 1,$$

como queríamos probar.

Podemos exigir que $\mathfrak{m}$ sea admisible para K/k, y entonces los argumentos que hemos empleado al principio de la sección prueban que el núcleo del homomorfismo de Artin es $P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$. ∎

Teorema 7.40 *Sea K/k una extensión cíclica de cuerpos numéricos. Entonces, para todo divisor admisible $\mathfrak{m}$, el núcleo del homomorfismo de Artin restringido a $I(\mathfrak{m})$ es igual a $P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$.*

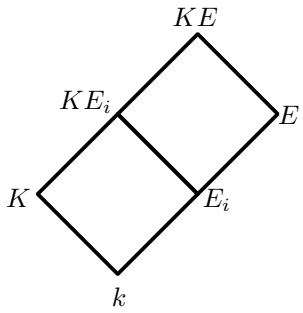
DEMOSTRACIÓN: Basta demostrar que, para todo divisor admisible $\mathfrak{m}$, el núcleo del homomorfismo de Artin está contenido en $P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$, y aplicar después la primera desigualdad fundamental, que tenemos probada para extensiones cíclicas. Sea, pues, $\alpha \in I(\mathfrak{m})$ tal que

$$\left(\frac{K/k}{\mathfrak{a}}\right) = 1. \tag{7.16}$$

Descompongamos

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{u_i},$$

donde los exponentes son números enteros no nulos y los primos $\mathfrak{p}_i$ son no ramificados. Sea $E = E_1 \cdots E_r$ según el teorema 7.38. Para cada índice i, la situación es



Además $KE_i \subset K(\zeta_i)E_i(\zeta_i) = E_i(\zeta_i)$, es decir, KE_i está contenido en una extensión ciclotómica de E_i, por lo que el teorema anterior se aplica a la extensión KE_i/E_i. Esto es lo que hemos de aprovechar.

Puesto que $K \cap E = k$, se cumple $G(KE/E) \cong G(K/k) \cong G(KE_i/E_i)$. El isomorfismo es la restricción, de modo que si σ es un generador de $G(KE/E)$, podemos considerarlo también como generador de las demás extensiones (identificándolo con sus restricciones). Sea m el producto de todos los m_i dados por el teorema 7.38. Por el teorema 7.16 existe un ideal fraccional $\mathfrak{b}_E \in I_E(\mathfrak{m}m)$ tal que

$$\left(\frac{KE/E}{\mathfrak{b}_E}\right) = \sigma.$$

Llamando $\mathfrak{b}_k = \mathrm{N}_k^E(\mathfrak{b}_E)$, las propiedades del símbolo de Artin implican que

$$\left(\frac{K/k}{\mathfrak{b}_k}\right) = \sigma.$$

Así pues, el símbolo de Artin de $\mathfrak{b}_k$ es un generador de $G(K/k)$, y podemos escribir

$$\left(\frac{K/k}{\mathfrak{p}_i^{u_i}}\right) = \left(\frac{K/k}{\mathfrak{b}_k}\right)^{d_i}, \tag{7.17}$$

para ciertos números naturales d_i. Vemos, pues, que $\mathfrak{p}_i^{u_i}\mathfrak{b}_k^{-d_i}$ está en el núcleo del homomorfismo de Artin de K/k.

Ahora observamos que $\mathfrak{p}_i^{u_i}\mathfrak{b}_k^{-d_i}$ es una norma de la extensión E_i/k. En efecto, $\mathfrak{p}_i$ es la norma de cualquiera de sus divisores en E_i, pues se escinde completamente, y $\mathfrak{b}_k$ es la norma de la norma de $\mathfrak{b}_E$ en E_i. Digamos que $\mathfrak{p}_i^{u_i}\mathfrak{b}_k^{-d_i} = \mathrm{N}_k^{E_i}(\mathfrak{c}_i)$, donde $\mathfrak{c}_i$ ha de ser primo con $\mathfrak{m}$ y con m. Entonces

$$\left(\frac{KE_i/E_i}{\mathfrak{c}_i}\right) = \left(\frac{K/k}{\mathrm{N}(\mathfrak{c}_i)}\right) = 1.$$

De este modo, $\mathfrak{c}_i$ está en el núcleo del homomorfismo de Artin de KE_i/E_i y, según hemos comentado, podemos aplicar el teorema anterior para concluir que $\mathfrak{c}_i \in P_\mathfrak{n}\,\mathrm{N}(\mathfrak{n})$, donde $\mathfrak{n}$ es un divisor que podemos tomar divisible entre todos los primos que dividen a $\mathfrak{m}$ y los primos arquimedianos. Así pues, tenemos que $\mathfrak{c}_i = (\beta_i)\,\mathrm{N}_{E_i}^{KE_i}(\mathfrak{d}_i)$, donde $\mathfrak{d}_i \in I(\mathfrak{m}m)$, y $\beta_i \equiv^* 1$ (mód $\mathfrak{b}$).

Podemos exigir que los primos que dividen a $\mathfrak{m}$ dividan a $\mathfrak{n}$ con exponentes arbitrariamente grandes. Usando la continuidad de las normas locales como en el teorema anterior, podemos garantizar que la condición $\beta_i \equiv^* 1$ (mód $\mathfrak{n}$) implique a su vez que $\mathrm{N}_k^{E_i}(\beta_i) \equiv^* 1$ (mód $\mathfrak{m}$). Tomando normas queda

$$\mathfrak{p}_i^{u_i}\mathfrak{b}_k^{-d_i} = \mathrm{N}_k^{E_i}(\beta_i)\,\mathrm{N}_k^K(\mathrm{N}_K^{KE_i}(\mathfrak{d}_i)) \in P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}). \tag{7.18}$$

Vamos a multiplicar para todo i, pero antes observamos que multiplicando en (7.17) y teniendo en cuenta (7.16) (así como que el símbolo de Artin de $\mathfrak{b}_k$ tiene orden $n = |K : k|$) resulta que $\sum_{i=1}^{r} d_i = nd$, para un cierto natural d.

Ahora multiplicamos ya en (7.18) y obtenemos que $\mathfrak{a}\mathfrak{b}_k^{-dn} \in P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$, pero $\mathfrak{b}_k^{-dn} = \mathrm{N}_k^K(\mathfrak{b}_k^{-d}) \in \mathrm{N}(\mathfrak{m})$, luego $\mathfrak{a} \in P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$. ∎

Ahora ya es fácil probar el caso general: si K/k es una extensión abeliana de cuerpos numéricos, podemos expresar $K = K_1 \cdots K_r$ como producto de extensiones cíclicas de k. Los primos de k ramificados en un K_i son ramificados en K, luego podemos tomar un divisor $\mathfrak{m}$ admisible para K/k que sea divisible sólo entre primos ramificados en K y que a la vez sea admisible para todas las extensiones K_i/k. Por el teorema anterior $P_\mathfrak{m}$ está contenido en el núcleo del homomorfismo de Artin de cada K_i. Ahora bien, si $\mathfrak{a} \in P_\mathfrak{m}$, entonces el símbolo de Artin de $\mathfrak{a}$ para K/k es la identidad restringido a cada K_i, luego es la identidad en K. Esto prueba que $P_\mathfrak{m}$ está contenido en el núcleo del homomorfismo de Artin de K/k y, según hemos visto al principio de la sección, esto prueba el teorema 7.32.

En particular tenemos que la primera desigualdad fundamental es válida para todas las extensiones abelianas, y es, de hecho, una igualdad. De todos modos esto carece interés teniendo el teorema 7.32.

Capítulo VIII

Cuerpos de clases

Finalmente podemos plantear y demostrar los resultados básicos de la teoría de cuerpos de clases. Por supuesto que ya tenemos uno de ellos: el isomorfismo de Artin. Para enunciar los restantes conviene trasladarlo a clases de elementos ideales, de lo cual nos ocupamos en la primera sección.

8.1 El isomorfismo de Artin sobre clases de elementos ideales

Si K/k es una extensión abeliana de cuerpos numéricos y $\mathfrak{m}$ es un ideal admisible, podemos considerar el isomorfismo dado por 6.21 y componerlo con el isomorfismo de Artin:

$$J_k/k^* \,\mathrm{N}[J_K] \cong I(\mathfrak{m})/P_{\mathfrak{m}} \,\mathrm{N}(\mathfrak{m}) \cong G(K/k).$$

Si componemos con la proyección de J_k en el cociente obtenemos un homomorfismo en el grupo de elementos ideales:

Definición 8.1 Sea K/k una extensión abeliana de cuerpos numéricos. Llamaremos *homomorfismo de Artin* de la K/k al homomorfismo $\omega : J_k \longrightarrow G(K/k)$ determinado por la composición de la proyección $J_k \longrightarrow J_k/k^* \,\mathrm{N}[J_K]$ con los isomorfismos anteriores.

La definición de ω no depende de la elección de $\mathfrak{m}$: dado un elemento ideal α elegimos un elemento $\beta \in k^*$ tal que $\alpha\beta \in J_{\mathfrak{m}}$, y entonces, por definición,

$$\omega(\alpha) = \omega(\alpha\beta) = \left(\frac{K/k}{(\alpha\beta)}\right).$$

Ahora bien, si $\mathfrak{f}$ es el conductor de la extensión, también se cumple $\alpha\beta \in J_{\mathfrak{f}}$, luego el automorfismo que hemos obtenido con $\mathfrak{m}$ es el mismo que se obtiene con $\mathfrak{f}$.

Si $\alpha \in J_k$ escribiremos también

$$\omega(\alpha) = \left(\frac{K/k}{\alpha}\right) \in G(K/k),$$

y a este automorfismo lo llamaremos *símbolo de Artin* del elemento ideal α.

Obviamente ω es un epimorfismo de grupos cuyo núcleo es exactamente $k^* \,\mathrm{N}[J_K]$, e induce un epimorfismo en C_k cuyo núcleo es el grupo de normas $\mathrm{N}[C_K]$. Los isomorfismos $C_k/\,\mathrm{N}[C_K] \cong J_k/k^*\,\mathrm{N}[J_K] \cong G(K/k)$ inducidos por ω en los grupos de clases se llaman también *isomorfismos de Artin*.

El homomorfismo de Artin sobre elementos ideales extiende al homomorfismo sobre ideales en el sentido de que si $\mathfrak{a}$ es un ideal fraccional no divisible entre primos ramificados y α es un elemento ideal tal que $(\alpha) = \mathfrak{a}$, entonces el símbolo de Artin de α coincide con el símbolo de Artin de $\mathfrak{a}$. Sin embargo, ahora tenemos definido el símbolo de Artin sobre cualquier elemento ideal aunque su ideal fraccional asociado sea divisible entre primos ramificados. Más adelante interpretaremos debidamente esta extensión.

El teorema siguiente recoge las propiedades principales del símbolo de Artin sobre elementos ideales. Son todas consecuencias inmediatas de 4.4 (basta sustituir los elementos ideales por ideales fraccionales no divisibles entre primos no ramificados en ninguna de las extensiones involucradas).

Teorema 8.2 *Se cumple*

a) Si $k \subset L \subset K$ es una cadena de cuerpos numéricos de manera que la extensión K/k es abeliana y $\alpha \in J_k$ entonces

$$\left(\frac{K/k}{\alpha}\right)\Big|_L = \left(\frac{L/k}{\alpha}\right).$$

b) En la situación anterior, si $\alpha \in J_L$ entonces

$$\left(\frac{K/L}{\alpha}\right) = \left(\frac{K/k}{\mathrm{N}(\alpha)}\right).$$

c) Si K/k es una extensión abeliana de cuerpos numéricos y L/k es una extensión finita, entonces KL/L es abeliana y si $\alpha \in J_L$ entonces

$$\left(\frac{KL/L}{\alpha}\right)\Big|_K = \left(\frac{K/k}{\mathrm{N}(\alpha)}\right).$$

Ahora introducimos el concepto central de la teoría de cuerpos de clases:

Definición 8.3 Sea k un cuerpo numérico. Para cada extensión abeliana K/k, llamaremos *grupo de clases* de K al grupo $H = k^*\,\mathrm{N}[J_K]$ (o bien al grupo $H = N[C_K]$). Equivalentemente, diremos que K es el *cuerpo de clases* de H. Abreviaremos esta relación escribiendo $H \leftrightarrow K$ o bien $K \leftrightarrow H$.

De este modo, si K es el cuerpo de clases de H, el grupo de Galois $G(K/k)$ es isomorfo al grupo J_k/H a través del isomorfismo de Artin. Notar que sería más adecuado llamar "grupo de clases" de K al grupo cociente J_k/H, pero es más cómodo trabajar con el subgrupo H, y por otra parte H y J_k/H se determinan mutuamente.

Puesto que los grupos de normas $N[J_k]$ son abiertos, tenemos que el grupo de clases H de un cuerpo K es un subgrupo abierto de J_k que contiene a k^*, o bien un subgrupo abierto de C_k. Observar que la aplicación $H \mapsto HK^*/k^*$ biyecta los subgrupos abiertos de J_k que contienen a k^* con los subgrupos abiertos de C_k, luego es indistinto trabajar con unos o con otros.

El teorema siguiente prueba entre otras cosas que a extensiones distintas corresponden grupos de clases distintos.

Teorema 8.4 *Sea k un cuerpo numérico. La correspondencia $K \mapsto k^*\,\mathrm{N}[J_K]$ (o equivalentemente $K \mapsto \mathrm{N}[C_K]$) es una aplicación inyectiva entre el conjunto de extensiones abelianas (finitas) de k y el conjunto de subgrupos abiertos de J_k que contienen a k^* (respectivamente, el conjunto de los subgrupos abiertos de C_k). Además si $K \leftrightarrow H$ y $K' \leftrightarrow H'$ se cumple:*

a) $K \subset K'$ si y sólo si $H' \le H$.

b) $KK' \leftrightarrow H \cap H'$ y $K \cap K' \leftrightarrow HH'$.

Demostración: Basta demostrar a) y b), pues la propiedad a) ya implica la inyectividad de la correspondencia. Probamos primero b). Es claro que el núcleo del homomorfismo de Artin $C_k \longrightarrow G(KK'/k)$ es $H \cap H'$ (por 8.2 a), luego $KK' \leftrightarrow H \cap H'$.

Por otra parte el núcleo del homomorfismo de Artin $C_k \longrightarrow G\big((K \cap K')/k\big)$ contiene claramente a HH', luego basta probar que $|C_k : HH'| = |(K \cap K') : k|$ y tendremos la igualdad. El razonamiento es elemental:

$$|C_k : HH'| = \frac{|C_k : H|}{|HH' : H|} = \frac{|K : k|}{|H' : H \cap H'|} = \frac{|K : k|\,|C_k : H'|}{|C_k : H \cap H'|} = \frac{|K : k|\,|K' : k|}{|KK' : k|}$$

$$= \frac{|K : k|}{|KK' : K'|} = \frac{|K : k|}{|K : K \cap K'|} = |K \cap K' : k|.$$

Veamos a). Si $K \subset K'$ la transitividad de las normas implica claramente que $H' \le H$. Recíprocamente, si $H' \le H$ entonces $H \cap H' = H'$, luego $|C_k : H'| = |K' : k| = |KK' : k|$, de donde $K' = KK'$ y en consecuencia $K \subset K'$. ∎

8.2 El teorema de existencia

El teorema de existencia es otro de los resultados centrales de la teoría de cuerpos de clases. Afirma que todo subgrupo abierto de J_k que contenga a k^* (equivalentemente, todo subgrupo abierto de C_k es un grupo de clases

para alguna extensión abeliana del cuerpo numérico k. Consecuentemente, las extensiones abelianas de k se corresponden biunívocamente con los subgrupos abiertos de C_k.

Los razonamientos que empleamos en la prueba de la segunda desigualdad fundamental contienen un caso particular sobre existencia de cuerpos de clases:

Teorema 8.5 *Sea k un cuerpo numérico que contenga a las raíces n-simas de la unidad. Sea E un conjunto finito de primos de k que contenga todos los primos arquimedianos, todos los divisores de n y tal que $J_k = k^* J_E$. Sea $E = E_1 \cup E_2$ una partición de E en dos subconjuntos disjuntos (uno de los cuales puede ser vacío). Sea D_i el subgrupo abierto de J_k dado por* (7.11)*, para $i = 1, 2$ y sea K_i la extensión de Kummer de k asociada a $\Delta_i = D_i \cap k^*$. Entonces $k^* D_i \leftrightarrow K_j$ (donde $j = 3 - i$).*

Demostración: Basta aplicar el teorema 7.30, que por una parte nos da las inclusiones

$$k^* D_i \leq k^* \,\mathrm{N}[J_{K_j}], \tag{8.1}$$

de donde se sigue que

$$|J_k : k^* D_i| \geq |J_k : k^* \,\mathrm{N}[J_{K_j}]| = |K_j : k|,$$

y por otra parte nos da la igualdad

$$|J_k : k^* D_1|\,|J_k : k^* D_2| = |K_1 : k|\,|K_2 : k|,$$

que obliga a que las desigualdades anteriores sean igualdades, es decir,

$$|J_k : k^* D_i| = |J_k : k^* \,\mathrm{N}[J_{K_j}]|.$$

Por lo tanto, las inclusiones (8.1) son también igualdades, y esto prueba el teorema. ∎

Ahora veremos que el caso general del teorema de existencia se reduce fácilmente al teorema anterior. En primer lugar notamos un hecho general que sería pura rutina detallar en cada caso: todos los conceptos que estamos manejando (elementos ideales, cuerpos de clases, etc) están definidos a partir de la estructura algebraica de un cuerpo K o de una extensión K/k (incluso las compleciones y sus topologías están definidas únicamente a partir de esta estructura algebraica). Por lo tanto un isomorfismo de cuerpos $\sigma : K \longrightarrow L$ conserva todas las propiedades de forma natural. Por ejemplo, es claro que si K/k una extensión abeliana de cuerpos numéricos y $\sigma : K \longrightarrow \sigma[K]$ es un isomorfismo (no necesariamente trivial sobre k) entonces para todo elemento ideal $\alpha \in J_k$ se cumple

$$\left(\frac{\sigma[K]/\sigma[k]}{\sigma(\alpha)}\right) = \sigma^{-1}\left(\frac{K/k}{\alpha}\right)\sigma.$$

La clave de la reducción a extensiones de Kummer está en los dos teoremas siguientes. El primero es elemental.

Teorema 8.6 *Sea k un cuerpo numérico y sea H un subgrupo abierto de C_k que tenga cuerpo de clases K. Si $H \leq H' \leq C_k$ entonces H' tiene cuerpo de clases, y éste es concretamente el cuerpo fijado por*

$$\left(\frac{K/k}{H}\right) \leq G(K/k).$$

DEMOSTRACIÓN: Sea K' dicho cuerpo fijado. Es inmediato que H' es el núcleo del homomorfismo de Artin $C_k \longrightarrow G(K'/k)$. ∎

Teorema 8.7 *Sea F/k una extensión cíclica de cuerpos numéricos. Sea H un subgrupo abierto de J_k que contenga a k^*. Sea $H_F = \mathrm{N}_{F/k}^{-1}[H]$. Si H_F tiene un cuerpo de clases (sobre F) entonces H tiene un cuerpo de clases (sobre k).*

DEMOSTRACIÓN: Observar que H_F es un subgrupo abierto de J_F, pues la norma es continua También es claro que contiene a F^*.

Sea K el cuerpo de clases de H_F. Vamos a probar que la extensión K/k es abeliana. Sea K' la menor extensión de Galois de k que contenga a K. La situación es, pues,

$$k \quad \subset \quad F \quad \subset \quad K \quad \subset \quad K'.$$

Sea $\sigma \in G(K'/k)$. Como F/k es normal, $\sigma[F] = F$, y claramente $\sigma[H_F] = H_F$ (pues σ conserva las normas). Ahora bien, K es el cuerpo de clases de H_F, luego $\sigma[K]$ es el cuerpo de clases de $\sigma[H_F] = H_F$, luego $\sigma[K] = K$. Es claro que esto implica que la extensión K/k es de Galois (y por construcción $K = K'$). Sea ahora σ el automorfismo de K cuya restricción a F genera $G(F/k)$. Todo automorfismo de K/k se expresa como $\sigma^i\tau$, con $\tau \in G(K/F)$. Como la extensión K/F es abeliana, para que K/k también lo sea basta con que todo $\tau \in G(K/F)$ conmute con σ.

Sea $\alpha \in J_F$ tal que $\tau = \left(\frac{K/F}{\alpha}\right)$. Entonces, según hemos observado,

$$\sigma^{-1}\tau\sigma = \left(\frac{K/F}{\sigma(\alpha)}\right),$$

pero $\mathrm{N}_{F/k}(\sigma(\alpha)/\alpha) = 1$, luego $\sigma(\alpha)/\alpha \in H_F$ y consecuentemente

$$\sigma^{-1}\tau\sigma = \left(\frac{K/F}{\sigma(\alpha)}\right) = \left(\frac{K/F}{\alpha}\right) = \tau,$$

como queríamos probar.

Así tenemos que K/k es abeliana y $k^*\,\mathrm{N}[J_K] \leq H$ (pues una norma para K/k es una norma para K/F —que está en H_F porque K es su cuerpo de clases— seguida de una norma para F/k —que está en H por definición de H_F). Como $k^*\,\mathrm{N}[J_K]$ es el grupo de clases de K, el teorema 8.6 nos da que H tiene también cuerpo de clases. ∎

Ahora veamos cómo se aplica esto a la demostración del teorema de existencia. Recordemos que un grupo abeliano tiene exponente n si todos sus elementos

tienen orden divisor de n. En las condiciones del teorema anterior observamos que si el grupo J_k/H tiene exponente n entonces J_F/H_F también tiene exponente n (pues si $\alpha \in J_F$ entonces $\mathrm{N}(\alpha^n) = \mathrm{N}(\alpha)^n \in H$, luego $\alpha^n \in H_F$).

Si tenemos un cuerpo numérico k y un subgrupo abierto H de J_k que contenga a k^*, en primer lugar notamos que J_k/H es finito, pues por 6.12 tenemos que $k^*W_{\mathfrak{m}} \leq H$ para cierto divisor $\mathfrak{m}$ y entonces

$$|J_k : H| \leq |J_k : k^*W_{\mathfrak{m}}| = |I(\mathfrak{m}) : P_{\mathfrak{m}}|.$$

Sea n un exponente de J_k/H, sea ζ una raíz n-sima primitiva de la unidad y consideremos $F = k(\zeta)$. La extensión F/k es abeliana, luego podemos construir una sucesión de extensiones $k = F_0 \subset F_1 \subset \cdots \subset F_r = F$ donde cada extensión F_{i+1}/F_i sea cíclica. Aplicando el teorema anterior varias veces, la existencia de un cuerpo de clases para H se reduce a la existencia de un cuerpo de clases para un cierto subgrupo H' de J_F, que tendrá también exponente n, con la diferencia de que ahora el cuerpo F contiene una raíz n-sima primitiva de la unidad. En definitiva, ahora buscamos una extensión de Kummer de F.

Teorema 8.8 (Teorema de existencia) *Sea k un cuerpo numérico. Entonces todo subgrupo abierto de J_k que contiene a k^* (equivalentemente, todo subgrupo abierto de C_k) tiene un cuerpo de clases.*

Demostración: Sea H un subgrupo abierto de J_k que contenga a k^*. Según acabamos de ver podemos suponer que J/H tiene exponente n y que k contiene las raíces n-simas de la unidad.

Como H es abierto ha de contener a un grupo $W_{\mathfrak{m}}$ para cierto divisor $\mathfrak{m}$. Sea E un conjunto finito de primos de k que contenga a todos los primos arquimedianos, a los divisores de n, a los divisores de $\mathfrak{m}$ y de modo que $J_k = k^*J_E$. Consideramos los grupos (7.11) correspondientes a la partición $E_1 = \varnothing$, $E_2 = E$. Concretamente

$$D_1 = \prod_{\mathfrak{p}\in E} k_{\mathfrak{p}}^{*n} \times \prod_{\mathfrak{p}\in P\setminus E} U_{\mathfrak{p}},$$

mientras que $D_2 = J_E$.

Cada $\alpha \in D_1$ se descompone como $\alpha = \beta^n\gamma$, según (7.12), y así vemos que $\beta^n \in H$ porque J_k/H tiene exponente n y $\gamma \in W_{\mathfrak{m}} \leq H$. En definitiva, $D_1 \leq H$. El teorema 8.5 nos da que k^*D_1 tiene cuerpo de clases y el teorema 8.6 implica que H también lo tiene. ∎

Aunque ya está todo demostrado, enunciamos seguidamente el teorema fundamental, incluyendo el teorema de existencia:

Teorema 8.9 (Tª fundamental de la teoría de cuerpos de clases) *Sea k un cuerpo numérico. La relación $K \leftrightarrow H$, determinada por $H = k^*\,\mathrm{N}[J_K]$, (respectivamente, $H = \mathrm{N}[C_K]$) es una biyección entre el conjunto de extensiones abelianas (finitas) de k y el conjunto de subgrupos abiertos de J_k que contienen a k^* (respectivamente, el conjunto de los subgrupos abiertos de C_k).*

Si $K \leftrightarrow H$, el símbolo de Artin induce un isomorfismo $J_k/H \cong G(K/k)$.

Es interesante observar que el teorema de existencia cuando el cuerpo base es $\mathbb{Q}$ se prueba fácilmente sin necesidad de los argumentos sofisticados del caso general. En efecto, en el capítulo V obtuvimos el isomorfismo

$$\omega : I(m\,\infty)/P_{m\,\infty} \longrightarrow G(K/\mathbb{Q}),$$

donde K es el cuerpo ciclotómico de orden m. Componiendo con el isomorfismo dado por (6.2) obtenemos un isomorfismo

$$J_{\mathbb{Q}}/\mathbb{Q}^* W_{m\,\infty} \cong G(K/\mathbb{Q}). \tag{8.2}$$

No podemos decir que sea por definición el isomorfismo de Artin, pues no sabemos si el divisor $m\,\infty$ es admisible. Ahora bien, dado $\alpha \in J_{\mathbb{Q}}$, su imagen por (8.2) se calcula tomando un $\beta \in \mathbb{Q}^*$ tal que $\alpha\beta \in J_{m\infty}$ y después aplicando ω sobre el ideal $(\alpha\beta) \in I(m\,\infty)$. Sabemos que el resultado es independiente de β. En particular, podemos tomar β de modo que $\alpha\beta \in J_{\mathfrak{m}}$, donde $\mathfrak{m}$ es un divisor admisible divisible entre $m\,\infty$. Entonces el resultado es por una parte el símbolo de Artin de α y por otro es el mismo que da (8.2).

Concluimos, pues, que (8.2) es ciertamente el isomorfismo de Artin de K, con lo que hemos probado el teorema siguiente:

Teorema 8.10 *Si K es la extensión ciclotómica de orden m de $\mathbb{Q}$, entonces*

$$K \leftrightarrow \mathbb{Q}^* W_{m\,\infty}.$$

Es importante destacar que con esto seguimos sin saber si $m\infty$ es o no admisible para la extensión. Más adelante será evidente que sí lo es.

Una vez sabemos que los grupos $W_{m\,\infty}$ tienen cuerpo de clases, el teorema 8.6 prueba que todo subgrupo abierto H de $J_{\mathbb{Q}}$ que contenga a $\mathbb{Q}^*$ tiene cuerpo de clases, pues ciertamente H contendrá un subgrupo de la forma $W_{m\,\infty}$.

Pese a ser más fácil de probar que el caso general, el teorema de existencia para $\mathbb{Q}$ no es trivial en absoluto, sino que de él se deduce que la conjetura de Kronecker que comentábamos en el capítulo IV es correcta:

Teorema 8.11 *Toda extensión abeliana de $\mathbb{Q}$ está contenida en un cuerpo ciclotómico.*

Demostración: Sea K una extensión abeliana de $\mathbb{Q}$, sea H su grupo de clases. Según acabamos de ver, existe un natural m tal que $\mathbb{Q}^* W_{m\,\infty} \leq H$, luego K está contenido en el cuerpo de clases de $\mathbb{Q}^* W_{m\,\infty}$, que es un cuerpo ciclotómico. ∎

8.3 Conexión con la teoría local

La práctica totalidad de los conceptos que hemos introducido en los capítulos anteriores tienen una versión global y otra local. Resulta innecesario a estas

alturas explicar la utilidad de los métodos locales a la hora de obtener resultados globales. Normalmente hemos desarrollado las versiones locales y globales de los resultados de modo más o menos simultáneo para después relacionar ambos casos. Sin embargo, aunque existe una teoría local de cuerpos de clases, apenas hemos dicho nada sobre ella hasta ahora. Lo único que sabemos es que el símbolo de Artin está definido para cualquier extensión abeliana de dominios de Dedekind, lo que incluye las extensiones locales para los primos no ramificados (en el caso ramificado el símbolo de Artin, tal y como lo hemos definido, se vuelve trivial porque no hay primos sobre los que esté definido).

Por razones que luego se comprenderán, en lugar de desarrollar una teoría paralela para las extensiones locales, lo que haremos será deducir la teoría local a partir de la teoría global. Como es habitual, esta teoría local nos aportará mucha información global de interés.

En esta sección estudiaremos los conceptos que involucra la teoría local y los relacionaremos con sus análogos globales.

Consideremos un cuerpo numérico k y uno de sus divisores primos $\mathfrak{p}$. Lo primero que necesitamos es un análogo local al grupo de elementos ideales J_k. Éste es simplemente el grupo multiplicativo del cuerpo local $k_\mathfrak{p}^*$. Su relación con el grupo global es evidente: la aplicación que a cada elemento de $k_\mathfrak{p}^*$ le asigna un elemento ideal completándolo con unos es un monomorfismo topológico (o sea, monomorfismo y homeomorfismo en la imagen) pues las propiedades de la topología producto nos dan que esto es cierto si consideramos que la imagen está en J_E, donde E contiene a los primos arquimedianos y el primo $\mathfrak{p}$, y a su vez J_E es abierto y cerrado en J. Por lo tanto podemos considerar que $k_\mathfrak{p}^* \leq J_k$. Más aún, también por las propiedades de la topología producto $k_\mathfrak{p}^*$ es cerrado en J_k.

En este punto hay que tener una precaución, podemos considerar a k^* contenido en $k_\mathfrak{p}^*$ y a $k_\mathfrak{p}^*$ contenido en J_k, pero este k^* no es el grupo al que venimos llamando así hasta ahora. En efecto, k^* en el sentido usual es cerrado y discreto, mientras que este k^* tiene la topología $\mathfrak{p}$-ádica y su clausura es $k_\mathfrak{p}^*$. La intersección de ambos subgrupos es trivial.

Precisamente a causa de que $k_\mathfrak{p}^*$ tiene intersección trivial con k^* (en el sentido usual como subgrupos de J_k) el análogo del grupo de clases C_k no es $k_\mathfrak{p}^*/k^*$ (que no sería ni siquiera un espacio de Hausdorff porque k^* no es cerrado) sino el mismo $k_\mathfrak{p}^*$.

Ahora hemos de confirmar que C_k se relaciona adecuadamente con su pretendido análogo local $k_\mathfrak{p}^*$. La prueba no es compleja pero tampoco evidente.

Teorema 8.12 *Sea k un cuerpo numérico y $\mathfrak{p}$ un primo en k. Entonces la composición de la inclusión $k_\mathfrak{p}^* \longrightarrow J_k$ con la proyección $J_k \longrightarrow C_k$ es un monomorfismo topológico, con lo que podemos considerar que $k_\mathfrak{p}^* \leq C_k$.*

DEMOSTRACIÓN: Observar que la composición es inyectiva, pues si $\alpha, \beta \in k_\mathfrak{p}^*$ y sus clases módulo k^* coinciden, entonces $\alpha = \beta\gamma$ para un cierto $\gamma \in k^*$, pero igualando cualquier componente distinta de la de índice $\mathfrak{p}$ vemos que $1 = 1\gamma$, luego $\alpha = \beta$.

También es obvio que la composición es continua. El problema es demostrar que es un homeomorfismo en la imagen, o lo que es lo mismo, que la inversa es continua.

Supongamos primero que $\mathfrak{p}$ es no arquimediano. Sea π un primo en $k_\mathfrak{p}$. Entonces cada elemento de $k_\mathfrak{p}^*$ se expresa de forma única como $u\pi^n$, con $u \in U_\mathfrak{p}$. Partimos de una clase $[u\pi^n] \in C_k$ y vamos a aplicar una sucesión de funciones continuas:

En primer lugar $\|[u\pi^n]\| = \|u\pi^n\| = \|u\pi^n\|_\mathfrak{p} = \|\pi^n\|_\mathfrak{p} = \|\pi\|_\mathfrak{p}^n$. Con esto tenemos una aplicación continua de $k_\mathfrak{p}^*$ (como subconjunto de C_k) en $\mathbb{R}^+$. Componiendo con un logaritmo llegamos a n (en $\mathbb{Z}$) y la función $n \mapsto \pi^n$ es continua porque $\mathbb{Z}$ es discreto. Con esto tenemos la continuidad de $[u\pi^n] \mapsto \pi^n$. Componiendo de nuevo con la inclusión $k_\mathfrak{p}^* \longrightarrow C_k$ y dividiendo, obtenemos la continuidad de $[u\pi^n] \mapsto [u]$.

Ahora, como $U_\mathfrak{p}$ es compacto, la inclusión $U_\mathfrak{p} \longrightarrow C_k$ es un homeomorfismo en la imagen, luego la aplicación $[u] \mapsto u$ es continua y por lo tanto la función $[u\pi^n] \mapsto u\pi^n$ también lo es.

Si $\mathfrak{p}$ es arquimediano se razona análogamente, usando que $\mathbb{R} = \{\pm 1\} \times \mathbb{R}^+$ en el caso real y que $\mathbb{C} = S \times \mathbb{R}^+$ en el caso complejo (donde S es la circunferencia unidad). ∎

Ahora veamos un primer esbozo de factorización local del homomorfismo de Artin.

Teorema 8.13 *Sea K/k una extensión abeliana de cuerpos numéricos. Entonces, para cada $\alpha \in J_k$ se cumple que*

$$\left(\frac{K/k}{\alpha}\right) = \prod_\mathfrak{p} \left(\frac{K/k}{\alpha_\mathfrak{p}}\right),$$

donde el producto tiene sentido porque todos los factores salvo un número finito de ellos son triviales.

Demostración: Sea E el conjunto de los primos de k formado por los primos arquimedianos, los ramificados en K y aquellos para los que $\mathfrak{a}_\mathfrak{p}$ no es una unidad.

Descompongamos $\alpha = \beta\gamma$, donde las componentes de β coinciden con las de α en E y son 1 en $P \setminus E$ y con γ sucede lo contrario.

Así, todas las componentes de γ son normas locales, luego $\gamma \in \mathrm{N}[J_K]$ y en consecuencia el símbolo de Artin de γ es trivial. Por lo tanto:

$$\left(\frac{K/k}{\alpha}\right) = \left(\frac{K/k}{\beta}\right) = \prod_{\mathfrak{p}\in E} \left(\frac{K/k}{\alpha_\mathfrak{p}}\right).$$

Ahora, si $\mathfrak{p} \in P \setminus E$, tenemos que $\alpha_\mathfrak{p}$ es una norma local luego su símbolo de Artin es trivial y así la factorización anterior equivale a la del enunciado. ∎

Esta descomposición no es satisfactoria porque los factores son automorfismos de la extensión K/k y no de las extensiones locales correspondientes. La

clave de la teoría local es demostrar que en realidad el factor de índice $\mathfrak{p}$ pertenece al grupo de descomposición de $\mathfrak{p}$, al que según 2.28 podemos identificar con el grupo de Galois de la extensión local.

En la prueba de este hecho interviene el teorema de escisión completa, un teorema importante de la teoría de cuerpos de clases del que demostraremos un caso particular, de él deduciremos la factorización del homomorfismo de Artin y a partir de aquí demostraremos el caso general.

Teorema 8.14 (Teorema de escisión completa) *Sea K/k una extensión abeliana de cuerpos numéricos y sea H el grupo de clases de K. Entonces un primo $\mathfrak{p}$ de k se escinde completamente en K si y sólo si $k_{\mathfrak{p}}^* \le H$.*

Demostración: Si $\mathfrak{p}$ se escinde completamente en K entonces la extensión local tiene grado 1, luego todo elemento de $k_{\mathfrak{p}}^*$ es una norma local y por lo tanto $k_{\mathfrak{p}}^* \le H$.

Respecto al recíproco, aquí probaremos sólo el caso en que la extensión K/k es de Kummer, es decir, el grupo de Galois tiene exponente n y k contiene las raíces n-simas de la unidad. El caso general será inmediato tras el teorema 8.16

Supongamos, pues, que $k_{\mathfrak{p}_0}^* \le H$. Sea E un conjunto finito de primos de k que contenga a $\mathfrak{p}_0$, a los primos arquimedianos, a los ramificados en K y tal que $J_k = k^* J_E$. Consideramos los subgrupos (7.11) asociados a la partición $E_1 = \{\mathfrak{p}_0\}$, $E_2 = E \setminus \{\mathfrak{p}_0\}$. Sean K_i las extensiones de Kummer de k asociadas a los grupos $\Delta_i = D_i \cap k^*$. Por el teorema 8.5 sabemos que $k^* D_i \leftrightarrow K_j$, donde $j = 3 - i$.

Veamos la estructura de D_1:

$$D_1 = k_{\mathfrak{p}_0}^* \times \prod_{\mathfrak{p} \in E_2} k_{\mathfrak{p}}^{*n} \times \prod_{\mathfrak{p} \in P \setminus E} U_{\mathfrak{p}}.$$

El primer factor está en H por hipótesis, el segundo porque J_k/H tiene exponente n y el tercero porque está contenido en $\mathrm{N}[J_K]$ (ya que los primos de $P \setminus E$ son no ramificados en K).

Así pues, $k^* D_1 \le H$, lo que a su vez implica que $K \subset K_2$. Pero la propiedad b) en la página 7.4 implica que $\mathfrak{p}_0$ se escinde completamente en K_2, luego también en K. ∎

Ahora ya podemos investigar el isomorfismo de Artin local. Recordemos que si K/k es una extensión abeliana y $\mathfrak{p}$ es un primo en k, entonces los grupos de descomposición de los divisores de $\mathfrak{p}$ en K son todos iguales a un mismo grupo al que podemos llamar grupo de descomposición de $\mathfrak{p}$ y que representaremos por $G_{\mathfrak{p}}$. Necesitaremos este sencillo resultado:

Teorema 8.15 *Sea K/k una extensión abeliana de cuerpos numéricos. Sea $\mathfrak{p}$ un primo en k y sea F el cuerpo de descomposición de $\mathfrak{p}$, es decir, el cuerpo fijado por el grupo $G_{\mathfrak{p}}$. Entonces F es el mayor cuerpo intermedio donde $\mathfrak{p}$ se escinde completamente.*

DEMOSTRACIÓN: Por 1.38 sabemos que $\mathfrak{p}$ se escinde completamente en F. Supongamos ahora que F' es un cuerpo intermedio donde $\mathfrak{p}$ se escinde completamente. Si $\mathfrak{p}'$ es un divisor de $\mathfrak{p}$ en F' y $\mathfrak{P}$ es un divisor de $\mathfrak{p}'$ en K, tenemos que $n(\mathfrak{p}'/\mathfrak{p}) = 1$, luego $n(\mathfrak{P}/\mathfrak{p}') = n(\mathfrak{P}/\mathfrak{p})$, es decir, $|G_{\mathfrak{P}}(K/F')| = |G_{\mathfrak{P}}(K/k)|$, pero es claro que $G_{\mathfrak{P}}(K/F')$ es un subgrupo de $G_{\mathfrak{P}}(K/k)$ y, al tener el mismo orden, concluimos que $G_{\mathfrak{p}} = G_{\mathfrak{P}}(K/k) = G_{\mathfrak{P}}(K/F') \leq G(K/F')$. Tomando cuerpos fijados queda $F' \subset F$. ∎

El resultado fundamental sobre el isomorfismo de Artin local es el siguiente:

Teorema 8.16 *Sea K/k una extensión abeliana de cuerpos numéricos. Sea $\mathfrak{p}$ un divisor de k. Entonces la restricción a $k_{\mathfrak{p}}^*$ del homomorfismo de Artin es un epimorfismo $\omega_{\mathfrak{p}} : k_{\mathfrak{p}}^* \longrightarrow G_{\mathfrak{p}}$ y su núcleo es el grupo de normas locales $\mathrm{N}_{\mathfrak{P}}[K_{\mathfrak{P}}^*]$, donde $\mathfrak{P}$ es cualquier divisor de $\mathfrak{p}$ en K. Por lo tanto $\omega_{\mathfrak{p}}$ induce un isomorfismo*

$$k_{\mathfrak{p}}^*/\,\mathrm{N}_{\mathfrak{P}}[K_{\mathfrak{P}}^*] \cong G_{\mathfrak{p}} \cong G(K_{\mathfrak{P}}/k_{\mathfrak{p}}).$$

DEMOSTRACIÓN: Sea L el cuerpo fijado por $G_{\mathfrak{p}}$ y sea $\mathfrak{p}'$ un divisor de $\mathfrak{p}$ en L. Por el teorema anterior $\mathfrak{p}$ se escinde completamente en L, luego $L_{\mathfrak{p}'} = k_{\mathfrak{p}}$. Así, para todo $\alpha \in k_{\mathfrak{p}}^*$ se cumple $\alpha = \mathrm{N}_k^L(\alpha)$, considerando que $\alpha \in J_k$ a la izquierda y $\alpha \in J_L$ a la derecha (al completar con unos son objetos distintos). Por el teorema 8.2 b) concluimos que

$$\left(\frac{K/k}{\alpha}\right) = \left(\frac{K/k}{\mathrm{N}(\alpha)}\right) = \left(\frac{K/L}{\alpha}\right) \in G(K/L) = G_{\mathfrak{p}}.$$

Con esto tenemos probado que la restricción del homomorfismo de Artin toma imágenes en $G_{\mathfrak{p}}$, es decir, tenemos $\omega_{\mathfrak{p}} : k_{\mathfrak{p}}^* \longrightarrow G_{\mathfrak{p}}$.

Ahora probaremos la suprayectividad. Sea S la imagen de $k_{\mathfrak{p}}^*$. Sea E su cuerpo fijado. Queremos probar que $S = G_{\mathfrak{p}}$ o, equivalentemente, que $E = L$. Tenemos $L \subset E \subset K$. Si no se da la igualdad que buscamos existe un cuerpo intermedio $L \subset F \subset E$ tal que la extensión F/L es cíclica de grado primo p.

Si $\alpha \in L_{\mathfrak{p}'}^*$ se cumple

$$\left(\frac{F/L}{\alpha}\right) = \left(\frac{F/k}{\mathrm{N}(\alpha)}\right) = \left(\frac{K/k}{\mathrm{N}(\alpha)}\right)\Bigg|_F = 1,$$

pues por construcción

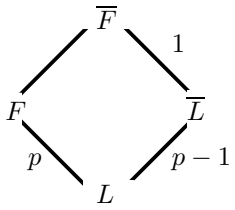
$$\left(\frac{K/k}{\mathrm{N}(\alpha)}\right) \in S = G(K/E).$$

Por consiguiente, el homomorfismo de Artin $L_{\mathfrak{p}'}^* \longrightarrow G_{\mathfrak{p}'}(F/L)$ es trivial. Por otra parte, $\mathfrak{p}'$ no se escinde completamente en L, o de lo contrario $\mathfrak{p}$ también se escindiría completamente en L.

Si pudiéramos usar el teorema de escisión completa tendríamos ya una contradicción, pues el hecho de que el homomorfismo de Artin de la extensión F/L sea trivial equivale a que $L_{\mathfrak{p}'}^*$ esté contenido en el grupo de clases de F, luego $\mathfrak{p}'$ debería escindirse completamente en F. No obstante, sólo tenemos probado

el teorema para extensiones de Kummer, luego necesitamos adjuntarle a L una raíz p-ésima primitiva de la unidad ζ.

Consideremos los cuerpos $\overline{L} = L(\zeta)$ y $\overline{F} = F\,\overline{L} = F(\zeta)$. Sea $\overline{\mathfrak{p}}'$ un divisor de $\mathfrak{p}'$ en $\overline{L}$. El grupo $G(\overline{F}'/\overline{L}')$ es trivial o tiene orden p, luego la extensión $\overline{F}'/\overline{L}'$ es de Kummer, y podemos aplicarle el teorema de escisión completa. Por 8.2 c) podemos afirmar que el homomorfismo de Artin de la extensión $\overline{F}'/\overline{L}'$ es trivial, luego $\overline{\mathfrak{p}}'$ se escinde completamente en $\overline{F}$.



El grado local de $\mathfrak{p}$ en F ha de ser p (pues no es trivial y ha de dividir al grado $|F : L| = p$). Por otra parte ha de dividir al producto del grado local de $\mathfrak{p}$ en $\overline{L}$ (que divide al grado de $\overline{L}/L$, divisor a su vez de $p-1$) por el grado local de $\overline{\mathfrak{p}}'$ en $\overline{F}$, que es 1. Tenemos, pues, una contradicción.

Falta calcular el núcleo de $\omega_\mathfrak{p}$. Ciertamente, el grupo de normas $\mathrm{N}_\mathfrak{P}[K_\mathfrak{P}^*]$ está contenido en el núcleo (pues está contenido en el grupo de normas global). Basta probar que

$$|k_\mathfrak{p}^* : \mathrm{N}_\mathfrak{P}[K_\mathfrak{P}^*]| \le |K_\mathfrak{P} : k_\mathfrak{p}|.$$

El teorema 7.9 nos da la igualdad para extensiones cíclicas. La prueba del teorema 7.26 vale igualmente para extensiones de cuerpos arbitrarias y permite reducir el caso abeliano al caso cíclico. ∎

Ahora es obvio el caso general del teorema de escisión completa: dada una extensión abeliana K/k y un primo $\mathfrak{p}$ en k, la escisión completa de $\mathfrak{p}$ en k equivale a que el grado local en $\mathfrak{p}$ es trivial, y que $k_\mathfrak{p}^*$ esté contenido en el grupo de clases equivale a que el isomorfismo de Artin local $\omega_\mathfrak{p}$ sea trivial. ∎

Otra consecuencia inmediata del teorema anterior es la siguiente:

Teorema 8.17 *Sea K/k una extensión abeliana de cuerpos numéricos. Sea $\mathfrak{p}$ un primo en k y $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en K. Si $K \leftrightarrow H$ entonces*

$$H \cap k_\mathfrak{p}^* = \mathrm{N}_\mathfrak{P}[K_\mathfrak{P}^*] \qquad y \qquad H \cap U_\mathfrak{p} = \mathrm{N}_\mathfrak{P}[U_\mathfrak{p}].$$

(Podemos considerar indistintamente que $H \le J_k$ o bien $H \le C_k$.)

De aquí se sigue a su vez una caracterización interesante de los divisores admisibles de una extensión abeliana. Recordemos que los hemos definido como los divisores admisibles para el grupo de normas, es decir, los divisores $\mathfrak{m}$ tales que $W_\mathfrak{m} \le \mathrm{N}[J_K]$.

Teorema 8.18 *Sea K/k una extensión abeliana de cuerpos numéricos. Sea H el grupo de clases de K. Entonces un divisor $\mathfrak{m}$ de k es admisible para K/k si y sólo si lo es para H. En particular el conductor de K/k coincide con el conductor de H.*

DEMOSTRACIÓN: Puesto que $\mathrm{N}[J_K] \le H$, es claro que los divisores admisibles para el grupo de normas lo son para H. Recíprocamente, si $W_\mathfrak{m} \le H$ entonces, para cada primo $\mathfrak{p}$ de k y cada divisor $\mathfrak{P}$ de $\mathfrak{p}$ en K tenemos

$$W_\mathfrak{m}(\mathfrak{p}) = W_\mathfrak{m} \cap k_\mathfrak{p}^* \le H \cap k_\mathfrak{p}^* = \mathrm{N}\mathfrak{P}[K_\mathfrak{P}^*],$$

luego claramente $W_\mathfrak{m} \le \mathrm{N}[J_K] \le H$. ∎

Por ejemplo, ahora podemos asegurar que el divisor $m\,\infty$ es admisible para el cuerpo ciclotómico de orden m, pues según el teorema 8.10 su grupo de clases es $H = \mathbb{Q}^* W_{m\,\infty}$.

8.4 La teoría local de cuerpos de clases

En esta sección probaremos los teoremas principales de la teoría local de cuerpos de clases para extensiones de cuerpos p-ádicos enunciados sin hacer referencia a cuerpos numéricos, si bien todos los resultados los deduciremos del caso global. Primeramente necesitamos algunos hechos técnicos para conectar debidamente las extensiones abelianas de cuerpos numéricos con las de cuerpos p-ádicos.

Teorema 8.19 *Sea k un cuerpo numérico, $m = 2^t m'$ un número natural no nulo (con m' impar) y E un conjunto finito de primos no arquimedianos de k. Sea $\alpha \in k$ y supongamos que $\alpha \in k_\mathfrak{p}^m$ para todo primo $\mathfrak{p} \in P \setminus E$. Entonces*

a) Si ζ es una raíz 2^t-ésima primitiva de la unidad y la extensión $k(\zeta)/k$ es cíclica (por ejemplo si $t \le 2$), entonces $\alpha \in k^m$.

b) En otro caso, al menos $\alpha \in k^{m/2}$.

DEMOSTRACIÓN: Si m y n son números naturales primos entre sí, existen enteros r y s de manera que $rm + sn = 1$. Si $\alpha = \beta^m$ y $\alpha = \gamma^n$ con β, $\gamma \in k$ entonces $\alpha = \alpha^{rm}\alpha^{sn} = \gamma^{rmn}\beta^{smn} \in k^{mn}$, luego basta probar el teorema en el caso en que $m = p^r$, donde p es primo.

Sea ζ una raíz m-sima primitiva de la unidad. Supongamos que $\zeta \in k$. Entonces el cuerpo $K = k\big(\sqrt[m]{\alpha}\big)$ es una extensión abeliana de k y para todo primo $\mathfrak{p} \in P \setminus E$ y todo divisor $\mathfrak{P}$ de $\mathfrak{p}$ en K se cumple que $K_\mathfrak{P} = k_\mathfrak{p}\big(\sqrt[m]{\alpha}\big) = k_\mathfrak{p}$, luego $\mathfrak{p}$ se escinde completamente en K. Por el teorema 7.15 concluimos que $K = k$, luego $\alpha \in k^m$.

Si $\zeta \notin k$ consideramos el cuerpo $k' = k(\zeta)$. Por el caso anterior tenemos que $\alpha = \beta^m$, con $\beta \in k'$. Entonces el polinomio $x^m - \alpha$ tiene todas sus raíces en k', pues éstas son los números $\zeta^i\beta$. Sea

$$x^m - \alpha = \prod_j f_j(x)$$

su descomposición en factores irreducibles en $k[x]$.

Si $\alpha = \gamma^m$, con $\gamma \in k_\mathfrak{p}$, entonces

$$\prod_j f_j(\gamma) = 0,$$

luego $f_j(\gamma) = 0$ para algún j. Por otra parte, las raíces de $f_j(x)$ están todas en k', luego concluimos que $k(\gamma) \subset k'$ es un cuerpo donde $\mathfrak{p}$ se escinde completamente (el grado local en $\mathfrak{p}$ es 1).

Supongamos ahora que k'/k es cíclica de grado potencia de primo. Entonces los cuerpos intermedios están totalmente ordenados por la inclusión. Podemos suponer que β es la raíz de $x^m - \alpha$ para la que el cuerpo $k(\beta)$ es el mínimo posible. Si $\mathfrak{p} \in P \setminus E$ entonces $\mathfrak{p}$ se escinde completamente en la adjunción a k de una raíz de $x^m - \alpha$, luego también en $k(\beta)$. Por el teorema 7.15 tenemos que $\beta \in k$, y $\alpha = \beta^m \in k^m$.

Supongamos que p es impar. Sea ω una raíz p-ésima primitiva de la unidad y llamemos $k_1 = k(\omega)$. Es fácil ver que k'/k_1 es cíclica de grado potencia de primo (la restricción induce un monomorfismo $G(k'/k_1) \longrightarrow G(\mathbb{Q}(\zeta)/\mathbb{Q}(\omega))$). El caso anterior nos permite concluir que $\alpha = \beta^m$, con $\beta \in k_1$. Tomando normas queda $\alpha^d \in k^m$, donde d es el grado de k_1/k, que divide a $p-1$. Tomando $1 = rd + sm$ concluimos que $\alpha \in k^m$.

Finalmente, sea $p = 2$. La extensión k'/k tiene grado potencia de 2. Si es cíclica ya hemos probado que $\alpha \in k^m$. En caso contrario tenemos $t > 2$. Sea $k_1 = k(i)$. Es fácil ver que k'/k_1 es cíclica, luego sabemos que $\alpha = \beta^m$, con $\beta \in k_1$. Al tomar normas queda $\alpha^2 = \gamma^m$, con $\gamma \in k$, luego $\alpha = \pm\gamma^{m/2}$. Sólo queda probar que el signo negativo no puede darse.

Si fuera $-1 = \alpha/\gamma^{m/2}$, como $t > 2$, tendríamos que -1 es un cuadrado en $k_\mathfrak{p}$ para todo $\mathfrak{p} \in P \setminus E$, luego por el teorema 7.15 concluimos una vez más que $k_1 = k$, lo cual no es posible porque k'/k no es cíclica y k'/k_1 sí lo es. ∎

Teorema 8.20 *Sea k un cuerpo numérico y m un número natural. Entonces C_k tiene una base de entornos de 1 formada por abiertos V tales que los conjuntos $C_k^m V$ son subgrupos abiertos.*

Demostración: Podemos tomar una base de entornos de 1 del grupo de elementos ideales J_k formada por conjuntos $A = \prod_\mathfrak{p} A_\mathfrak{p}$ de modo que las componentes no arquimedianas $A_\mathfrak{p}$ sean bolas compactas (subgrupos) y las componentes arquimedianas sean bolas de centro 1 y radio menor que 1.

Los conjuntos $J^m A$ son subgrupos, pues si $\alpha^m u$, $\beta^m v \in J^m A$, entonces

$$\alpha^m u(\beta^m v)^{-1} = (\alpha\beta^{-1})^m uv - 1 = \gamma^m w \in J^m A,$$

donde las componentes no arquimedianas de γ son las de $\alpha\beta^{-1}$, las de w son las de uv^{-1}, las componentes arquimedianas de γ son raíces m-simas de las de $\alpha\beta^{-1}uv^{-1}$ y las de w son iguales a 1.

Obviamente $J^m A$ es abierto (porque contiene a A, que lo es). ∎

Con todo esto estamos en condiciones de probar una relación muy importante entre el grupo C_k y los grupos $k_\mathfrak{p}^*$:

Teorema 8.21 *Sea k un cuerpo numérico, sea $\mathfrak{p}$ un primo de k, sea F un subgrupo abierto de índice finito en $k_\mathfrak{p}^*$. Entonces existe un subgrupo abierto H de C_k tal que $H \cap k_\mathfrak{p}^* = F$.*

DEMOSTRACIÓN: Como el cociente $k_\mathfrak{p}^*/F$ es finito, existe un número natural m tal que $k_\mathfrak{p}^{*m} \subset F$. Entonces se cumple que $k_\mathfrak{p}^* \cap C^{2m} \subset k_\mathfrak{p}^{*m} \subset F$. En efecto, un elemento de $k_\mathfrak{p}^* \cap C^{2m}$ es de la forma $[\alpha] = [\beta^{2m}]$, con $\alpha \in k_\mathfrak{p}^*$ (es decir, todas sus componentes salvo la $\mathfrak{p}$-ésima son 1) Por lo tanto existe un $\gamma \in k^*$ tal que $\alpha = \gamma\beta^{2m}$. Igualando componentes obtenemos que γ es una potencia $2m$-ésima local en todos los primos salvo quizá en $\mathfrak{p}$, luego el teorema 8.19 nos da que γ es una potencia m-sima, luego α también. Sustituimos m por $2m$, y así $k_\mathfrak{p}^* \cap C^m \subset F$.

Como $k_\mathfrak{p}^*/k_\mathfrak{p}^{*m}$ es finito (teorema 7.22), $F/k_\mathfrak{p}^{*m}$ también lo es, luego podemos expresar $F = \bigcup_{j=1}^{r} p_j k_\mathfrak{p}^{*m}$ para ciertos $p_j \in F$, de donde $FC^m = \bigcup_{j=1}^{r} p_j C^m$.

Por otra parte $C^m = (\mathbb{R}^+ \times C^0)^m = \mathbb{R}^+ \times (C^0)^m$ y, como C^0 es compacto, $(C^0)^m$ (una imagen continua) también lo es, luego C^m es cerrado en C. Concluimos que FC^m es cerrado en C, luego en $k_\mathfrak{p}^* C^m$. Como F tiene índice finito en $k_\mathfrak{p}^*$, también FC^m tiene índice finito en $k_\mathfrak{p}^* C^m$, luego FC^m es abierto en $k_\mathfrak{p}^* C^m$.

Existe un entorno abierto V de 1 en C tal que $k_\mathfrak{p}^* C^m \cap V \subset FC^m$. Sea $H = FC^m V$. Por el teorema anterior podemos exigir que $C^m V$ sea un subgrupo abierto, luego H también lo es. Ahora:

$$k_\mathfrak{p}^* C^m \cap H = k_\mathfrak{p}^* C^m \cap (FC^m)V = FC^m(k_\mathfrak{p}^* C^m \cap V) = FC^m.$$

(Notar que si $B \le A$, entonces $A \cap BC = B(A \cap C)$, aunque C no sea un subgrupo). Por lo tanto

$$k_\mathfrak{p}^* \cap H = k_\mathfrak{p}^* \cap k_\mathfrak{p}^* C^m \cap H = k_\mathfrak{p}^* \cap FC^m = F(k_\mathfrak{p}^* \cap C^m) = F.$$

∎

Ahora demostramos el resultado fundamental que relaciona las extensiones locales con las globales:

Teorema 8.22 *Sea K/k una extensión abeliana de cuerpos p-ádicos. Sea E un cuerpo numérico denso en k. Entonces existe un cuerpo numérico F denso en K tal que la extensión F/E es abeliana.*

DEMOSTRACIÓN: Probaremos varios resultados intermedios hasta llegar al deseado.

1) Dada la extensión abeliana K/k, existe una extensión abeliana de cuerpos numéricos F/E tal que E es denso en k y F es denso en K.

Por 2.19 existen cuerpos numéricos E y F densos en k y K respectivamente. Cambiando F por EF podemos suponer que $E \subset F$. Si $F = E(\alpha)$, el polinomio mínimo de α en E tiene todas sus raíces en K, luego cambiando F por la

adjunción a E de tales raíces seguimos teniendo un cuerpo numérico denso en K, pero ahora además F/E es una extensión de Galois.

Sea $\mathfrak{p}$ el primo de E inducido por el valor absoluto de k y $\mathfrak{P}$ el primo en F inducido por el valor absoluto de K. Entonces $K = F_{\mathfrak{P}}$ y $k = E_{\mathfrak{p}}$.

Sea $G_{\mathfrak{P}}$ el grupo de descomposición de $\mathfrak{P}$. Según 2.28 la restricción a F es un isomorfismo entre $G(K/k)$ y $G_{\mathfrak{P}}$, luego $G_{\mathfrak{P}}$ es abeliano. Sea E' cuerpo fijado por $G_{\mathfrak{P}}$. Como lo fijan todos los k-automorfismos de K, se cumple $E \subset E' \subset k$, luego E' es denso en k y la extensión F/E' es abeliana.

2) Si K/k es una extensión abeliana de cuerpos p-ádicos, entonces

$$|k^* : \mathrm{N}[K^*]| = |K : k|.$$

(Basta aplicar 1) y el teorema 8.16).

3) Si K/k y L/k son extensiones abelianas de cuerpos p-ádicos entonces

$$\mathrm{N}_k^{KL}[KL^*] = \mathrm{N}_k^K[K^*] \cap \mathrm{N}_k^L[L^*].$$

Tomamos cuerpos numéricos D, D', E y F densos en k los dos primeros y en K, L los últimos, de modo que E/D y F/D' sean extensiones abelianas. Las extensiones ED'/DD' y FD/DD' cumplen lo mismo, por lo que podemos suponer $D = D'$.

Claramente EF es denso en KL. Sean H_{EF}, H_E y H_F los grupos de clases de los cuerpos que indican los subíndices. Sabemos que $H_{EF} = H_E \cap H_F$. Intersecando con k^* el teorema 8.17 nos da la igualdad buscada.

4) Si K/k y L/k son extensiones abelianas de cuerpos p-ádicos tales que $\mathrm{N}_k^K[K^*] = \mathrm{N}_k^L[L^*]$, entonces $K = L$.

Aplicando 3) vemos que $\mathrm{N}_k^{KL}[KL^*] = \mathrm{N}_k^K[K^*] = \mathrm{N}_k^L[L^*]$ y por 2) resulta que $|KL : k| = |K : k| = |L : k|$, luego $K = KL = L$.

Por último probamos el teorema: Sea K/k una extensión abeliana de cuerpos p-ádicos y sea E un cuerpo numérico denso en k. Sea $\mathfrak{p}$ el primo de E inducido por el valor absoluto de k, de modo que $k = E_{\mathfrak{p}}$. El grupo de normas $\mathrm{N}_k^K[K^*]$ es abierto en k^* (por 6.17) y tiene índice finito. Por el teorema anterior existe un subgrupo abierto $H \leq C_E$ de manera que $H \cap k^* = \mathrm{N}_k^K[K^*]$. Sea L el cuerpo de clases de H y sea $\mathfrak{P}$ un divisor primo de $\mathfrak{p}$ en L. El teorema 8.17 nos da que $\mathrm{N}_k^L[L_{\mathfrak{P}}^*] = \mathrm{N}_k^K[K^*]$, luego por 4) queda que $L_{\mathfrak{P}} = K$ y así L es el buscado. ∎

Este teorema nos permite definir el homomorfismo de Artin para una extensión arbitraria de cuerpos p-ádicos:

Definición 8.23 Sea K/k una extensión abeliana de cuerpos p-ádicos. Según el teorema anterior podemos tomar una extensión abeliana de cuerpos numéricos F/E de modo que F es denso en K y E es denso en k. Sea $\mathfrak{p}$ el primo que induce en E el valor absoluto de k. Definimos $\omega : k^* \longrightarrow G(K/k)$ como la composición de la restricción del homomorfismo de Artin $k^* \longrightarrow G_{\mathfrak{p}}$ con el isomorfismo $G_{\mathfrak{p}} \longrightarrow G(K/k)$ cuya inversa es la restricción.

Es claro que se trata de un epimorfismo de grupos cuyo núcleo es el grupo de normas $\mathrm{N}_k^K[K^*]$. Vamos a probar que no depende de la elección de la extensión F/E.

En primer lugar fijamos E y probamos que no importa la elección de F. Consideremos dos extensiones abelianas F/E y F'/E tales que F y F' son densos en K. Entonces FF'/E también es abeliana y FF' es denso en K. Basta comparar F con FF' o, equivalentemente, podemos suponer que $F \subset F'$.

El teorema 8.2 nos da que, para todo $\alpha \in J_E$, el automorfismo $\omega_{F'E}(\alpha)$ extiende a $\omega_{FE}(\alpha)$, luego si $\alpha \in k^*$ las extensiones de estos automorfismos a K^* son iguales.

Ahora supongamos que tenemos dos cuerpos E y E' densos en k. Basta comparar los homomorfismos definidos mediante E y E' con el definido con EE', por lo que podemos suponer que $E \subset E'$.

Sea F una extensión abeliana de E densa en K. Por la parte ya probada podemos elegir como extensión abeliana de F a $F' = FE'$.

Sean $\mathfrak{p}$ y $\mathfrak{p}'$ los primos de E y E' respectivamente inducidos por el valor absoluto de k. Tenemos que $E_{\mathfrak{p}} = E'_{\mathfrak{p}'} = k$ (o sea, $\mathfrak{p}$ se escinde completamente en E') y por lo tanto la norma $\mathrm{N} : E'^*_{\mathfrak{p}'} \longrightarrow E_{\mathfrak{p}}$ es trivial.

El teorema 8.2 nos da que si $\alpha \in E'^*_{\mathfrak{p}'}$ se cumple $\omega_{F'E'}(\alpha)|_F = \omega_{FE}(\alpha)$, y de nuevo al extender a K obtenemos el mismo automorfismo.

Este epimorfismo $\omega : k^* \longrightarrow G(K/k)$ se llama *homomorfismo de Artin* de la extensión K/k. Usaremos también la notación habitual

$$\omega(\alpha) = \left(\frac{K/k}{\alpha}\right).$$

Resumimos en un teorema lo que hemos probado junto a algunos hechos adicionales. Los últimos apartados se demuestran reduciéndolos al teorema 8.2 mediante el apartado b), que ya está probado.

Teorema 8.24 *Se cumple:*

a) Si K/k es una extensión abeliana de cuerpos p-ádicos, el homomorfismo de Artin $\omega : k^* \longrightarrow G(K/k)$ es suprayectivo y su núcleo es el grupo de normas $\mathrm{N}_k^K[K^*]$.

b) Si K/k es una extensión abeliana de cuerpos numéricos, $\mathfrak{p}$ es un primo en k, $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en K y $\alpha \in k_{\mathfrak{p}}^*$, entonces

$$\left(\frac{K_{\mathfrak{P}}/k_{\mathfrak{p}}}{\alpha}\right)\Bigg|_K = \left(\frac{K/k}{\alpha}\right).$$

c) Si $k \subset L \subset K$ son cuerpos p-ádicos tales que la extensión K/k es abeliana y $\alpha \in k^*$, entonces

$$\left(\frac{K/k}{\alpha}\right)\Bigg|_L = \left(\frac{L/k}{\alpha}\right).$$

d) En la situación anterior, si $\alpha \in L^*$ entonces

$$\left(\frac{K/L}{\alpha}\right) = \left(\frac{K/k}{\mathrm{N}(\alpha)}\right).$$

e) Si K/k es una extensión abeliana de cuerpos p-ádicos y L/k es una extensión finita, entonces KL/L es abeliana y si $\alpha \in L^*$ entonces

$$\left(\frac{KL/L}{\alpha}\right)\Big|_K = \left(\frac{K/k}{\mathrm{N}(\alpha)}\right).$$

El teorema fundamental de la teoría local es ya inmediato:

Teorema 8.25 *Sea k un cuerpo p-ádico. La relación $H \leftrightarrow K$ definida mediante $H = \mathrm{N}_k^K[K^*]$ es una correspondencia biunívoca entre el conjunto de extensiones abelianas (finitas) de k y el conjunto de subgrupos abiertos de k^* de índice finito. Además si $K \leftrightarrow H$ y $K' \leftrightarrow H'$ se cumple:*

a) $K \subset K'$ si y sólo si $H' \le H$.

b) $KK' \leftrightarrow H \cap H'$ y $K \cap K' \leftrightarrow HH'$.

Demostración: Todas las afirmaciones del teorema excepto la existencia de cuerpos de clases se obtienen traduciendo de forma obvia los argumentos empleados en 8.4.

Dado un subgrupo abierto H de índice finito en k^*, tomamos un cuerpo numérico E denso en k. Sea $\mathfrak{p}$ el primo de E inducido por el valor absoluto de k. Entonces $k = E_\mathfrak{p}$. Aplicamos el teorema 8.21 para obtener un subgrupo abierto $L \le J_E$ tal que $L \cap k^* = H$. Tomamos el cuerpo de clases de L, llamémoslo K. Sea $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en K. Entonces el teorema 8.17 nos da que $\mathrm{N}[K_\mathfrak{P}^*] = H$, es decir, $K_\mathfrak{P}$ es el cuerpo de clases de H. ∎

Nota Hay que tener presente una diferencia importante entre la teoría local y la global: mientras que todo subgrupo abierto de C_k (donde k es un cuerpo numérico) tiene índice finito, y por lo tanto se corresponde con una extensión abeliana finita de k, no es cierto que todo subgrupo abierto de k^* (donde k es un cuerpo p-ádico) tenga índice finito. Basta pensar en el grupo de unidades U, que es abierto pero $k^*/U \cong \mathbb{Z}$.

8.5 El teorema de ramificación

El teorema de ramificación relaciona los primos que se ramifican en una extensión abeliana con su grupo de clases, de forma similar a como el teorema de escisión completa relaciona los primos que se escinden completamente. Para tratar simultáneamente el caso arquimediano y el no arquimediano convenimos en que el grupo de unidades de un primo arquimediano $\mathfrak{p}$ de un cuerpo K es

$U_\mathfrak{p} = K_\mathfrak{p}^*$ y que el grupo de inercia $T_\mathfrak{p}$ (respecto a una extensión K/k) coincide con el grupo de descomposición $G_\mathfrak{p}$ (en concordancia con el convenio según el cual el grado de inercia es $f = 1$). Notemos que si $\mathfrak{p}$ es un primo en k podemos llamar $T_\mathfrak{p}$ al grupo de inercia $T_\mathfrak{P}$ para cualquier primo $\mathfrak{P} \mid \mathfrak{p}$, pues todos coinciden.

Teorema 8.26 (Teorema de ramificación) *Sea K/k una extensión abeliana de cuerpos numéricos. Sea H el grupo de clases de K. Entonces un primo $\mathfrak{p}$ de k es no ramificado en K si y sólo sí $U_\mathfrak{p} \leq H$. Más en general,*

$$\left(\frac{K/k}{U_\mathfrak{p}}\right) = T_\mathfrak{p}.$$

Demostración: Por el teorema 7.9 tenemos que $\mathfrak{p}$ es no ramificado si y sólo si $U_\mathfrak{p} = \mathrm{N}_\mathfrak{P}[U_\mathfrak{P}]$ (para cualquier $\mathfrak{P} \mid \mathfrak{p}$). Allí está probado para primos no arquimedianos, pero es trivialmente cierto en el caso arquimediano.

Así pues, si $\mathfrak{p}$ es no ramificado, $U_\mathfrak{p} \leq H$ y, recíprocamente, si $U_\mathfrak{p} \leq H$ entonces $U_\mathfrak{p} = H \cap U_\mathfrak{p} = \mathrm{N}_\mathfrak{P}[U_\mathfrak{P}]$, luego $\mathfrak{p}$ es no ramificado.

Sea F el cuerpo fijado por $G_\mathfrak{p}$ y Z el cuerpo fijado por $T_\mathfrak{p}$. Tenemos las inclusiones $k \subset F \subset Z \subset K$.

Sea $\mathfrak{p}'$ un divisor de $\mathfrak{p}$ en F, $\mathfrak{p}''$ un divisor de $\mathfrak{p}'$ en Z y $\mathfrak{P}$ un divisor de $\mathfrak{p}''$ en K. Según el teorema 1.41 el primo $\mathfrak{p}$ se escinde completamente en F y $\mathfrak{p}'$ es no ramificado en Z. Claramente entonces

$$\left(\frac{K/k}{U_\mathfrak{p}}\right) = \left(\frac{K/F}{U_{\mathfrak{p}'}}\right) = \left(\frac{K/Z}{U_{\mathfrak{p}''}}\right),$$

pues $k_\mathfrak{p} = F_{\mathfrak{p}'}$ y $U_{\mathfrak{p}'} = \mathrm{N}[U_{\mathfrak{p}''}]$. (El teorema 1.41 está probado para primos no arquimedianos, pero en el caso arquimediano $F = Z$ y la comprobación es trivial).

Por otra parte es obvio que todo Z-automorfismo de K (todo elemento de $T_\mathfrak{p}$) fija a $\mathfrak{P}$, luego la suprayectividad del homomorfismo de Artin nos da que

$$\left(\frac{K/Z}{Z_{\mathfrak{p}''}^*}\right) = T_\mathfrak{p}.$$

La extensión $K_\mathfrak{P}/Z_{\mathfrak{p}''}$ tiene grado igual al índice de ramificación $e = e(\mathfrak{P}/\mathfrak{p}'')$. En el caso no arquimediano tomamos un primo π en el anillo de enteros de $K_\mathfrak{P}$ y tenemos claramente que la multiplicidad de π en $\mathrm{N}(\pi)$ es exactamente e, pero entonces $\rho = \mathrm{N}(\pi)$ es primo en $Z_{\mathfrak{p}''}$ y está en el núcleo del homomorfismo de Artin para K/Z (por ser una norma). Como todo elemento de $Z_{\mathfrak{p}''}^*$ se descompone como producto de una unidad por una potencia de ρ, concluimos que

$$\left(\frac{K/Z}{U_{\mathfrak{p}''}}\right) = \left(\frac{K/Z}{Z_{\mathfrak{p}''}^*}\right) = T_\mathfrak{p}.$$

En el caso arquimediano la igualdad es obvia. ∎

Sea K/k una extensión abeliana de cuerpos p-ádicos no ramificada y $\mathfrak{a}$ un ideal fraccional de k. Entonces $\mathfrak{a}$ es principal, es decir, $\mathfrak{a} = \alpha E$, donde E es el anillo de enteros de k y $\alpha \in k^*$. Dos generadores de α se diferencian en una unidad y, como la unidades están en el núcleo del homomorfismo de Artin, podemos definir

$$\left(\frac{K/k}{\mathfrak{a}}\right) = \left(\frac{K/k}{\alpha}\right).$$

Es claro que de este modo tenemos un homomorfismo $I_k \longrightarrow G(K/k)$ (donde I_k es el grupo de los ideales fraccionales de k) cuya imagen es la misma que la del homomorfismo de Artin $k^* \longrightarrow G(K/k)$, es decir, es suprayectivo.

Si E/F es una extensión abeliana de cuerpos numéricos tal que $k = F_{\mathfrak{p}}$, es inmediato comprobar que el símbolo de Artin de $\mathfrak{p} \in I_k$ es la extensión del símbolo de Artin de $\mathfrak{p}$ como ideal de F (que está definido porque $\mathfrak{p}$ es no ramificado en E), y de aquí es fácil deducir que el epimorfismo de Artin en I_k es el mismo que habíamos definido en el capítulo IV, es decir, cumple

$$\left(\frac{K/k}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}} \ (\text{mód } \mathfrak{p}),$$

para todo $\alpha \in k^*$.

Sin embargo, cuando la extensión K/k es ramificada las unidades son relevantes y no podemos definir el símbolo de Artin en términos de ideales. Esta es la razón por la que no hemos desarrollado la teoría local paralelamente a la global. Era mucho más sencillo trabajar con el símbolo de Artin global sobre ideales, transportarlo a elementos ideales globales y de aquí a los elementos ideales locales. Esto no significa que no sea posible definir directamente los homomorfismos locales y desarrollar la teoría local con independencia de la global, pero ello requiere un tratamiento algebraico más sofisticado.

Aunque en el caso no ramificado podemos trabajar indistintamente con elementos ideales locales o con ideales fraccionales, dado que la estructura de ambos grupos es tan simple (teniendo en cuenta que en el primero podemos despreciar las unidades) y dado que el homomorfismo de Artin sobre ideales no tiene equivalente en el caso ramificado, en la práctica trabajaremos siempre con elementos ideales. No así en el caso global, donde el trabajar con clases de ideales es mucho más simple en la práctica, pues la estructura del grupo de elementos ideales no es tan sencilla. Los elementos ideales son, en cambio, más útiles para los razonamientos teóricos.

8.6 Ejemplos de cuerpos de clases

Terminamos el capítulo con algunos ejemplos que ilustren la teoría que conocemos hasta ahora. De momento nos limitaremos al caso en que el cuerpo base es $\mathbb{Q}$. Paralelamente iremos introduciendo algunos conceptos teóricos generales que nos ayuden a tratar con los ejemplos. Esencialmente se trata de traducir conceptos que hasta ahora hemos tratado en términos de elementos

ideales —más útiles en teoría— a términos de clases de similitud de ideales —más convenientes en la práctica.

Cuerpos radiales Los cuerpos radiales sobre un cuerpo numérico k son los cuerpos de clases correspondientes a los grupos más sencillos:

Definición 8.27 Sea k un cuerpo numérico y $\mathfrak{m}$ un divisor de k. El *cuerpo radial* del divisor $\mathfrak{m}$ es el cuerpo de clases del grupo $k^*W_\mathfrak{m}$. El grupo $I(\mathfrak{m})/P_\mathfrak{m}$ se le llama el *grupo de clases radiales* módulo el divisor $\mathfrak{m}$.

La razón de este nombre hay que buscarla en el caso $k = \mathbb{Q}$ y $\mathfrak{m} = m\,\infty$. Vimos en el capítulo V que, por ejemplo, el grupo $P_{5\,\infty}$ contiene a los ideales (1), (6), (11), ... pero no a (−4), (−9), (−14), ... es decir, que, en lugar de contener a toda la "recta" completa de ideales generados por los números $a \equiv 1 \pmod 5$, contiene sólo a la "semirrecta", "rayo" o "radio" formada por los ideales generados por los números $a \equiv 1 \pmod 5$ y $a > 0$.

Puede parecer algo forzado, pero hay que tener presente que los primos arquimedianos fueron introducidos precisamente para "partir" las clases de equivalencia de ideales y evitar así que la congruencia módulo m degenere al pasar de números a ideales, luego ésta es una de las ideas que motivaron una parte importante de la teoría.

En virtud del teorema 8.18 el divisor $\mathfrak{m}$ es admisible para su cuerpo radial K, luego el teorema 6.21 nos da el isomorfismo

$$J_k/k^*W_\mathfrak{m} \cong I(\mathfrak{m})/P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m}).$$

Por otra parte en el capítulo V obtuvimos que $J_k/k^*W_\mathfrak{m} \cong I(\mathfrak{m})/P_\mathfrak{m}$. De estos isomorfismos se sigue que $P_\mathfrak{m} = P_\mathfrak{m}\,\mathrm{N}(\mathfrak{m})$, luego el isomorfismo de Artin es

$$J_k/k^*W_\mathfrak{m} \cong I(\mathfrak{m})/P_\mathfrak{m} \cong G(K/k).$$

Así pues, el isomorfismo de Artin hace corresponder el grupo radial de $\mathfrak{m}$ con el grupo de Galois del cuerpo radial de $\mathfrak{m}$.

Diremos que H es un *grupo de ideales* definido módulo $\mathfrak{m}$ si cumple

$$P_\mathfrak{m} \le H \le I(\mathfrak{m}).$$

Observemos que la correspondencia $H \leftrightarrow H/P_\mathfrak{m}$ es una biyección entre los grupos de ideales módulo $\mathfrak{m}$ y los subgrupos del grupo radial módulo $\mathfrak{m}$. En lo sucesivo llamaremos grupos de ideales módulo $\mathfrak{m}$ indistintamente a unos u otros.

El isomorfismo $J_k/k^*W_\mathfrak{m} \cong I(\mathfrak{m})/P_\mathfrak{m}$ biyecta los subgrupos de J_k que contienen a $k^*W_\mathfrak{m}$, es decir, los grupos de clases para los que $\mathfrak{m}$ es admisible, con los subgrupos módulo $\mathfrak{m}$. El isomorfismo de Artin biyecta éstos últimos con los subgrupos del grupo de Galois, y el teorema de Galois les asigna biunívocamente los cuerpos intermedios de la extensión K/k. Esquemáticamente:

Subgrupos de J_k con $\mathfrak{m}$ admisible	Grupos de ideales mód $\mathfrak{m}$	Subgrupos del grupo radial	Subgrupos del grupo de Galois	Cuerpos intermedios

Por lo tanto, esta cadena de correspondencias asigna a cada subgrupo H de J_k para el que $\mathfrak{m}$ es admisible una extensión abeliana de k. El teorema 8.6 afirma que esta extensión es precisamente el cuerpo de clases de H.

Vemos así que el hecho de que un divisor $\mathfrak{m}$ sea admisible para un cuerpo K significa que K es un subcuerpo del cuerpo radial de $\mathfrak{m}$. El conductor de K determina el menor cuerpo radial que contiene a K.

Tenemos, pues, que a cada grupo de ideales H módulo $\mathfrak{m}$ le corresponde un subcuerpo L del cuerpo radial de $\mathfrak{m}$. Diremos entonces que L es el *cuerpo de clases* de H. En tal caso $\mathfrak{m}$ es admisible para L/k y está definido el epimorfismo de Artin $\omega : I(\mathfrak{m}) \longrightarrow G(L/k)$. Para cada $\mathfrak{a} \in I(\mathfrak{m})$ el automorfismo $\omega(\mathfrak{a})$ es la restricción a L del automorfismo que le asigna a $\mathfrak{a}$ el epimorfismo de Artin $I(\mathfrak{m}) \longrightarrow G(K/k)$. Por lo tanto, el núcleo de ω es la antiimagen del grupo $G(K/L)$, pero éste es H por construcción.

Concluimos que si L es el cuerpo de clases de un grupo de ideales H módulo $\mathfrak{m}$, entonces H es el núcleo del epimorfismo de Artin en $I(\mathfrak{m})$, y por 7.32 es $H = P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$. Alternativamente, podemos considerar el epimorfismo de Artin para L/k definido sobre el grupo radial $I(\mathfrak{m})/P_{\mathfrak{m}}$, y entonces su núcleo es el grupo de ideales $H/P_{\mathfrak{m}}$.

Resumimos estos hechos en un teorema:

Teorema 8.28 *Sea k un cuerpo numérico y $\mathfrak{m}$ un divisor de k. Sea K el cuerpo radial de $\mathfrak{m}$. Entonces la relación $H \leftrightarrow L$ dada por $H = P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$ biyecta los grupos de ideales módulo $\mathfrak{m}$ con los cuerpos intermedios de la extensión K/k.*

Si se cumple $H \leftrightarrow L$ entonces $\mathfrak{m}$ es admisible para la extensión L/k y el homomorfismo de Artin induce un isomorfismo $I(\mathfrak{m})/H \cong G(L/k)$.

Es fácil probar las relaciones usuales de inversión de inclusiones etc.

Hay que señalar que para cada extensión abeliana L de un cuerpo k hay infinitos grupos de ideales H tales que $H \leftrightarrow L$, uno para cada divisor $\mathfrak{m}$ admisible para L/k. Después volveremos sobre este asunto.

Los cuerpos radiales de $\mathbb{Q}$ Detengámonos ahora en el caso $k = \mathbb{Q}$. El punto de partida es el teorema 8.10, según el cual el cuerpo radial correspondiente al divisor $m\,\infty$ es el cuerpo ciclotómico de orden m. Por fijar notación, llamemos $\zeta_m = e^{2\pi i/m}$. Conviene observar que esta correspondencia es válida incluso en los casos $m = 1$, 2, para los que $\mathbb{Q}(\zeta_m) = \mathbb{Q}$.

Esto nos muestra (bien es cierto que en un caso trivial) que dos divisores distintos como ∞ y $2\,\infty$ tienen el mismo cuerpo radial $\mathbb{Q}$. Sin embargo esto es un caso particular de un hecho no trivial, y es que si m es impar entonces $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$ (pues $\zeta_{2m} = -\zeta_m$). Por la unicidad del grupo de clases esto significa que

$$\mathbb{Q}^* W_{m\,\infty} = \mathbb{Q}^* W_{2m\,\infty}. \tag{8.3}$$

Veamos que no hay más coincidencias, es decir, que si m y m' son impares o múltiplos de 4 y $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{m'})$ entonces $m = m'$. En efecto, el teorema

3.29 nos da que los primos ramificados en esta extensión son exactamente los divisores de m (o de m'), luego m y m' son divisibles entre los mismos primos. Si p es el mayor primo que los divide, del hecho de que $\phi(m) = \phi(m')$ se sigue que la multiplicidad de p en m y m' es la misma. Inductivamente se llega a que $m = m'$.

La igualdad (8.3) muestra que $m\,\infty$ no es siempre —en contra de lo que hubiera podido pensarse— el conductor de $\mathbb{Q}(\zeta_m)$, pues, por ejemplo, $5\,\infty$ es admisible para $\mathbb{Q}(\zeta_{10})$. Más precisamente, los divisores de la forma $2m\,\infty$ con m impar no son el conductor de ningún cuerpo, pues si $2m\,\infty$ es admisible para un cuerpo, también lo es $m\,\infty$.

Ésta es en realidad la única excepción, es decir, si m es impar o $4 \mid m$ entonces el conductor de $\mathbb{Q}(\zeta_m)$ es exactamente $m\,\infty$. Para demostrarlo basta calcular los cuerpos radiales asociados a los divisores finitos m y comprobar que no son cuerpos ciclotómicos.

Si K es el cuerpo radial de m, entonces el núcleo del epimorfismo de Artin en $I(m)$ es P_m. Teniendo en cuenta que $I(m) = I(m\,\infty)$, el grupo de ideales de K módulo $m\,\infty$ es también P_m, luego el subgrupo asociado en $I(m\,\infty)/P_{m\,\infty}$ es $P_m/P_{m\,\infty}$.

Recordemos que $P_{m\,\infty}$ está formado por los ideales (a) con $a \equiv 1 \pmod m$ y $a > 0$, mientras que P_m está formado por los ideales (a) con $a \equiv 1 \pmod m$, no necesariamente positivo.

Así, si $(a) \in P_m$, o bien $a > 0$ y entonces $(a) \in P_{m\,\infty}$ (o sea, $[(a)] = [(1)]$), o bien $a < 0$ y entonces $(a) = (-a)$ con $-a \equiv m - 1 \pmod m$, con lo que $[(a)] = [(m-1)]$. Esto prueba que $P_m = [(1)] \cup [(m-1)]$. (Aquí hemos usado que toda clase de ideales (fraccionales) está generada por un ideal (entero).)

Por simplificar la notación conviene identificar cada clase $[(a)]$ en el grupo $I(m\,\infty)/P_{m\,\infty}$ con la clase $[a]$ en $(\mathbb{Z}/m\mathbb{Z})^*$ siempre que $a > 0$. A través de esta identificación podemos escribir $[(m-1)] = [-1]$, entendiendo que no se trata de la clase $[(-1)] = [(1)] = [1]$.

Separamos dos casos triviales: se cumple $[1] = [-1]$ si y sólo si $m \mid 2$, o sea, para $m = 1, 2$. En estos casos $\mathbb{Q}(\zeta) = \mathbb{Q}$ y el cuerpo radial de m es también $\mathbb{Q}$.

En los demás casos el grupo de ideales de m módulo $m\,\infty$ tiene dos elementos, luego el cuerpo radial tiene grado $\phi(m)/2$ sobre $\mathbb{Q}$.

El automorfismo de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ asociado a $[1]$ es obviamente la identidad. Falta calcular el asociado a $[-1]$. Para ello tomamos un primo $p \equiv -1 \pmod m$ (existe por el teorema de Dirichlet). Entonces

$$\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{[-1]}\right)(\zeta_m) = \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right)(\zeta_m) = \zeta^{-1}.$$

El inverso de ζ_m es su conjugado complejo, luego el automorfismo asociado a $[-1]$ es la conjugación compleja y el cuerpo que buscamos es el cuerpo fijado en $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ por la conjugación.

Este cuerpo es obviamente $\mathbb{Q}(\zeta_m) \cap \mathbb{R} = \mathbb{Q}(\zeta_m + \zeta_m^{-1}) = \mathbb{Q}\big(\cos(2\pi/m)\big)$. Esto es válido incluso en los casos triviales $m = 1, 2$.

Llamemos $\alpha_m = \cos(2\pi/m)$. Del hecho de que $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$ cuando m es impar se sigue que también $\mathbb{Q}(\alpha_m) = \mathbb{Q}(\alpha_{2m})$. Otras coincidencias triviales son

$$\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_3) = \mathbb{Q}(\alpha_4) = \mathbb{Q}.$$

No hay más coincidencias. Es fácil ver que los cuerpos anteriores son los únicos que cumplen $\mathbb{Q}(\alpha_m) = \mathbb{Q}$. Salvo estos casos, un cuerpo $\mathbb{Q}(\alpha_m)$ no puede coincidir con un cuerpo $\mathbb{Q}(\zeta_{m'})$ porque los primeros son reales y los segundos imaginarios (las únicas excepciones son $\mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2) = \mathbb{Q}$). Así mismo, si m y m' son impares o múltiplos de 4 la igualdad $\mathbb{Q}(\alpha_m) = \mathbb{Q}(\alpha_{m'})$ implica $m = m'$. En efecto, si $k = \mathbb{Q}(\alpha_m) = \mathbb{Q}(\alpha_{m'})$ tenemos $k \subset \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_{m'}) \subset \mathbb{Q}(\zeta_m)$. Como el grado total es 2 ha de ser

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_{m'}) = k \qquad \text{o bien} \qquad \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_{m'}) = \mathbb{Q}(\zeta_m).$$

La segunda igualdad implica que $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_{m'})$ y, como tienen el mismo grado, tendríamos $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{m'})$, lo cual es imposible.

Por lo tanto $k = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_{m'}) = \mathbb{Q}(\zeta_d)$, donde $d = (m, m')$. Como k es real esto implica $k = \mathbb{Q}$, y estamos en uno de los casos triviales. En resumen tenemos:

Teorema 8.29 *Para cada natural $m > 0$ sea $\zeta_m = e^{2\pi i/m}$ y $\alpha_m = \cos(2\pi i/m)$. Entonces*

a) El cuerpo radial de m es $\mathbb{Q}(\alpha_m)$ y el de $m\infty$ es $\mathbb{Q}(\zeta_m)$.

b) Todos estos cuerpos son distintos excepto en los casos siguientes:

- *Si m es impar $\mathbb{Q}(\alpha_m) = \mathbb{Q}(\alpha_{2m})$ y $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$.*
- $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_3) = \mathbb{Q}(\alpha_4) = \mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2) = \mathbb{Q}$.

c) Los divisores que son conductores de alguna extensión abeliana de $\mathbb{Q}$ son los de la forma m o $m\infty$, con m impar o múltiplo de 4, excepto 3, 4, ∞.

Otra consecuencia inmediata es que el conductor de una extensión abeliana K de $\mathbb{Q}$ es divisible entre ∞ si y sólo si K es imaginario, es decir, no está contenido en $\mathbb{R}$. ∎

Equivalencia de grupos de ideales Sea K/k una extensión abeliana de cuerpos numéricos. Si $\mathfrak{m}$ es un divisor admisible, cualquier múltiplo $\mathfrak{m}'$ también lo es. Entonces K tiene asociado un grupo de ideales H módulo $\mathfrak{m}$ y otro H' módulo $\mathfrak{m}'$. Veamos cuál es la relación entre ambos.

Tenemos que H es el núcleo del epimorfismo de Artin $I(\mathfrak{m}) \longrightarrow G(K/k)$ y H' es el núcleo del epimorfismo de Artin $I(\mathfrak{m}') \longrightarrow G(K/k)$. Ahora bien, $I(\mathfrak{m}') \leq I(\mathfrak{m})$ y el segundo epimorfismo es la restricción del primero, luego $H' = H \cap I(\mathfrak{m}')$.

Si, en general, H y H' son grupos de ideales módulo dos divisores $\mathfrak{m}$ y $\mathfrak{m}'$, respectivamente, que tienen asociado el mismo cuerpo de clases K, entonces

ambos son admisibles para K/k, y el divisor $\mathfrak{m}\mathfrak{m}'$ también lo será. Por el razonamiento anterior tenemos que $H \cap I(\mathfrak{m}\mathfrak{m}') = H' \cap I(\mathfrak{m}\mathfrak{m}')$ es el grupo de ideales asociado a K módulo $\mathfrak{m}\mathfrak{m}'$.

Recíprocamente, si dados H y H' se cumple $H \cap I(\mathfrak{m}'') = H' \cap I(\mathfrak{m}'')$ para un cierto múltiplo común $\mathfrak{m}''$ de $\mathfrak{m}$ y $\mathfrak{m}'$, el argumento anterior prueba que el cuerpo de clases de este grupo es el mismo que el de H y que el de H'. Esto justifica la definición siguiente:

Definición 8.30 Sean H y H' grupos de ideales módulo $\mathfrak{m}$ y $\mathfrak{m}'$ respectivamente. Diremos que son *equivalentes* si existe un divisor $\mathfrak{m}''$ múltiplo de $\mathfrak{m}$ y $\mathfrak{m}'$ de manera que $H \cap I(\mathfrak{m}'') = H' \cap I(\mathfrak{m}'')$.

El razonamiento anterior prueba que dos grupos de ideales son equivalentes si y sólo si tienen el mismo cuerpo de clases.

Si H es un grupo de clases módulo $\mathfrak{m}$ y $\mathfrak{f}$ es el conductor de su cuerpo de clases K, entonces H es equivalente al grupo de clases de K módulo $\mathfrak{f}$, llamémoslo H_0. Cualquier grupo de ideales de la clase de equivalencia de H (o de H_0) tiene cuerpo de clases K, luego ha de estar definido módulo un divisor $\mathfrak{m}'$ múltiplo de $\mathfrak{f}$, luego ha de ser de la forma $H_0 \cap I(\mathfrak{m}')$. Así pues, H_0 contiene a todos sus grupos equivalentes o, en otros términos, H_0 es maximal respecto a la inclusión en su clase de equivalencia.

Hemos probado que toda clase de equivalencia de grupos de ideales contiene un (único) grupo maximal respecto a la inclusión.

Si llamamos *conductor* de un grupo de ideales al conductor de su cuerpo de clases, entonces todos los grupos de una misma clase de equivalencia tienen el mismo conductor, al que podemos llamar *conductor* de la clase, la clase contiene un único subgrupo definido módulo cada múltiplo de su conductor. El grupo maximal es el definido módulo el propio conductor. Si H_0 es el grupo maximal de una clase de grupos y $\mathfrak{m}$ es un múltiplo del conductor, entonces el grupo módulo $\mathfrak{m}$ de la clase es $H_0 \cap I(\mathfrak{m})$.

Claramente el teorema 8.28 nos da una biyección entre las extensiones abelianas de un cuerpo numérico k y los grupos maximales de ideales de k.

A la hora de reconocer la maximalidad de un grupo de ideales conviene trabajar con los subgrupos asociados en los grupos radiales porque son finitos. El problema que se presenta es, dado un subgrupo H de un grupo radial módulo $\mathfrak{m}$, determinar si H es maximal o si, por el contrario, es equivalente a un subgrupo módulo un divisor de $\mathfrak{m}$. Como $\mathfrak{m}$ tiene un número finito de divisores, el problema puede resolverse efectivamente siempre que se conozca la estructura de los grupos radiales. Concretamente, si $\mathfrak{m}' \mid \mathfrak{m}$ tenemos las inclusiones $I(\mathfrak{m}) \le I(\mathfrak{m}')$ y $P_{\mathfrak{m}} \le P_{\mathfrak{m}'}$, que inducen un homomorfismo $I(\mathfrak{m})/P_{\mathfrak{m}} \longrightarrow I(\mathfrak{m}')/P_{\mathfrak{m}'}$.

De hecho es un epimorfismo, pues si $H = I(\mathfrak{m}) \cap P_{\mathfrak{m}'}$, entonces el núcleo es $H/P_{\mathfrak{m}}$ y, como H es equivalente a $P_{\mathfrak{m}'}$, el cociente $I(\mathfrak{m})/H$ tiene el mismo orden que $I(\mathfrak{m}')/P_{\mathfrak{m}'}$, pues ambos grupos son isomorfos al grupo de Galois del cuerpo radial de $\mathfrak{m}'$.

Ahora es claro que los subgrupos de $I(\mathfrak{m})/P_{\mathfrak{m}}$ correspondientes a grupos de ideales con un equivalente módulo $\mathfrak{m}'$ son las antiimágenes de los subgrupos

de $I(\mathfrak{m}')/P_{\mathfrak{m}'}$ a través de este epimorfismo (pues si $H/P_{\mathfrak{m}'}$ es un subgrupo de $I(\mathfrak{m}')/P_{\mathfrak{m}'}$ su antiimagen es el grupo $(H \cap I(\mathfrak{m}))/P_{\mathfrak{m}}$ y, ciertamente, $H \cap I(\mathfrak{m})$ es el grupo equivalente a H módulo $\mathfrak{m}$).

Más simplemente aún, los subgrupos inducidos desde $I(\mathfrak{m})/P_{\mathfrak{m}}$ son los que contienen al núcleo del epimorfismo, o sea, a $(I(\mathfrak{m}) \cap P_{\mathfrak{m}'})/P_{\mathfrak{m}}$.

Cuerpos de clases sobre $\mathbb{Q}$ Apliquemos esto al caso concreto $k = \mathbb{Q}$. El primer conductor es 1, que induce el grupo radial trivial $H(1) = \{[1]\}$, cuyo cuerpo radial asociado es $\mathbb{Q}$.

El conductor siguiente es $3\,\infty$, cuyo grupo radial es $H(3\,\infty) = \{[1], [2]\}$. Este grupo tiene dos subgrupos. El propio $H(3\,\infty)$ no es maximal, pues es la antiimagen del epimorfismo $H(3\,\infty) \longrightarrow H(1)$ y le corresponde el mismo cuerpo $\mathbb{Q}$. En cambio el subgrupo trivial es maximal y su cuerpo de clases es el cuerpo ciclotómico tercero, o también, $\mathbb{Q}\big(\sqrt{-3}\,\big)$.

El siguiente es $4\,\infty$, cuyo grupo radial es $H(4\,\infty) = \{[1], [3]\}$. Los divisores de $4\,\infty$ tienen todos grupo radial trivial, luego el único grupo inducido resulta ser $H(4\,\infty) \leftrightarrow \mathbb{Q}$, mientras que $\{[1]\} \leftrightarrow \mathbb{Q}(i)$ (el cuerpo ciclotómico cuarto).

El divisor siguiente es 5, pero ahorramos trabajo tratándolo junto a $5\,\infty$. El grupo radial es $H(5\,\infty) = \{[1], [2], [3], [4]\}$, y la correspondencia es:

$$\begin{aligned} \{[1]\} &\leftrightarrow \mathbb{Q}(e^{2\pi i/5}), \\ \{[1],[4]\} &\leftrightarrow \mathbb{Q}\big(\cos(2\pi/5)\big) = \mathbb{Q}\big(\sqrt{5}\,\big), \\ \{[1],[2],[3],[4]\} &\leftrightarrow \mathbb{Q}. \end{aligned}$$

El tercer grupo está inducido desde 1, el segundo desde 5 y el primero es maximal. En general un grupo módulo $m\,\infty$ está inducido desde m si y sólo si contiene a $[-1]$ (en este caso la clase $[4]$), pues ya hemos visto que el núcleo del epimorfismo $H(m\,\infty) \longrightarrow H(m)$ es exactamente $P_m/P_{m\,\infty} = \{[1], [-1]\}$. A su vez esto equivale a que el cuerpo de clases sea real (pues el automorfismo asociado a $[-1]$ es la conjugación compleja).

La igualdad $\mathbb{Q}(\cos(2\pi/5)) = \mathbb{Q}\big(\sqrt{5}\,\big)$ la da el teorema 4.8.

Enunciamos en tablas otros ejemplos y comentamos el caso $20\,\infty$, más ilustrativo.

Subgrupos de $H(7\,\infty)$	Orden	Cuerpo de clases	Conductor
$\langle[3]\rangle$	6	$\mathbb{Q}$	1
$\langle[2]\rangle$	3	$\mathbb{Q}\big(\sqrt{-7}\,\big)$	$7\,\infty$
$\langle[6]\rangle$	2	$\mathbb{Q}\big(\cos(2\pi/7)\big)$	7
$\langle[1]\rangle$	1	$\mathbb{Q}(e^{2\pi i/7})$	$7\,\infty$

Subgrupos de $H(8\,\infty)$	Orden	Cuerpo de clases	Conductor
$\langle[3],[5]\rangle$	4	$\mathbb{Q}$	1
$\langle[3]\rangle$	2	$\mathbb{Q}\big(\sqrt{-2}\,\big)$	$8\,\infty$
$\langle[5]\rangle$	2	$\mathbb{Q}(i)$	$4\,\infty$
$\langle[7]\rangle$	2	$\mathbb{Q}\big(\cos(2\pi/4)\big) = \mathbb{Q}\big(\sqrt{2}\,\big)$	8
$\langle[1]\rangle$	1	$\mathbb{Q}(e^{2\pi i/8}) = \mathbb{Q}\big(i,\sqrt{2}\,\big)$	$8\,\infty$

Subgrupos de $H(9\,\infty)$	Orden	Cuerpo de clases	Conductor
$\langle[2]\rangle$	6	$\mathbb{Q}$	1
$\langle[4]\rangle$	3	$\mathbb{Q}\big(\sqrt{-3}\,\big)$	$3\,\infty$
$\langle[8]\rangle$	2	$\mathbb{Q}\big(\cos(2\pi/9)\big)$	9
$\langle[1]\rangle$	1	$\mathbb{Q}(e^{2\pi i/9})$	$9\,\infty$

Subgrupos de $H(11\,\infty)$	Orden	Cuerpo de clases	Conductor
$\langle[2]\rangle$	10	$\mathbb{Q}$	1
$\langle[4]\rangle$	5	$\mathbb{Q}\big(\sqrt{-11}\,\big)$	$11\,\infty$
$\langle[10]\rangle$	2	$\mathbb{Q}\big(\cos(2\pi/11)\big)$	11
$\langle[1]\rangle$	1	$\mathbb{Q}(e^{2\pi i/11})$	$11\,\infty$

Ahora estudiemos los subgrupos de $H(20\,\infty)$. En primer lugar notamos que $H(20\,\infty) \cong H(4\,\infty) \times H(5\,\infty)$, de donde deducimos que se trata del producto de un grupo cíclico de orden 2 por un grupo cíclico de orden 4. Sus subgrupos tendrán todos uno o dos generadores. Un generador de $H(4\,\infty)$ es [3], que se corresponde con [11] módulo 20, y un generador de $H(5\,\infty)$ es [2], que se corresponde con [17] módulo 20.

Por lo tanto $\langle[17]\rangle$ es el núcleo del epimorfismo $H(20\,\infty) \longrightarrow H(4\,\infty)$ y su cuerpo de clases es el cuarto cuerpo ciclotómico. Igualmente $\langle[11]\rangle$ es el núcleo del epimorfismo $H(20\,\infty) \longrightarrow H(5\,\infty)$ y se corresponde con el quinto cuerpo ciclotómico.

Este cuerpo contiene al cuerpo $\mathbb{Q}\big(\sqrt{5}\,\big)$, que se corresponderá con un subgrupo de orden 4 por encima de $\langle[11]\rangle$, concretamente, el producto de este grupo con el subgrupo de orden 2 de $\langle[17]\rangle$, que es $\langle[9]\rangle$.

Subgrupos de $H(20\,\infty)$	Orden	Cuerpo de clases	Conductor
$\langle[11],[17]\rangle$	8	$\mathbb{Q}$	1
$\langle[17]\rangle$	4	$\mathbb{Q}(i)$	$4\,\infty$
$\langle[7]\rangle$	4	$\mathbb{Q}\big(\sqrt{-5}\,\big)$	$20\,\infty$
$\langle[9],[11]\rangle$	4	$\mathbb{Q}\big(\sqrt{5}\,\big)$	5
$\langle[11]\rangle$	2	$\mathbb{Q}(e^{2\pi i/5})$	$5\,\infty$
$\langle[9]\rangle$	2	$\mathbb{Q}\big(\sqrt{5},i\big)$	$20\,\infty$
$\langle[19]\rangle$	2	$\mathbb{Q}\big(\cos(2\pi/20)\big)$	20
$\langle[1]\rangle$	1	$\mathbb{Q}(e^{2\pi i/20})$	$20\,\infty$

Los elementos de orden 2 en $H(4\,\infty)\times H(5\,\infty)$ son los pares $([1],[4])$, $([3],[1])$ y $([3],[4])$, que se corresponden con las clases [9], [11] y [19].

La clase $[19] = [-1]$ genera el núcleo del epimorfismo $H(20\,\infty) \longrightarrow H(20)$, luego su cuerpo de clases es el cuerpo radial de 20.

Tenemos que $\langle[9]\rangle = \langle[9],[11]\rangle \cap \langle[17]\rangle$, luego el cuerpo de clases de este grupo es el producto de los cuerpos de clases, es decir, $\mathbb{Q}\big(\sqrt{5}, i\big)$.

Finalmente, el único subgrupo cíclico de orden 4 aparte de $\langle[17]\rangle$ es el generado por el par $([3],[2]) \in H(4\,\infty) \times H(5\,\infty)$, que se corresponde con $[7] \in H(20\,\infty)$. Como no contiene a $[-1]$ es imaginario, luego es maximal (sólo nos queda hallar los subgrupos inducidos por 20 y éste no es uno de ellos). Su cuerpo de clases es el último cuerpo cuadrático que falta por aparecer, y como tenemos a $\mathbb{Q}(i)$ y a $\mathbb{Q}\big(\sqrt{5}\big)$, ha de ser $\mathbb{Q}\big(\sqrt{-5}\big)$.

El isomorfismo de Artin de una extensión cuadrática Sea K/k una extensión cuadrática de cuerpos numéricos. Es claro que $K = k\big(\sqrt{\alpha}\big)$, para cierto $\alpha \in k$. Sea $\mathfrak{m}$ un divisor admisible para la extensión y sea H el grupo de clases de K módulo $\mathfrak{m}$. Entonces, para cada $\mathfrak{a} \in I(\mathfrak{m})$ podemos expresar

$$\left(\frac{K/k}{\mathfrak{a}}\right)\big(\sqrt{\alpha}\,\big) = \chi_K(\mathfrak{a})\,\sqrt{\alpha},$$

donde $\chi_K : I(\mathfrak{m}) \longrightarrow \{\pm 1\}$. El hecho que que el símbolo de Artin sea un epimorfismo implica que χ_K también lo es. Además ambos tienen el mismo núcleo: el grupo de clases H de K. En otras palabras, χ_K es un carácter del grupo $I(\mathfrak{m})$, que podemos ver también como un carácter del grupo radial $I(\mathfrak{m})/P_{\mathfrak{p}}$ con núcleo $H/P_{\mathfrak{m}}$.

Más aún, recordemos que el orden del símbolo de Artin de un ideal primo $\mathfrak{p} \in I(\mathfrak{m})$ es su grado de inercia, de donde se sigue claramente que $\chi_K(\mathfrak{p}) = 1$ si y sólo si $\mathfrak{p}$ se escinde (completamente) en K. Así mismo, $\chi_K(\mathfrak{p}) = -1$ si y sólo si $\mathfrak{p}$ se conserva primo en K.

Si $\mathfrak{m}$ es divisible únicamente entre los primos ramificados en K (en particular si es el conductor de la extensión) y definimos $\chi_K(\mathfrak{a}) = 0$ cuando $\mathfrak{a}$ no es primo con $\mathfrak{m}$, tenemos que un primo $\mathfrak{p}$ se ramifica, se escinde o se conserva en K según si $\chi_K(\mathfrak{p})$ es igual a 0, 1 o -1, respectivamente.

Vemos así que la factorización de primos en la extensión está completamente regulada por un carácter cuadrático del grupo radial, carácter que en esencia no es ni más ni menos que el símbolo de Artin de la extensión. Esto generaliza

Esto generaliza al teorema [9.24] y vuelve inmediato a [9.25], pues si K es un cuerpo cuadrático sobre $\mathbb{Q}$ de discriminante Δ entonces K está contenido en el cuerpo ciclotómico de orden $|\Delta|$ y $|\Delta|\infty$ es, pues, un divisor admisible para K. Observar en especial la interpretación de [9.25.4]: puesto que la clase $[-1]$ módulo $|\Delta|$ se corresponde, según ya sabemos, con la conjugación compleja, se cumple $\chi_K(-1) = 1$ si y sólo si la conjugación compleja en K es la identidad, o sea, si y sólo si K es real, si y sólo si $\Delta > 0$.

El carácter de un cuerpo cuadrático puede usarse para calcular su grupo de clases. Por ejemplo, hemos visto que el grupo de clases (maximal) de $\mathbb{Q}\big(\sqrt{-7}\big)$

es $H = \{[1], [2], [4]\}$. Podíamos haberlo predicho calculando χ_K para todas las clases módulo 7 (y usando que H es el núcleo de χ_K):

$$\begin{aligned}
\chi_K(1) &= 1 \\
\chi_K(2) &= 1 \qquad (\text{pues } -7 \equiv 1 \ (\text{mód } 8)), \\
\chi_K(3) &= (-7/3) = (2/3) = -1, \\
\chi_K(4) &= \chi_K(2)^2 = 1, \\
\chi_K(5) &= (-7/5) = (3/5) = (5/3) = (2/3) = -1, \\
\chi_K(6) &= \chi_K(2)\chi_K(3) = -1.
\end{aligned}$$

(Detallamos los cálculos a modo de ilustración, aunque por supuesto es posible abreviarlos considerablemente)

En [11.22] vimos que los caracteres de los cuerpos cuadráticos son primitivos. Esto se traduce inmediatamente en que el grupo H correspondiente no está inducido desde otro divisor $n\,\infty$ con $n < |\Delta|$, aunque puede estar inducido desde $|\Delta|$. Concluimos que el conductor de K es exactamente $|\Delta|\,\infty$ si $\Delta < 0$ o simplemente Δ si $\Delta > 0$. En el capítulo X daremos otra prueba de este hecho basada en la teoría de cuerpos de clases y no en los cálculos de [11.22].

Capítulo IX

Funciones dseta

En [11.27] demostramos el teorema de Dirichlet sobre primos en progresiones aritméticas. La prueba descansa en el hecho de que $L(1,\chi) \neq 0$ para todo carácter modular χ, lo que a su vez probamos a partir de la descomposición de la función dseta de los cuerpos ciclotómicos en producto de las funciones $L(s,\chi)$ (teorema [11.23]). Ahora podemos entender mejor por qué el cuerpo ciclotómico de orden m interviene en la prueba de un hecho concerniente al grupo U_m de unidades módulo m. La razón es que U_m es esencialmente el grupo de clases del cuerpo ciclotómico de orden m. Ésta es también la razón por la que los cálculos del teorema [11.23] cuadraron tan bien. La teoría de cuerpos de clases permite probar un resultado general de factorización de funciones dseta que engloba a [11.23], a su análogo [11.32] para cuerpos ciclotómicos reales y la fórmula $\zeta_K(s) = \zeta(s)L(s,\chi_K)$ que obtuvimos también para cuerpos cuadráticos.

De este resultado deduciremos a su vez una versión general del teorema de Dirichlet, que nos garantizará que toda clase de similitud de ideales contiene infinitos ideales primos. En la última sección daremos una prueba alternativa de la segunda desigualdad fundamental mediante funciones dseta.

9.1 Funciones dseta generalizadas

A la generalización de la similitud de ideales que hemos introducido, le corresponde la siguiente generalización de la función dseta de un cuerpo numérico:

Definición 9.1 Sea K un cuerpo numérico y $\mathfrak{m}$ un divisor de K. Sea C una clase de similitud módulo $\mathfrak{m}$. Definimos

$$\begin{aligned}\zeta_C(s,\mathfrak{m}) &= \sum_{\mathfrak{a}\in C}\frac{1}{(\mathrm{N}\,\mathfrak{a})^s},\\ \zeta(s,\mathfrak{m}) &= \sum_{\mathfrak{a}\in I(\mathfrak{m})}\frac{1}{(\mathrm{N}\,\mathfrak{a})^s} = \sum_{C\in H(\mathfrak{m})}\zeta_C(s,\mathfrak{m}),\end{aligned}$$

donde $\mathfrak{a}$ recorre sólo los ideales enteros (no fraccionales) en los conjuntos considerados.

La función $\zeta(s,1)$ es simplemente la *función dseta de Dedekind* de K [11.1], a la que llamaremos también $\zeta_K(s)$. Cuando $K=\mathbb{Q}$ nos encontramos con la *función dseta de Riemann* usual

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}.$$

La prueba del teorema [11.8], usando 5.13 en lugar de [11.7] vale literalmente para probar que las funciones dseta convergen en $]1,+\infty[$. Más aún:

Teorema 9.2 *Sea K un cuerpo numérico de grado n con s primos infinitos reales y t complejos, sea Δ el discriminante de K, sea $\mathfrak{m}$ un divisor de K, sea $R_\mathfrak{m}$ el regulador módulo $\mathfrak{m}$, sea $w_\mathfrak{m}$ el número de raíces de la unidad contenidas en el grupo de unidades $U_\mathfrak{m}$ y $h_\mathfrak{m}$ el número de clases de similitud módulo $\mathfrak{m}$. Si C es una de estas clases, entonces*

a) La serie

$$\zeta_C(s,\mathfrak{m})=\sum_{\mathfrak{a}\in C}\frac{1}{(\mathrm{N}\,\mathfrak{a})^s}$$

converge uniformemente en los compactos del intervalo $]1,+\infty[$ y existe

$$\lim_{s\to 1^+}(s-1)\zeta_C(s,\mathfrak{m})=\frac{2^s(2\pi)^t R_\mathfrak{m}}{(\mathrm{N}\,\mathfrak{m})\,w_\mathfrak{m}\,\sqrt{|\Delta|}}.$$

b) La serie

$$\zeta(s,\mathfrak{m})=\sum_{\mathfrak{a}\in I(\mathfrak{m})}\frac{1}{(\mathrm{N}\,\mathfrak{a})^s}$$

converge uniformemente en los compactos del intervalo $]1,+\infty[$ y existe

$$\lim_{s\to 1^+}(s-1)\zeta(s,\mathfrak{m})=\frac{2^s(2\pi)^t R_\mathfrak{m}}{(\mathrm{N}\,\mathfrak{m})\,w_\mathfrak{m}\,\sqrt{|\Delta|}}\,h_\mathfrak{m}.$$

Por último, la prueba de [11.9] se generaliza sin dificultad al teorema siguiente:

Teorema 9.3 *Sea K un cuerpo numérico y $\mathfrak{m}$ un divisor de K. Entonces*

$$\zeta(s,\mathfrak{m})=\prod_{\mathfrak{p}\in I(\mathfrak{m})}\frac{1}{1-\frac{1}{(\mathrm{N}\,\mathfrak{p})^s}},\qquad \text{para } s>1,$$

donde $\mathfrak{p}$ recorre los ideales primos de K que no dividen a $\mathfrak{m}$. La convergencia del producto es absoluta.

9.2 Caracteres modulares

Antes de generalizar el concepto de función L debemos ocuparnos de los caracteres modulares, en particular de generalizar la noción de carácter primitivo. Vamos a ver que la teoría de cuerpos de clases también está relacionada con estas nociones.

Definición 9.4 Sea k un cuerpo numérico y $\mathfrak{m}$ un divisor de k. Un *carácter modular* de k (o, más precisamente, un *carácter módulo* $\mathfrak{m}$) es una función $\chi : I_k \longrightarrow \mathbb{C}$ que cumpla las condiciones siguientes:

a) Para todo $\mathfrak{a} \in I_k$ se cumple $\chi(a) = 0$ si y sólo si $\mathfrak{a} \notin I(\mathfrak{m})$.

b) Si $\mathfrak{a} \equiv \mathfrak{a}'$ (mód $P_\mathfrak{m}$), entonces $\chi(\mathfrak{a}) = \chi(\mathfrak{a}')$.

c) Si $\mathfrak{a}$, $\mathfrak{b} \in I_k$, entonces $\chi(\mathfrak{ab}) = \chi(\mathfrak{a})\chi(\mathfrak{b})$.

Es claro que cada carácter módulo $\mathfrak{m}$ induce un carácter en el grupo $I(\mathfrak{m})/P_\mathfrak{m}$ mediante $\chi([\mathfrak{a}]) = \chi(\mathfrak{a})$ y viceversa, de modo que tenemos una biyección entre los caracteres módulo $\mathfrak{m}$ y los caracteres de $I(\mathfrak{m})/P_\mathfrak{m}$.

Si $\mathfrak{m} \mid \mathfrak{n}$ entonces tenemos un epimorfismo natural $I(\mathfrak{n})/P_\mathfrak{n} \longrightarrow I(\mathfrak{m})/P_\mathfrak{m}$, luego cada carácter módulo $\mathfrak{m}$ induce por composición con este epimorfismo un carácter módulo $\mathfrak{n}$.

Si χ es un carácter módulo $\mathfrak{m}$, llamamos $N_\chi/P_\mathfrak{m}$ al núcleo de χ, K_χ al cuerpo de clases de N_χ y $\mathfrak{f}_\chi$ al conductor de la extensión K_χ/k. Obviamente $\mathfrak{f}_\chi \mid \mathfrak{m}$.

Si un carácter χ módulo $\mathfrak{m}$ induce un carácter ψ módulo $\mathfrak{n}$ entonces es claro que $N_\psi = I(\mathfrak{n}) \cap N_\chi$, luego los grupos N_ψ y N_χ son equivalentes en el sentido de 8.30. De aquí se sigue que si χ induce a ψ entonces $K_\chi = K_\psi$ y $\mathfrak{f}_\chi = \mathfrak{f}_\psi$.

Recíprocamente, si ψ es un carácter módulo $\mathfrak{n}$ entonces ψ es inducido por un carácter módulo $\mathfrak{m} = \mathfrak{f}_\chi$. En efecto, sea H el grupo de clases de K_ψ módulo $\mathfrak{m}$. Se cumple que $I(\mathfrak{m})/H \cong I(\mathfrak{n})/N_\psi$, luego ψ determina un carácter en $I(\mathfrak{m})/H$, luego en $I(\mathfrak{m})/P_\mathfrak{m}$, que a su vez es claro que induce a ψ.

Un carácter módulo $\mathfrak{m}$ es *primitivo* si no es inducido desde ningún módulo menor.

Las consideraciones anteriores prueban que un carácter χ módulo $\mathfrak{m}$ es primitivo si y sólo si $\mathfrak{m} = \mathfrak{f}_\chi$, así como que cada carácter modular χ es inducido por un único carácter primitivo χ_0.

Al pasar de un carácter modular primitivo a otro inducido estamos perdiendo parte de la información que éste contiene, pues estamos haciendo que tome el valor 0 en ciertos ideales donde antes no lo tomaba. Por ello conviene trabajar sólo con caracteres primitivos e identificar cada carácter modular con el carácter primitivo que lo induce, es decir, convendremos en que $\chi(\mathfrak{a})$ no es el valor que le corresponde como carácter modular, sino que $\chi(\mathfrak{a}) = \chi_0(\mathfrak{a})$. Por ejemplo, si χ es el carácter principal módulo $\mathfrak{m}$, en principio sería $\chi(\mathfrak{a}) = 0$ si $\mathfrak{a}$ no es primo con $\mathfrak{m}$, pero, como χ está inducido por el carácter principal módulo 1, convenimos en que $\chi(\mathfrak{a}) = 1$ para todo ideal $\mathfrak{a}$.

Nota La noción de carácter modular que acabamos de introducir generaliza a [11.17] en cuanto que un carácter módulo m en el sentido de [11.7] es un carácter módulo $m\,\infty$ en el sentido actual. Esto hace que un carácter primitivo módulo m en el sentido de [11.19] no sea necesariamente primitivo módulo $m\,\infty$, ya que puede ser inducido desde un carácter módulo m. Aparte de casos triviales, esto sucede exactamente cuando $\chi(-1) = 1$. En cualquier caso, un carácter primitivo módulo m en el sentido de [11.9] es un carácter primitivo módulo m o módulo $m\,\infty$ en el sentido actual. Así mismo, si un carácter tiene conductor f en el sentido de [11.19], su conductor ahora será f o bien $f\,\infty$.

Si K/k es una extensión abeliana de cuerpos numéricos y H es su grupo de clases módulo un divisor admisible $\mathfrak{m}$, llamaremos *caracteres* de la extensión a los caracteres (modulares) primitivos asociados a los caracteres del grupo $I(\mathfrak{m})/H$, es decir, a los caracteres de $I(\mathfrak{m})/P_{\mathfrak{m}}$ cuyo núcleo contiene a H.

Es obvio que la definición no depende de la elección de $\mathfrak{m}$. A través del isomorfismo de Artin podemos identificar los caracteres de K/k con los del grupo de Galois $G(K/k)$. En particular, si $K/\mathbb{Q}$ es una extensión abeliana, llamaremos *caracteres* de K a los caracteres de $K/\mathbb{Q}$. Esto generaliza al concepto de carácter de un cuerpo cuadrático, que en este sentido no es sino el carácter no principal del cuerpo.

Si χ es un carácter de una extensión K/k de conductor $\mathfrak{f}$, entonces, visto como carácter módulo $\mathfrak{f}$, se cumple $P_{\mathfrak{f}} \le N_\chi$, lo cual significa que $\mathfrak{f}$ es admisible para la extensión K_χ/k o, equivalentemente, que $\mathfrak{f}_\chi \mid \mathfrak{f}$. Más aún, tenemos $k \subset K_\chi \subset K$. Si identificamos a χ con un carácter de $G(K/k)$, entonces el grupo de clases N_χ de K_χ se corresponde con su imagen por el isomorfismo de Artin y, de acuerdo con lo visto en el capítulo anterior, K_χ es el cuerpo fijado por N_χ.

Vamos a introducir ahora un enfoque equivalente en términos de elementos ideales que nos será más útil en la teoría.

Sea k un cuerpo numérico. Un *carácter* del grupo C_k es un homomorfismo continuo $\chi : C_k \longrightarrow \mathbb{C}^*$. Diremos que tiene *periodo finito* si su núcleo N_χ tiene índice finito en C_k. Entonces N_χ es un subgrupo abierto de C_k (ya que es cerrado por continuidad). El *conductor* de χ será el conductor f_χ de N_χ. Un divisor $\mathfrak{m}$ será *admisible* para χ si lo es para N_χ.

Si $\mathfrak{m}$ es un divisor admisible para χ, es claro que χ induce un carácter módulo $\mathfrak{m}$ a través del isomorfismo

$$C_k/W_{\mathfrak{m}} \cong I(\mathfrak{m})/P_{\mathfrak{m}}.$$

Más aún, es fácil ver que el carácter que χ induce módulo $\mathfrak{m}$ es el inducido por el carácter que induce módulo $\mathfrak{f}_\chi$. Recíprocamente, todo carácter módulo $\mathfrak{m}$ está inducido por un carácter de C_k y fácilmente se llega a que los caracteres de C_k de periodo finito se corresponden biunívocamente con los caracteres modulares primitivos de k. El conductor de un carácter de C_k es el mismo que el de su carácter modular correspondiente.

Si K es una extensión abeliana de k y $H \leq C_k$ es su grupo de clases, los caracteres de K se corresponden con los caracteres χ de C_k tales que $\chi[H] = 1$.

Por ejemplo, así es más fácil probar que el conductor de K/k es

$$\mathfrak{f} = \operatorname{mcm}_\chi \mathfrak{f}_\chi,$$

donde χ recorre los caracteres de K/k. En efecto, si $\mathfrak{m}$ es el mínimo común múltiplo, ya hemos visto que $\mathfrak{m} \mid \mathfrak{f}$, luego basta probar que $\mathfrak{m}$ es admisible para la extensión. Ahora bien,

$$W_\mathfrak{m} \leq \bigcap_\chi N_\chi = H,$$

pues, en un grupo abeliano finito, la intersección de los núcleos de los caracteres es siempre trivial.

9.3 El teorema de factorización

Vamos a probar que la función dseta de un cuerpo numérico se descompone en producto de funciones L. La definición de función L generaliza de forma obvia a la dada en [11.23]:

Definición 9.5 Sea k un cuerpo numérico de grado n y sea χ un carácter modular de k Definimos

$$L(s,\chi) = \sum_\mathfrak{a} \frac{\chi(\mathfrak{a})}{(\mathrm{N}\,\mathfrak{a})^s} = \prod_\mathfrak{p} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{(\mathrm{N}\,\mathfrak{p})^s}}, \qquad \text{para } s > 1,$$

donde $\mathfrak{a}$ recorre los ideales de k y $\mathfrak{p}$ los ideales primos de k.

En esta definición adoptamos el convenio indicado en la sección anterior, según el cual $\chi(\mathfrak{a})$ ha de entenderse como $\chi_0(\mathfrak{a})$, donde χ_0 es el carácter primitivo que induce a χ.

Teniendo en cuenta que cada $|\chi(\mathfrak{a})| \leq 1$ es obvio que la serie converge absolutamente en el intervalo $s > 1$ y el razonamiento de [11.9] prueba la segunda igualdad. Observar que $L(s,1) = \zeta_K(s)$.

Necesitamos probar que las funciones L correspondientes a caracteres no principales convergen en 1. Para ello no nos sirve el teorema [11.24]. Observemos que para aplicarlo deberíamos expresar la serie en la forma

$$L(s,\chi) = \sum_{n=1}^\infty \frac{a_n}{n^s}, \tag{9.1}$$

para lo cual ha de ser

$$a_n = \sum_{\mathrm{N}\,\mathfrak{a}=n} \chi(\mathfrak{a}). \tag{9.2}$$

Sin embargo, las relaciones de ortogonalidad no nos garantizan ahora que las sumas $A_k = a_1 + \cdots + a_k$ estén acotadas. Necesitamos un teorema de convergencia con una hipótesis menos severa:

Teorema 9.6 *Sea $\{a_n\}$ una sucesión de números complejos y para cada k sea $A_k = a_1 + \cdots + a_k$. Supongamos que existen constantes $C > 0$ y $s_0 \geq 0$ tales que $|A_k| \leq Ck^{s_0}$ para todo k. Entonces la serie*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

converge uniformemente en los compactos del intervalo $]s_0, +\infty[$.

Demostración: El mismo cálculo elemental visto en la prueba de [11.24] nos da que si $N < M$ entonces

$$\sum_{k=N}^{M} \frac{a_k}{k^s} = \frac{A_M}{M^s} - \frac{A_{N-1}}{N^s} + \sum_{k=N}^{M-1} \left(\frac{A_k}{k^s} - \frac{A_k}{(k+1)^s} \right).$$

Por consiguiente

$$\left| \sum_{k=N}^{M} \frac{a_k}{k^s} \right| \leq C \left(\frac{1}{M^{s-s_0}} + \frac{1}{N^{s-s_0}} + \sum_{k=N}^{M-1} k^{s_0} \left(\frac{1}{k^s} - \frac{1}{(k+1)^s} \right) \right).$$

Ahora bien,

$$\sum_{k=N}^{M-1} k^{s_0} \left(\frac{1}{k^s} - \frac{1}{(k+1)^s} \right) = \sum_{k=N}^{M-1} s \int_k^{k+1} k^{s_0} \frac{dx}{x^{s+1}} \leq \sum_{k=N}^{M-1} s \int_k^{k+1} \frac{dx}{x^{s-s_0+1}}$$

$$= s \int_N^M \frac{dx}{x^{s-s_0+1}} = \frac{s}{s-s_0} \left(\frac{1}{N^{s-s_0}} - \frac{1}{M^{s-s_0}} \right) \leq \frac{s}{(s-s_0)N^{s-s_0}}.$$

Así pues, si K es un subconjunto compacto de $]s_0, +\infty[$, podemos tomar $C' > 0$ y $\delta > 0$ tales que $\delta < s - s_0$, $s < C'$ para todo $s \in K$, con lo que

$$\left| \sum_{k=N}^{M} \frac{a_k}{k^s} \right| \leq \frac{C}{M^\delta} + \frac{C}{N^\delta} + \frac{CC'}{\delta N^\delta} < \frac{2C}{N^\delta} + \frac{CC'}{\delta N^\delta}.$$

El miembro derecho tiende a 0 cuando N tiende a ∞, luego la serie es uniformemente de Cauchy en el compacto K. ∎

Ahora sí podemos probar:

Teorema 9.7 *Sea K un cuerpo numérico de grado n y χ un carácter modular no principal de k. Entonces la función $L(s, \chi)$ converge uniformemente en los compactos del intervalo $]1 - 1/n, +\infty[$.*

Demostración: Sea $\mathfrak{f}$ el conductor de χ, de modo que χ induce un carácter en $H(\mathfrak{f}) = I(\mathfrak{f})/P_{\mathfrak{f}}$ y se anula en los ideales que no pertenecen a $I(\mathfrak{f})$.

Expresamos la serie en la forma (9.1) con los coeficientes (9.2). Para aplicar el teorema anterior hemos de estimar

$$A_k = \sum_{\mathrm{N}\,\mathfrak{a}\le k} \chi(\mathfrak{a}) = \sum_{C\in H(\mathfrak{f})} \sum_{\substack{\mathfrak{a}\in C\\ \mathrm{N}\,\mathfrak{a}\le k}} \chi(\mathfrak{a}) = \sum_{C\in H(\mathfrak{f})} \chi(C) j_C(k).$$

Ahora usamos el teorema 5.13, según el cual existen constantes M y N tales que la función $r_C(k) = j_C(k) - Mk$ cumple $r_C(k) \le Nk^{1-1/n}$. Además usamos las relaciones de ortogonalidad [11.16]:

$$\begin{aligned} |A_k| &= \Big| \sum_{C\in H(\mathfrak{f})} \chi(C) Mk + \sum_{C\in H(\mathfrak{f})} \chi(C) r_C(k) \Big| \\ &\le \sum_{C\in H(\mathfrak{f})} |\chi(C)|\, |r_C(k)| \le h_{\mathfrak{f}} N k^{1-1/n}. \end{aligned}$$

Ahora basta aplicar el teorema anterior. ∎

Veamos el teorema de factorización:

Teorema 9.8 *Sea K/k una extensión abeliana de cuerpos numéricos y sea H su grupo de clases en C_k. Entonces*

$$\zeta_K(s) = \prod_{\chi} L(s,\chi) = \zeta_k(s) \prod_{\chi\ne 1} L(s,\chi),$$

donde en el primer producto χ recorre los caracteres de C_k cuyo núcleo contiene a H (o, equivalentemente, los caracteres de la extensión K/k) y en el segundo producto χ recorre estos mismos caracteres excepto el trivial.

Demostración: Tenemos que

$$\zeta_K(s) = \prod_{\mathfrak{P}} \left(1 - \frac{1}{(\mathrm{N}\,\mathfrak{P})^s}\right)^{-1} = \prod_{\mathfrak{p}} \prod_{\mathfrak{P}|\mathfrak{p}} \left(1 - \frac{1}{(\mathrm{N}\,\mathfrak{P})^s}\right)^{-1},$$

donde $\mathfrak{P}$ recorre los primos de K y $\mathfrak{p}$ los de k.

Basta probar que para cada primo $\mathfrak{p}$ se cumple

$$\prod_{\mathfrak{P}|\mathfrak{p}} \left(1 - \frac{1}{(\mathrm{N}\,\mathfrak{P})^s}\right) = \prod_{\chi} \left(1 - \frac{\chi(\mathfrak{p})}{(\mathrm{N}\,\mathfrak{p})^s}\right). \tag{9.3}$$

Digamos que la factorización de $\mathfrak{p}$ en K es

$$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e,$$

de modo que $n = |K:k| = efr$, $\mathrm{N}\,\mathfrak{P}_i = (\mathrm{N}\,\mathfrak{p})^f$. Haciendo el cambio $u = (\mathrm{N}\,\mathfrak{p})^{-s}$ la igualdad (9.3) equivale a

$$(1-u^f)^r = \prod_{\chi} \big(1 - \chi(\mathfrak{p})u\big). \tag{9.4}$$

Tenemos claramente

$$1 - u^f = \prod_\zeta (1 - \zeta u),$$

donde ζ recorre las raíces de la unidad de orden f. Hay que probar que $\chi(\mathfrak{p})$ recorre las raíces de la unidad de orden f pasando r veces por cada una.

Supongamos primero que $e = 1$, es decir, que $\mathfrak{p}$ es no ramificado en K. Si χ es un carácter de K y $K_\chi \subset K$ es el cuerpo de clases de su núcleo, entonces $\mathfrak{p}$ es no ramificado en K_χ, por lo que no divide al conductor $\mathfrak{f}_\chi$. Así, cualquier primo $\pi \in k_\mathfrak{p}^*$ se corresponde con $\mathfrak{p}$ a través del isomorfismo

$$C_k/W_{\mathfrak{f}_\chi} \cong I(\mathfrak{f}_\chi)/P_{\mathfrak{f}_\chi},$$

luego $\chi(\mathfrak{p}) = \chi(\pi)$.

Sea $H_\mathfrak{p} = Hk_\mathfrak{p}^*$. Entonces $H_\mathfrak{p}$ es el menor grupo de clases que contiene a H y a $k_\mathfrak{p}^*$, luego por el teorema de escisión completa el cuerpo de clases de $H_\mathfrak{p}$ es el mayor subcuerpo de K donde $\mathfrak{p}$ se escinde completamente, o sea, el cuerpo de descomposición de $\mathfrak{p}$ y, por lo tanto, $|H_\mathfrak{p} : H| = f$. Como $\mathfrak{p}$ no es ramificado, $U_\mathfrak{p} \le H$ luego, si π es un primo de $k_\mathfrak{p}$, el grupo $H_\mathfrak{p}/H$ es cíclico, generado por π. Cuando ψ recorre los caracteres de $H_\mathfrak{p}/H$, entonces $\psi(\pi)$ recorre las f raíces de la unidad de orden f. Cada carácter ψ se extiende a r caracteres χ de C_k/H, de modo que todos ellos cumplen que $\chi(\mathfrak{p}) = \chi(\pi) = \psi(\pi)$ es una misma raíz. Las rf extensiones recorren todos los caracteres de C_k/H, luego se cumple lo que queríamos probar.

Consideremos ahora el caso general. Según el teorema de ramificación, el homomorfismo de Artin envía $U_\mathfrak{p}$ al grupo de inercia de $\mathfrak{p}$, luego $|HU_\mathfrak{p} : H| = |U_\mathfrak{p} : U_\mathfrak{p} \cap H| = e$.

Sean $1 = \psi_1, \dots, \psi_e$ los caracteres de $HU_\mathfrak{p}/H$ extendidos a C_k/H (elegimos una extensión para cada carácter). Sean $1 = \chi_1, \dots, \chi_{fr}$ los caracteres de $C_k/HU_\mathfrak{p}$. Entonces los caracteres $\psi_i\chi_j$ son distintos dos a dos, luego recorren todos los caracteres de C_k/H.

Si $i \ne 1$ entonces $\psi_i(\mathfrak{p}) = 0$ (pues $U_\mathfrak{p}$ no está contenido en el núcleo de ψ_i y por lo tanto $\mathfrak{p}$ divide al conductor de ψ_i), luego los únicos caracteres que contribuyen en el miembro derecho de (9.4) son $\chi_1, \dots, \chi_{fr}$, que son exactamente los caracteres que cumplen $\chi[HU_\mathfrak{p}] = 1$ y, como $\mathfrak{p}$ no se ramifica en el cuerpo de clases de $HU_\mathfrak{p}$, el caso ya probado nos da que $\chi_j(\mathfrak{p})$ recorre las raíces f-ésimas de la unidad pasando r veces por cada una. ∎

De aquí se deducen diversas fórmulas que relacionan el número de clases de K con el de k. La más inmediata se obtiene calculando el residuo en 1 de los dos miembros de la fórmula del teorema anterior (es decir, multiplicando por $s - 1$ y tomando límites). Si llamamos

$$\rho_K = \frac{2^s(2\pi)^t R}{w\sqrt{|\Delta|}},$$

donde s y t son el número de primos arquimedianos reales y complejos de K, R es el regulador, w el número de raíces de la unidad contenidas en K y Δ el discriminante, entonces el teorema 9.2 nos da que

$$\rho_K h_K = \rho_k h_k \prod_{\chi\neq 1} L(1,\chi). \tag{9.5}$$

Explícitamente, para el caso $k=\mathbb{Q}$, hemos probado que si K es una extensión abeliana de $\mathbb{Q}$ entonces el número de clases de K viene dado por

$$h_K = \frac{w\sqrt{|\Delta|}}{2^s(2\pi)^t R}\prod_{\chi\neq 1} L(1,\chi). \tag{9.6}$$

Teniendo en cuenta que los caracteres involucrados son primitivos, el teorema [11.31] (junto con [12.8]) nos permite calcular los valores $L(1,\chi)$. El único inconveniente serio es el cálculo del regulador R, pues supone calcular las unidades fundamentales de K. El caso más simple en el que esta fórmula es aplicable es cuando K es un cuerpo cuadrático imaginario, pues entonces $R=1$, seguido del caso de los cuerpos cuadráticos reales, para el que hay algoritmos sencillos que nos dan la unidad fundamental. En estos casos obtenemos las fórmulas de [12.9]. No obstante, otro caso en el que el cálculo no es excesivamente complejo se da cuando K es un cuerpo complejo de grado 4, pues entonces K tiene una única unidad fundamental E y $R=2\log|E|$. Como ejemplo probamos el teorema siguiente:

Teorema 9.9 (Dirichlet) *Sea $d>1$ un número natural libre de cuadrados y consideremos los cuerpos $k=\mathbb{Q}(\sqrt{d}\,)$ y $k'=\mathbb{Q}(\sqrt{-d}\,)$. Sean h y h' sus números de clases. Entonces el número de clases del cuerpo $K=\mathbb{Q}(\sqrt{d},\sqrt{-d}\,)$ viene dado por*

$$H=\frac{u}{2}\,h\,h',$$

donde $u=2$ si 2 es el cuadrado de un ideal principal en k y $u=1$ en caso contrario.

Demostración: Vamos a analizar por separado los casos $d=2,3$. En ambos es inmediato que 2 es el cuadrado de un ideal principal en k y, por otro lado, la fórmula del enunciado da $H=1$, luego hemos de probar que K tiene factorización única.

Admitamos que el discriminante de K es 256 si $d=2$ y 144 si $d=3$. Esto lo obtendremos fácilmente en el capítulo próximo. Concretamente, en el ejemplo 1 de la sección 10.6 se prueba que el discriminante de K es el producto de los discriminantes de sus tres subcuerpos.

La constante de Minkowski para K es $M_{02}=0{,}151982$, y el teorema [4.14] nos da que todo ideal de K es similar a uno de norma menor o igual que 2 para $d=2$ o de norma menor o igual que 1 para $d=3$. Esto prueba ya la factorización única en el segundo caso. Para el primero basta observar que si ζ es una raíz octava primitiva de la unidad entonces $\mathrm{N}(1+\zeta)=2$, luego los ideales de norma 2 son principales.

Así pues, podemos probar el teorema suponiendo $d \neq 2, 3$. Si llamamos

$$k_1 = \mathbb{Q}\big(\sqrt{d}\,\big), \qquad k_2 = \mathbb{Q}\big(\sqrt{-d}\,\big), \qquad k_3 = \mathbb{Q}(i),$$

las raíces de la unidad contenidas en k_1, k_2 son ± 1, mientras que las de k_3 (y las de K) son ± 1, $\pm i$. Sea χ_i el carácter de k_i. Es claro que éstos son los caracteres no principales de K.

Aplicándoles a los tres la fórmula (9.6) queda

$$\begin{aligned} h &= \frac{\sqrt{|\Delta_1|}}{2\log\epsilon}\,L(1,\chi_1),\\ h' &= \frac{\sqrt{|\Delta_1|}}{\pi}\,L(1,\chi_2),\\ 1 &= \frac{2\sqrt{|\Delta_3|}}{\pi}\,L(1,\chi_3), \end{aligned}$$

donde $\epsilon > 1$ es la unidad fundamental de $\mathbb{Q}\big(\sqrt{d}\,\big)$.

Ahora aplicamos (9.6) al cuerpo K sustituyendo los valores $L(1,\chi_i)$ que acabamos de obtener. El resultado es

$$H = \frac{hh'}{2}\,\frac{\log\epsilon}{\log|E|},$$

donde E es una unidad fundamental de K (y por lo tanto el regulador es $2\log|E|$).

El problema es, pues, calcular el valor de $\log\epsilon/\log|E|$. Sea $\sigma_i \neq 1$ el automorfismo de K que fija a k_i. Entonces, puesto que $\mathrm{N}(E) = 1$,

$$E^2 = \big(E\,\sigma_1(E)\big)\big(E\,\sigma_2(E)\big)\big(E\,\sigma_3(E)\big).$$

El primer factor está en k_1, el segundo en k_2 y el tercero en k_3. Como los tres son unidades, el primero es de la forma $\pm\epsilon^v$, y los otros dos son raíces de la unidad. Así pues, $E^2 = \zeta\epsilon^v$, donde ζ es una raíz de la unidad.

Si llamamos G al grupo de las unidades de K y H al producto del grupo de las unidades de k por el grupo de raíces de la unidad de K, es claro que $G/H = \langle[E]\rangle$, y acabamos de probar que $|G:H| = 1, 2$.

Por otro lado, como E es una unidad fundamental, ha de ser $\epsilon = \omega E^j$, done ω es una raíz de la unidad, de donde $E^2 = \zeta\omega^v E^{jv}$ y, por la unicidad de la expresión, $jv = 2$. Sustituyendo E por E^{-1} si es preciso queda o bien $E^2 = \zeta\epsilon$, en cuyo caso $\epsilon = \zeta^{-1}E^2$, o bien $E^2 = \zeta\epsilon^2$, en cuyo caso E/ϵ es una raíz de la unidad de K.

Reuniendo todas las posibilidades, $\epsilon = i^r E^u$, donde $u = 1, 2$. Obviamente $u = 1$ si y sólo si $|G:H| = 1$ (pues si $|G:H| = 1$ se ha de cumplir $E = \zeta\epsilon^s$, pero como E es una unidad fundamental ha de ser $s = \pm 1$ y, con la elección adecuada de E, $s = 1$, y así $u = 1$). En consecuencia, $u = |G:H|$.

Tomando módulos queda $\epsilon = |E|^u$, luego $u = \log\epsilon/\log|E|$, es decir, se trata de la constante que aparece en el enunciado. Hay que probar que $u = 2$ si y sólo si 2 es el cuadrado de un ideal principal en k.

Si $(2) = (\eta)^2$, entonces, representando con un apóstrofo la conjugación en k, tenemos que $(\eta) = (\eta')$, luego $\eta\eta' = \pm 2$ y $\pm\eta/\eta' = \epsilon_0$, para una unidad ϵ_0.

Llamamos $F = \eta/(1+i)$. Así

$$F^2 = \frac{\eta^2}{2i} = -\frac{\eta\eta'}{2}\,\frac{\eta}{\eta'}\,i = \pm i\epsilon_0.$$

En particular F es una unidad de K, y es claro que $F \notin H$, pues en caso contrario tendríamos $(1+i)i^t \in k \subset \mathbb{R}$, para cierto t, lo cual es imposible. Esto prueba que $H \neq G$ y por lo tanto $u = 2$.

Supongamos que $u = 2$. Tenemos $\epsilon = i^r E^2$, pero no puede ser $i^r = \pm 1$, pues entonces $E \in \mathbb{R}$ o bien $E/i \in \mathbb{R}$, pero $K \cap \mathbb{R} = k$, y concluiríamos que $E \in H$. Así pues, $E^2 = \pm i\,\epsilon$. Si σ_1 es el automorfismo que fija a k, es claro que $\sigma_1(E)^2 = -E^2$, luego $\sigma_1(E) = \pm iE$, y así

$$\eta = E + \sigma_1(E) = E(1 \pm i) \in k.$$

Claramente $(\eta)^2 = (2)$. ∎

Para probar un caso particular de este teorema especialmente sencillo necesitamos un interesante resultado muy simple también:

Teorema 9.10 *Sea $d \neq 1$ un entero libre de cuadrados. Si d tiene un divisor primo $p \equiv -1$ (mód 4) entonces la unidad fundamental de $\mathbb{Q}(\sqrt{d})$ tiene norma positiva.*

Demostración: Sea $(a + b\sqrt{d})/2$ la unidad fundamental de $\mathbb{Q}(\sqrt{d})$. Supongamos que tiene norma -1 y sea $p \neq 2$ un divisor primo de d. Entonces $(a^2 - db^2)/4 = -1$, o sea, $a^2 - db^2 = -4$ y, por lo tanto, $-4 \equiv a^2$ (mód p). De aquí que $1 = (-1/p) = (-1)^{(p-1)/2}$, luego $p \equiv 1$ (mód 4). ∎

Teorema 9.11 *Si p es un primo, el número de clases de $K = \mathbb{Q}(\sqrt{p}, \sqrt{-p})$ es*

$$H = \begin{cases} hh'/2 & \text{si } p \equiv \ \ 1 \text{ (mód 4)}, \\ hh' & \text{si } p \equiv -1 \text{ (mód 4) o } p = 2, \end{cases}$$

donde h y h' son los números de clases de los cuerpos $\mathbb{Q}(\sqrt{p})$ y $\mathbb{Q}(\sqrt{-p})$.

Demostración: Claramente 2 se ramifica en el cuerpo $k = \mathbb{Q}(\sqrt{p})$ si y sólo si $p \equiv -1$ (mód 4) o $p = 2$. Según el teorema 9.9, hay que probar que en tal caso el divisor primo de 2 es principal.

El caso $p = 2$ es inmediato, pues entonces k tiene factorización única. Supongamos, pues, que $p \equiv -1$ (mód 4). El discriminante de k es, por lo tanto, $\Delta = 2p$.

Por el teorema anterior la unidad fundamental de k tiene norma positiva. Esto significa que cada clase de similitud de ideales se descompone en dos clases de similitud estricta. En particular tenemos la clase 1 de los ideales principales

generados por elementos de norma positiva y la clase C de los ideales principales generados por elementos de norma negativa. Estas clases son distintas y cumplen $1^2 = C^2 = 1$, es decir, son lo que en [9.20] llamamos clases ambiguas.

Según [9.22] hay exactamente 2 clases ambiguas, luego no hay más aparte de 1 y C. Ahora bien, si $2 = \mathfrak{p}^2$, la clase $[\mathfrak{p}]$ es obviamente ambigua, luego $\mathfrak{p}$ está en una de las clases 1, C y, en cualquier caso, $\mathfrak{p}$ es principal. ∎

9.4 El teorema de Dirichlet

La consecuencia más importante del teorema de factorización es que, en virtud de la fórmula (9.5), si K/k es una extensión abeliana de cuerpos numéricos y χ es un carácter no principal de K, entonces $L(1,\chi) \neq 0$. Este hecho, que no es trivial en absoluto, y del cual no se conoce ninguna prueba algebraica, contiene la clave para generalizar el teorema de Dirichlet sobre primos en progresiones aritméticas al contexto en que estamos trabajando.

Teorema 9.12 (Teorema de Dirichlet) *Si k es un cuerpo numérico, toda clase de similitud de k módulo un divisor $\mathfrak{m}$ contiene infinitos ideales primos.*

Demostración: Consideremos la función de variable compleja definida para $|z| < 1$ por la serie de Taylor

$$\log \frac{1}{1-z} = \sum_{n=1}^{\infty} \frac{z^n}{n}.$$

Si χ es un carácter modular de k, la convergencia absoluta del producto infinito que define a la función $L(s,\chi)$ equivale a la convergencia absoluta de la serie

$$\log L(s,\chi) = \sum_{\mathfrak{p}} \log \frac{1}{1-\frac{\chi(\mathfrak{p})}{\mathrm{N}(\mathfrak{p})^s}} = \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{\chi(\mathfrak{p})^n}{n\,(\mathrm{N}\,\mathfrak{p})^{sn}}, \qquad \text{para } s > 1.$$

Además esta función es un logaritmo de la función $L(s,\chi)$. Es importante observar que la convergencia no sólo es absoluta en $\mathfrak{p}$, sino que la serie doble también converge absolutamente, ya que si tomamos módulos obtenemos una serie mayorada por la correspondiente a $\chi = 1$. Esto nos permite reordenar los sumandos como queramos.

Separamos los sumandos correspondientes a $n = 1$:

$$\log L(s,\chi) = \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{(\mathrm{N}\,\mathfrak{p})^s} + R(s,\chi), \tag{9.7}$$

donde

$$\begin{aligned} |R(s,\chi)| &= \Big|\sum_{\mathfrak{p},\, n\geq 2} \frac{\chi(\mathfrak{p})^n}{n\,(\mathrm{N}\,\mathfrak{p})^{sn}}\Big| \leq \sum_{\mathfrak{p},\, n\geq 2} \frac{1}{(\mathrm{N}\,\mathfrak{p})^{sn}} = \sum_{\mathfrak{p}} \frac{1}{(\mathrm{N}\,\mathfrak{p})^{2s} - (\mathrm{N}\,\mathfrak{p})^s} \\ &\leq \sum_{\mathfrak{p}} \frac{2}{(\mathrm{N}\,\mathfrak{p})^{2s}} \leq 2\zeta_k(2s). \end{aligned}$$

Vemos así que la función $R(s,\chi)$ permanece acotada a la derecha de 1.

Fijemos ahora un divisor $\mathfrak{m}$ de k y sea χ un carácter del grupo de clases $H(\mathfrak{m}) = I(\mathfrak{m})/P_{\mathfrak{m}}$. En particular el conductor de χ divide a $\mathfrak{m}$ y a lo sumo hay una cantidad finita de primos $\mathfrak{p}$ que dividen a $\mathfrak{m}$ pero no a $\mathfrak{f}_\chi$. Para cualquier otro primo, o bien $\chi(\mathfrak{p}) = 0$ (si $\mathfrak{p} \mid \mathfrak{f}_\chi$) o bien $\mathfrak{p}$ pertenece a una clase de $H(\mathfrak{m})$.

Si añadimos a $R(s,\chi)$ los posibles sumandos de la serie de (9.7) correspondientes a primos que dividen a $\mathfrak{m}$ pero no a $\mathfrak{f}$, seguimos teniendo una función acotada a la derecha de 1, y los sumandos restantes de la serie los podemos separar según su clase módulo $\mathfrak{m}$:

$$\log L(s,\chi) = \sum_{C\in H(\mathfrak{m})} \chi(C) \sum_{\mathfrak{p}\in C} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} + R(s,\chi).$$

Ahora usamos las relaciones de ortogonalidad para despejar la serie correspondiente a una clase fija C_0. Para ello multiplicamos por $\chi(C_0^{-1})$ y sumamos sobre los caracteres módulo $\mathfrak{m}$:

$$\sum_\chi \chi(C_0^{-1}) \log L(s,\chi) = \sum_{C\in H(\mathfrak{m})} \sum_\chi \chi(CC_0^{-1}) \sum_{\mathfrak{p}\in C} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} + R(s,C_0),$$

donde $R(s,C_0)$ es una función acotada a la derecha de 1. Por las relaciones de ortogonalidad [11.16] esta expresión se reduce a

$$\sum_\chi \chi(C_0^{-1}) \log L(s,\chi) = h_{\mathfrak{m}} \sum_{\mathfrak{p}\in C_0} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} + R(s,C_0), \tag{9.8}$$

donde $h_{\mathfrak{m}}$ es el número de clases módulo $\mathfrak{m}$.

Ahora examinemos el miembro izquierdo. Si $\chi \neq 1$, entonces $L(1,\chi) \neq 0$, de donde se sigue que $\log L(s,\chi)$ está acotado a la derecha de 1. En efecto, es sabido que en un entorno del número complejo $L(1,\chi)$ existe una determinación continua del logaritmo $\log_0(z)$. Componiéndola con $L(s,\chi)$ obtenemos una determinación del logaritmo de $L(s,\chi)$ definida en un entorno de 1, digamos en $]1-\epsilon, 1+\epsilon[$. La diferencia $\log_0 L(s,\chi) - \log L(s,\chi)$ es una función continua en $]1, 1+\epsilon[$ que sólo puede tomar valores $2k\pi i$, para k entero, luego por conexión ha de ser constante en $]1, 1+\epsilon[$, lo que implica que existe

$$\lim_{s\to 1^+} \log L(s,\chi) = \log_0 L(1,\chi) + 2k\pi i.$$

Si agrupamos todos los sumandos acotados de (9.8) la expresión se reduce a

$$\log \zeta_k(s) = h_{\mathfrak{m}} \sum_{\mathfrak{p}\in C_0} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} + R(s), \tag{9.9}$$

donde la función $R(s)$ está acotada a la derecha de 1.

Por otra parte, $\zeta_k(s)$ tiende a infinito cuando $s \to 1^+$ (por el teorema 9.2), luego su logaritmo también. Esto obliga a que la serie de la ecuación anterior

tenga infinitos sumandos (o si no estaría acotada en un entorno de 1), luego la clase C_0 contiene infinitos primos. ∎

De la demostración del teorema de Dirichlet podemos extraer mucha más información sobre las clases de ideales. Para ello observamos en primer lugar que, según el teorema 9.2, la función $h(s) = (s-1)\zeta_k(s)$ está acotada inferiormente a la derecha de 1 por una cota positiva, luego

$$\log \zeta_k(s) = \log \frac{1}{s-1} + \log h(s),$$

donde la función $\log h(s)$ está acotada a la derecha de 1.

La fórmula (9.7) para el carácter principal $\chi = 1$ se convierte en

$$\log \zeta_k(s) = \sum_{\mathfrak{p}} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} + R(s),$$

donde $R(s)$ es una función acotada a la derecha de 1. De las dos últimas fórmulas se sigue que existe

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s}}{\log \frac{1}{s-1}} = 1$$

Definición 9.13 Sea k un cuerpo numérico. Definimos la *densidad de Dirichlet* de un conjunto P de ideales primos de k como

$$d(P) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in P} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s}}{\log \frac{1}{s-1}}.$$

Este límite no tiene por qué existir, por lo que no todo conjunto de primos tiene necesariamente densidad de Dirichlet. Acabamos de probar que el conjunto P de todos los primos de k cumple $d(P) = 1$.

En estos términos, lo que hemos obtenido en la demostración del teorema de Dirichlet (fórmula (9.9)) es que si C es una clase de similitud módulo un divisor $\mathfrak{m}$, entonces existe

$$d(C) = \frac{1}{h_{\mathfrak{m}}}.$$

(Aquí, y en lo sucesivo, adoptamos el convenio de que $d(C)$, para un conjunto C de ideales fraccionales, es la densidad del conjunto de los primos que contiene.)

Para extraer las consecuencias de este hecho nada trivial observemos primero que se cumplen algunas propiedades obvias:

a) Si $P = P_1 \cup P_2$ es una unión disjunta de dos conjuntos de primos de k y dos de los tres conjuntos P, P_1 y P_2 tienen densidad de Dirichlet, entonces el tercero también la tiene, y $d(P) = d(P_1) + d(P_2)$.

b) Si $P_1 \subset P_2$ son conjuntos de primos con densidad de Dirichlet, entonces $d(P_1) \leq d(P_2)$.

c) Si P_2 es un conjunto de primos con $d(P_2) = 0$ y $P_1 \subset P_2$, entonces P_1 tiene densidad de Dirichlet y $d(P_1) = 0$. (Aquí adoptamos el convenio $d(\varnothing) = 0$.)

d) Todo conjunto finito tiene densidad de Dirichlet nula.

En primer lugar refinamos el teorema de Dirichlet considerando grupos de clases arbitrarios (no necesariamente módulo un divisor):

Teorema 9.14 *Sea K/k una extensión abeliana de cuerpos numéricos y sea H un grupo de clases de K sobre k. Entonces cada clase de ideales C módulo H tiene densidad de Dirichlet $d(C) = |K : k|^{-1}$.*

DEMOSTRACIÓN: Sea $\mathfrak{m}$ un divisor de k tal que $P_\mathfrak{m} \subset H \subset I(\mathfrak{m})$. Entonces

$$|K : k| = |I(\mathfrak{m}) : H| = \frac{|I(\mathfrak{m}) : P_\mathfrak{m}|}{|H : P_\mathfrak{m}|},$$

luego

$$|K : k|^{-1} = |H : P_m| \frac{1}{h_\mathfrak{m}} = d(C),$$

pues C es la unión disjunta de $|H : P_\mathfrak{m}|$ clases de densidad $1/h_\mathfrak{m}$. ∎

Ahora ya podemos obtener consecuencias sobre grupos de clases. Observemos en primer lugar que este teorema proporciona una interpretación a los teoremas 7.15 y 7.17. Los primos de los que habla 7.15 son simplemente los contenidos en cualquier clase no trivial del grupo de clases, mientras que los primos de 7.17 son los de la clase que genera el grupo de clases de la extensión cíclica.

Definición 9.15 Diremos que dos conjuntos de ideales fraccionales P_1 y P_2 de un cuerpo numérico k son *casi iguales* (y lo representaremos $P_1 \approx P_2$) si el conjunto de los ideales primos que están en P_1 y no en P_2 o viceversa tiene densidad de Dirichlet nula.

Teorema 9.16 *Dos grupos de ideales de un cuerpo numérico son equivalentes si y sólo si son casi iguales.*

DEMOSTRACIÓN: Sean H_1 y H_2 dos grupos de ideales de un cuerpo numérico k y sea $\mathfrak{m}$ el mínimo común múltiplo de los divisores respecto a los que están definidos. Llamemos $H_1' = H_1 \cap I(\mathfrak{m})$, $H_2' = H_2 \cap I(\mathfrak{m})$.

Tenemos que H_i es equivalente a H_i' y $H_i \approx H_i'$ (pues se diferencian en un número finito de primos). Por lo tanto podemos suponer que H_1 y H_2 están definidos módulo un mismo divisor $\mathfrak{m}$. Hemos de probar que si son casi iguales entonces son iguales.

Notemos ahora que $H_1 \approx H_1 \cap H_2 \approx H_2$, luego basta demostrar el teorema bajo la hipótesis adicional de que $H_1 \subset H_2$. Ahora bien, por el teorema anterior,

$$|I(\mathfrak{m}) : H_1| = d(H_1) = d(H_2) = |I(\mathfrak{m}) : H_2|,$$

luego $H_1 = H_2$. ∎

En términos de extensiones abelianas el teorema anterior se expresa como sigue:

Teorema 9.17 *Sea k un cuerpo numérico, H un grupo de ideales de k y K una extensión abeliana de k. Entonces*

$$H \leftrightarrow K \quad \leftrightarrow \quad \{\mathfrak{p} \mid \mathfrak{p} \in H\} \approx \{\mathfrak{p} \mid \mathfrak{p} \text{ se escinde completamente en } K\}.$$

DEMOSTRACIÓN: Sea H' el grupo de clases maximal de K. Entonces el conjunto $\{\mathfrak{p} \mid p \in H'\}$ es el conjunto de los primos que se escinden completamente en K. Lo que hay que probar es que H es equivalente a H' si y sólo si $H \approx H'$, pero eso es lo que afirma el teorema anterior. ∎

En particular, dos extensiones abelianas finitas de un mismo cuerpo numérico son iguales si y sólo si en ellas se escinden completamente casi los mismos primos del cuerpo base.

Ejercicio: Sean K_1 y K_2 dos extensiones abelianas finitas de un cuerpo numérico k. Demostrar que $K_1 \subset K_2$ si y solo si casi todos los primos de k que se escinden completamente en K_2 se escinden completamente en K_1.

Los teoremas anteriores siguen siendo ciertos si entendemos "casi iguales" como "iguales salvo un número finito de excepciones". Tenemos así versiones más débiles de estos resultados pero que no involucran la noción de densidad de Dirichlet. No obstante, la versión fuerte es mucho más potente, pues nos permite aprovechar, por ejemplo, el teorema siguiente:

Teorema 9.18 *Si k es un cuerpo numérico, el conjunto de los ideales primos de k con grado de inercia 1 sobre $\mathbb{Q}$ tiene densidad de Dirichlet igual a 1.*

DEMOSTRACIÓN: Si $\mathfrak{p}_2$ recorre los primos de k con grado de inercia mayor que 1 sobre el primo p de $\mathbb{Q}$ al cual dividen, se cumple que $\mathrm{N}\,\mathfrak{p}_2 \geq p^2$ luego, si n es el grado de k y $s > 1/2$,

$$\sum_{\mathfrak{p}_2} \frac{1}{(\mathrm{N}\,\mathfrak{p}_2)^s} \leq n \sum_p \frac{1}{p^{2s}} \leq n\,\zeta(2s).$$

Esto prueba que la serie permanece acotada a la derecha de 1, luego la densidad de los primos $\mathfrak{p}_2$ existe y es nula. ∎

De aquí se sigue que dos conjuntos de primos son casi iguales si y sólo si contienen casi los mismos primos de grado 1. Así, por ejemplo, para demostrar que dos extensiones abelianas finitas de un mismo cuerpo numérico son iguales,

basta comprobar que los primos de grado 1 que se escinden completamente en cada una de ellas son los mismos salvo a lo sumo un número finito de excepciones.

Una de las razones por las que los resultados de este tipo son interesantes es porque se generalizan a extensiones no abelianas. Veamos un ejemplo:

Teorema 9.19 (Tchebotarev) *Sea K/k una extensión de Galois de cuerpos numéricos y sea $\sigma \in G(K/k)$. Sea c el cardinal de la clase de conjugación de σ y $n = |K : k|$. Entonces, el conjunto de los primos $\mathfrak{p}$ de k no ramificados en K y tales que existe un primo $\mathfrak{P} \mid \mathfrak{p}$ en K tal que*

$$\sigma = \left(\frac{K/k}{\mathfrak{P}}\right)$$

tiene densidad de Dirichlet igual a c/n.

Demostración: Sea f el orden de σ y sea L su cuerpo fijado, de modo que $k \subset L \subset K$ y la extensión K/L es cíclica de grado f. Sea $\mathfrak{m}$ un divisor admisible para la extensión K/L y sea H un grupo de clases módulo $\mathfrak{m}$, de modo que tenemos el isomorfismo de Artin $I(\mathfrak{m})/H \longrightarrow G(K/L)$. Llamemos S al conjunto de los primos $\mathfrak{p}$ de k que cumplen el teorema y que son primos con $\mathfrak{m}$. Así mismo, sea S_K el conjunto de los primos $\mathfrak{P}$ de K que cumplen el teorema para un primo $\mathfrak{p} \in S$.

Fijado $\mathfrak{P} \in S_K$, sea $\mathfrak{q}$ el primo de L y $\mathfrak{p}$ el primo de k de manera que $\mathfrak{p} \mid \mathfrak{q} \mid \mathfrak{P}$. Tenemos que el grupo de descomposición $G_{\mathfrak{P}}$ para la extensión K/k está generado por σ, luego es $G(K/L)$. Esto implica que $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{q}) = f$ y $f(\mathfrak{q}/\mathfrak{p}) = 1$. En particular, como no hay ramificación, $\mathfrak{P} = \mathfrak{q}$. Además

$$\sigma = \left(\frac{K/k}{\mathfrak{P}}\right) = \left(\frac{K/L}{\mathfrak{P}}\right) = \left(\frac{K/L}{\mathfrak{q}}\right).$$

Si C es la clase de ideales correspondiente a σ por el isomorfismo de Artin, tenemos que $\mathfrak{q} \in C$.

Llamemos S_L al conjunto de los primos $\mathfrak{q}$ de L tales que $\mathfrak{q} \in C$ y $f(\mathfrak{q}/\mathfrak{p}) = 1$, donde $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{q}$. Acabamos de probar que si $\mathfrak{P} \in S_K$, el primo $\mathfrak{q} \in L$ al cual divide cumple $\mathfrak{q} \in S_L$ y, recíprocamente, si $\mathfrak{q} \in S_L$ y $\mathfrak{P}$ es un divisor primo de $\mathfrak{q}$ en K, entonces

$$\sigma = \left(\frac{K/L}{\mathfrak{q}}\right) = \left(\frac{K/L}{\mathfrak{P}}\right) = \left(\frac{K/k}{\mathfrak{P}}\right),$$

luego $\mathfrak{P} \in S_K$. Vemos, pues, que los primos $\mathfrak{q} \in S_L$ se corresponden biunívocamente (de hecho, se identifican) con los primos $\mathfrak{P} \in S_K$.

Por el teorema anterior, el conjunto S_L tendrá densidad de Dirichlet si y sólo si lo tiene el conjunto de sus primos de grado 1 (y en tal caso ambos tendrán la misma densidad). Ahora bien, los primos de grado 1 de S_L son simplemente los primos de grado 1 de la clase C, pues la condición $f(\mathfrak{q}/\mathfrak{p}) = 1$ se cumple trivialmente. Así pues, el teorema 9.14 nos da que S_L tiene densidad $1/f$.

Por otra parte, cada primo $\mathfrak{p} \in S_k$ tiene al menos un divisor $\mathfrak{q} \in S_L$. Si $\mathfrak{q}_1$ y $\mathfrak{q}_2$ son dos de ellos, entonces existe un $\tau \in G(K/k)$ tal que $\mathfrak{q}_1 = \mathfrak{q}_2^\tau$ (donde identificamos a $\mathfrak{q}_1$ y $\mathfrak{q}_2$ con primos de K). Además

$$\sigma = \left(\frac{K/L}{\mathfrak{q}_1}\right) = \left(\frac{K/L}{\mathfrak{q}_2^\tau}\right) = \left(\frac{K/L}{\mathfrak{q}_2}\right)^\tau = \sigma^\tau.$$

Recíprocamente, si $\sigma^\tau = \sigma$ y $\mathfrak{q} \in S_L$ divide a $\mathfrak{p}$, lo mismo le sucede a $\mathfrak{q}^\tau$. Concluimos que el número de divisores en S_L de un primo de S_k es $|G_\sigma : G_\mathfrak{q}|$, donde G_σ es el centralizador de σ en $G(K/k)$ (el grupo de los $\tau \in G(K/k)$ tales que $\sigma^\tau = \sigma$) y $G_\mathfrak{q}$ es el grupo de descomposición de $\mathfrak{q}$ (formado por los $\tau \in G(K/k)$ tales que $\mathfrak{q}^\tau = \mathfrak{q}$).

Es claro que $|G_\sigma| = n/c$, mientras que $|G_\mathfrak{q}| = f$, luego concluimos que cada primo $\mathfrak{p} \in S_k$ es divisible entre n/fc primos de S_L. Por consiguiente,

$$d(S_k) = \lim_{s\to 1^+} \frac{\sum\limits_{\mathfrak{p}\in S_k} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s}}{\log\frac{1}{s-1}} = \frac{fc}{n} \lim_{s\to 1^+} \frac{\sum\limits_{\mathfrak{p}\in S_k}\sum\limits_{\mathfrak{q}|\mathfrak{p}} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s}}{\log\frac{1}{s-1}}$$

$$= \frac{fc}{n} \lim_{s\to 1^+} \frac{\sum\limits_{\mathfrak{p}\in S_k}\sum\limits_{\mathfrak{q}|\mathfrak{p}} \frac{1}{(\mathrm{N}\,\mathfrak{q})^s}}{\log\frac{1}{s-1}} = \frac{fc}{n} \lim_{s\to 1^+} \frac{\sum\limits_{\mathfrak{q}\in S_L} \frac{1}{(\mathrm{N}\,\mathfrak{q})^s}}{\log\frac{1}{s-1}} = \frac{fc}{n} d(S_L) = \frac{c}{n}.$$

Se entiende que el sumatorio sobre $\mathfrak{q} \mid \mathfrak{p}$ recorre los primos $\mathfrak{q} \in S_L$ que dividen a $\mathfrak{p}$. Hemos usado que $\mathrm{N}(\mathfrak{q}) = \mathrm{N}(\mathfrak{p})$ porque $f(\mathfrak{q}/\mathfrak{p}) = 1$. ∎

Este teorema es una extensión de 9.14. En particular, si lo aplicamos a $\sigma = 1$ obtenemos el siguiente caso particular:

Teorema 9.20 *Si K/k es una extensión de Galois de cuerpos numéricos, entonces el conjunto de los primos de k que se escinden completamente en K tiene densidad de Dirichlet igual a $|K : k|^{-1}$.*

Ahora podemos generalizar el teorema 9.17:

Teorema 9.21 *Sean K/k y E/k dos extensiones de cuerpos numéricos, la primera de Galois. Si casi todos los primos de k que se escinden completamente en K también se escinden completamente en E, entonces $E \subset K$.*

Demostración: Si un primo $\mathfrak{p}$ de k se escinde completamente en K y K' es un cuerpo conjugado con K sobre k, entonces $\mathfrak{p}$ se escinde completamente en K', luego, de hecho, $\mathfrak{p}$ se escinde completamente en la clausura normal L de k sobre K. El recíproco es trivial, luego podemos suponer que E/k es normal.

La extensión KE/k es de Galois y casi todo primo de k que se escinde completamente en K también se escinde completamente en E, luego también en KE. Si probamos el teorema para K y KE tendremos que $KE \subset K$, luego $E \subset K$. Equivalentemente, podemos suponer que $K \subset E$. Ahora bien, el teorema anterior nos da entonces que $|K : k|^{-1} \leq |E : k|^{-1}$, luego $E = K$. ∎

En particular, si en dos extensiones normales de un cuerpo numérico se escinden completamente casi los mismos primos, ambas coinciden.

9.5 La segunda desigualdad fundamental

En esta sección daremos una prueba analítica de la segunda desigualdad fundamental usando funciones dseta y funciones L. Los resultados que veremos aquí no serán necesarios más adelante. Supondremos que el lector está familiarizado con las funciones de variable compleja, en especial con las series de Dirichlet, es decir, funciones de la forma

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

donde los coeficientes a_n son números complejos.

En lo sucesivo $s = \sigma + i\tau$ será una variable compleja. Esto significa que cuando hablemos de σ y τ se entenderá que son la parte real y la parte compleja de s respectivamente. Es conocido que si una serie de dirichlet converge en un punto s_0, entonces converge en todo el semiplano $\sigma > \sigma_0$ a una función analítica.

Las funciones L nos plantean ahora un problema. Recordemos que, si χ es un carácter modular en un cuerpo numérico k, hemos definido $L(s,\chi)$ como la serie determinada por el carácter primitivo que induce a χ. Sin embargo, dado que queremos probar la segunda desigualdad fundamental, no podemos apoyarnos en la teoría de cuerpos de clases, y en la discusión de los caracteres inducidos la hemos usado. Lo más sencillo es redefinir $L(s,\chi)$ para un carácter módulo $\mathfrak{m}$ como

$$L(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{(\mathrm{N}\,\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{(\mathrm{N}\,\mathfrak{p})^s}},$$

es decir, sin pasar al carácter primitivo.

Esta serie $L(s,\chi)$ puede reescribirse como una serie de Dirichlet (9.1) con los coeficientes (9.2). El teorema 9.7 vale igual con esta nueva definición (trabajando con $\mathfrak{m}$ en lugar de con el conductor de χ) y así obtenemos que $L(s,\chi)$ converge en el intervalo $]1-1/n, +\infty[$ y, en consecuencia, en el semiplano $\sigma > 1 - 1/n$. Es fácil ver que el desarrollo en producto infinito también es válido en este semiplano.

Comparando los desarrollos en producto de $L(s,\chi)$ según la definición que adoptamos ahora y la que habíamos dado antes, vemos que ambas funciones se diferencian a lo sumo en un número finito de factores (los correspondientes a los primos que dividen a $\mathfrak{m}$ y no al conductor). En definitiva, se diferencian en un factor entero que no se anula en todo $\mathbb{C}$. Observar que si χ es el carácter principal módulo $\mathfrak{m}$, ahora ya no es cierto que $L(s,\chi) = \zeta_k(s)$ (sí es cierto si $\mathfrak{m} = 1$).

El teorema siguiente es una consecuencia sencilla de 9.6 y de él se sigue inmediatamente que $\zeta_k(s)$ se prolonga a una función meromorfa en el semiplano $\sigma > 1 - 1/n$ con un único polo en 1. Usaremos el hecho conocido de que la función dseta de Riemann usual se prolonga a una función meromorfa en $\mathbb{C}$ con un único polo simple en 1 con residuo 1. De hecho nos basta con saber que se prolonga al semiplano $\sigma > 0$.

Teorema 9.22 *Sea una serie de Dirichlet*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

y para cada k sea $A_k = a_1 + \cdots + a_k$. Supongamos que existen un $\rho \in \mathbb{C}$ y unos números reales $C > 0$ y $0 \le \sigma_1 < 1$ tales que para cada k se cumpla $|A_k - k\rho| \le Ck^{\sigma_1}$. Entonces la serie define una función analítica en el semiplano $\sigma > 1$ que se prolonga analíticamente al semiplano $\sigma > \sigma_1$ salvo un polo simple en $s = 1$ con residuo ρ (entendiendo que si $\rho = 0$ entonces la extensión es analítica en 1).

Demostración: Basta considerar la serie de Dirichlet $f(s) - \rho\,\zeta(s)$. Sus coeficientes satisfacen las condiciones del teorema 9.6, luego converge en el semiplano $\sigma > \sigma_1$. Como la serie de $\zeta(s)$ converge en $\sigma > 1$, lo mismo le ocurre a la serie de $f(s)$. Como $\zeta(s)$ se extiende a una función analítica en $\sigma > \sigma_1$ con un polo simple en $s = 1$, lo mismo vale para $f(s)$. También es claro que el residuo es ρ. ∎

De aquí deducimos ya el comportamiento de las funciones dseta. Para el caso en que $f(s)$ es la función $\zeta_C(s, \mathfrak{m})$, la suma A_k es precisamente la función $j_C(k)$, y según 5.13 tenemos que $|A_k - k\rho| \le Ck^{1-1/n}$, donde ρ es la constante que aparece en el teorema. Por consiguiente:

Teorema 9.23 *Sea K un cuerpo numérico de grado n con s primos infinitos reales y t complejos, sea Δ el discriminante de K, sea $\mathfrak{m}$ un divisor de K, sea $R_\mathfrak{m}$ el regulador módulo $\mathfrak{m}$ y $w_\mathfrak{m}$ el número de raíces de la unidad contenidas en el grupo de unidades $U_\mathfrak{m}$. Sea C una clase de similitud de ideales módulo $\mathfrak{m}$. Entonces*

a) La serie

$$\zeta_C(s, \mathfrak{m}) = \sum_{\mathfrak{a} \in C} \frac{1}{(\mathrm{N}\,\mathfrak{a})^s}$$

converge en el semiplano $\sigma > 1$ a una función analítica que se prolonga analíticamente al semiplano $\sigma > 1 - 1/n$ salvo un polo simple en $s = 1$ con residuo

$$\rho = \frac{2^s (2\pi)^t R_\mathfrak{m}}{(\mathrm{N}\,\mathfrak{m})\, w_\mathfrak{m} \sqrt{|\Delta|}}.$$

b) La serie

$$\zeta(s, \mathfrak{m}) = \sum_{\mathfrak{a} \in I(\mathfrak{m})} \frac{1}{(\mathrm{N}\,\mathfrak{a})^s}$$

converge en el semiplano $\sigma > 1$ a una función analítica que se prolonga analíticamente al semiplano $\sigma > 1 - 1/n$ salvo un polo simple en $s = 1$ con residuo

$$\rho h_\mathfrak{m} = \frac{2^s (2\pi)^t R_\mathfrak{m}}{(\mathrm{N}\,\mathfrak{m})\, w_\mathfrak{m} \sqrt{|\Delta|}}\, h_\mathfrak{m}.$$

Usaremos la notación $f \sim g$ para indicar que la función $f - g$ se extiende a una función analítica alrededor de 1.

Por ejemplo, en la prueba del teorema de Dirichlet hemos construido los logaritmos $\log L(s,\chi)$. Es fácil ver que el desarrollo en producto de Euler de las funciones L es válido en el semiplano $\sigma > 1$, por lo que el logaritmo también está definido en este semiplano. Ahora observamos que la función $R(s,\chi)$ que aparece en (9.7) está definida y es analítica en el semiplano $\sigma > 1/2$, pues la acotación tras (9.7) es válida en dicho semiplano (tras la primera desigualdad hay que sustituir s por σ y la penúltima desigualdad es válida salvo para los primos $\mathfrak{p}$ para los cuales $(\mathrm{N}\,\mathfrak{p})^\sigma$ no sea mayor que 2, pero éstos son un número finito y no afectan a la conclusión). Por consiguiente

$$\log L(s,\chi) \sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{(\mathrm{N}\,\mathfrak{p})^s}. \tag{9.10}$$

Todavía podemos afinar más: si nos restringimos al caso del carácter principal módulo 1 tenemos

$$\log \zeta_k(s) \sim \sum_{\mathfrak{p}} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s}.$$

Si $\mathfrak{p}_2$ recorre los primos de k con grado de inercia mayor que 1 sobre el primo p de $\mathbb{Q}$ al cual dividen, se cumple que $\mathrm{N}\,\mathfrak{p}_2 \geq p^2$ luego, si n es el grado de k,

$$\Big|\sum_{\mathfrak{p}_2} \frac{1}{(\mathrm{N}\,\mathfrak{p}_2)^s}\Big| \leq n \sum_{p} \frac{1}{p^{2\sigma}} \leq n\,\zeta(2\sigma).$$

Usando que la función dseta de Riemann es decreciente y el criterio de mayoración de Weierstrass concluimos que la serie converge a una función analítica en el semiplano $\sigma > 1/2$.

Por consiguiente, si $\mathfrak{p}_1$ recorre los primos de k con grado de inercia 1 sobre $\mathbb{Q}$ tenemos

$$\log \zeta_k(s) \sim \sum_{\mathfrak{p}_1} \frac{1}{(\mathrm{N}\,\mathfrak{p}_1)^s}.$$

Consideremos ahora la función $h(s) = (s-1)\zeta_k(s)$, que es analítica en el semiplano $\sigma > 1 - 1/n$ y $h(1) \neq 0$. Tenemos, por consiguiente, un logaritmo $\log h(s)$ definido alrededor de 1. Podemos elegirlo adecuadamente para que, si $\sigma > 1$,

$$\log h(s) = \log(s-1) + \log \zeta_k(s),$$

donde $\log(s-1)$ extiende al logaritmo real y $\log \zeta_k(s)$ es el logaritmo que ya teníamos definido. Concluimos que

$$\log \zeta_k(s) \sim \log \frac{1}{s-1}.$$

Resumimos lo que hemos probado:

Teorema 9.24 *Sea k un cuerpo numérico. Entonces*

$$\log \zeta_k(s) \sim \sum_{\mathfrak{p}} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} \sim \sum_{\mathfrak{p}_1} \frac{1}{(\mathrm{N}\,\mathfrak{p}_1)^s} \sim \log \frac{1}{s-1},$$

donde $\mathfrak{p}$ recorre los primos de k y $\mathfrak{p}_1$ recorre los primos con grado de inercia 1 sobre $\mathbb{Q}$.

En particular vemos que todo cuerpo numérico tiene infinitos primos con grado de inercia 1 sobre $\mathbb{Q}$ (esto ya lo probamos en [11.10]). Ahora ya podemos probar:

Teorema 9.25 (Segunda desigualdad fundamental) *Sea K/k una extensión de cuerpos numéricos (no necesariamente abeliana) y $\mathfrak{m}$ un divisor de k. Entonces*

$$|I(\mathfrak{m}) : P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})| \le |K : k|.$$

Demostración: Llamemos $T = P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$ y $t = |I(\mathfrak{m}) : T|$. Sea χ un carácter no principal de $I(\mathfrak{m}) : P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$. Claramente χ induce un carácter módulo $\mathfrak{m}$. Sea $m(\chi)$ el orden del cero de $L(s,\chi)$ en $s = 1$ (vamos a probar que $m(\chi) = 0$, es decir, que $L(1,\chi) \neq 0$.

Sea $L(s,\chi) = (s-1)^{m(\chi)} g(s,\chi)$, donde g es una función analítica que no se anula en un entorno de 1. Entonces g tiene un logaritmo L_g analítico en un entorno de 1 y la función $m(\chi)\log(s-1) + L_g(s)$ es un logaritmo de $L(s,\chi)$, luego se diferencia en una constante de $\log L(s,\chi)$, es decir,

$$\log L(s,\chi) \sim m(\chi)\log(s-1) = -m(\chi)\log\frac{1}{s-1}. \tag{9.11}$$

Por otra parte podemos escribir (9.10) en la forma

$$\log L(s,\chi) \sim \sum_C \chi(C) \sum_{\mathfrak{p}\in C} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s},$$

donde C recorre las clases de $I(\mathfrak{m})/T$.

Esta última igualdad es cierta también para el carácter principal χ_1, donde se reduce a

$$\log L(s,\chi_1) \sim \sum_{\mathfrak{p}\in I(\mathfrak{m})} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} \sim \sum_{\mathfrak{p}} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} \sim \log \zeta_k(s).$$

En la última equivalencia hemos usado el teorema 9.24. Sumando para todos los caracteres de $I(\mathfrak{m})/T$ obtenemos

$$\log \zeta_k(s) + \sum_{\chi\neq\chi_1} \log L(s,\chi) \sim \sum_C \Big(\sum_\chi \chi(C)\Big) \sum_{\mathfrak{p}\in C} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s}.$$

Aplicamos (9.11), el teorema 9.24 y las relaciones de ortogonalidad, con lo que obtenemos

$$\Big(1 - \sum_{\chi\neq\chi_1} m(\chi)\Big) \log\frac{1}{s-1} \sim t \sum_{\mathfrak{p}\in T} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s}.$$

Ahora observamos lo siguiente: si un primo $\mathfrak{p}$ de k se escinde completamente en K entonces coincide con la norma de cualquiera de sus divisores en K, luego está en $\mathrm{N}(\mathfrak{m})$ (y por lo tanto en T) salvo si $\mathfrak{p} \mid \mathfrak{m}$. Así pues, T contiene a todos los primos de k que se escinden completamente en K excepto a un número finito de ellos.

Si llamamos E al conjunto de los primos de k que se escinden completamente en K y consideramos valores reales $s \geq 1$ tenemos que

$$t \sum_{\mathfrak{p}\in T} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} \geq t \sum_{\mathfrak{p}\in E} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} - u(s),$$

donde $u(s)$ es t veces la suma para los primos de E que no están en T, o sea, una función entera. Sea F el conjunto de primos de K que se escinden completamente sobre k. Si llamamos $n = |K : k|$, cada primo $\mathfrak{p} \in E$ divide exactamente a n primos $\mathfrak{P} \in F$ con la misma norma. Por lo tanto

$$t \sum_{\mathfrak{p}\in E} \frac{1}{(\mathrm{N}\,\mathfrak{p})^s} - u(s) = \frac{t}{n} \sum_{\mathfrak{P}\in F} \frac{1}{(\mathrm{N}\,\mathfrak{P})^s} - u(s).$$

Ahora, si $\mathfrak{P}_1$ es un primo de K con grado de inercia 1 sobre $\mathbb{Q}$, entonces también tiene grado de inercia 1 sobre k y, si además no se ramifica sobre k, entonces se escinde completamente sobre k. Así, todos los primos $\mathfrak{P}_1$ con grado de inercia 1 sobre $\mathbb{Q}$ están en F salvo un número finito de ellos y, por lo tanto,

$$\frac{t}{n} \sum_{\mathfrak{P}\in F} \frac{1}{(\mathrm{N}\,\mathfrak{P})^s} - u(s) \geq \frac{t}{n} \sum_{\mathfrak{P}_1} \frac{1}{(\mathrm{N}\,\mathfrak{P})^s} - v(s),$$

donde $v(s)$ es $u(s)$ más t/n veces la suma sobre los primos $\mathfrak{P}_1$ que no están en F, que es también una función entera.

Reuniendo todos estos hechos y aplicando el teorema 9.24 concluimos

$$\Big(1 - \sum_{\chi\neq\chi_1} m(\chi)\Big) \log\frac{1}{s-1} + w(s) \geq \frac{t}{n} \log\frac{1}{s-1}$$

donde $w(s)$ es una cierta función analítica en un entorno de 1. Tomando $s < 2$ el logaritmo es positivo y podemos dividir sin invertir la desigualdad. Tomando límites cuando $s \to 1^+$ queda

$$1 - \sum_{\chi\neq\chi_1} m(\chi) \geq \frac{t}{n}.$$

Esto sólo es posible si cada $m(\chi) = 0$ y $t \leq n$. ∎

Este teorema proporciona una prueba alternativa de que $L(1,\chi) \neq 0$ cuando χ es un carácter no principal (usando la teoría de cuerpos de clases pero no el teorema de factorización). En efecto, hemos visto que esto es cierto suponiendo que exista una extensión K de k tal que $P_{\mathfrak{m}} = P_{\mathfrak{m}}\,\mathrm{N}(\mathfrak{m})$, es decir, suponiendo que $P_{\mathfrak{m}}$ tenga un cuerpo de clases.

Capítulo X

Teoría de la ramificación

Sabemos que el diferente, el discriminante y el conductor de una extensión abeliana de cuerpos numéricos son divisibles exactamente entre los primos ramificados, pero no sabemos nada sobre los exponentes con que aparecen dichos primos. (Tan sólo el teorema 3.15 nos da una mínima información sobre las multiplicidades de los primos en el diferente.) Sucede que estos exponentes también están relacionados con el modo en que los primos se ramifican en una extensión, por lo que ahora estudiaremos más a fondo este proceso de ramificación. De este estudio no sólo obtendremos consecuencias de gran interés teórico, sino también resultados valiosísimos para el cálculo de diferentes, discriminantes y conductores en casos concretos.

En el capítulo I obtuvimos los primeros resultados en torno a la descomposición de un primo $\mathfrak{p}$ en una extensión de Galois K/k. Concretamente, en el teorema 1.41 vimos que si $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en K, la factorización de $\mathfrak{p}$ puede descomponerse en tres pasos, correspondientes a los cuerpos F y Z fijados por los grupos de descomposición y de inercia de $\mathfrak{P}$ respectivamente. En el primer paso el primo $\mathfrak{p}$ se escinde de sus conjugados sin aumentar el grado de inercia ni el índice de ramificación, en el segundo paso aumenta únicamente el grado de inercia y en el tercero se produce la ramificación. Es este último tramo el que ahora vamos a estudiar con más detalle, descomponiéndolo en más pasos intermedios.

El proceso es más claro si la extensión es abeliana, pues entonces todos los divisores de $\mathfrak{p}$ tienen el mismo cuerpo de descomposición F y el mismo cuerpo de inercia Z (ya que sus grupos de Galois son conjugados, luego iguales). Entonces la descomposición de $\mathfrak{p}$ en F es de la forma $\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, donde el grado de inercia de todos los factores es 1, es decir, $\mathfrak{p}$ se escinde completamente en F. De hecho sabemos por 8.15 que F es el mayor cuerpo intermedio donde esto ocurre. Cada factor $\mathfrak{p}_i$ sigue siendo primo en Z, luego la descomposición de $\mathfrak{p}$ no varía, pero el grado de inercia de cada factor aumenta todo lo que va a aumentar en la extensión K/k. Al pasar de Z a K todos los primos se ramifican y obtenemos la descomposición completa $\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$.

Los nuevos pasos intermedios que vamos a considerar entre Z y K los obten-

dremos definiendo una cadena de subgrupos del grupo de inercia. Recordemos que si E/D es una extensión finita de Galois de dominios de Dedekind, $\mathfrak{P}$ es un primo en E, $\mathfrak{p}$ es su divisor en D y la extensión $\overline{E}/\overline{D}$ de los cuerpos de restos determinados por $\mathfrak{P}$ y $\mathfrak{p}$ es separable, entonces el grupo de inercia $T_\mathfrak{P}$ es el núcleo del epimorfismo $G_\mathfrak{P} \longrightarrow G(\overline{E}/\overline{D})$ dado por $\overline{\sigma}([\alpha]) = [\sigma(\alpha)]$, luego

$$T_\mathfrak{P} = \{\sigma \in G_\mathfrak{P} \mid \sigma(\alpha) \equiv \alpha \text{ (mód } \mathfrak{P}) \text{ para todo } \alpha \in E\}.$$

Éste será nuestro punto de partida.

10.1 Grupos y cuerpos de ramificación

Definición 10.1 Sea E/D una extensión finita de Galois de dominios de Dedekind, sea K/k la extensión de sus cuerpos de cocientes, sea $\mathfrak{P}$ un ideal primo en E y sea $\mathfrak{p}$ el primo de D divisible entre $\mathfrak{P}$. Supongamos que la extensión $\overline{E}/\overline{D}$ de los cuerpos de restos determinados por $\mathfrak{P}$ y $\mathfrak{p}$ es separable. Para cada número natural $i \geq 0$ definimos el i-ésimo *grupo de ramificación* de $\mathfrak{P}$ como

$$G^i_\mathfrak{P} = \{\sigma \in G_\mathfrak{P} \mid \sigma(\alpha) \equiv \alpha \text{ (mód } \mathfrak{P}^{i+1}) \text{ para todo } \alpha \in E\},$$

donde $G_\mathfrak{P} = \{\sigma \in G(E/D) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ es el grupo de descomposición de $\mathfrak{P}$.

Claramente tenemos las inclusiones

$$\cdots\ G^{i+1}_\mathfrak{P} \ \leq\ G^i_\mathfrak{P} \ \leq\ \cdots \ \leq\ G^0_\mathfrak{P} \ \leq\ G_\mathfrak{P}.$$

Además, según los comentarios precedentes, el grupo $G^0_\mathfrak{P}$ no es sino el grupo de inercia de $\mathfrak{P}$. A veces conviene adoptar el convenio de que $G_\mathfrak{P} = G^{-1}_\mathfrak{P}$. Cuando no haya confusión suprimiremos el subíndice $\mathfrak{P}$.

A la hora de calcular explícitamente los grupos de ramificación de una extensión E/D resulta útil la observación siguiente: si $E = D[\alpha_1, \ldots, \alpha_n]$, entonces

$$G^i_\mathfrak{P} = \{\sigma \in G_\mathfrak{P} \mid \sigma(\alpha_j) \equiv \alpha_j \text{ (mód } \mathfrak{p}^{i+1}) \text{ para } j = 1, \ldots, n\}.$$

Así reducimos a un número finito las condiciones para que un automorfismo pertenezca a un grupo de ramificación.

El i-ésimo *cuerpo de ramificación* de $\mathfrak{P}$ será el cuerpo K_i fijado por G_i. Entonces K_0 es el cuerpo de inercia y, llamando F al cuerpo de descomposición, tenemos las inclusiones

$$k \subset F \subset K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K$$

Si K/k es una extensión de Galois de cuerpos numéricos, $\mathfrak{P}$ es un primo en K y $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$, sabemos que el grupo de descomposición $G_\mathfrak{P}$ es isomorfo al grupo local $G(K_\mathfrak{P}/k_\mathfrak{p})$ y es inmediato comprobar que este isomorfismo hace corresponder los grupos de ramificación locales y globales (usando que los automorfismos locales son continuos, que el anillo de enteros

globales es denso en el anillo de enteros locales y que el ideal global es denso en el local). En consecuencia los cuerpos de descomposición globales se corresponden también con los locales. Los resultados probados en el caso local y que se refieran únicamente a propiedades algebraicas de los grupos de ramificación serán válidos también para cuerpos globales.

El teorema siguiente nos proporcionará otra reducción importante en el estudio de los grupos de ramificación. La demostración es inmediata.

Teorema 10.2 *Consideremos una cadena de extensiones de dominios de Dedekind $D \subset E \subset F$ de modo que F/D sea de Galois. Sea $k \subset L \subset K$ la cadena de cuerpos de cocientes. Sea $\mathfrak{P}$ un ideal primo en L, sea $\mathfrak{p}$ el primo de D al cual divide y supongamos que la extensión de cuerpos de restos $\overline{F}/\overline{D}$ es separable. Entonces, para todo índice $i \geq -1$ se cumple*

$$\begin{aligned} G^i_{K/L} &= G^i_{K/k} \cap G(K/L), \\ K^i_{K/L} &= K^i_{K/k} L. \end{aligned}$$

De este modo, si partimos de una extensión de Galois K/k de cuerpos numéricos y $\mathfrak{P}$ es un primo en K, el teorema anterior nos da que los grupos de ramificación de $\mathfrak{P}$ en la extensión K/k son los mismos que en la extensión K/F, donde F es el cuerpo de inercia. Por lo tanto, para estudiar estos grupos podemos suponer que $k = F$ y así, si $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$, se cumple $\mathfrak{p} = \mathfrak{P}^e$ y el grado de inercia es $f = 1$.

Por consiguiente, la extensión local $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ es totalmente ramificada y, según hemos comentado, los grupos de ramificación de $\mathfrak{P}$ en esta extensión son isomorfos a los de la extensión K/k, con la ventaja de que ahora $\mathfrak{P}$ es el único primo de $K_{\mathfrak{P}}$. Además ahora es principal, es decir, $\mathfrak{P} = (\pi)$ para cierto entero π. Si llamamos E/D a los anillos de enteros, el teorema 3.11 nos da que $E = D[\pi]$ (notar que como $f = 1$ se cumple $E/\mathfrak{P} = D/\mathfrak{p}$). Más aún, observar que podemos elegir como π a cualquier elemento del cuerpo de partida K que sea divisible entre $\mathfrak{P}$ pero no entre $\mathfrak{P}^2$.

Estas consideraciones nos llevan a una expresión más sencilla para los grupos de ramificación:

Teorema 10.3 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K y sea π un elemento de $\mathfrak{P}$ no divisible entre $\mathfrak{P}^2$. Entonces, para cada $i \geq 0$,*

$$G^i_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} \mid \sigma(\pi) \equiv \pi \ (\text{mód } \mathfrak{P}^{i+1})\}.$$

DEMOSTRACIÓN: Supongamos que los cuerpos son numéricos (el caso p-ádico es más sencillo). Por las observaciones previas al teorema podemos suponer que k es el grupo de inercia de $\mathfrak{P}$, y entonces tenemos $E = D[\pi]$, donde E/D es la extensión de enteros de $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. Por lo tanto

$$G^i = \{\sigma \in G(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \mid \sigma(\pi) \equiv \pi \ (\text{mód } \mathfrak{P}^{i+1})\}.$$

Ahora basta restringir a K. ∎

Otra aplicación de la reducción al caso local completamente ramificado es el apartado c) del teorema siguiente, que enunciamos junto con otros hechos elementales.

Teorema 10.4 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos, sea $\mathfrak{P}$ un ideal primo en K. Entonces*

a) Para todo $\sigma \in G(K/k)$ y todo $i \geq 0$ se cumple $(G^i_{\mathfrak{P}})^\sigma = G^i_{\sigma(\mathfrak{P})}$.

b) En particular $G^i_{\mathfrak{P}} \trianglelefteq G_{\mathfrak{P}}$.

c) Existe un índice i tal que $G^i_{\mathfrak{P}} = 1$ (y por lo tanto $K_i = K$).

Demostración: a) Si $\tau \in G^i_{\mathfrak{P}}$ entonces, todo entero α de K cumple $\tau(\sigma^{-1}(\alpha)) \equiv \sigma^{-1}(\alpha)$ (mód $\mathfrak{P}^{i+1}$), luego

$$(\sigma^{-1}\tau\sigma)(\alpha) = \sigma(\tau(\sigma^{-1}(\alpha)) \equiv \alpha \text{ (mód } \sigma(\mathfrak{P})^{i+1}),$$

con lo que $\sigma^{-1}\tau\sigma \in G^i_{\sigma(\mathfrak{P})}$. Así pues, $(G^i_{\mathfrak{P}})^\sigma \leq G^i_{\sigma(\mathfrak{P})}$. Como σ^{-1} cumple esto mismo, también es cierta la otra inclusión.

b) Es consecuencia inmediata de a).

c) Según las observaciones previas al teorema 10.3 podemos suponer que K/k es una extensión de cuerpos p-ádicos completamente ramificada y, si π es un generador de $\mathfrak{P}$, entonces $K = k(\pi)$. En consecuencia, los valores $\sigma(\pi)$ para $\sigma \in G_{\mathfrak{P}} = G(K/k)$ son todos distintos dos a dos. Así, si $\sigma \neq 1$, se cumple $\sigma(\pi) - \pi \neq 0$, y basta tomar i suficientemente grande para que $\pi^{i+1} \nmid \sigma(\pi) - \pi$ para ningún $\sigma \in G_{\mathfrak{P}} \setminus 1$. El teorema anterior nos da entonces que $G^i_{\mathfrak{P}} = 1$. ∎

Ahora caracterizamos completamente el primer grupo de ramificación y parcialmente los grupos siguientes.

Teorema 10.5 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un primo en K, sea $\mathfrak{p}$ el primo de k divisible entre $\mathfrak{P}$, sea e el grado de ramificación y p la característica de sus cuerpos de restos (en el caso numérico p es el primo racional al cual dividen). Sea $e = p^s e_0$, con $(p, e_0) = 1$. Entonces:*

a) G^0/G^1 es cíclico de orden e_0.

b) Para $i \geq 1$ se cumple que G^i/G^{i+1} es producto de grupos cíclicos de orden p (sin excluir la posibilidad de que sea trivial).

Demostración: Basta demostrarlo en el caso p-ádico. Sea $\mathfrak{P} = (\pi)$. Si $\sigma \in G(K/k)$ entonces $\sigma(\pi)$ es primo en K, luego $\sigma(\pi) = \epsilon_\sigma \pi$ para una cierta unidad ϵ_σ. Si $\sigma, \tau \in G^0$ entonces

$$(\sigma\tau)(\pi) = \epsilon_{\sigma\tau}\pi = \tau(\sigma(\pi)) = \tau(\epsilon_\sigma \pi) = \tau(\epsilon_\sigma)\tau(\pi) = \tau(\epsilon_\sigma)\epsilon_\tau \pi,$$

luego $\epsilon_{\sigma\tau} = \tau(\epsilon_\sigma)\epsilon_\tau \equiv \epsilon_\sigma \epsilon_\tau$ (mód $\mathfrak{P}$).

Por lo tanto, si llamamos $\overline{K}$ al cuerpo de restos de K, podemos definir el homomorfismo $G^0 \longrightarrow \overline{K}^*$, dado por $\sigma \mapsto [\epsilon_\sigma]$.

Su núcleo es claramente G^1, luego G^0/G^1 es isomorfo a un subgrupo de $\overline{K}^*$, que es un grupo cíclico, luego G^0/G^1 es cíclico también. Más aún, $E/\mathfrak{P}$ es un cuerpo finito de orden potencia de p, luego $\overline{K}^*$ tiene orden primo con p y G^0/G^1 también.

Ahora probaremos b), con lo que el orden de G^1 será potencia de p y, en consecuencia, el orden de G^0/G^1 tendrá que ser exactamente e_0.

Sea $\sigma \in G^i$. Entonces $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$, luego $\sigma(\pi) = \pi + \eta_\sigma \pi^{i+1}$ para un cierto $\eta_\sigma \in E$. Si ahora tomamos σ, $\tau \in G^i$, tenemos

$$\begin{aligned}(\sigma\tau)(\pi) &= \pi + \eta_{\sigma\tau}\pi^{i+1} = \tau(\pi + \eta_\sigma\pi^{i+1}) = \tau(\pi) + \tau(\eta_\sigma)\tau(\pi)^{i+1}\\ &= \pi + \eta_\tau\pi^{i+1} + \tau(\eta_\sigma)\tau(\pi)^{i+1} = \pi + \eta_\tau\pi^{i+1} + \tau(\eta_\sigma)\epsilon_\tau^{i+1}\pi^{i+1},\end{aligned}$$

luego $\eta_{\sigma\tau} = \eta_\tau + \tau(\eta_\sigma)\epsilon_\tau^{i+1} \equiv \eta_\tau + \eta_\sigma \pmod{\mathfrak{P}}$ pues, como $\tau \in G^i$, se cumple $\epsilon_\tau \equiv 1 \pmod{\mathfrak{P}}$.

Con esto tenemos otro homomorfismo $G^i \longrightarrow \overline{K}$ dado por $\sigma \mapsto [\eta_\sigma]$, cuyo núcleo es claramente G^{i+1}. Por lo tanto G^i/G^{i+1} es isomorfo a un subgrupo del grupo aditivo de $\overline{K}$, pero esto es lo mismo que un subespacio vectorial de $\overline{K}$ considerado como espacio vectorial sobre el cuerpo de p elementos. Claramente entonces G^i/G^{i+1} es producto de grupos cíclicos de orden p. ∎

En las condiciones del teorema anterior, si $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$ y su norma absoluta (el número de clases módulo $\mathfrak{p}$) es n, entonces el cuerpo $\overline{K}$ tiene n^f elementos, donde $f = f(\mathfrak{P}/\mathfrak{p})$, y tenemos que $e_0 \mid n^f - 1$, así como que $|G^i : G^{i+1}| \,\big|\, n^f$.

En términos de la teoría de grupos el teorema nos dice que G^1 es un p-subgrupo de Sylow de G^0. El hecho de que sea normal implica que es, de hecho, el único p-subgrupo de Sylow de G^0, luego en la práctica es fácil de identificar. Esto explica los términos "ramificación dominada" y "ramificación libre": cuando la ramificación es dominada la serie de los grupos de ramificación termina en $G^1 = 1$, luego la ramificación está "controlada" gracias al teorema anterior, pero si la ramificación es libre no disponemos de ningún resultado general para determinar el modo en que descienden los grupos G^i, y para saberlo hay que analizar separadamente cada caso.

Del teorema anterior se deduce un hecho interesante sobre las extensiones de cuerpos p-ádicos:

Teorema 10.6 *Si K/k es una extensión de Galois de cuerpos p-ádicos, entonces el grupo de Galois $G(K/k)$ es resoluble.*

Demostración: Sea $G = G(K/k) = G^{-1}$ y consideremos la sucesión de subgrupos

$$1 = G^r \trianglelefteq \cdots \trianglelefteq G^1 \trianglelefteq G^0 \trianglelefteq G.$$

La extensión K_0/k es no ramificada y, de acuerdo con 2.37, su grupo de Galois G/G^0 es cíclico. Por el teorema anterior G^0/G^1 también es cíclico y los demás cocientes son abelianos, luego G es resoluble. ∎

Los teoremas anteriores están relacionados con los resultados que obtuvimos en el capítulo II sobre cuerpos locales: Si K/k es una extensión de Galois de cuerpos p-ádicos, tenemos la sucesión de cuerpos $k \subset K_0 \subset K_1 \subset K$.

La extensión K_0/k es no ramificada y K/K_0 es totalmente ramificada. Es fácil ver que K_0 es precisamente el cuerpo K_{nr} descrito en 2.39. El teorema 10.5 prueba que K_1/K_0 es también cíclica de grado primo con p, luego es total y dominadamente ramificada. Es claro que K_1 es el cuerpo K_d descrito en 2.46, que nos anticipaba también que el grado $|K : K_1|$ es potencia de p, tal y como hemos probado.

Del teorema siguiente deduciremos resultados más precisos sobre la estructura de los grupos de ramificación.

Teorema 10.7 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K, sea $\tau \in G^0$ y $\sigma \in G^i$ para $i \geq 1$. Entonces $\sigma^{-1}\tau^{-1}\sigma\tau \in G^{i+1}$ si y sólo si $\sigma \in G^{i+1}$ o $\tau^i \in G^1$.*

Demostración: Basta probarlo en el caso p-ádico. Sea $\mathfrak{P} = (\pi)$. Sea $\tau(\pi) = \epsilon\pi$, donde ϵ es una unidad de K. Como por hipótesis $\tau \in G^0$, tenemos que $\tau(\epsilon) \equiv \epsilon \pmod{\mathfrak{P}}$, luego $\tau^i(\pi) \equiv \epsilon^i\pi \pmod{\mathfrak{P}^2}$ (por ejemplo, $\tau(\epsilon)\pi \equiv \epsilon\pi \pmod{\mathfrak{P}^2}$, luego $\tau^2(\pi) = \tau(\epsilon)\epsilon\pi \equiv \epsilon^2\pi \pmod{\mathfrak{P}^2}$, etc.).

De aquí que la afirmación $\tau^i \in G^1$ equivale a que $\epsilon^i \equiv 1 \pmod{\mathfrak{P}}$. Así mismo, si $\sigma(\pi) = \pi + \eta\pi^{i+1}$, donde η es un entero en K, la afirmación $\sigma \in G^{i+1}$ equivale a que $\mathfrak{P} \mid \eta$.

Hemos de probar, pues, que $\sigma^{-1}\tau^{-1}\sigma\tau \in G^{i+1}$ si y sólo si $\epsilon^i \equiv 1 \pmod{\mathfrak{P}}$ o bien $\mathfrak{P} \mid \eta$.

Calculamos

$$(\tau\sigma)(\pi) = \sigma(\tau(\pi)) = \sigma(\epsilon\pi) = \sigma(\epsilon)\pi + \sigma(\epsilon)\eta\pi^{i+1}.$$

Como $\sigma(\epsilon) \equiv \epsilon \pmod{\mathfrak{P}^{i+1}}$ tenemos que $\sigma(\epsilon)\pi \equiv \epsilon\pi \pmod{\mathfrak{P}^{i+2}}$, luego

$$(\tau\sigma)(\pi) \equiv \epsilon\pi + \epsilon\eta\pi^{i+1} \pmod{\mathfrak{P}^{i+2}} \tag{10.1}$$

Por otro lado

$$(\sigma\tau)(\pi) = \tau(\sigma(\pi)) = \tau(\pi + \eta\pi^{i+1}) = \tau(\pi) + \tau(\eta)\tau(\pi)^{i+1} = \epsilon\pi + \tau(\eta)\epsilon^{i+1}\pi^{i+1}$$

y, como $\tau(\eta) \equiv \eta \pmod{\mathfrak{P}}$, se cumple $\tau(\eta)\pi^{i+1} \equiv \eta\pi^{i+1} \pmod{\mathfrak{P}^{i+2}}$, y así

$$(\sigma\tau)(\pi) \equiv \epsilon\pi + \eta\epsilon^{i+1}\pi^{i+1} \pmod{\mathfrak{P}^{i+2}}. \tag{10.2}$$

Restando (10.1) y (10.2) queda

$$(\tau\sigma - \sigma\tau)(\pi) \equiv (\epsilon\pi)^{i+1}\eta(\epsilon^{-i} - 1) \pmod{\mathfrak{P}^{i+2}}.$$

Llamemos $\pi' = (\tau\sigma)(\pi)$, con lo que $\pi = (\sigma^{-1}\tau^{-1})(\pi')$. Sustituyendo llegamos a que

$$\pi' - (\sigma^{-1}\tau^{-1}\sigma\tau)(\pi') \equiv (\epsilon\pi)^{i+1}\eta(\epsilon^{-i} - 1) \pmod{\mathfrak{P}^{i+2}}.$$

Puesto que también se cumple $\mathfrak{P} = (\pi')$, el teorema 10.3 nos permite concluir que $\sigma^{-1}\tau^{-1}\sigma\tau \in G^{i+1}$ si y sólo si $\mathfrak{P} \mid \eta(\epsilon^{-i} - 1)$. ∎

Como primera consecuencia inmediata obtenemos un resultado general sobre la sucesión de grupos de ramificación que en la práctica no nos será de mucha ayuda, pues es trivial en el caso de extensiones abelianas, pero que tiene valor desde el punto de vista de la teoría de grupos. Recordemos que el centro de un grupo G es el subgrupo

$$Z(G) = \{g \in G \mid gh = hg \text{ para todo } h \in G\}.$$

Teorema 10.8 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K. Sea $i \geq 1$. Entonces*

$$G^i/G^{i+1} \leq Z(G^1/G^{i+1}).$$

Demostración: Si tomamos $\tau \in G^1$ se cumple $\sigma^{-1}\tau^{-1}\sigma\tau \in G^{i+1}$, luego $[\sigma] \in Z(G^1/G^{i+1})$. ∎

En términos de la teoría de grupos esto significa que la sucesión de grupos de ramificación es una serie central del p-grupo G^1.

Ahora veamos una consecuencia del teorema 10.7 mucho más importante.

Teorema 10.9 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K tal que G^0 sea abeliano. Si $G^i \neq G^{i+1}$ entonces $e_0 \mid i$.*

Demostración: Sea $[\tau]$ un generador de G^0/G^1. Por hipótesis podemos tomar $\sigma \in G^i \setminus G^{i+1}$, con lo que el teorema 10.7 nos da que $[\tau]^i = 1$, luego $e_0 \mid i$. ∎

Definición 10.10 Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K. Los índices $i \geq 0$ tales que $G^i \neq G^{i+1}$ se llaman *números de ramificación* de $\mathfrak{P}$. Los representaremos por $v_1, \ldots, v_t$. Así, la serie de grupos de ramificación puede abreviarse a

$$1 = G^{v_t+1} \lhd \cdots \lhd G^{v_1+1} \lhd G^0 \trianglelefteq G_{\mathfrak{P}}.$$

El teorema anterior afirma que si $G_{\mathfrak{P}}$ es abeliano entonces los números v_i han de ser múltiplos de e_0.

Con los grupos de ramificación podemos mejorar el teorema 3.15 y calcular exactamente los exponentes de los primos en el diferente de una extensión.

Teorema 10.11 *Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos y sea $\mathfrak{P}$ un ideal primo en K. Entonces el exponente de $\mathfrak{P}$ en el diferente de K/k es*

$$E = \sum_{i=0}^{\infty} (|G^i| - 1).$$

DEMOSTRACIÓN: Por el teorema 3.10 podemos suponer que la extensión es p-ádica. Si Z es el cuerpo de inercia de $\mathfrak{P}$, la extensión Z/k es no ramificada, luego su diferente es 1. Por el teorema 3.9 podemos suponer que $Z = k$. Entonces $G(K/k) = G^0$ y, si llamamos E/D a la extensión de los anillos de enteros, tenemos que $E = D[\alpha]$, para un cierto $\alpha \in E$ (por 3.12).

Sea $f(x)$ el polinomio mínimo de α. El teorema 3.8 nos da que el diferente de la extensión es

$$\mathfrak{D} = \big(f'(\alpha)\big) = \prod_{\sigma \in G^0 \setminus 1} (\sigma(\alpha) - \alpha).$$

Pero $G^0 \setminus 1 = \bigcup_{i=0}^{\infty} (G^i \setminus G^{i+1})$, la unión es disjunta y, si $\sigma \in G^i \setminus G^{i+1}$, esto significa por definición que $(\sigma(\alpha) - \alpha) = \mathfrak{P}^{i+1}$. Por lo tanto

$$E = \sum_{i=0}^{\infty} (i+1)\big(|G^i| - |G^{i+1}|\big).$$

Supongamos que G^t es el primer grupo de ramificación trivial. Entonces

$$\begin{aligned} E &= |G^0| - |G^1| + 2(|G^1| - |G^2|) + 3(|G^2| - |G^3|) + \cdots + t(|G^{t-1}| - 1) \\ &= |G^0| + |G^1| + |G^2| + \cdots + |G^{t-1}| - t = \sum_{i=0}^{t-1} (|G^i| - 1) = \sum_{i=0}^{\infty} (|G^i| - 1). \end{aligned}$$

■

10.2 Cálculo de grupos de ramificación

Antes de seguir con la teoría vamos a examinar algunos ejemplos concretos.

Cuerpos cuadráticos Sea K un cuerpo cuadrático de discriminante Δ y consideremos la extensión $K/\mathbb{Q}$. Sea $\mathfrak{p}$ un primo de K y sea p el primo racional al cual divide. La tabla siguiente indica el cuerpo de descomposición F de $\mathfrak{p}$ junto con los cuerpos de ramificación en cada uno de los casos posibles:

		F	K_0	K_1	K_2	K_3
	$(\Delta/p) = 1$	K	K	K	K	K
p impar	$(\Delta/p) = -1$	$\mathbb{Q}$	K	K	K	K
	$p \mid \Delta$	$\mathbb{Q}$	$\mathbb{Q}$	K	K	K
$p = 2$	$\Delta = 4m$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	K	K
	$\Delta = 8m$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	K

Las tres primeras columnas se calculan inmediatamente a partir de los valores r, f, e y e_0. Con esto se completan las tres primeras filas.

Para calcular las restantes observamos que una base entera de K es en cualquier caso la formada por 1 y $\omega = \big(\Delta + \sqrt{\Delta}\,\big)/2$. El grupo de ramificación

i-ésimo será trivial o no según si contiene a la conjugación σ, y esto a su vez equivale a que $\mathfrak{p}^{i+1} \mid \omega - \sigma(\omega) = \sqrt{\Delta}$.

Si $p = 2$ y el discriminante es de tipo $\Delta = 4m$, con m impar, entonces el exponente de $\mathfrak{p}$ en $\sqrt{\Delta}$ es 2, luego $G^1 \neq 1$ y $G^2 = 1$.

Si $\Delta = 8m$ entonces el exponente de $\mathfrak{p}$ en $\sqrt{\Delta}$ es 3 y concluimos que $G^2 \neq 1$ y $G^3 = 1$. ∎

Cuerpos ciclotómicos Para calcular los grupos de ramificación de los cuerpos ciclotómicos probamos en primer lugar un resultado que reduce el problema al caso de extensiones de orden potencia de primo.

Teorema 10.12 *Sea K el cuerpo ciclotómico de orden $n = p^r m$, donde p es primo y $(m, p) = 1$. Sean k y k' los cuerpos ciclotómicos de orden p^r y m respectivamente. Sea $\mathfrak{P}$ un divisor primo de p en K y sea $\mathfrak{p}$ el primo de k divisible entre $\mathfrak{P}$. Entonces*

a) Los grupos de ramificación de $\mathfrak{P}$ respecto a la extensión $K/\mathbb{Q}$ (a partir de $i = 0$) coinciden con los de la extensión K/k'.

b) El isomorfismo natural $G(K/k') \cong G(k/\mathbb{Q})$ hace corresponder los grupos de ramificación de $\mathfrak{P}$ con los correspondientes de $\mathfrak{p}$.

Demostración: Es claro que podemos sustituir cada cuerpo por su compleción respecto al primo adecuado, de modo que K será ahora $K_{\mathfrak{P}}$, k será $k_{\mathfrak{p}}$, etc.

Según el teorema 4.6, el índice de ramificación de $\mathfrak{P}$ sobre $\mathbb{Q}_p$ es el mismo que sobre k' y a su vez coincide con el de $\mathfrak{p}$ sobre $\mathbb{Q}_p$ (todos ellos valen $e = \phi(p^r)$).

Según el teorema 10.2, el grupo de inercia G^0 para la extensión K/k' es un subgrupo del correspondiente a $K/\mathbb{Q}_p$, pero como ambos tienen orden e, son el mismo.

La extensión K/k es no ramificada, luego podemos identificar $\mathfrak{p} = \mathfrak{P}$. Más precisamente, $\mathfrak{p}$ y $\mathfrak{P}$ dividen a los enteros de k con la misma multiplicidad, luego las congruencias de enteros de k módulo $\mathfrak{p}$ son las mismas que módulo $\mathfrak{P}$. Si fijamos $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ entonces el teorema 10.3 nos da que el i-ésimo grupo de ramificación tanto para la extensión K/k' como para $K/\mathbb{Q}_p$ viene dado por

$$G^i = \{\sigma \in G^0 \mid \sigma(\pi) \equiv \pi \ (\text{mód } \mathfrak{P}^{i+1})\},$$

luego ambas extensiones tienen los mismos grupos de ramificación. También es inmediato que los grupos respecto a $k/\mathbb{Q}_p$ se corresponden con éstos a través del isomorfismo natural (inducido por la restricción a k). ∎

Para las extensiones de orden potencia de primo tenemos:

Teorema 10.13 *Sea p un número primo, ζ una raíz p^r-ésima primitiva de la unidad y $K = \mathbb{Q}(\zeta)$. Sea $\mathfrak{p}$ el único primo que divide a p en K. Identificamos $G(K/\mathbb{Q})$ con el grupo U_{p^r} de las unidades módulo p^r. Entonces $G^0 = U_{p^r}$ y, si $p^k \leq i < p^{k+1}$, se cumple*

$$G^i = \big\{[n] \in U_{p^r} \mid n \equiv 1 \ (\text{mód } p^{k+1})\big\}.$$

DEMOSTRACIÓN: Llamemos $H_k = \big\{[n] \in U_{p^r} \mid n \equiv 1 \pmod{p^k}\big\}$ y veamos que si $k \geq 1$ entonces $H_k \leq G^{p^k-1}$.

Si σ es el automorfismo identificado con una clase $[n]$ tal que $n \equiv 1 \pmod{p^k}$, para probar que $\sigma \in G^{p^k-1}$ basta ver que $\mathfrak{p}^{p^k} \mid \sigma(\zeta) - \zeta = \zeta^n - \zeta$. Pero ζ es una unidad y $\mathfrak{p} = (\zeta - 1)$, luego esto equivale a que $(\zeta-1)^{p^k} \mid \zeta^{n-1} - 1$. Tomamos clases módulo $(\zeta-1)^{p^k}$, con lo que trabajamos en un anillo de característica p. Se cumple que $[0] = [\zeta - 1]^{p^k} = ([\zeta] - [1])^{p^k} = [\zeta]^{p^k} - [1]$, o sea, $[\zeta]^{p^k} = [1]$ y, como por hipótesis $p^k \mid n-1$, también $[\zeta]^{n-1} = [1]$, luego $[\zeta^{n-1} - 1] = [0]$, como queríamos probar.

Cambiando k por $k+1$ queda que $H_{k+1} \leq G^{p^{k+1}-1}$, para todo $k \geq 0$, luego también $H_{k+1} \leq G^i$ para $p^k \leq i < p^{k+1}$.

Considerando el epimorfismo natural $U_{p^r} \longrightarrow U_{p^{k+1}}$ para $0 \leq k < r$ vemos que $|H_{k+1}| = p^{r-(k+1)}$. Por lo tanto tenemos que si $p^k \leq i < p^{k+1}$ se cumple $|G^i| \geq p^{r-(k+1)}$.

Vamos a calcular la fórmula del teorema 10.11 usando estas cotas inferiores. Si vemos que el resultado E es exactamente el exponente de $\mathfrak{p}$ en el diferente de la extensión, entonces todas las desigualdades tendrán que ser igualdades y tendremos el teorema.

Según el teorema 3.27, el exponente de p en el discriminante de la extensión es $E = r(p-1)p^{r-1} - p^{r-1} = p^{r-1}(pr - r - 1)$. Como el discriminante es la norma del diferente y $\mathrm{N}(\mathfrak{p}) = p$, este número E es también el exponente de $\mathfrak{p}$ en el diferente. Veamos qué obtenemos con las cotas.

Las cotas valen 1 a partir del término $i = p^{r-1}$, luego tenemos p^{r-1} sumandos no nulos del tipo $C_i - 1$ (para $i = 0, \ldots, p^{r-1} - 1$). Agrupando todos los unos, hemos de sumar todas las cotas C_i y restar p^{r-1} al resultado.

En primer lugar $C_0 = |U_{p^r}| = (p-1)p^{r-1}$, para $i = 1, \ldots, p-1$ tenemos $p-1$ sumandos iguales a p^{r-1}, para $i = p, \ldots, p^2 - 1$ tenemos $p(p-1)$ sumandos iguales a p^{r-2}, para $i = p^2, \ldots, p^3 - 1$ tenemos $p^2(p-1)$ sumandos iguales a p^{r-3}, etc.

Así pues, tenemos r bloques que suman $(p-1)p^{r-1}$ cada uno. El total, después de restar p^{r-1}, es

$$r(p-1)p^{r-1} - p^{r-1} = p^{r-1}(pr - r - 1) = E.$$

■

En particular los números de ramificación son 0, $p-1$, p^2-1, $\ldots$, $p^{r-1}-1$, excepto cuando $p = 2$, en cuyo caso 0 no es un número de ramificación (tanto G^0 como G^1 tienen 2^{r-1} elementos). El grado entre dos cuerpos de ramificación sucesivos es igual a p.

Cuerpos cúbicos puros Por último estudiamos la clausura normal de un cuerpo cúbico puro $\mathbb{Q}\big(\sqrt[3]{m}\,\big)$, es decir, un cuerpo de la forma $K = \mathbb{Q}\big(\sqrt[3]{m}, \sqrt{-3}\,\big)$. Para mayor comodidad del lector reproducimos la tabla construida en el capítulo II con el tipo de factorización de cada primo (ver la [Tabla 2.1] para la clasificación de los cuerpos cúbicos puros).

Casos		$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt[3]{m})$	K	e	f
$p \nmid ab$	$p \equiv 1(3)$ $x^3 \equiv ab^2(p)$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6$	1	1
	$x^3 \not\equiv ab^2(p)$	$\mathfrak{p}_1\mathfrak{p}_2$	p	$\mathfrak{p}_1\mathfrak{p}_2$	1	3
	$p \equiv -1(3)$	p	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	1	2
$p \mid ab$	$p \equiv 1(3)$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}^3$	$(\mathfrak{p}_1\mathfrak{p}_2)^3$	3	1
	$p \equiv -1(3)$	p	$\mathfrak{p}^3$	$\mathfrak{p}^3$	3	2
$p = 3$	Tipo I	$\mathfrak{p}^2$	$\mathfrak{p}^3$	$\mathfrak{p}^6$	6	1
	Tipo II	$\mathfrak{p}^2$	$\mathfrak{p}_1\mathfrak{p}_2^2$	$(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$	2	1

La tabla siguiente indica los cuerpos de ramificación en cada caso. Como de costumbre, F es el cuerpo de descomposición. Llamaremos $L_3 = \mathbb{Q}\big(\sqrt[3]{m}\,\big)$ y $L_2 = \mathbb{Q}\big(\sqrt{-3}\,\big)$.

Casos		F	K_0	K_1	K_2	K_3	K_4
$p \nmid ab$	$p \equiv 1(3)$ $x^3 \equiv ab^2(p)$	K	K	K	K	K	K
	$x^3 \not\equiv ab^2(p)$	L_2	K	K	K	K	K
	$p \equiv -1(3)$	L_3	K	K	K	K	K
$p \mid ab$	$p \equiv 1(3)$	L_2	L_2	K	K	K	K
	$p \equiv -1(3)$	$\mathbb{Q}$	L_2	K	K	K	K
$p = 3$	Tipo I $3 \nmid ab$	$\mathbb{Q}$	$\mathbb{Q}$	L_2	K	K	K
	Tipo I $3 \mid ab$	$\mathbb{Q}$	$\mathbb{Q}$	L_2	L_2	L_2	K
	Tipo II	L_3	L_3	K	K	K	K

Notar que la extensión $K/\mathbb{Q}$ contiene tres cuerpos intermedios conjugados de grado 3. Cuando en la tabla aparece L_3 hay que entender que los cada uno de los tres divisores de p en K tiene como cuerpo de ramificación a uno de estos tres cuerpos.

Observar también que el penúltimo caso de la primera tabla se ha desdoblado en dos en la segunda. Excepto estos dos casos, todos los demás se razonan fácilmente.

Por ejemplo, tomemos la última fila: el número de factores en que se descompone p es $r = 3 = |F : \mathbb{Q}|$, luego $F = L_3$. Ahora, $f = 1 = |K_0 : F|$, con lo que $K_0 = L_3$. Finalmente tenemos $|K_1 : K_0| = e_0 = 2$, luego $K_1 = K$.

El único caso a analizar es $p = 3$ cuando el cuerpo cúbico es de tipo I, que se corresponde con las filas penúltima y antepenúltima de la tabla. En ambos casos es claro que $K_1 = L_2$. Para determinar los cuerpos siguientes usaremos el teorema 10.11, para lo cual hemos de calcular el diferente de la extensión. En realidad nos bastaría calcular el diferente local correspondiente al divisor 3, pero por completitud calcularemos el diferente global tanto para cuerpos de tipo I como de tipo II. La idea es que si consideramos la cadena

$\mathbb{Q} \subset L_2 \subset K$ tenemos problemas con K/L_2 debido a la ramificación libre, pero si consideramos $\mathbb{Q} \subset L_3 \subset K$ la ramificación libre está en el tramo $L_3/\mathbb{Q}$, pero aquí podemos calcular el diferente a partir del discriminante, que es conocido.

Llamemos $\mathfrak{f} = 3ab$ si L_3 es de tipo I y $\mathfrak{f} = ab$ si L_3 es de tipo II (la razón de esta notación es que más adelante[1] probaremos que $\mathfrak{f}$ es el conductor de K/L_2). Según el teorema [2.27], el discriminante de L_3 es $3\mathfrak{f}^2$ (consideramos a $\mathfrak{f}$ como ideal, por lo que prescindimos del signo).

Fijemos notación para la factorización del 3: Si L_3 es de tipo II tenemos que $3 = \mathfrak{p}_1\mathfrak{p}_2^2$ en L_3, $3 = \mathfrak{q}^2$ en L_2, $\mathfrak{p}_1 = \mathfrak{P}_1^2$, $\mathfrak{p}_2 = \mathfrak{P}_2\mathfrak{P}_3$, $\mathfrak{q} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ en K.

El tipo I también se ajusta a este esquema si convenimos que $\mathfrak{p}_1 = \mathfrak{p}_2$, $\mathfrak{P}_1 = \mathfrak{P}_2 = \mathfrak{P}_3$.

Cada divisor primo (racional) de $\mathfrak{f}$ tiene un único divisor en L_3, que lo divide con multiplicidad 3, luego podemos escribir $\mathfrak{f}^{1/3}$ para referirnos al ideal de L_3 que resulta de dividir entre tres los exponentes de los primos de L_3 que aparecen en $\mathfrak{f}$.

De los divisores de 3, el único que se ramifica en L_3 es $\mathfrak{p}_2$, luego es el único que puede aparecer en el diferente de $L_3/\mathbb{Q}$. Teniendo esto en cuenta, es claro que dicho diferente ha de ser $\mathfrak{D}_{3/1} = \mathfrak{p}_2\mathfrak{f}^{2/3}$.

Respecto a la extensión K/L_3, el único primo ramificado es $\mathfrak{P}_1$, con índice 2, luego la ramificación es dominada, los grupos de ramificación son $G^0 \cong C_2$, $G^1 = 1$, y el teorema 10.11 nos da que el diferente es exactamente $\mathfrak{D}_{6/3} = \mathfrak{P}_1$.

Con esto tenemos el diferente de toda la extensión $K/\mathbb{Q}$, que resulta ser

$$\mathfrak{D}_{6/1} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{f}^{2/3} = 3^{1/2}\mathfrak{f}^{2/3}.$$

Por otro lado, el diferente de la extensión $L_2/\mathbb{Q}$ se calcula inmediatamente a partir del discriminante, que es -3. Evidentemente $\mathfrak{D}_{2/1} = \mathfrak{q} = 3^{1/2}$. Así llegamos al diferente que nos interesaba, el de la extensión K/L_2, que es

$$\mathfrak{D}_{6/2} = \mathfrak{f}^{2/3}. \tag{10.3}$$

Necesitábamos el exponente de $\mathfrak{P} = \mathfrak{P}_1 = \mathfrak{P}_2 = \mathfrak{P}_3$ en $\mathfrak{D}_{6/2}$ cuando L_3 es de tipo I. Como $\mathfrak{f} = 3ab$, dicho exponente será $E = 4$ si $p \nmid ab$ o bien $E = 8$ si $p \mid ab$.

Los grupos G_i para K/L_2 tienen orden 3 o son triviales, luego aportan sumandos iguales a 2 en el teorema 10.11. Así pues, si $p \nmid ab$ hay 2 grupos no triviales (los correspondientes a $i = 0, 1$) y si $p \mid ab$ hay 4 grupos no triviales ($i = 0, 1, 2, 3$). Esto es lo que refleja la tabla anterior.

10.3 Grupos de ramificación de subcuerpos

Dada una cadena de cuerpos $k \subset L \subset K$, el teorema 10.2 muestra la relación entre los grupos de ramificación de K/k y los de K/L. Aquí investigaremos los grupos de ramificación de la extensión L/k (suponiendo que es normal). Como

[1] Ver el ejemplo 3 de la sección 10.6

cabría esperar, si H es el grupo de Galois de K/L, los grupos de ramificación de L/k son los grupos G^iH/H, pero sucede que los índices no se corresponden, es decir, G^iH/H no es necesariamente el grupo de ramificación i-ésimo. El problema es encontrar la relación correcta entre los índices. Esto nos llevará al concepto de la *función de Hasse* de una extensión, de gran importancia en la teoría.

Para simplificar la notación convendremos en que una barra sobre sobre un símbolo indicará que se refiere a la extensión K/L, mientras que bajo él hará referencia a la extensión L/k. Por ejemplo, fijado un primo $\mathfrak{P}$ de K, los grupos $\overline{G}^i$ serán los grupos de ramificación de $\mathfrak{P}$ en K/L, y los grupos $\underline{G}_i$ serán los grupos de ramificación en L/k del primo $\mathfrak{p}$ divisible entre $\mathfrak{P}$.

En primer lugar probamos el único caso que no tiene equivalente local (porque el caso local es trivial).

Teorema 10.14 *Sea $k \subset L \subset K$ una cadena de cuerpos numéricos de modo que las tres extensiones sean de Galois. Sea $\mathfrak{P}$ un ideal primo en K y $\mathfrak{p}$ el primo de L divisible entre $\mathfrak{P}$. Sea $H = G(K/L)$. Sean K', L' los cuerpos de descomposición sobre k de $\mathfrak{P}$ y $\mathfrak{p}$ respectivamente. Entonces $\underline{G}_\mathfrak{p} = G_\mathfrak{P}H/H$ y $L' = K' \cap L$.*

Demostración: Es claro que la restricción a L de un automorfismo de $G_\mathfrak{P}$ está en $\underline{G}_\mathfrak{p}$, es decir, $G_\mathfrak{P}H/H \le \underline{G}_\mathfrak{p}$.

Recíprocamente, todo automorfismo de $\underline{G}_\mathfrak{p}$ induce un automorfismo del cuerpo local $L_\mathfrak{p}$, que se extiende a un automorfismo de $K_\mathfrak{P}$, que a su vez se restringe a un automorfismo de $G_\mathfrak{P}$, luego el automorfismo de partida está en $G_\mathfrak{P}H/H$. La segunda afirmación la da el teorema de Galois. ∎

Para abordar las sutilezas del caso general hemos de introducir algunas definiciones:

Definición 10.15 Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos y sea $\mathfrak{P}$ un primo en K. Para cada $\sigma \in G_\mathfrak{P}$ llamaremos $i(\sigma)$ al mayor número natural tal que $\sigma \in G^{i(\sigma)}$. Convenimos que $i(1) = +\infty$.

En términos de la función i, los grupos de ramificación se expresan como

$$G^i = \{\sigma \in G_\mathfrak{P} \mid i(\sigma) \ge i\}.$$

Nuestra intención es estudiar la relación entre los grupos de distintas extensiones a través de esta función. Otra relación de utilidad es la siguiente:

$$i(\sigma) = -1 + \sum_{r=0}^{\infty} \chi_{G^r}(\sigma),$$

donde χ_A representa a la función característica del conjunto A.

Para trabajar estos conceptos necesitamos un teorema técnico.

Teorema 10.16 *Sea $k \subset L \subset K$ una cadena de cuerpos p-ádicos tal que K/k sea de Galois, sea $H = G(K/L)$, sea $D \subset F \subset E$ la cadena de sus anillos de enteros, sea $\mathfrak{P}$ el primo de K y sean α y β tales que $E = D[\alpha]$ y $F = D[\beta]$. Entonces para todo $\sigma \in G(K/k)$ se cumple que los elementos*

$$\sigma(\beta) - \beta \quad y \quad \prod_{\tau \in H\sigma} (\tau(\alpha) - \alpha) = \prod_{\gamma \in H} (\sigma(\gamma(\alpha)) - \alpha)$$

son asociados en E.

Demostración: Sea $f(x) = \prod_{\gamma \in H} (x - \gamma(\alpha))$ el polinomio mínimo de α en L. Entonces

$$\sigma(f) = \prod_{\gamma \in H} (x - \sigma(\gamma(\alpha)))$$

es el polinomio mínimo de $\sigma(\alpha)$ en $\sigma[L]$.

Los coeficientes de $\sigma(f) - f$ son de la forma $\sigma(a) - a$ con $a \in F$. Expresando a como polinomio en β vemos que todo elemento de esta forma es divisible entre $\sigma(\beta) - \beta$ (por ejemplo, tomando clases módulo $\sigma(\beta) - \beta$). En consecuencia

$$(\sigma(\beta) - \beta) \mid \sigma(f)(\alpha) - f(\alpha) = \sigma(f)(\alpha).$$

Recíprocamente, si $\beta = g(\alpha)$ para un cierto $g(x) \in D[x]$, entonces $\sigma(g) = g$. Como $g(x) - \beta$ tiene raíz α, tenemos $g(x) - \beta = f(x)h(x)$, para un cierto $h(x) \in F[x]$. Así $g(x) - \sigma(\beta) = \sigma(f)(x)\,\sigma(h)(x)$ y

$$\beta - \sigma(\beta) = g(\alpha) - \sigma(\beta) = \sigma(f)(\alpha)\,\sigma(h)(\alpha).$$

Hemos probado que $\beta - \sigma(\beta)$ y $\sigma(f)(\alpha)$ son asociados, y claramente

$$\sigma(f)(\alpha) = \prod_{\gamma \in H} (\alpha - \sigma(\gamma(\alpha)))$$

■

Ahora relacionamos la función i de la extensión inferior con los grupos $\overline{G}^i$ de la superior.

Teorema 10.17 *Sea $k \subset L \subset K$ una cadena de cuerpos numéricos o p-ádicos tal que las tres extensiones sean de Galois. Sea $H = G(K/L)$, sea $\sigma \in G^{-1}$ y supongamos que $H\sigma \cap G^i \neq \varnothing$ para algún i. Entonces*

$$\underline{i}(\underline{\sigma}) = -1 + \sum_{r=0}^{l(\sigma)} \frac{1}{|\overline{G}^0 : \overline{G}^r|},$$

donde $l(\sigma)$ es el mayor entero i tal que $H\sigma \cap G^i \neq \varnothing$.

Demostración: Podemos suponer que los cuerpos son p-ádicos, con lo que según el teorema 3.12 existen α y β en las hipótesis del teorema anterior. Sea $\mathfrak{P}$ el primo de K.

El valor $\mathfrak{P}$-ádico de los elementos asociados en un cuerpo local es el mismo, luego el teorema anterior nos da que

$$v_{\mathfrak{P}}(\sigma(\beta)-\beta)=\sum_{\gamma\in H} v_{\mathfrak{P}}(\sigma(\gamma(\alpha))-\alpha). \tag{10.4}$$

Como las potencias de α forman una base entera de K/k es claro que un automorfismo σ está en un grupo G^i si y sólo si $v_{\mathfrak{P}}(\sigma(\alpha)-\alpha)>i$, de donde

$$i(\sigma)+1=+v_{\mathfrak{P}}(\sigma(\alpha)-\alpha).$$

Igualmente se prueba que

$$\underline{i}(\underline{\sigma})+1=+v_{\mathfrak{p}}(\sigma(\beta)-\beta),$$

donde $\mathfrak{p}$ es el primo de L. Teniendo en cuenta que $v_{\mathfrak{P}}|_L=\overline{e}v_{\mathfrak{p}}$ la ecuación (10.4) se transforma en

$$\begin{aligned}\overline{e}(\underline{i}(\underline{\sigma})+1) &= \sum_{\gamma\in H}(i(\gamma\sigma)+1)=\sum_{\gamma\in H}\sum_{r=0}^{\infty}\chi_{G^r}(\gamma\sigma)\\ &= \sum_{r=0}^{\infty}\sum_{\gamma\in H}\chi_{G^r}(\gamma\sigma)=\sum_{r=0}^{\infty}|H\sigma\cap G^r|=\sum_{r=0}^{l(\sigma)}|H\sigma\cap G^r|.\end{aligned}$$

Si $H\sigma\cap G^r\neq\varnothing$, digamos $h\sigma\in G^r$, entonces para todo $\gamma\in H$ se cumple

$$\gamma\sigma\in G^r\Leftrightarrow\gamma h^{-1}h\sigma\in G^r\Leftrightarrow\gamma h^{-1}\in G^r$$

$$\Leftrightarrow\gamma h^{-1}\in G^r\cap H\Leftrightarrow\gamma\in(G^r\cap H)h.$$

En consecuencia, $|H\sigma\cap G^r|=|(G^r\cap H)h|=|G^r\cap H|=|\overline{G}^r|$ (por 10.2), y la fórmula se convierte en

$$\overline{e}(\underline{i}(\underline{\sigma})+1)=\sum_{r=0}^{l(\sigma)}|\overline{G}^r|.$$

Dividiendo entre $\overline{e}=|\overline{G}^0|$ queda la fórmula buscada. ∎

Notemos que, en las condiciones del teorema anterior, si $H\sigma\cap G^i=\varnothing$ para todo i, la fórmula sigue siendo cierta si la interpretamos como que $\underline{i}(\underline{\sigma})=-1$.

Las definiciones siguientes introducen los conceptos necesarios para expresar el teorema anterior de la forma más conveniente en la teoría:

Definición 10.18 Sea K/k una extensión de Galois de cuerpos numéricos o p-ádicos. Sea $\mathfrak{P}$ un ideal primo en K. Para cada número natural x definimos

$$\phi_{\mathfrak{P}}(x)=-1+\sum_{r=0}^{x}\frac{1}{|G^0:G^r|}.$$

Si no hay confusión suprimiremos el subíndice. Notar que $\phi(0) = 0$. Extendemos ϕ al conjunto de los números reales positivos estableciendo que sea lineal entre enteros o, equivalentemente, para cada $x \geq 0$ definimos

$$\phi(x) = \int_0^x \frac{1}{|G^0 : G^t|}\, dt,$$

con el convenio de que $G^t = G^{\{t\}}$, donde $\{t\}$ es el menor número natural mayor o igual que t. Para extender ϕ a toda la recta real convenimos que $G^t = G^0$ si $-1 < t \leq 0$ y $G^t = G^{-1}$ si $t \leq -1$. Además, para $t < 0$, entenderemos que $|G^0 : G^t| = |G^t : G^0|^{-1}$.

Con estos convenios el integrando $1/|G^0 : G^t|$ es una función escalonada en $\mathbb{R}$ con un número finito de escalones, descritos en la tabla siguiente:

intervalo	$1/\lvert G^0 : G^t\rvert$	
$]-\infty,\ -1\ ]$	f	
$]-1\ ,\ \ 0\ ]$	1	
$]\ \ 0\ ,\ \ 1\ ]$	$1/e_0$	
$]\ \ i\ \ , i+1]\quad (i>0)$	e_{i+1}/e	$(e_{i+1} = \lvert G^{i+1}\rvert)$
$]\ \ i\ \ , +\infty]\quad (G^i = 1)$	$1/e$	

De aquí se deducen inmediatamente las propiedades de la función ϕ:

a) ϕ es una función continua estrictamente monótona creciente.

b) $\phi(-\infty) = -\infty$, $\phi(-1) = -1$, $\phi(0) = 0$, $\phi(+\infty) = +\infty$.

c) ϕ tiene derivadas laterales ϕ'_i y ϕ'_d en todos los puntos y ambas son monótonas decrecientes.

d) Si x no es un entero o $G^x = G^{x+1}$ entonces

$$\phi'_i(x) = \phi'_d(x) = 1/|G^0 : G^x|.$$

e) Si i es un entero tal que $G^i \neq G^{i+1}$ entonces

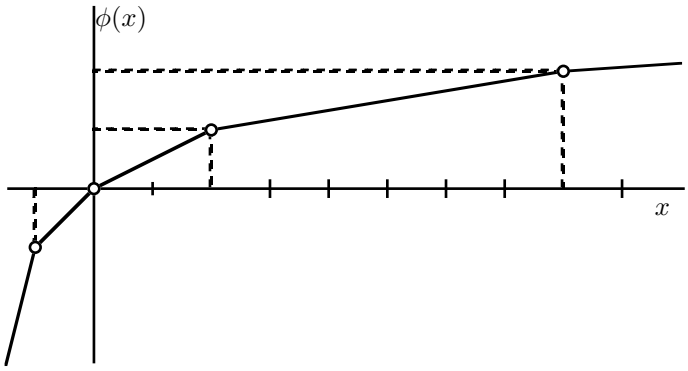
$$\phi'_i(i) = 1/|G^0 : G^i|, \qquad \phi'_d(i) = 1/|G^0 : G^{i+1}|.$$

f) $\phi'(-\infty) = f$, $\phi'(+\infty) = 1/e$.

La propiedad d) implica que ϕ es derivable en $\mathbb{R}$ excepto en un número finito de puntos. Concretamente, ϕ es derivable en -1 si y sólo si $f = 1$, ϕ es derivable en 0 si y sólo si $e_0 = 1$ y los demás puntos donde ϕ no es derivable son los números de ramificación definidos en 10.10.

Por ejemplo, la figura siguiente muestra la función ϕ de cualquiera de los divisores de 3 en el cuerpo ciclotómico de orden $3^3 \cdot 5$. Se cumple $f = 4$, $e = 18$, $e_0 = 2$ y los números de ramificación son $v_1 = 0$, $v_2 = 2$, $v_3 = 8$, de modo que

$$G^{-1} > G^0 > G^1 = G^2 > G^3 = G^4 = G^5 = G^6 = G^7 = G^8 > G^9 = 1.$$



Se define la *función de Hasse* como la inversa de la función ϕ. La representaremos por $\psi_{\mathfrak{P}}$, o simplemente ψ. Sus propiedades se deducen inmediatamente de las de la función ϕ por los resultados del análisis elemental. Las enumeramos a continuación:

a) ψ es una función continua estrictamente monótona creciente.

b) $\psi(-\infty) = -\infty$, $\psi(-1) = -1$, $\psi(0) = 0$, $\psi(+\infty) = +\infty$.

c) ψ tiene derivadas laterales ψ'_i y ψ'_d en todos los puntos y ambas son monótonas crecientes.

d) Para todo $x \geq -1$ los números $\psi'_i(x)$ y $\psi'_d(x)$ son naturales (excepto $\psi'_i(-1)$).

e) $\psi'(-\infty) = 1/f$, $\psi'(+\infty) = e$.

f) Si i es un número entero $i \geq -1$ entonces $\psi(i)$ también es entero.

La última propiedad se demuestra fácilmente a partir de d).

Si $k \subset L \subset K$ es una cadena de cuerpos numéricos o p-ádicos donde las tres extensiones sean de Galois, representaremos por $\overline{\phi}$ y $\overline{\psi}$ las funciones en K/L (para un primo dado $\mathfrak{P}$) y por $\underline{\phi}$, y $\underline{\psi}$ las de L/k (para el divisor de $\mathfrak{P}$ en L). En estos términos el teorema 10.17 afirma que

$$\underline{i}(\underline{\sigma}) = \overline{\phi}(l(\sigma)).$$

Ahora ya podemos relacionar los grupos de ramificación de L/k con los de K/k.

Teorema 10.19 *Sea $k \subset L \subset K$ una cadena de cuerpos numéricos o p-ádicos donde las tres extensiones sean de Galois. Sea $H = G(K/L)$ y $\mathfrak{P}$ un primo en K. Entonces, para cada número real x, se cumple*

$$\underline{G}^x = G^{\overline{\psi}(x)}H/H, \qquad L_x = K_{\overline{\psi}(x)} \cap L.$$

DEMOSTRACIÓN: Tomemos $\sigma \in G_{\mathfrak{P}}$. La notación $\underline{\sigma}$ representa indistintamente la clase σH o la restricción $\sigma|_L$. Entonces

$$\underline{\sigma} \in \underline{G}^{\overline{\phi}(x)} \Leftrightarrow \underline{i}(\underline{\sigma}) \geq \overline{\phi}(x), \Leftrightarrow \overline{\phi}(l(\sigma)) \geq \overline{\phi}(x), \Leftrightarrow l(\sigma) \geq x, \Leftrightarrow l(\sigma) \geq \{x\}$$

$$\Leftrightarrow \sigma \in G^{\{x\}}H \text{ (por definición de } l(\sigma)) \Leftrightarrow \sigma \in G^x H.$$

(Recordemos que $\{x\}$ representa al menor entero $\geq x$.)

Esto prueba que $\underline{G}^{\overline{\phi}(x)} = G^x H/H$ para todo $x \in \mathbb{R}$, pero esto equivale a la igualdad del enunciado. ∎

Con esto hemos cumplido el objetivo que nos habíamos propuesto. Terminamos la sección con un resultado de interés en torno a la función de Hasse y su inversa.

Teorema 10.20 *Sea $k \subset L \subset K$ es una cadena de cuerpos numéricos o p-ádicos donde las tres extensiones sean de Galois. Sea $\mathfrak{P}$ un primo en K. Entonces para todo $x \in \mathbb{R}$ se cumple*

$$\phi(x) = \underline{\phi}\big(\overline{\phi}(x)\big), \qquad \psi(x) = \overline{\psi}\big(\underline{\psi}(x)\big).$$

DEMOSTRACIÓN: Sea $H = G(K/L)$. Las funciones ϕ, $\underline{\phi}$ y $\overline{\phi}$ son continuas y derivables excepto en un número finito de puntos. En los puntos donde son derivables tenemos

$$\frac{d}{dx}\underline{\phi}\big(\overline{\phi}(x)\big) = \underline{\phi}'\big(\overline{\phi}(x)\big)\,\overline{\phi}'(x) = \frac{1}{|\underline{G}^0 : \underline{G}^{\overline{\phi}(x)}|}\,\frac{1}{|\overline{G}^0 : \overline{G}^x|}$$

$$= \frac{1}{|G^0H : G^xH|}\,\frac{1}{|G^0 \cap H : G^x \cap H|} = \frac{1}{|G^0 : G^x|} = \phi'(x).$$

Teniendo en cuenta que ambas funciones valen 0 en 0, el análisis elemental muestra que en estas condiciones $\phi(x) = \underline{\phi}\big(\overline{\phi}(x)\big)$. La otra igualdad es consecuencia inmediata de ésta. ∎

10.4 La ramificación y el isomorfismo de Artin

Toda la teoría que hemos desarrollado hasta ahora en este capítulo es independiente de la teoría de cuerpos de clases. Ahora vamos a involucrarla demostrando una generalización del teorema de ramificación. Recordemos que este teorema afirma que en una extensión abeliana de cuerpos p-ádicos K/k, el grupo de inercia G^0 se corresponde a través del isomorfismo de Artin con el grupo de las unidades U de k^*. Lo que vamos a probar es que si llamamos $U_i = \{u \in U \mid u \equiv 1 \text{ (mód } \mathfrak{p}^i)\}$, donde $\mathfrak{p}$ es el primo de k, entonces la imagen de U_i por el homomorfismo de Artin es el grupo de ramificación $G^{\psi(i)}$. De aquí obtendremos resultados para el cálculo de conductores. Recordemos que ya habíamos tocado los grupo U_i en el teorema 7.20.

Empezamos con un par de teoremas auxiliares. Notar que si E/D es una extensión de dominios de Dedekind y K/k es la extensión de cuerpos de cocientes, la imagen de un ideal fraccional $\mathfrak{a}$ de K por la traza $\mathrm{Tr} : K \longrightarrow k$ es un ideal fraccional de k que llamaremos $\mathrm{Tr}(\mathfrak{a})$. Si $\mathfrak{a}$ es un ideal entonces $\mathrm{Tr}(\mathfrak{a})$ también es un ideal.

Teorema 10.21 *Sea K/k una extensión cíclica de grado primo q de cuerpos p-ádicos. Sea $\mathfrak{P}$ el primo de K, sea s un número natural y α_s un elemento de K tal que $v_{\mathfrak{P}}(\alpha_s) \geq s$. Entonces, para todo x entero en k se cumple*

$$\mathrm{N}(1 + x\alpha_s) \equiv 1 + x\,\mathrm{Tr}(\alpha_s) + x^q\,\mathrm{N}(\alpha_s) \ (\mathrm{mód}\ \ \mathrm{Tr}(\mathfrak{P}^{2s})).$$

Demostración: Sea σ un generador del grupo de Galois. Entonces

$$\mathrm{N}(1 + x\alpha_s) = \big(1 + x\alpha_s\big)\big(1 + x\sigma(\alpha_s)\big)\big(1 + x\sigma^2(\alpha_s)\big)\cdots\big(1 + x\sigma^{q-1}(\alpha_s)\big).$$

Los tres términos de la congruencia del enunciado aparecen al desarrollar este producto. Hemos de ver que los restantes son divisibles entre $\mathrm{Tr}(\mathfrak{P}^{2s})$.

Dichos términos son de la forma $x^r\alpha_s^{P(\sigma)}$, donde $P(\sigma)$ es un polinomio en σ de grado r con todos los coeficientes iguales a 0 o a 1 y con al menos dos monomios (usamos el convenio de que $\alpha^{\sigma+\tau} = \sigma(\alpha)\tau(\alpha)$). De hecho, todo polinomio en estas condiciones da lugar a un termino.

El único polinomio que cumple $P(\sigma)\sigma = \sigma$ es $1 + \sigma + \sigma^2 + \cdots + \sigma^{q-1}$, que da lugar al término $x^q\,\mathrm{N}(\alpha_s)$, pero éste es uno de los de la fórmula del enunciado, luego no lo estamos considerando ahora. Dado cualquier otro polinomio, los polinomios $P(\sigma)$, $P(\sigma)\sigma, \ldots, P(\sigma)\sigma^{q-1}$ son todos distintos.[2] Agrupando los términos que les corresponden, obtenemos un término de la forma $x^r\,\mathrm{Tr}(\alpha_s^{P(\sigma)})$. Como P tiene al menos dos monomios, $\alpha_s^{P(\sigma)}$ es divisible entre $\mathfrak{P}^{2s}$, luego $\mathrm{Tr}(\alpha_s^{P(\sigma)}) \in \mathrm{Tr}(\mathfrak{P}^{2s})$. ∎

Teorema 10.22 *Sea K/k una extensión de Galois de cuerpos p-ádicos de grado primo q y totalmente ramificada. Sean $\mathfrak{P}$ y $\mathfrak{p}$ los primos de K y k respectivamente y sea $\mathfrak{D} = \mathfrak{P}^m$ el diferente de la extensión. Entonces, para todo entero s se tiene que $\mathrm{Tr}(\mathfrak{P}^s) = \mathfrak{p}^r$, donde r es la parte entera de $(m+s)/q$.*

Demostración: Sea $\mathrm{Tr}(\mathfrak{P}^s) = \mathfrak{p}^r$ y vamos a calcular r. Observemos que el hecho de que la extensión sea totalmente ramificada significa que $\mathfrak{p} = \mathfrak{P}^q$. Es fácil comprobar que $1 = \mathfrak{p}^{-r}\,\mathrm{Tr}(\mathfrak{P}^s) = \mathrm{Tr}(\mathfrak{p}^{-r}\mathfrak{P}^s) = \mathrm{Tr}(\mathfrak{P}^{s-qr})$. Teniendo en cuenta la definición del diferente, esto implica que $\mathfrak{P}^{s-qr} \subset \mathfrak{D}^{-1}$, luego $\mathfrak{D} \subset \mathfrak{P}^{qr-s}$ y por lo tanto $qr - s \leq m$, o también, $r \leq E[(m+s)/q]$.

Recíprocamente, como $\mathrm{Tr}(\mathfrak{P}^s)$ no está contenido en $\mathfrak{p}^{r+1}$, el mismo razonamiento nos lleva a que $\mathrm{Tr}(\mathfrak{P}^{s-q(r+1)})$ no está contenido en 1 (o sea, en el anillo de enteros de k). En consecuencia, $\mathfrak{P}^{s-q(r+1)}$ no está contenido en $\mathfrak{D}^{-1}$ y $\mathfrak{D}$ no está contenido en $\mathfrak{P}^{q(r+1)-s}$, luego $q(r+1) - s > m$ y así $r + 1 > E[(m+s)/q]$. ∎

[2]Por ejemplo porque G actúa sobre el conjunto de los polinomios del tipo indicado, luego la órbita de uno de ellos ha de tener cardinal 1 o q, y el primer caso ya está descartado.

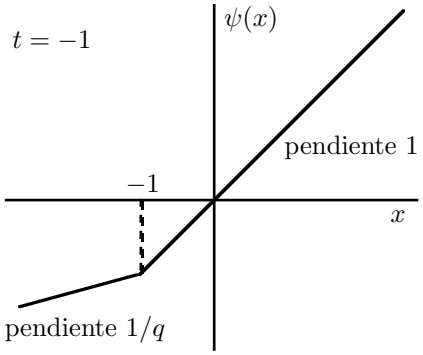
Ahora abordamos el núcleo de la demostración, consistente en analizar las extensiones cíclicas de grado primo. Como tenemos que trabajar simultáneamente con los grupos de unidades de dos cuerpos K y k, conviene que cambiemos temporalmente la notación y llamemos $K_i = 1 + \mathfrak{P}^i$ a los grupos de unidades de K y $k_i = 1 + \mathfrak{p}^i$ a los de k. No hay peligro de confundirlos con los cuerpos de ramificación porque no van a intervenir en los próximos razonamientos. Convenimos también en que K_0 es el grupo de todas las unidades de K y que K_{-1} es el grupo multiplicativo K^*.

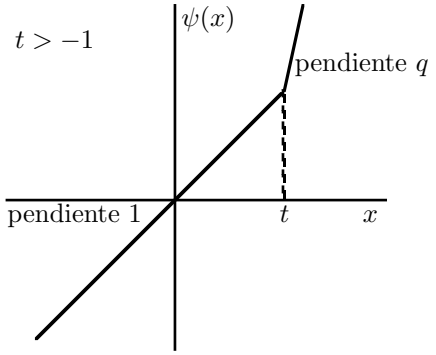
Teorema 10.23 *Sea K/k una extensión de cuerpos p-ádicos cíclica de grado primo q. Sea t el mayor entero tal que $G^t \neq 1$. Para todo entero $i \geq -1$ se cumple*

a) $\mathrm{N}[K_{\psi(i)}] \leq k_i, \quad \mathrm{N}[K_{\psi(i)+1}] \leq k_{i+1}.$

b) $|k_i : k_{i+1}\,\mathrm{N}[K_{\psi(i)}]| \leq \begin{cases} 1 & \text{si } i \neq t, \\ q & \text{si } i = t. \end{cases}$

Demostración: Sea $\mathfrak{P}$ el primo de K, sea $\mathfrak{p}$ el primo de k y p la característica del cuerpo de restos módulo $\mathfrak{P}$. Como el grupo de Galois G tiene orden primo, los grupos de ramificación son $G^i = G$ si $i \leq t$ y $G^i = 1$ si $i > t$. La extensión es no ramificada si y sólo si $t = -1$. Si $t = 0$ la ramificación es dominada ($q \neq p$), mientras que si $t > 0$ la ramificación es libre ($q = p$). La función de Hasse es como sigue:





$\psi(x) = x \quad$ para $x \geq -1$

$$\psi(x) = \begin{cases} x & \text{si } -1 \leq x \leq t, \\ t + q(x - t) & \text{si } \quad t \leq x. \end{cases}$$

Distinguimos varios casos.

a) $i = -1$.

En este caso $\psi(-1) = -1$ y las inclusiones son obvias: $\mathrm{N}[K_{-1}] \leq k_{-1}$, $\mathrm{N}[K_0] \leq k_0$. Respecto al índice, el teorema 8.24 nos da que $|k_{-1} : \mathrm{N}[K_{-1}]| = q$, y por 7.9 sabemos que $k_0\,\mathrm{N}[K_{-1}] = \mathrm{N}[K_{-1}]$ si y sólo si $t = -1$, luego tenemos que $|k_{-1} : k_0\,\mathrm{N}[K_{-1}]|$ vale 1 o q según el valor de t.

b) $i = 0$.

Ahora $\psi(0) = 0$. Obviamente $\mathrm{N}[K_0] \le k_0$ y la inclusión $\mathrm{N}[K_1] \le k_1$ se demuestra fácilmente. Si $t = -1$ entonces la extensión es no ramificada y por el teorema 7.9 se cumple

$$|k_0 : k_1\,\mathrm{N}[K_0]| \le |k_0 : \mathrm{N}[K_0]| = 1.$$

Supongamos, pues, $t \ge 0$. En la prueba del teorema 7.20 vimos que el cociente k_0/k_1 es isomorfo al cuerpo de restos $\overline{k}^*$, donde el isomorfismo es el natural (asigna a la clase de u la clase de u). Sea H la imagen de $k_1\,\mathrm{N}[K_0]/k_1$ a través de este isomorfismo. Entonces $|k_0 : k_1\,\mathrm{N}[K_0]| = |\overline{k}^* : H|$.

Un elemento de H es de la forma $[\mathrm{N}(\alpha)]$, con $\alpha \in K_0$, pero la extensión $\overline{K}/\overline{k}$ es trivial, y todos los k-automorfismos de K inducen la identidad en $\overline{K}$, luego $[\mathrm{N}(\alpha)] = [\alpha]^q$. Por consiguiente $H = \overline{k}^{*q}$.

Si $t > 0$ la ramificación es libre, luego $q = p$ (la característica de $\overline{k}$) y como $\overline{k}$ es perfecto tenemos $|\overline{k}^* : \overline{k}^{*q}| = 1$.

Si $t = 0$ entonces $q \ne p$, pero el índice $|\overline{k}^* : \overline{k}^{*q}|$ es el orden del núcleo del homomorfismo $\overline{k}^* \longrightarrow \overline{k}^{*q}$ dado por $u \mapsto u^q$ y éste a lo sumo tiene q elementos (pues el polinomio $x^q - 1$ no puede tener más de q raíces en $\overline{k}$).

c) $i \ge 1$.

Vamos a aplicar los teoremas 10.22 y 10.21 en varias ocasiones. Según el teorema 10.11, el exponente del diferente es $m = (t+1)(q-1)$. Sea π un primo de k. Distinguimos varios subcasos.

c.1) $t = -1$.

Tenemos $\psi(i) = i$. La extensión es no ramificada, luego π también es primo en K. En lugar de aplicar el teorema 10.21, en este caso es más rápido comprobar que para todo entero α de K se cumple

$$\mathrm{N}(1 + \alpha\pi^i) \equiv 1 + \mathrm{Tr}(\alpha)\pi^i \ (\text{mód } \mathfrak{p}^{i+1}).$$

Esto nos da inmediatamente las inclusiones $\mathrm{N}[K_i] \le k_i$, $\mathrm{N}[K_{i+1}] \le k_{i+1}$. Falta probar la igualdad $k_i = k_{i+1}\,\mathrm{N}[K_i]$. Para ello tomamos un elemento arbitrario $u = 1 + \beta\pi^i \in k_i$. Consideramos la extensión de cuerpos de restos $\overline{K}/\overline{k}$ y usamos que la traza de esta extensión es suprayectiva, así como que sus automorfismos se corresponden biunívocamente con los de la extensión K/k. Por ello podemos afirmar que existe un entero $\alpha \in K$ tal que $[\beta] = \mathrm{Tr}([\alpha]) = [\mathrm{Tr}(\alpha)]$. Llamando $v = 1 + \alpha\pi^i \in K_i$, tenemos que

$$\mathrm{N}(v) \equiv 1 + \mathrm{Tr}(\alpha)\pi^i \equiv 1 + \beta\pi^i \ (\text{mód } \mathfrak{p}^{i+1}),$$

luego $u/\,\mathrm{N}(v) \in k_{i+1}$ y $u \in k_{i+1}\,\mathrm{N}[K_i]$.

c.2) $0 \le t \le i$.

En este caso $\psi(i) = t + q(i-t) = -(q-1)t + qi$, luego $\psi(i) + m = qi + (q-1)$. Usando 10.22 obtenemos

$$\mathrm{Tr}(\mathfrak{P}^{\psi(i)}) = \mathfrak{p}^i, \quad \mathrm{Tr}(\mathfrak{P}^{\psi(i)+1}) = \mathfrak{p}^{i+1}, \quad \mathrm{Tr}(\mathfrak{P}^{2\psi(i)}) \subset \mathfrak{p}^{i+1}.$$

Por otro lado, como $\psi(i) \geq i$, tenemos $\mathrm{N}(\mathfrak{P}^{\psi(i)}) \subset \mathfrak{p}^i$ y $\mathrm{N}(\mathfrak{P}^{\psi(i)+1}) \subset \mathfrak{p}^{i+1}$ (pues en el caso ramificado $\mathrm{N}(\mathfrak{P}) = \mathfrak{p}$). Con estos datos, el teorema 10.21 nos da

$$\begin{aligned} \mathrm{N}(1+\alpha_{\psi(i)}) &\equiv 1 \ (\text{mód } \mathfrak{p}^i), \\ \mathrm{N}(1+\alpha_{\psi(i)+1}) &\equiv 1 \ (\text{mód } \mathfrak{p}^{i+1}), \end{aligned}$$

para cualquier $\alpha_{\psi(i)} \in \mathfrak{P}^{\psi(i)}$, $\alpha_{\psi(i)+1} \in \mathfrak{P}^{\psi(i)+1}$, luego tenemos las inclusiones $\mathrm{N}[K_{\psi(i)}] \leq k_i$ y $\mathrm{N}[K_{\psi(i)+1}] \leq k_{i+1}$. Para acotar el índice distinguimos dos casos más.

c.2.1) $t < i$.

Entonces $\psi(i) > i$, luego $\mathrm{N}(\mathfrak{P}^{\psi(i)}) \subset \mathfrak{p}^{i+1}$, y el teorema 10.21 nos da que

$$\mathrm{N}(1+\alpha_{\psi(i)}) \equiv 1 + \mathrm{Tr}(\alpha_{\psi(i)}) \ (\text{mód } \mathfrak{p}^{i+1}).$$

Como $\mathrm{Tr}(\mathfrak{P}^{\psi(i)}) = \mathfrak{P}^i$, dado un $u = 1+\beta \in k_i$, existe un $\alpha_{\psi(i)} \in \mathfrak{P}^{\psi(i)}$ tal que $\mathrm{Tr}(\alpha_{\psi(i)}) = \beta$, con lo que $v = 1+\alpha_{\psi(i)} \in K_{\psi(i)}$ y $\mathrm{N}(v) \equiv u$ (mód $\mathfrak{p}^{i+1}$). Así pues, $u/\mathrm{N}(v) \in k_{i+1}$ y $u \in k_{i+1}\,\mathrm{N}[K_{\psi(i)}]$.

c.2.2) $t = i$.

Como estamos suponiendo $i > 0$, tenemos de hecho $t > 0$, luego la ramificación es libre ($q = p$). Ahora $\psi(i) = i = t$, $\mathrm{Tr}(\mathfrak{P}^i) = \mathfrak{p}^i$, $\mathrm{Tr}(\mathfrak{P}^{i+1}) = \mathfrak{p}^{i+1}$. Existe un $\alpha \in \mathfrak{P}^i$ tal que $\mathrm{Tr}(\alpha) \notin \mathfrak{p}^{i+1}$, con lo que $\alpha \notin \mathfrak{P}^{i+1}$. Sea $\mathrm{Tr}(\alpha) = b\pi^i$, con $b \notin \mathfrak{p}$. También tenemos que $\mathrm{N}(\mathfrak{P}^i) = \mathfrak{p}^i$, luego $\mathrm{N}(\alpha) = a\pi^i$, con $a \notin \mathfrak{p}$.

Para todo entero x de k el teorema 10.21 nos da que

$$\mathrm{N}(1+x\alpha) \equiv 1 + x\,\mathrm{Tr}(\alpha) + x^q\,\mathrm{N}(\alpha) \ (\text{mód } \mathfrak{p}^{i+1}),$$

o sea,

$$\mathrm{N}(1+x\alpha) \equiv 1 + \pi^i(ax^q + b) \ (\text{mód } \mathfrak{p}^{i+1}).$$

Sea $f : \overline{k} \longrightarrow \overline{k}$ el homomorfismo dado por $f(x) = [a]x^q + [b]$ (recordar que $q = p$). Consideramos también el homomorfismo $k_i \longrightarrow \overline{k}/f[\overline{k}]$ determinado por $1 + \beta\pi^i \mapsto [\beta]$.

Si un elemento $u = 1+\beta\pi^i$ está en su núcleo entonces $\beta \equiv ax^q + b$ (mód $\mathfrak{p}$) para cierto entero x de k, luego $1+\beta\pi^i \equiv 1+\pi^i(ax^q+b)$ (mód $\mathfrak{p}^{i+1}$), lo que a su vez implica que $u \equiv \mathrm{N}(1+x\alpha)$ (mód $\mathfrak{p}^{i+1}$). De aquí se sigue como en casos anteriores que $u \in k_{i+1}\,\mathrm{N}[K_i]$.

Así pues, si llamamos N al núcleo del homomorfismo, tenemos

$$|k_i : k_{i+1}\,\mathrm{N}[K_i]| \leq |k_i : N| = |\overline{k} : f[\overline{k}]|.$$

Este último índice es igual al orden del núcleo de f, o sea, al número de raíces en $\overline{k}$ del polinomio $[a]x^q + [b]$, que a lo sumo es q, que es la cota buscada.

c.3) $0 \leq i < t$.

En este caso $\psi(i) = i < t$, luego

$$\psi(i) + m = i + (t+1)(q-1) > i + (i+1)(q-1) = qi + q - 1.$$

Así, $\psi(i) + m \geq q(i+1)$ y usando 10.22 obtenemos

$$\mathrm{Tr}(\mathfrak{P}^{\psi(i)}) \subset \mathfrak{p}^{i+1}, \quad \mathrm{Tr}(\mathfrak{P}^{\psi(i)+1}) \subset \mathfrak{p}^{i+1}, \quad \mathrm{Tr}(\mathfrak{P}^{2\psi(i)}) \subset \mathfrak{p}^{i+1}.$$

Como $f = 1$, se cumple $\mathrm{N}(\mathfrak{P}^{\psi(i)}) = \mathfrak{p}^i$, $\mathrm{N}(\mathfrak{P}^{\psi(i)+1}) = \mathfrak{p}^{i+1}$. El teorema 10.21 nos da

$$\begin{aligned} \mathrm{N}(1 + \alpha_{\psi(i)}) &\equiv 1 \ (\text{mód } \mathfrak{p}^i), \\ \mathrm{N}(1 + \alpha_{\psi(i)+1}) &\equiv 1 \ (\text{mód } \mathfrak{p}^{i+1}), \end{aligned}$$

de donde se siguen las inclusiones.

Para calcular el índice observamos que, con más precisión,

$$\mathrm{N}(1 + \alpha_{\psi(i)}) \equiv 1 + \mathrm{N}(\alpha_{\psi(i)}) \ (\text{mód } \mathfrak{p}^{i+1}).$$

Por lo tanto, si $u = 1 + \beta \in k_i$, entonces $\beta \in \mathfrak{p}^i = \mathrm{N}(\mathfrak{P}^{\psi(i)})$, luego existe un $\alpha_{\psi(i)} \in \mathfrak{P}^{\psi(i)}$ de modo que $v = 1 + \alpha_{\psi(i)} \in K_{\psi(i)}$ cumple $\mathrm{N}(v) \equiv u$ (mód $\mathfrak{p}^{i+1}$), luego $u/\mathrm{N}(v) \in k_{i+1}$ y $u \in k_{i+1}\,\mathrm{N}[K_{\psi(i)}]$. ∎

Ahora generalizamos el teorema a extensiones de Galois cualesquiera. En realidad sólo nos hace falta para extensiones abelianas, pero la prueba es la misma en ambos casos.

Dada una extensión de Galois K/k, definimos $\psi'_{d/i}(x) = \psi'_d(x)/\psi'_i(x)$. Esta función vale 1 excepto en los vértices de la función ψ, donde cumple $\psi'_{d/i}(x) > 1$.

En las hipótesis del teorema anterior el único vértice es t y $\psi'_{d/i}(t) = q$.

Teorema 10.24 *Sea K/k una extensión de Galois de cuerpos p-ádicos. Para todo entero $i \geq -1$ se cumple*

a) $\mathrm{N}[K_{\psi(i)}] \leq k_i, \quad \mathrm{N}[K_{\psi(i)+1}] \leq k_{i+1}$.

b) $|k_i : k_{i+1}\,\mathrm{N}[K_{\psi(i)}]| \leq \psi'_{d/i}(i)$.

Demostración: El teorema está probado para extensiones cíclicas de grado primo. Por el teorema 10.6 sabemos que K/k es resoluble, luego podemos formar una cadena de cuerpos intermedios de modo que cada uno sea una extensión cíclica de grado primo del anterior. Todo se reduce a probar que si tenemos una cadena $k \subset L \subset K$ y el teorema se cumple para L/k y K/L, entonces también se cumple para K/k.

Tenemos la transitividad de las normas: $\mathrm{N}(\alpha) = \underline{\mathrm{N}}(\overline{\mathrm{N}}(\alpha))$ y la de la función de Hasse: $\psi(x) = \overline{\psi}(\underline{\psi}(x))$.

Por hipótesis

$$\begin{aligned} &\underline{\mathrm{N}}[L_{\underline{\psi}(i)}] \leq k_i \quad &&\text{y} \quad \overline{\mathrm{N}}[K_{\overline{\psi}(\underline{\psi}(i))}] \leq L_{\underline{\psi}(i)}, \\ &\underline{\mathrm{N}}[L_{\underline{\psi}(i)+1}] \leq k_{i+1} \quad &&\text{y} \quad \overline{\mathrm{N}}[K_{\overline{\psi}(\underline{\psi}(i))+1}] \leq L_{\underline{\psi}(i)+1}, \end{aligned}$$

y en consecuencia

$$\begin{aligned} \mathrm{N}[K_{\psi(i)}] &= \underline{\mathrm{N}}[\overline{\mathrm{N}}[K_{\psi(i)}]] \leq \underline{\mathrm{N}}[L_{\underline{\psi}(i)}] \leq k_i, \\ \mathrm{N}[K_{\psi(i)+1}] &= \underline{\mathrm{N}}[\overline{\mathrm{N}}[K_{\psi(i)+1}]] \leq \underline{\mathrm{N}}[L_{\underline{\psi}(i)+1}] \leq k_{i+1}. \end{aligned}$$

Respecto al índice, teniendo en cuenta la primera inclusión, se descompone en

$$|k_i : k_{i+1}\,\mathrm{N}[K_{\psi(i)}]| = |k_i : k_{i+1}\underline{\mathrm{N}}[L_{\underline{\psi}(i)}]|\,|k_{i+1}\underline{\mathrm{N}}[L_{\underline{\psi}(i)}] : k_{i+1}\,\mathrm{N}[K_{\psi(i)}]|. \quad (10.5)$$

El primer índice lo tenemos acotado por $\underline{\psi}'_{d/i}(i)$. Ocupémonos del segundo. Puesto que $\underline{\mathrm{N}}[L_{\underline{\psi}(i)+1}] \leq k_{i+1}$, se cumple

$$k_{i+1}\,\mathrm{N}[K_{\psi(i)}] = k_{i+1}\,\underline{\mathrm{N}}[L_{\underline{\psi}(i)+1}]\,\underline{\mathrm{N}}[\overline{\mathrm{N}}[K_{\psi(i)}]] = k_{i+1}\,\underline{\mathrm{N}}[L_{\underline{\psi}(i)+1}\,\overline{\mathrm{N}}[K_{\psi(i)}]].$$

Así pues,

$$|k_{i+1}\,\underline{\mathrm{N}}[L_{\underline{\psi}(i)}] : k_{i+1}\,\mathrm{N}[K_{\psi(i)}]| = |k_{i+1}\,\underline{\mathrm{N}}[L_{\underline{\psi}(i)}] : k_{i+1}\,\underline{\mathrm{N}}[L_{\underline{\psi}(i)+1}\,\overline{\mathrm{N}}[K_{\psi(i)}]]|.$$

Esto es el orden del cociente de

$$k_{i+1}\,\underline{\mathrm{N}}[L_{\underline{\psi}(i)}]/k_{i+1} \quad (10.6)$$

sobre el subgrupo

$$k_{i+1}\,\underline{\mathrm{N}}\big[L_{\underline{\psi}(i)+1}\,\overline{\mathrm{N}}[K_{\psi(i)}]\big]/k_{i+1}. \quad (10.7)$$

Aplicamos el teorema de isomorfía a (10.6):

$$k_{i+1}\,\underline{\mathrm{N}}[L_{\underline{\psi}(i)}]/k_{i+1} \cong \underline{\mathrm{N}}[L_{\underline{\psi}(i)}]/\big(k_{i+1} \cap \underline{\mathrm{N}}[L_{\underline{\psi}(i)}]\big).$$

La imagen de (10.7) por el isomorfismo es

$$\underline{\mathrm{N}}\big[L_{\underline{\psi}(i)+1}\,\overline{\mathrm{N}}[K_{\psi(i)}]\big]\big(k_{i+1} \cap \underline{\mathrm{N}}[L_{\underline{\psi}(i)}]\big)/\big(k_{i+1} \cap \underline{\mathrm{N}}[L_{\underline{\psi}(i)}]\big).$$

Por lo tanto, el segundo factor de (10.5) es

$$|\underline{\mathrm{N}}[L_{\underline{\psi}(i)}] : \underline{\mathrm{N}}\big[L_{\underline{\psi}(i)+1}\,\overline{\mathrm{N}}[K_{\psi(i)}]\big]\big(k_{i+1} \cap \underline{\mathrm{N}}[L_{\underline{\psi}(i)}]\big)|$$

$$\leq |\underline{\mathrm{N}}[L_{\underline{\psi}(i)}] : \underline{\mathrm{N}}\big[L_{\underline{\psi}(i)+1}\,\overline{\mathrm{N}}[K_{\psi(i)}]\big]| \leq |L_{\underline{\psi}(i)} : L_{\underline{\psi}(i)+1}\,\overline{\mathrm{N}}[K_{\psi(i)}]|$$

La última desigualdad se sigue, por ejemplo, de 7.8. Así pues, retomando (10.5) llegamos a

$$\begin{aligned} |k_i : k_{i+1}\,\mathrm{N}[K_{\psi(i)}]| &\leq |k_i : k_{i+1}\underline{\mathrm{N}}[L_{\underline{\psi}(i)}]|\,|L_{\underline{\psi}(i)} : L_{\underline{\psi}(i)+1}\,\overline{\mathrm{N}}[K_{\overline{\psi}(\underline{\psi}(i))}]| \\ &\leq \underline{\psi}'_{d/i}\overline{\psi}'_{d/i}(\underline{\psi}(i)) = \psi'_{d/i}(i). \end{aligned}$$

La última igualdad se obtiene aplicando la regla de la cadena a las derivadas laterales. Notar que esto puede hacerse porque la función ψ está formada

por segmentos de rectas (las funciones se hacen derivables en un punto modificándolas sólo a la izquierda o sólo a la derecha de un punto dado, se aplica la regla de la cadena usual y se restringe al lado no modificado). ∎

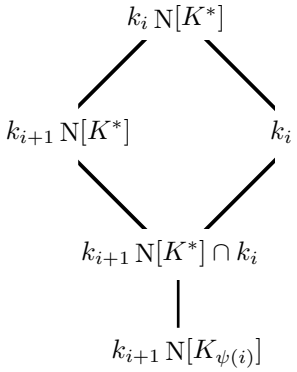
Estamos a punto de obtener las consecuencias deseadas. Consideremos una extensión de Galois de cuerpos p-ádicos K/k. Sabemos que el grupo de normas $\mathrm{N}[K^*]$ es abierto en k, y los grupos k_i forman una base de entornos del neutro, luego existe un natural s tal que $k_s \le \mathrm{N}[K^*]$. Entonces

$$|k^* : \mathrm{N}[K^*]| = |k^* : k_0\,\mathrm{N}[K^*]|\,|k_0\,\mathrm{N}[K^*] : k_1\,\mathrm{N}[K^*]|\cdots|k_{s-1}\,\mathrm{N}[K^*] : k_s\,\mathrm{N}[K^*]|.$$

Como los factores siguientes serían unos, podemos escribir

$$|k^* : \mathrm{N}[K^*]| = \prod_{i=-1}^{\infty} |k_i\,\mathrm{N}[K^*] : k_{i+1}\,\mathrm{N}[K^*]|.$$

Por el teorema anterior sabemos que $\mathrm{N}[K_{\psi(i)}] \le k_i \cap \mathrm{N}[K^*]$. Tenemos la siguiente disposición de subgrupos:



Así,

$$|k_i\,\mathrm{N}[K^*] : k_{i+1}\,\mathrm{N}[K^*]| = |k_i : k_{i+1}\,\mathrm{N}[K^*] \cap k_i| \le |k_i : k_{i+1}\,\mathrm{N}[K_{\psi(i)}]| \le \psi'_{d/i}(i),$$

y en consecuencia

$$|k : \mathrm{N}[K^*]| \le \prod_{i=-1}^{\infty} \psi'_{d/i}(i).$$

Tomando $\epsilon > 0$ suficientemente pequeño, es claro que $\psi'_d(i) = \psi'_i(i+\epsilon) \le \psi'_i(i+1)$, luego $\psi'_d(i)/\psi'_i(i+1) \le 1$ para todo i. Empleando estas cotas queda

$$\prod_{i=-1}^{\infty} \psi'_{d/i}(i) \le \frac{\psi'_d(\infty)}{\psi'_i(-1)} = ef = |K : k|.$$

Si llamamos n al grado de K/k, hemos llegado a que $|k^* : \mathrm{N}[K^*]| \le n$. Esto es la versión local de la segunda desigualdad fundamental. Si la extensión K/k es abeliana el isomorfismo de Artin local prueba que es de hecho una igualdad, y esto implica a su vez que todas las desigualdades intermedias que

hemos empleado son en realidad igualdades. Concretamente, tenemos toda la información siguiente:

$$|k_i\,\mathrm{N}[K^*] : k_{i+1}\,\mathrm{N}[K^*]| = |k_i : k_{i+1}\,\mathrm{N}[K_{\psi(i)}]| = \psi'_{d/i}(i),$$

$$|k_{i+1}\,\mathrm{N}[K^*] \cap k_i : k_{i+1}\,\mathrm{N}[K_{\psi(i)}]| = 1,$$

$$\prod_{i=-1}^{\infty} \psi'_{d/i}(i) = n.$$

Reunimos en un teorema las consecuencias relevantes de estos hechos. Empleamos de nuevo la notación habitual $U_i = 1 + \mathfrak{p}^i$ para los grupos que temporalmente llamábamos k_i. Ahora el contexto deja claro a qué cuerpo se refieren en cada ocasión:

Teorema 10.25 *Sea K/k una extensión abeliana de cuerpos p-ádicos. Entonces*

a) $U_i \cap \mathrm{N}[K^*] \le U_{i+1}\,\mathrm{N}[U_{\psi(i)}]$.

b) $|U_i : U_{i+1}\,\mathrm{N}[U_{\psi(i)}]| = |U_i\,\mathrm{N}[K^*] : U_{i+1}\,\mathrm{N}[K^*]| = \psi'_{d/i}(i)$.

c) Todos los vértices de la función ψ ocurren en argumentos enteros.

Demostración: a) Claramente

$$U_i \cap \mathrm{N}[K^*] \le U_{i+1}\,\mathrm{N}[K^*] \cap U_i = U_{i+1}\,\mathrm{N}[K_{\psi(i)}].$$

b) Ya está probado.

c) El producto de $\psi'_{d/i}(x)$ para todos los valores de x donde ψ tiene un vértice es igual a $n = |K : k|$, pues cada derivada derecha se cancela con la derivada izquierda siguiente y sólo queda $\psi'_d(\infty)/\psi'_i(-1) = ef = n$.

Por otro lado sabemos que si sólo multiplicamos los $\psi'_{d/i}(i)$ para i entero obtenemos también n, y si ψ tiene un vértice en x se cumple $\psi'_{d/i}(x) > 1$, luego ψ no puede tener más vértices que los enteros. ∎

Observar que la propiedad c) no era conocida: sabíamos que los vértices de la función ϕ tienen argumentos enteros (el -1 y los números de ramificación), pero ψ tiene vértices en las imágenes por ϕ de estos números, y no es cierto en general que la imagen por ϕ de un entero sea un entero. Esto tiene interés porque significa que la sucesión $G^{\psi(i)}$, para $i = -1, 0, 1, 2, \ldots$ pasa por todos los grupos de ramificación (quizá con menos repeticiones).

De aquí deducimos por fin los resultados fundamentales:

Teorema 10.26 *Sea K/k una extensión abeliana de cuerpos p-ádicos y sea $i \ge -1$ un número entero. Entonces*

$$U_i \le \mathrm{N}[K^*] \qquad \textit{si y sólo si} \qquad G^{\psi(i)} = 1.$$

DEMOSTRACIÓN: Se cumple $U_i \le \mathrm{N}[K^*]$ si y sólo si

$$|U_j\,\mathrm{N}[K^*] : U_{j+1}\,\mathrm{N}[K^*]| = 1 \qquad \text{para todo } j \ge i.$$

En efecto, si se da la igualdad de los índices tenemos

$$U_i\,\mathrm{N}[K^*] = U_{i+1}\,\mathrm{N}[K^*] = U_{i+2}\,\mathrm{N}[K^*] = \cdots,$$

pero para un j suficientemente grande se tiene que cumplir $U_j \le \mathrm{N}[K^*]$, luego $U_i\,\mathrm{N}[K^*] = \mathrm{N}[K^*]$.

Por el teorema anterior, $U_i \le \mathrm{N}[K^*]$ si y sólo si $\psi'_{d/i}(j) = 1$ para todo $j \ge i$, si y sólo si $\psi'_d(j) = \psi'_i(j)$ para todo $j \ge i$, si y sólo si $G^{\psi(i)} = 1$. ∎

Ahora es fácil probar la generalización del teorema de ramificación, de la que el teorema anterior es un simple caso particular:

Teorema 10.27 *Sea K/k una extensión abeliana de cuerpos p-ádicos. Entonces, para todo entero $i \ge -1$ se cumple*

$$\left(\frac{K/k}{U_i}\right) = G^{\psi(i)}.$$

DEMOSTRACIÓN: Sea $L = K_{\psi(i)}$. Según el teorema 10.19 se cumple que $L = K_{\overline{\psi}(\underline{\psi}(i))} \cap L = L_{\underline{\psi}(i)}$, luego $\underline{G}^{\psi(i)} = 1$ y, por el teorema anterior (aplicado a la extensión L/k), $U_i \le \mathrm{N}[L^*]$. Consecuentemente $\left(\frac{L/k}{U_i}\right) = 1$, lo que equivale a que el grupo $\left(\frac{K/k}{U_i}\right)$ fija a L, es decir, a que $\left(\frac{K/k}{U_i}\right) \le G^{\psi(i)}$.

Sea ahora L el cuerpo fijado por $H = \left(\frac{K/k}{U_i}\right)$. Entonces $\left(\frac{L/k}{U_i}\right) = 1$, con lo que tenemos $U_i \le \mathrm{N}[L^*]$. Por el teorema anterior $\underline{G}^{\psi(i)} = 1$ y, por el teorema 10.19, $G^{\overline{\psi}(\underline{\psi}(i))}H/H = 1$, o sea, $G^{\psi(i)} \le H$. ∎

Terminamos la sección observando que todos los conceptos que hemos definido para primos no arquimedianos tienen, como es habitual, análogos triviales para el caso arquimediano. Una extensión de cuerpos arquimedianos completos ha de ser trivial o isomorfa s $\mathbb{C}/\mathbb{R}$. En el primer caso los grupos de ramificación son necesariamente (por definición) todos triviales. Las extensiones de tipo $\mathbb{C}/\mathbb{R}$ las estamos considerando ramificadas con $e = 2$, $f = 1$. Para definir los grupos de ramificación precisamos este convenio y establecemos que su ramificación es dominada, de modo que los grupos G^{-1} y G^0 tienen orden 2 y los siguientes son triviales. Es fácil ver que todos los teoremas sobre ramificación se extienden ahora trivialmente al caso arquimediano. La función de Hasse es $\psi(x) = x$ en el caso no ramificado y $\psi(x) = 2x$ para $x \ge 0$ en el caso ramificado.

10.5 El conductor y la ramificación

El teorema 10.26 contiene la información necesaria para calcular el conductor de una extensión abeliana de cuerpos numéricos a partir de su ramificación. Con

más precisión, vamos a definir el conductor de una extensión local, probaremos que el conductor de una extensión de cuerpos numéricos es el producto de sus conductores locales y veremos que 10.26 nos da inmediatamente los conductores locales.

Definición 10.28 Sea K/k una extensión abeliana de cuerpos p-ádicos. Sea $\mathfrak{p}$ el primo de k. Definimos el *conductor* de la extensión como $\mathfrak{f} = \mathfrak{p}^i$, donde i es el mínimo natural tal que $U_i \leq \mathrm{N}[K^*]$.

La definición es correcta, pues el grupo de normas es abierto y los grupos U_i forman una base de entornos del neutro. Si la extensión es no ramificada entonces toda unidad es una norma y por lo tanto $\mathfrak{f} = 1$.

Si K/k es una extensión de cuerpos completos arquimedianos y $\mathfrak{p}$ es el divisor de k, definimos $\mathfrak{f} = \mathfrak{p}$ si $K \neq k$ (es decir, si la extensión es $\mathbb{C}/\mathbb{R}$) y $\mathfrak{f} = 1$ si $K = k$.

Si K/k es una extensión abeliana de cuerpos numéricos, para cada primo $\mathfrak{p}$ de k (finito o infinito), la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ no depende de la elección del divisor $\mathfrak{P}$ de $\mathfrak{p}$ en K, y tenemos definido el conductor local $\mathfrak{f}_\mathfrak{p}$. Puesto que el número de primos ramificados es finito, casi todos los conductores locales son iguales a 1.

Teorema 10.29 *Sea K/k una extensión abeliana de cuerpos numéricos y sea $\mathfrak{f}$ su conductor. Entonces*

$$\mathfrak{f} = \prod_\mathfrak{p} \mathfrak{f}_\mathfrak{p},$$

donde el producto se puede restringir a los primos ramificados de k, pues los conductores restantes son iguales a 1.

Demostración: Según el teorema 8.18, un divisor $\mathfrak{m}$ de k es admisible para K/k si y sólo si $W_\mathfrak{m} \leq H$, donde H es el grupo de clases de K. Esto equivale a que $W_\mathfrak{m}(\mathfrak{p}) \leq \mathrm{N}[K_\mathfrak{P}]$ para todo primo $\mathfrak{p}$ de k y todo $\mathfrak{P}$ que lo divida en K.

En efecto, una implicación es clara y, si $\mathfrak{m}$ es admisible, entonces

$$W_\mathfrak{m}(\mathfrak{p}) = W_\mathfrak{m} \cap k_\mathfrak{p}^* \leq H \cap k_\mathfrak{p}^* = \mathrm{N}[K_\mathfrak{P}^*],$$

por el teorema 8.17.

Si $\mathfrak{p}$ es finito entonces $W_\mathfrak{m}(\mathfrak{p}) = U_{\mathfrak{m}_\mathfrak{p}}$, luego la condición $W_\mathfrak{m}(\mathfrak{p}) \leq \mathrm{N}[K_\mathfrak{P}]$ equivale a que $\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}$ sea admisible para la extensión local $K_\mathfrak{P}/k_\mathfrak{p}$ (a que sea múltiplo de $\mathfrak{f}_\mathfrak{p}$).

Con los convenios que hemos adoptado, esto es cierto también para los primos infinitos. En efecto, si $\mathfrak{p}$ es real y $W_\mathfrak{m}(\mathfrak{p}) \leq \mathrm{N}[K_\mathfrak{P}]$ entonces, o bien, $\mathfrak{p} \mid \mathfrak{m}$ y entonces trivialmente $\mathfrak{f}_\mathfrak{p} \mid \mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}$, o bien $\mathfrak{p} \nmid \mathfrak{m}$, y entonces $\mathrm{N}[K_\mathfrak{P}] = k_\mathfrak{p}^*$, luego $K_\mathfrak{P} = k_\mathfrak{p}$, $\mathfrak{f}_\mathfrak{p} = 1$ y trivialmente $\mathfrak{f}_\mathfrak{p} \mid \mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}$. El recíproco se prueba de forma similar. Para los primos complejos se cumple siempre tanto $\mathrm{N}[K_\mathfrak{P}] = k_\mathfrak{p}^*$ como $\mathfrak{f}_\mathfrak{p} \mid p^{\mathfrak{m}_\mathfrak{p}}$.

Ahora es claro que si $\mathfrak{f}$ es el conductor de K/k, entonces $\mathfrak{p}^{\mathfrak{f}_\mathfrak{p}} = \mathfrak{f}_\mathfrak{p}$. ∎

El teorema 10.26 afirma que en una extensión de cuerpos p-ádicos el exponente del conductor es el mínimo natural i tal que $G^{\psi(i)} = 1$. En el caso

arquimediano esto es cierto trivialmente. Si r es el último número de ramificación de la extensión, entonces $G^r \neq 1$ pero $G^{r+1} = 1$, luego el exponente es $u = \phi(r) + 1$. El teorema siguiente es ahora inmediato:

Teorema 10.30 (Teorema del conductor) *Sea K/k una extensión abeliana de cuerpos numéricos o p-ádicos. Para cada primo $\mathfrak{p}$ de k ramificado en K sea $r_\mathfrak{p}$ su último número de ramificación y sea $u_\mathfrak{p} = \phi(r_\mathfrak{p})+1$. Entonces el conductor de K/k viene dado por*

$$\mathfrak{f} = \prod_\mathfrak{p} \mathfrak{p}^{u_\mathfrak{p}}.$$

Aunque este teorema nos da una expresión explícita para el conductor de una extensión, tiene el inconveniente de que involucra a la función de Hasse (o más exactamente a su inversa). Esto no es ningún problema en la práctica, pues la función de Hasse se puede calcular perfectamente, pero lo cierto es que resulta engorroso trabajar con ella y no es muy útil para obtener consecuencias teóricas. Hay otra fórmula en torno al conductor que, aunque no es explícita como ésta, se maneja con más comodidad tanto a nivel teórico como en los casos concretos. Nos ocupamos de ella a continuación.

En primer lugar hemos de observar que los resultados sobre caracteres de cuerpos numéricos que vimos en la sección 9.2 tienen análogos naturales sobre cuerpos p-ádicos. Si k es un cuerpo p-ádico podemos considerar los *caracteres* del grupo k^*, es decir, los homomorfismos continuos $\chi : k^* \longrightarrow \mathbb{C}^*$. Concretamente nos interesan los caracteres de *período finito*, es decir, aquellos cuyo núcleo N_χ tiene índice finito en k^*, con lo que N_χ es además un subgrupo abierto y tiene un cuerpo de clases K_χ. El conductor de χ será el conductor $\mathfrak{f}_\chi$ de la extensión K_χ/k.

Los caracteres de una extensión abeliana K/k de cuerpos p-ádicos serán los caracteres χ de k^* tales que $\chi[H] = 1$, donde H es el grupo de clases de K. El isomorfismo de Artin $k^*/H \cong G(K/k)$ permite identificar los caracteres de K/k con los del grupo de Galois. Además, si consideramos a χ como carácter de $G(K/k)$, entonces K_χ es el cuerpo fijado por N_χ, de modo que $k \subset K_\chi \subset K$: El mismo argumento que en la sección 9.2 prueba que el conductor de K/k es

$$\mathfrak{f} = \operatorname{mcm}_\chi \mathfrak{f}_\chi,$$

donde χ recorre los caracteres de K/k.

Para tratar conjuntamente el caso de los cuerpos numéricos y los cuerpos p-ádicos consideraremos a los caracteres de una extensión K/k como caracteres de su grupo de Galois. Recordemos que G^* representa al grupo de los caracteres de un grupo abeliano G. El teorema que queremos demostrar es que el producto de todos los conductores $\mathfrak{f}_\chi$ es igual al discriminante de la extensión K/k. Esto nos dará una relación recurrente que en muchos casos nos permitirá calcular conductores más rápidamente que con el teorema 10.30, así como deducir algunas propiedades teóricas de interés. Para ello vamos a encontrar una expresión para el exponente de cada primo $\mathfrak{p}$ en cada conductor $\mathfrak{f}_\chi$.

Definición 10.31 Sea K/k una extensión abeliana de cuerpos numéricos o p-ádicos, sea G su grupo de Galois, sea $\chi \in G^*$ y sea $\mathfrak{p}$ un primo en k. Consideremos un divisor $\mathfrak{P}$ de $\mathfrak{p}$ en K (todo cuanto digamos será independiente de la elección de $\mathfrak{P}$). Definimos

$$f_{\mathfrak{p}\,\chi}(t) = \frac{1}{|G^{\psi(t)}|} \sum_{\sigma \in G^{\psi(t)}} \big(1 - \chi(\sigma)\big) \qquad \text{para } t \geq -1.$$

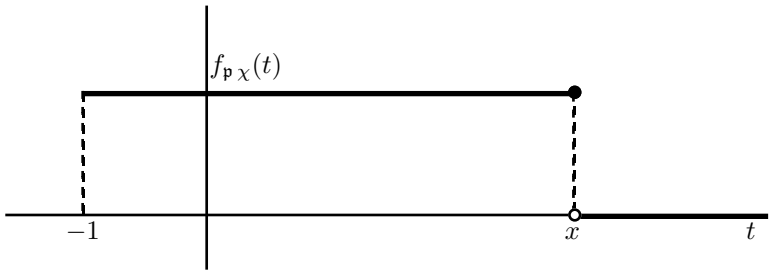
Equivalentemente,

$$f_{\mathfrak{p}\,\chi}(t) = 1 - \frac{1}{|G^{\psi(t)}|} \sum_{\sigma \in G^{\psi(t)}} \chi(\sigma).$$

Las relaciones de ortogonalidad nos dan que

$$f_{\mathfrak{p}\,\chi}(t) = \begin{cases} 1 & \text{si } G^{\psi(t)} \not\leq N_\chi, \\ 0 & \text{si } G^{\psi(t)} \leq N_\chi. \end{cases}$$

Ahora es evidente que $f_{\mathfrak{p}\,\chi}$ es una función escalonada con un único salto en un punto x:



En realidad, $f_{\mathfrak{p}\,\chi}$ puede ser constantemente nula. Esto ocurre si $G_\mathfrak{p} \leq N_\chi$. Entonces convenimos que $x = -1$. En caso contrario $f_{\mathfrak{p}\,\chi}(-1) = 1$.

Teniendo en cuenta que G^t se define como G^i, donde i es el menor entero mayor o igual que t, es claro que $\psi(x)$ ha de ser un número entero y que $G^{\psi(x)}$ no está contenido en N_χ, mientras que $G^{\psi(x)+1}$ sí lo está. Así pues, $\psi(x)$ es un número de ramificación de $\mathfrak{p}$ (salvo que sea -1). En cualquier caso x es un número entero mayor o igual que -1 o, en otras palabras, $x + 1$ es un número natural. Definimos $E_{\mathfrak{p}\,\chi} = x + 1$ o, equivalentemente,

$$E_{\mathfrak{p}\,\chi} = \int_{-1}^{+\infty} f_{\mathfrak{p}\,\chi}(t)\, dt.$$

Teorema 10.32 *En las condiciones anteriores, el número $E_{\mathfrak{p}\,\chi}$ es el exponente de $\mathfrak{p}$ en $\mathfrak{f}_\chi$.*

Demostración: Supongamos que k y K son cuerpos numéricos. La prueba en el caso p-ádico se obtiene simplificando ésta.

Si i es un número natural, tenemos que $E_{\mathfrak{p}\,\chi} \le i$ si y sólo si $G^{\psi(i)} \le N_\chi$, si y sólo si $\left(\frac{K/k}{U_i}\right) \le N_\chi$, donde U_i corresponde al cuerpo $k_\mathfrak{p}$. El grupo de clases de K_χ es la antiimagen de N_χ por el homomorfismo de Artin. Llamémoslo H_χ. La última condición equivale a que $U_i \le H_\chi \cap k_\mathfrak{p}^*$, el grupo de clases local.

Así pues, $E_{\mathfrak{p}\,\chi}$ es el mínimo natural i tal que U_i está contenido en el grupo de clases local de K_χ,luego $E_{\mathfrak{p}\,\chi}$ es el exponente del conductor local $(f_\chi)_\mathfrak{p}$ o, lo que es lo mismo, el exponente de $\mathfrak{p}$ en $\mathfrak{f}_\chi$. ∎

El inconveniente del teorema 10.30 es que en la expresión de los exponentes de los primos del conductor interviene la función de Hasse. En la definición de $E_{\mathfrak{p}\,\chi}$ también aparece, pero lo que vamos a hacer ahora es precisamente encontrar una expresión equivalente en la que ya no intervenga.

Teorema 10.33 *Sea K/k una extensión abeliana de cuerpos numéricos o p-ádicos y sea χ un carácter de su grupo de Galois. Entonces, para cada primo $\mathfrak{p}$ de k se cumple*

$$E_{\mathfrak{p}\,\chi} = \frac{1}{e}\sum_{i=0}^{\infty}\sum_{\sigma\in G^i}\big(1-\chi(\sigma)\big).$$

Demostración: Por definición tenemos

$$E_{\mathfrak{p}\,\chi} = \int_{-1}^{+\infty} f_{\mathfrak{p}\,\chi}(t)\,dt.$$

Hacemos el cambio de variable $t = \phi(s)$, con lo que $dt = \phi'(s)\,ds$. Observar que podemos descomponer la integral en una suma finita de integrales en intervalos donde tanto el integrando como la función ϕ sean derivables (pues el integrando es derivable salvo en un punto y la función ϕ lo es salvo en un número finito de puntos). Nos queda

$$\begin{aligned} E_{\mathfrak{p}\,\chi} &= \int_{-1}^{+\infty} f_{\mathfrak{p}\,\chi}\big(\phi(s)\big)\,ds = \int_{-1}^{+\infty}\frac{1}{|G^s|}\sum_{\sigma\in G^s}\big(1-\chi(\sigma)\big)\frac{|G^s|}{e}\,ds \\ &= \frac{1}{e}\int_{-1}^{+\infty}\sum_{\sigma\in G^s}\big(1-\chi(\sigma)\big)\,ds = \frac{1}{e}\sum_{i=0}^{\infty}\sum_{\sigma\in G^i}\big(1-\chi(\sigma)\big), \end{aligned}$$

pues el integrando de la penúltima expresión es constante en cada intervalo $]i, i+1]$. ∎

Podríamos haber tomado esta fórmula como definición del exponente $E_{\mathfrak{p}\,\chi}$, pero la otra expresión es necesaria de todos modos para probar el teorema 10.32.

Teorema 10.34 (Teorema del conductor y el discriminante) *Sea K/k una extensión abeliana de cuerpos numéricos o p-ádicos. Sea G el grupo de Galois. Entonces el discriminante de la extensión viene dado por*

$$\Delta = \prod_{\chi\in G^*}\mathfrak{f}_\chi.$$

DEMOSTRACIÓN: En realidad en los conductores hay que eliminar los factores infinitos, pues el discriminante no los tiene. También podemos hablar de un discriminante generalizado que contenga a los primos infinitos ramificados. En cualquier caso podemos limitarnos a probar que cada primo finito $\mathfrak{p}$ de k tiene el mismo exponente en los dos miembros de la fórmula. Más aún, podemos limitarnos a los primos que se ramifican.

Sea e el índice de ramificación de $\mathfrak{p}$, sea f su grado de inercia y r el número de factores primos que tiene en K. Tenemos $|G| = efr$. El exponente de $\mathfrak{p}$ en el producto de los conductores es

$$\sum_{\chi\in G^*} E_{\mathfrak{p}}\,\chi,$$

donde, según el teorema anterior,

$$E_{\mathfrak{p}}\,\chi = \frac{1}{e}\sum_{i=0}^{\infty}\sum_{\sigma\in G^i}\big(1-\chi(\sigma)\big).$$

Recordemos que, si $\sigma \in G$, el número $i(\sigma)$ es el mayor entero i tal que $\sigma \in G^i$ (con el convenio $i(1) = +\infty$). En la fórmula anterior el automorfismo 1 da lugar a sumandos nulos, luego podemos prescindir de él. Cualquier otro $\sigma \in G^0$ da lugar a $i(\sigma)+1$ sumandos $1-\chi(\sigma)$, luego se cumple

$$E_{\mathfrak{p}}\,\chi = \frac{1}{e}\sum_{\substack{\sigma\in G^0\\ \sigma\neq 1}}(i(\sigma)+1)\big(1-\chi(\sigma)\big).$$

Así pues,

$$\begin{aligned}\sum_{\chi\in G^*} E_{\mathfrak{p}}\,\chi &= \frac{1}{e}\sum_{\substack{\sigma\in G^0\\ \sigma\neq 1}}(i(\sigma)+1)\sum_{\chi\in G^*}\big(1-\chi(\sigma)\big)\\ &= \frac{1}{e}\sum_{\substack{\sigma\in G^0\\ \sigma\neq 1}}\big(i(\sigma)+1\big)|G| = fr\sum_{i=0}^{\infty}(|G^i|-1).\end{aligned}$$

Respecto a la última igualdad, notar que si contamos cada automorfismo σ (excepto el 1) tantas veces como grupos a los que pertenece, estamos contando los elementos distintos de 1 de cada grupo de ramificación.

Si $\mathfrak{P}$ es un divisor de $\mathfrak{p}$ en K, el teorema 10.11 afirma que el sumatorio de la última expresión es el exponente de $\mathfrak{P}$ en el diferente de K/k, y al multiplicarlo por rf obtenemos el exponente de $\mathfrak{p}$ en el discriminante de K/k (pues cada uno de los r divisores de $\mathfrak{p}$ contribuye con un exponente igual a f veces su exponente en el diferente). ∎

Veamos un ejemplo sencillo en el que se aplica este teorema:

Teorema 10.35 *Sea K/k una extensión cíclica de grado primo q de cuerpos numéricos o p-ádicos. Entonces el diferente $\mathfrak{D}$, el discriminante Δ y (la parte finita de) el conductor $\mathfrak{f}$ están relacionados del modo siguiente:*

$$\Delta = \mathfrak{D}^q = \mathfrak{f}^{p-1}.$$

En particular en las extensiones cuadráticas el conductor es igual al discriminante.

DEMOSTRACIÓN: La igualdad $\Delta = \mathfrak{D}^q$ es elemental: los primos ramificados cumplen $e = q$, $f = 1$, luego la norma de $\mathfrak{D}$ se obtiene sustituyendo cada primo $\mathfrak{P}$ por $\mathfrak{p} = \mathfrak{P}^q$.

Respecto al conductor, el grupo de Galois G tiene q caracteres, de los cuales el principal tiene núcleo G y los $q-1$ restantes tienen núcleo trivial. Por lo tanto, si $\chi = 1$ se cumple $K_\chi = k$, $\mathfrak{f}_\chi = 1$ y si $\chi \neq 1$ entonces $K_\chi = K$, $\mathfrak{f}_\chi = \mathfrak{f}$. El teorema anterior nos da que $\Delta = \mathfrak{f}^{q-1}$. ∎

Al final del capítulo VIII observamos este hecho para cuerpos cuadráticos sobre $\mathbb{Q}$ como consecuencia de que los caracteres de los cuerpos cuadráticos son primitivos.

10.6 Cálculo de conductores

Terminamos el capítulo aplicando los teoremas que hemos visto para calcular el conductor de varias extensiones.

Ejemplo 1 $K = \mathbb{Q}\big(\sqrt{d_1}, \sqrt{d_2}\big)$, donde d_1 y d_2 son enteros distintos libres de cuadrados (y distintos de 1).

Claramente K contiene, además de a los dos subcuerpos $\mathbb{Q}\big(\sqrt{d_1}\big)$ y $\mathbb{Q}\big(\sqrt{d_2}\big)$, a un tercer cuerpo $\mathbb{Q}\big(\sqrt{d_3}\big)$. Concretamente d_3 es la parte libre de cuadrados de $d_1 d_2$. El grupo de Galois es producto de dos cíclicos de orden 2. Sus caracteres no triviales tienen núcleos de orden 2, correspondientes a los tres cuerpos cuadráticos intermedios. Por el teorema 10.35, los conductores $\mathfrak{f}_\chi$ son los discriminantes Δ_i de los cuerpos intermedios (por ∞ si el cuerpo es imaginario). Por consiguiente el conductor de K es $\mathfrak{f} = \mathrm{mcm}(\Delta_1, \Delta_2, \Delta_3)$ (por ∞ si K es imaginario).

Aplicando el teorema del conductor-discriminante, vemos que el discriminante de K es $\Delta_{4/1} = \Delta_1\Delta_2\Delta_3$ (usaremos el subíndice 4 en referencia a K, el 2 en referencia a $\mathbb{Q}\big(\sqrt{d_1}\big)$ y 1 en referencia a $\mathbb{Q}$).

Es claro que el diferente $\mathfrak{D}_{4/1}$ es invariante por los automorfismos de K, luego el teorema 1.43 implica que su norma es $\Delta_{4/1} = \mathfrak{D}_{4/1}^4$. Así pues, concluimos que $\mathfrak{D}_{4/1} = (\Delta_1\Delta_2\Delta_3)^{1/4}$.

Similarmente $\mathfrak{D}_{2/1} = \Delta_1^{1/2}$ y la transitividad de los diferentes implica que $\mathfrak{D}_{4/2} = (\Delta_2\Delta_3/\Delta_1)^{1/4}$. De aquí obtenemos $\Delta_{4/2} = (\Delta_2\Delta_3/\Delta_1)^{1/2}$.

La parte finita del conductor $\mathfrak{f}_{4/2}$ es $\Delta_{4/2}$. Además $\mathfrak{f}_{4/2}$ contendrá a ∞ si $\mathbb{Q}\big(\sqrt{d_1}\big)$ es real y K es imaginario. ∎

Ejemplo 2 $G(K_4/k_1) \cong C_4$.

En este caso dos de los caracteres de $G(K_4/k_1)$ tienen núcleo trivial, uno tiene núcleo de orden 2 y uno tiene núcleo $G(K_4/k_1)$. Los cuerpos asociados son K_4 (dos veces), K_2 (el único cuerpo intermedio) y k_1. El teorema del conductor-discriminante nos da que $\Delta_{4/1} = \mathfrak{f}_{4/1}^2\Delta_{2/1}$, luego $\mathfrak{f}_{4/1} = (\Delta_{4/1}/\Delta_{2/1})^{1/2}$. El conductor $\mathfrak{f}_{4/2}$ es el discriminante $\Delta_{4/2}$ y, calculando los diferentes como en el ejemplo anterior, resulta ser $\mathfrak{f}_{4/2} = (\Delta_{4/1})^{1/2}/\Delta_{2/1}$.

Por ejemplo, si tomamos como K_4 el quinto cuerpo ciclotómico, sabemos que K_4 contiene a $K_2 = \mathbb{Q}\big(\sqrt{5}\,\big)$ y los discriminantes son $\Delta_{4/1} = 5^3$ y $\Delta_{2/1} = 5$, luego la parte finita del conductor relativo es $\sqrt{5}$. El conductor completo es $\mathfrak{f} = \sqrt{5}\,\infty$, pues K es complejo y K_2 real. ∎

Ejemplo 3 $K_6 = \mathbb{Q}\big(\sqrt[3]{m}, \sqrt{-3}\,\big)$, $k_2 = \mathbb{Q}\big(\sqrt{-3}\,\big)$.

Como K_6/k_2 es cíclica, podemos aplicar el teorema 10.35 para calcular el conductor a partir del diferente, el cual a su vez lo tenemos calculado en (10.3). El resultado es $\mathfrak{f} = \mathfrak{D}_{6/2}^{3/2}$, donde $\mathfrak{f} = 3ab$ si $\mathbb{Q}\big(\sqrt[3]{m}\,\big)$ es de tipo I y $\mathfrak{f} = ab$ si es de tipo II. ∎

Ejemplo 4 $K_6 = \mathbb{Q}(\zeta)$, donde $\zeta = e^{2\pi i/7}$, $k_2 = \mathbb{Q}\big(\sqrt{-7}\,\big)$, $k_3 = \mathbb{Q}(\cos 2\pi/7)$.

Es claro que (la parte finita de) todos los conductores sobre $k_1 = \mathbb{Q}$ es 7. El teorema 10.35 nos da entonces que $\Delta_{3/1} = 7^2$. Por otra parte sabemos que $\Delta_{2/1} = -7$ y $\Delta_{6/1} = -7^5$.

El 7 se ramifica completamente en K_6, es decir, $7 = \mathfrak{p}^6$. Calculamos los diferentes:

$$\mathfrak{D}_{6/1} = \mathfrak{p}^5, \qquad \mathfrak{D}_{3/1} = \mathfrak{p}^4, \qquad \mathfrak{D}_{2/1} = \mathfrak{p}^3, \qquad \mathfrak{D}_{6/2} = \mathfrak{p}^2, \qquad \mathfrak{D}_{6/3} = \mathfrak{p}.$$

El teorema 10.35 nos da $\mathfrak{f}_{6/2} = \mathfrak{p}^3 = \sqrt{-7}$, $\mathfrak{f}_{6/3} = \mathfrak{p}^2$. ∎

Ejemplo 5 $K_8 = \mathbb{Q}\big(\sqrt{-2}, \sqrt{1+i}\,\big)$, $k_2 = \mathbb{Q}\big(\sqrt{-2}\,\big)$. Vamos a calcular el conductor de K_8/k_2.

En primer lugar observamos que $k_4 = \mathbb{Q}\big(\sqrt{-2}, i\big)$ es el octavo cuerpo ciclotómico. Concretamente, $\zeta = \sqrt{2}\,(1+i)/2$ es una raíz octava primitiva de la unidad. También es fácil ver que la extensión $K_8/\mathbb{Q}$ es normal, pues K_8 contiene a los cuatro conjugados de $\sqrt{1+i}$ (que son $\pm\sqrt{1\pm i}$). Basta tener en cuenta que

$$\sqrt{1+i}\,\sqrt{1-i} = \sqrt{2}. \tag{10.8}$$

El k_2-automorfismo no trivial de k_4 hace corresponder los polinomios mínimos de $\sqrt{1+i}$ y de $-\sqrt{1-i}$ (sobre k_4), luego se extiende a un k_2-automorfismo de K_8 tal que $\sqrt{1+i} \mapsto -\sqrt{1-i}$, y por (10.8) también $\sqrt{1-i} \mapsto \sqrt{1+i}$. De aquí se sigue que dicho automorfismo tiene orden 4, luego la extensión K_8/k_2

es cíclica. Calcularemos el conductor mediante la fórmula del ejemplo 2, pero para ello necesitamos el discriminante $\Delta_{8/2}$. El problema es calcular el diferente $\mathfrak{D}_{8/2}$.

Los cálculos del ejemplo 1 nos dan $\Delta_{4/1} = 2^8$, $\Delta_{4/2} = 2$ y, por supuesto, $\Delta_{2/1} = -2^3$. Vemos que el 2 se ramifica en k_2 y su divisor se vuelve a ramificar en k_4, con lo que $2 = \mathfrak{p}^4$, donde $\mathfrak{p}$ es un primo en k_4. Además 2 es el único primo ramificado en k_4. Claramente $\mathfrak{D}_{4/2} = \Delta_{4/2}^{1/2} = \mathfrak{p}^2$. Falta calcular $\mathfrak{D}_{8/4}$.

Aplicamos el teorema 3.13 al elemento $\sqrt{1+i}$ para obtener una cota. La conclusión es que $\mathfrak{D}_{8/4} \mid 2\sqrt{1+i}$.

Observemos que $\mathrm{N}_{8/2}\big(\sqrt{1+i}\,\big) = 2$, lo que implica que los divisores primos de $\mathfrak{D}_{8/2}$ son divisores de 2 o, lo que es lo mismo, divisores de $\mathfrak{p}$. El punto más delicado es determinar si $\mathfrak{p}$ se ramifica o no en K_8. Comencemos estudiando la situación:

El divisor de 2 en k_2 es $\big(\sqrt{2}\,\big)$, mientras que en k_4 es $\mathfrak{p} = (1-\zeta)$. Lo más cercano que tenemos a una factorización de 2 en K_8 es $\mathrm{N}_{8/1}\big(\sqrt{1\pm i}\,\big) = 4$. Precisando un poco más vemos que $\mathrm{N}_{4/1}(1 \pm i) = 4$, luego $1 \pm i = \mathfrak{p}^2$, luego $\sqrt{1\pm i} = \mathfrak{p})(1-\zeta)$.

Esto quiere decir que $\sqrt{1\pm i}$ y $1-\zeta$ son conjugados en K_8, o sea, que los números $(1-\zeta)/\sqrt{1\pm i}$ son unidades de K_8.

Las unidades son idóneas para obtener elementos de norma pequeña (como suma de dos de ellas). Si queremos elementos de norma divisible entre 2 es natural trabajar con unidades como éstas, relacionadas con el 2. Un tanteo nos lleva a considerar

$$\alpha = 1 + \frac{1-\zeta}{\sqrt{1-i}},$$

(el signo + dentro de la raíz no da el mismo resultado). Teniendo en cuenta que $\zeta^2 = i$ calculamos

$$\begin{aligned}
\mathrm{N}_{8/4}(\alpha) &= \left(1 + \frac{1-\zeta}{\sqrt{1-i}}\right)\left(1 - \frac{1-\zeta}{\sqrt{1-i}}\right) = 2\,\frac{\zeta - i}{1-i},\\
\mathrm{N}_{8/2}(\alpha) &= 4\,\frac{\zeta-i}{1-i}\,\frac{\zeta^{-1}+i}{1+i} = 4\,\frac{2-\sqrt{2}}{2} = 2\big(2-\sqrt{2}\,\big),\\
\mathrm{N}_{8/1}(\alpha) &= 4\big(2-\sqrt{2}\,\big)\big(2+\sqrt{2}\,\big) = 2^3.
\end{aligned}$$

Esto es importante, pues implica que $\mathfrak{p}$ no es primo en K_8. Si lo fuera, puesto que $N_{8/1}(\mathfrak{p}) = 4$, no podría haber elementos de norma 8. Así pues, $\mathfrak{p}$ se ramifica o se escinde. Supongamos que se escinde: $\mathfrak{p} = \mathfrak{P}\mathfrak{P}'$. Entonces la factorización de α ha de ser $(\alpha) = \mathfrak{P}^3$ o bien $(\alpha) = \mathfrak{P}^2\mathfrak{P}'$. En cualquier caso, el conjugado de (α) (respecto a la extensión K_8/k_4) ha de ser un ideal distinto (pues su factorización es distinta). Los ideales en cuestión son

$$\left(1 + \frac{1-\zeta}{\sqrt{1-i}}\right) \qquad \text{y} \qquad \left(1 - \frac{1-\zeta}{\sqrt{1-i}}\right)$$

Si probamos que son iguales habremos demostrado que $\mathfrak{p}$ se ramifica en K_8. Un cálculo no muy complejo muestra que el cociente entre estos dos números es

$$-i\zeta\big(1+\sqrt{1-i}\,\big),$$

que es una unidad, luego los dos generadores son asociados y los ideales coinciden.

Así pues, $\mathfrak{p} = \mathfrak{P}^2$. Ahora ya podemos calcular $\mathfrak{D}_{8/4}$. Emplearemos una técnica válida siempre que el grado de inercia sea 1. El diferente coincide con el diferente local en $K_\mathfrak{P}/k_\mathfrak{p}$ (si $\mathfrak{p}$ tuviera más divisores podríamos calcular los diferentes locales por separado).

Necesitamos un elemento (no necesariamente entero) cuyo valor $\mathfrak{P}$-ádico sea exactamente 1. Por ejemplo $\pi = \alpha/\sqrt{1-i}$ (el numerador es divisible entre $\mathfrak{P}^3$ y el denominador entre $\mathfrak{P}^2$).

Aunque π pueda no ser entero, lo que importa es que sí es entero en $K_\mathfrak{P}$, más aún, en $K_\mathfrak{P}$ se cumple $\mathfrak{P} = (\pi)$. Además, como el grado de inercia es trivial, el teorema 3.11 nos da que el anillo de enteros de $K_\mathfrak{P}$ es la adjunción de π al anillo de enteros de $k_\mathfrak{p}$, por lo que podemos calcular el diferente mediante 3.8.

Si $f(x)$ es el polinomio mínimo de π, entonces $f'(\pi)$ es simplemente $(\pi - \pi')$, donde π' es el conjugado de π. Por lo tanto

$$\mathfrak{D}_{8/4} = \left(\frac{1+\frac{1-\zeta}{\sqrt{1-i}}}{\sqrt{1-i}} - \frac{1+\frac{1-\zeta}{-\sqrt{1-i}}}{-\sqrt{1-i}}\right) = \left(\frac{2}{\sqrt{1-i}}\right) = \mathfrak{P}^6.$$

Por consiguiente $\mathfrak{D}_{8/2} = \mathfrak{D}_{8/4}\,\mathfrak{D}_{4/2} = \mathfrak{P}^{10}$ y $\Delta_{8/2} = \mathfrak{P}^{40} = 2^5$. Según el ejemplo 2 tenemos que $\mathfrak{f}_{8/2} = (\Delta_{8/2}/\Delta_{4/2})^{1/2} = 4$. ∎

Ejercicio: Calcular los grupos de ramificación de $\mathfrak{P}$ respecto a la extensión K_8/K_2. (Tener en cuenta que los vértices de la función de Hasse han de tener coordenadas enteras.)

Capítulo XI

Ejemplos y aplicaciones

Dedicamos este capítulo a mostrar ejemplos explícitos de cuerpos de clases sobre cuerpos distintos de $\mathbb{Q}$, así como algunas aplicaciones variadas de la teoría de cuerpos de clases. Los resultados más notables que obtendremos se refieren al problema de la representación de enteros por formas cuadráticas binarias. De hecho, fue este problema el que motivó la teoría de cuerpos de clases. Veremos que con su ayuda podemos superar los resultados que proporciona la teoría de Gauss, especialmente en lo tocante a la representación de primos por formas cuadráticas.

11.1 El cuerpo de clases de Hilbert

Si k es un cuerpo numérico arbitrario, el cuerpo de clases más sencillo en que podemos pensar es el cuerpo radial de conductor 1. A este cuerpo se le llama *cuerpo de clases de Hilbert* del cuerpo k. Si K es el cuerpo de clases de Hilbert de k, el isomorfismo de Artin nos da

$$I/P \cong G(K/k).$$

Así pues, el grado $|K : k|$ es el número de clases de k, y se cumple $K = k$ si y sólo si k tiene factorización única. Como el conductor de la extensión es 1, resulta que ningún primo de k se ramifica en K, luego el discriminante es 1. También es claro que K es la mayor extensión abeliana de k no ramificada (entendiendo que los primos infinitos tampoco se ramifican).

Si permitimos que los primos infinitos se ramifiquen tenemos el *cuerpo de clases estrictas de Hilbert,* que es el cuerpo radial de ∞, la mayor extensión abeliana de k en la que ningún primo finito se ramifica. El discriminante de este cuerpo es también igual a 1.

Ahora es claro que un cuerpo k tiene extensiones abelianas con discriminante 1 si y sólo si $h_\infty \neq 1$, pues una extensión abeliana con discriminante 1 está contenida en el cuerpo de clases estrictas de Hilbert. Una condición necesaria

es que k tenga factorización única. Si k no tiene primos infinitos reales, la condición es suficiente (pues entonces $P_\infty = P_1$).

Es interesante comparar esto con el teorema [4.13], según el cual un cuerpo numérico no puede tener discriminante 1 sobre $\mathbb{Q}$. La observación anterior es más general en cuanto que vale para cuerpos arbitrarios, pero más particular en cuanto que sólo se aplica a extensiones abelianas.

El valor de h_∞ puede calcularse a partir de k mediante el teorema 5.8. Por ejemplo, para $k = \mathbb{Q}$ tenemos que $\Phi(\infty) = 2$, $U_1 = \{\pm 1\}$ y $U_\infty = 1$, luego obtenemos $h_\infty = 1$.

En general es posible una cadena de cuerpos numéricos $k \subset K \subset L$ de modo que K sea el cuerpo de clases de Hilbert de K y L sea el cuerpo de clases de Hilbert de K (sin que K coincida con L). La extensión L/k es no ramificada, pero no abeliana. De hecho puede probarse que la operación de tomar cuerpos de clases de Hilbert sucesivamente a partir de un cuerpo dado produce con frecuencia cadenas infinitas en estas condiciones. El teorema siguiente describe con más precisión estas cadenas $k \subset K \subset L$.

Teorema 11.1 *Sea K el cuerpo de clases (estrictas) de Hilbert de k y L el cuerpo de clases (estrictas) de Hilbert de K. Entonces la extensión L/k es de Galois y K es la mayor extensión abeliana de k contenida en L, equivalentemente, $G(L/K)$ es el grupo derivado de $G(L/k)$.*

Demostración: Sea $\sigma : L \longrightarrow \mathbb{C}$ un k-monomorfismo. Entonces $\sigma[K] = K$, luego $\sigma[L]/K$ es una extensión abeliana no ramificada (salvo quizá en los primos infinitos), por lo que podemos concluir que $\sigma[L] = L$. Esto prueba que L/k es de Galois.

Como las extensiones K/k y L/K son no ramificadas, la extensión L/k también lo es. Si M es un cuerpo intermedio $k \subset M \subset L$ de modo que la extensión M/k es abeliana, como también es no ramificada resulta que $M \subset K$. ∎

Veamos una aplicación interesante del cuerpo de clases de Hilbert.

Teorema 11.2 *Sea K el cuerpo de clases de Hilbert de un cuerpo numérico k y sea E/k una extensión finita. Sean h_k y h_E los números de clases de k y E respectivamente. Si $E \cap K = k$, entonces $h_k \mid h_E$.*

Demostración: La extensión EK/E es abeliana y no ramificada (por el teorema 2.35 aplicado localmente). En consecuencia EK está contenido en el cuerpo de clases de Hilbert de E, llamémoslo L. Así pues,

$$h_k = |K : k| = |EK : E| \,\Big|\, |L : E| = h_E.$$

∎

Por ejemplo, si K es un cuerpo ciclotómico de orden p^r y $k \subset L \subset K$, consideremos el cuerpo de clases de Hilbert E de k. El primo p se ramifica

completamente en K, luego su divisor en k se ramifica completamente en L, luego en $E \cap L$. Como E/k es no ramificada ha de ser $E \cap L = k$, y podemos aplicar el teorema anterior, que nos da que $h_k \mid h_L$.

En su investigación sobre el número de clases de los cuerpos ciclotómicos de orden primo, Kummer descompuso el número de clases en dos factores h_1 y h_2. El segundo factor era el número de clases de la intersección con $\mathbb{R}$ del cuerpo ciclotómico. El teorema anterior prueba entonces que h_1 ha de ser también un número natural, cosa que Kummer obtuvo mediante un largo cálculo (ver el [cap. XIII]). Por otra parte, los cálculos de Kummer permiten el cálculo explícito de h_1.

El cálculo de cuerpos de clases es un problema complicado incluso en el caso de los cuerpos de clases de Hilbert. En las secciones siguientes obtendremos varios resultados útiles para este fin. De momento nos limitaremos a dar un ejemplo relativamente simple.

Ejemplo *El cuerpo de clases de Hilbert de* $k_2 = \mathbb{Q}\big(\sqrt{-23}\big)$ *es el cuerpo de escisión del polinomio* $x^3 - x - 1$.

En efecto, es fácil ver que el polinomio es irreducible. Sea ξ una de sus raíces. Consideramos el cuerpo $K_3 = \mathbb{Q}(\xi)$. El ejemplo tras el teorema [2.8] nos da que el discriminante del anillo $\mathbb{Z}[\xi]$ es $\Delta = -23$. Como es primo, concluimos que se trata del discriminante de K_3. Además esto implica que el anillo de enteros de K_3 es $\mathbb{Z}[\xi]$.

Llamemos K_6 al cuerpo de escisión del polinomio dado, es decir, $K_6 = \mathbb{Q}(\xi, \xi', \xi'')$. La definición de discriminante implica que $\sqrt{-23} \in K_6$, con lo que vemos que $k_2 \subset K_6$ y que K_6 tiene grado 6 sobre $\mathbb{Q}$.

Hemos de probar que ningún primo de k_2 se ramifica en K_6. Cualquier primo distinto de 23 es no ramificado en k_2 y en K_3, luego localizando y aplicando 2.35 tenemos que es no ramificado en K_6 y que sus divisores en K_3 son no ramificados en K_6. El único primo que podría ramificarse es el divisor de 23. Veamos que no es así. En primer lugar factorizamos

$$x^3 - x - 1 \equiv (x-3)(x-10)^2 \text{ (mód 23)},$$

con lo que el teorema 3.15 nos da que la factorización de 23 en K_3 es $23 = \mathfrak{pq}^2$.

El índice de ramificación de 23 en K_6 ha de ser múltiplo de 2 (el índice en K_3) y divisor de 6, pero no puede ser 6 porque ha de tener al menos dos divisores primos distintos. Por consiguiente es 2 y su descomposición es $23 = (\mathfrak{PQR})^2$. Como 23 se ramifica en k_2, para dar lugar a esta factorización su divisor ha de escindirse completamente en K_6, luego no se ramifica. Esto concluye la prueba. ∎

11.2 Automorfismos del cuerpo base

En esta sección demostraremos algunos resultados de gran utilidad para tratar con ejemplos concretos de cuerpos de clases. Por ejemplo, según acabamos

de ver, el cuerpo de clases de Hilbert de $\mathbb{Q}\big(\sqrt{-23}\,\big)$ es una extensión de Galois de $\mathbb{Q}$. Esto no es casualidad, sino que el cuerpo de clases de Hilbert de cualquier cuerpo cuadrático es necesariamente normal sobre $\mathbb{Q}$, tal y como se desprende del teorema siguiente. Así, cuando nos propongamos calcular otros ejemplos de cuerpos de clases de Hilbert, sabremos a priori que estamos buscando extensiones normales de $\mathbb{Q}$. Más adelante obtendremos también información sobre el grupo de Galois y, en consecuencia, sobre los cuerpos intermedios en que podremos apoyarnos para obtener el cuerpo buscado.

Teorema 11.3 *Consideremos una cadena de cuerpos numéricos $k_0 \subset k \subset K$, donde k/k_0 es una extensión de Galois y K/k es abeliana. Sea H el grupo de clases de K/k módulo un divisor $\mathfrak{m}$ invariante por los k_0-automorfismos de k. Entonces K/k_0 es de Galois si y sólo si $\sigma[H] = H$ para todo $\sigma \in G(k/k_0)$.*

Demostración: Supongamos que K/k_0 es de Galois. Entonces todo automorfismo de $G(k/k_0)$ es la restricción a k de un automorfismo $\sigma \in G(K/k_0)$. Si $\mathfrak{a} \in H$ entonces $\left(\frac{K/k}{\mathfrak{a}}\right) = 1$, luego

$$1 = \left(\frac{K/k}{\mathfrak{a}}\right)^{\sigma} = \left(\frac{\sigma[K]/\sigma[k]}{\sigma(\mathfrak{a})}\right) = \left(\frac{K/k}{\sigma(\mathfrak{a})}\right).$$

Como $\mathfrak{a} \in I(\mathfrak{m})$, claramente $\sigma(\mathfrak{a}) \in I(\sigma(\mathfrak{m})) = I(\mathfrak{m})$, luego podemos concluir que $\sigma(\mathfrak{a}) \in H$. Esto prueba que $\sigma[H] \leq H$ y, aplicándolo a σ^{-1}, tenemos la igualdad.

Supongamos ahora que todos los automorfismos de $G(k/k_0)$ fijan a H. Para demostrar que K/k_0 es de Galois tomamos un k_0-monomorfismo σ y probamos que $\sigma[K] = K$.

Como k/k_0 sí es de Galois se cumple $\sigma[k] = k$ y la extensión $\sigma[K]/k$ es abeliana. Sea H' su grupo de clases módulo $\mathfrak{m}$ (claramente $\mathfrak{m} = \sigma(\mathfrak{m})$ es admisible para $\sigma[K]/k$).

El mismo razonamiento anterior nos da que si $\mathfrak{a} \in H$ entonces $\left(\frac{\sigma[K]/k}{\sigma(\mathfrak{a})}\right) = 1$, luego $\sigma(\mathfrak{a}) \in H'$, es decir, $H = \sigma[H] \leq H'$. Por consiguiente $\sigma[K] \subset K$ y, como ambos cuerpos tienen el mismo grado sobre k_0, de hecho $\sigma[K] = K$. ∎

Ejercicio: Si $k_0 \subset k \subset K$ están en las condiciones del teorema anterior y H es el grupo de clases maximal de K/k, probar que la extensión K/k_0 es de Galois si y sólo si H es invariante por los k_0-automorfismos de K (y en tal caso el conductor de K/k es invariante por los k_0-automorfismos de k).

Este teorema se aplica principalmente cuando $k_0 = \mathbb{Q}$. Es inmediato comprobar que si $\mathfrak{m}$ es un divisor de k y $\sigma \in G(k/\mathbb{Q})$, entonces $\sigma[P_{\mathfrak{m}}] = P_{\sigma(\mathfrak{m})}$. En particular, si K es el cuerpo radial (sobre k) de un divisor de $\mathbb{Q}$ se cumple que la extensión $K/\mathbb{Q}$ es de Galois (suponiendo que $k/\mathbb{Q}$ lo sea). Más concretamente, los cuerpos de clases de Hilbert (de extensiones de Galois de $\mathbb{Q}$) son siempre extensiones de Galois de $\mathbb{Q}$, tal y como anunciábamos.

En las hipótesis del teorema anterior, y suponiendo que la extensión K/k_0 es de Galois, resulta que el grupo $G(k/k_0)$ actúa sobre el grupo $I(\mathfrak{m})/H$. En efecto,

si $[\mathfrak{a}] = [\mathfrak{b}]$ entonces $\mathfrak{a}\mathfrak{b}^{-1} \in H$, luego $\sigma(\mathfrak{a})\sigma(\mathfrak{b})^{-1} \in \sigma[H] = H$, y $[\sigma(\mathfrak{a})] = [\sigma(\mathfrak{b})]$. Trivialmente, $G(K/k_0)$ actúa del mismo modo sobre $I(\mathfrak{m})/H$. Más aún, la igualdad

$$\left(\frac{K/k}{\mathfrak{a}}\right)^{\sigma} = \left(\frac{K/k}{\sigma(\mathfrak{a})}\right), \qquad \text{para todo } \sigma \in G(K/k_0)$$

se traduce en que la acción por conjugación de $G(K/k_0)$ sobre su subgrupo normal $G(K/k)$ es equivalente a la acción sobre $I(\mathfrak{m})/H$ a través del isomorfismo de Artin $I(\mathfrak{m})/H \cong G(K/k)$.

Teorema 11.4 *Consideremos una cadena de cuerpos numéricos $k_0 \subset k \subset K$, donde K/k_0 es de Galois, k/k_0 es cíclica y K/k es abeliana. Sea H el grupo de clases de K/k módulo un divisor $\mathfrak{m}$ invariante por los k_0-automorfismos de k. Sea K' la mayor extensión abeliana de k_0 contenida en K y sea H' el grupo de clases de K'/k módulo $\mathfrak{m}$. Entonces H'/H es el grupo generado por las clases de la forma $C\tau(C)^{-1}$ con $C \in I(\mathfrak{m})/H$ y $\tau \in G(k/k_0)$.*

Demostración: Por definición K' es el cuerpo fijado por el grupo derivado $G(K/k_0)'$. Como el cociente de $G(K/k)$ en $G(K/k_0)$ es abeliano, tenemos la inclusión $G(K/k_0)' \leq G(K/k)$, luego $k_0 \subset k \subset K' \subset K$. El grupo H'/H es la antiimagen de $G(K/k_0)'$ a través del isomorfismo de Artin $I(\mathfrak{m})/H \cong G(K/k)$.

El grupo derivado $G(K/k_0)'$ está generado por los automorfismos de la forma $\alpha\beta\alpha^{-1}\beta^{-1}$, con α, $\beta \in G(K/k_0)$. El cociente $G(K/k_0) \,/\, G(K/k)$ es cíclico, digamos generado por un cierto $[\tau_0]$ y, por lo tanto, todo elemento de $G(K/k_0)$ puede expresarse como $\sigma\tau$, donde $\sigma \in G(K/k)$ y τ es una potencia de τ_0. En particular $\alpha = \sigma_1\tau_1$ y $\beta = \sigma_2\tau_2$, con σ_1, $\sigma_2 \in G(K/k)$ y τ_1, $\tau_2 \in G(K/k_0)$ potencias de τ_0. De este modo σ_1 conmuta con σ_2 y τ_1 conmuta con τ_2.

$$\alpha\beta\alpha^{-1}\beta^{-1} = \sigma_1(\tau_1\sigma_2)\tau_2\tau_1^{-1}(\sigma_1^{-1}\tau_2^{-1})\sigma_2^{-1} = \sigma_1\sigma_2^{\tau_1^{-1}}\tau_1\tau_2\tau_1^{-1}\tau_2^{-1}(\sigma_1^{-1})^{\tau_2^{-1}}\sigma_2^{-1}$$

$$= \sigma_1(\sigma_1^{-1})^{\tau_2^{-1}}\sigma_2^{-1}\sigma_2^{\tau_1^{-1}} = \sigma_1(\sigma_1^{-1})^{\tau_2^{-1}}(\sigma_2(\sigma_2^{-1})^{\tau_1^{-1}})^{-1}.$$

Como entre estos generadores se encuentran los que cumplen $\sigma_2 = 1$, en realidad $G(K/k_0)'$ está generado por los automorfismos de la forma $\sigma_1(\sigma_1^{-1})^{\tau_2^{-1}}$ o, simplificando la notación, $\sigma(\sigma^{\tau})^{-1}$, donde $\sigma \in G(K/k)$ y τ varía entre las potencias de τ_0.

Si ahora aplicamos el isomorfismo de Artin en sentido inverso concluimos que H'/H está generado por las clases de la forma $C\tau(C)^{-1}$, donde $C \in I(\mathfrak{m})/H$ y $\tau \in G(k/k_0)$. ∎

En particular tenemos un criterio para decidir si la extensión K/k_0 es abeliana:

Teorema 11.5 *Consideremos una cadena de cuerpos numéricos $k_0 \subset k \subset K$, donde K/k_0 es de Galois, k/k_0 es cíclica y K/k es abeliana. Sea H el grupo de clases de K/k módulo un divisor $\mathfrak{m}$ invariante por los k_0-automorfismos de k. Entonces K/k_0 es abeliana si y sólo si la acción de $G(k/k_0)$ sobre $I(\mathfrak{m})/H$ es trivial (todas las clases son fijadas).*

DEMOSTRACIÓN: Estamos en las hipótesis del teorema anterior, y la extensión K/k será abeliana si y sólo si $K = K'$ o, equivalentemente, $H = H'$. Esto último sucede si y sólo si $C\tau(C)^{-1} = 1$ para toda clase $C \in I(\mathfrak{m})/H$ y todo automorfismo $\tau \in G(k/k_0)$, es decir, si $\tau(C) = C$ para todo C y todo τ. ∎

11.3 Grupos de órdenes

Recordemos de [4.16] que cada orden $\mathcal{O}$ de un cuerpo numérico k tiene asociado un grupo de clases relacionado con la factorización única ideal de los ideales de $\mathcal{O}$ que son primos con el conductor $\mathfrak{f}$, definido en [3.25]. Adaptando la notación a la que estamos empleando ahora, el grupo de clases de $\mathcal{O}$ es $I(\mathfrak{f})/H_{\mathcal{O}}$, donde

$$H_{\mathcal{O}} = \{(\alpha)/(\beta) \mid \alpha, \beta \in \mathcal{O},\ (\alpha) + \mathfrak{f} = (\beta) + \mathfrak{f} = 1\}.$$

Vamos a ver que $H_{\mathcal{O}}$ es un grupo de ideales módulo $\mathfrak{f}$, es decir, que $P_{\mathfrak{f}} \leq H_{\mathcal{O}}$. En efecto, un elemento de $P_{\mathfrak{f}}$ es de la forma $\mathfrak{a} = (\alpha)/(\beta)$, con $(\alpha)+\mathfrak{f} = (\beta)+\mathfrak{f} = 1$, $\alpha \equiv \beta$ (mód $\mathfrak{f}$). En particular $[\alpha] = [\beta]$ es una unidad del anillo $\mathcal{O}_1/\mathfrak{f}$, donde $\mathcal{O}_1$ es el anillo de enteros de k. Existe un $\gamma \in \mathcal{O}_1$ tal que $\alpha\gamma \equiv \beta\gamma \equiv 1$ (mód $\mathfrak{f}$). Como $\mathfrak{f} \subset \mathcal{O}$, esto implica que $\alpha\gamma$, $\beta\gamma \in \mathcal{O}$ y, claramente, $\mathfrak{a} = (\alpha\gamma)/(\beta\gamma) \in H_{\mathcal{O}}$.

Observar que $H_{\mathcal{O}}/P_{\mathfrak{f}}$ está formado por las clases de $I(\mathfrak{f})/P_{\mathfrak{f}}$ con un representante en $\mathcal{O}$ (como el cociente es finito, digamos de n elementos, se cumple que $[(\alpha)/(\beta)] = [(\alpha\beta^{n-1})]$).

Si $k = \mathbb{Q}\big(\sqrt{d}\big)$ es un cuerpo cuadrático, sabemos [2.24] que tiene un único orden $\mathcal{O}_m$ para cada natural no nulo m que, con la notación de este teorema, está formado por los números de la forma $\gamma = a + bm\alpha$, con a, $b \in \mathbb{Z}$. Por consiguiente $\gamma \equiv a$ (mód m). Además [3.29], el conductor de $\mathcal{O}_m$ es $\mathfrak{f} = m$, luego $(\gamma)/(a) \in P_m$ y así $[(\gamma)] = [(a)]$. En resumen, si llamamos H_m al grupo de clases de $\mathcal{O}_m$ tenemos que H_m/P_m está formado por las clases de $I(m)/P_m$ con representante en $\mathbb{Z}$ (primo con m). Equivalentemente:

$$H_m = \{\mathfrak{a} \in I(m) \mid \mathfrak{a} \equiv^* (r) \text{ (mód } m) \text{ para un } r \in \mathbb{Z}\}.$$

En los órdenes cuadráticos tenemos definidos también los grupos de clases estrictas y, según vimos en la sección [6.3], éstos pueden representarse como $I(m\infty)/H_{m\infty}$, donde ahora

$$H_{m\infty} = \{(\alpha)/(\beta) \mid \alpha, \beta \in \mathcal{O}_m,\ (\alpha)+(m) = (\beta)+(m) = 1,\ \mathrm{N}(\alpha) > 0,\ \mathrm{N}(\beta) > 0\}.$$

Modificando levemente los argumentos anteriores se ve que $P_{m\infty} \leq H_{m\infty}$ y que $H_{m\infty}/P_{m\infty}$ está formado por las clases de $I(m\infty)/P_{m\infty}$ con un representante $\gamma \in \mathcal{O}_m$ de norma positiva. Así mismo, $\gamma = a + bm\alpha$, con a, $b \in \mathbb{Z}$, pero ahora podemos afirmar que $(\gamma) \equiv^* (a)$ (mód $m\infty$), pues tanto γ como a tienen norma positiva. Recíprocamente, si $a \in \mathbb{Z}$ es primo con m es claro que $(a) \in H_{m\infty}$, luego en definitiva

$$H_{m\infty} = \{\mathfrak{a} \in I(m\infty) \mid \mathfrak{a} \equiv^* (r) \text{ (mód } m\infty) \text{ para un } r \in \mathbb{Z}\}.$$

Concluimos, pues, que los grupos de clases de los órdenes de un cuerpo cuadrático k se corresponden con los divisores de $\mathbb{Q}$ (considerados como divisores de k). A cada divisor $\mathfrak{m}$ de $\mathbb{Q}$ le corresponde el grupo de clases $I(\mathfrak{m})/H_\mathfrak{m}$ determinado por

$$H_\mathfrak{m} = \{\mathfrak{a} \in I(\mathfrak{m}) \mid \mathfrak{a} \equiv^* (r) \text{ (mód } \mathfrak{m}) \text{ para un } r \in \mathbb{Z}\}.$$

Los divisores $\mathfrak{m}$ divisibles entre ∞ se corresponden con los grupos de clases estrictas. Puesto que $\mathfrak{m}$ es invariante por los automorfismos de k, el teorema 11.3 implica que $K_\mathfrak{m}$ es una extensión de Galois de $\mathbb{Q}$.

Hay que señalar que el conductor de $H_\mathfrak{m}$ no es necesariamente $\mathfrak{m}$. Por ejemplo, si $k = \mathbb{Q}\big(\sqrt{-3}\big)$ y $\mathfrak{m} = 2$, entonces $\mathcal{O}_2 = \mathbb{Z}\big[\sqrt{-3}\,\big]$ y, según el ejemplo tras [4.18], el grupo $I(2)/H_2$ es trivial, luego el conductor de H_2 es $\mathfrak{f} = 1$ en lugar de $\mathfrak{m} = 2$.

El teorema [4.17] nos permite calcular el orden del grupo de clases de cualquier orden numérico. Para el caso cuadrático tenemos el teorema [4.17], que a continuación generalizamos para extenderlo a los grupos de clases estrictas.

Sea m un número natural no nulo y $\mathfrak{m} = m$ o bien $\mathfrak{m} = m\infty$. Llamaremos $\mathcal{O}_\mathfrak{m}^*$ al grupo de las unidades de $\mathcal{O}_m$ si $\infty \nmid \mathfrak{m}$ o a $\mathcal{O}_m^* \cap k_\infty$ si $\infty \mid \mathfrak{m}$. En otras palabras, si k es imaginario entonces $\mathcal{O}_{m\infty}^* = \mathcal{O}_m^*$ y si k es real entonces $\mathcal{O}_{m\infty}^*$ está formado por las unidades positivas cuyo conjugado también es positivo. Según la notación de 5.8 llamamos U_1 al grupo de las unidades del orden maximal $\mathcal{O}_1$ y $U_\mathfrak{m} = \{\epsilon \in U_1 \mid \epsilon \equiv^* 1 \text{ (mód } \mathfrak{m})\}$.

Teorema 11.6 *Sea k un cuerpo cuadrático, m un número natural y $\mathfrak{m} = m$ o bien $\mathfrak{m} = m\infty$. Entonces*

$$|H_\mathfrak{m} : P_\mathfrak{m}| = \frac{\phi(m)}{|\mathcal{O}_\mathfrak{m}^* : U_\mathfrak{m}|}.$$

Demostración: Partimos del epimorfismo $(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow H_\mathfrak{m}/P_\mathfrak{m}$ dado por $[r] \mapsto [(r)]$, donde el representante r se escoge positivo (por si $\infty \mid \mathfrak{m}$). Basta probar que su núcleo tiene orden $|\mathcal{O}_\mathfrak{m}^* : U_\mathfrak{m}|$. Una clase $[r]$ está en el núcleo si y sólo si $(r) \in P_\mathfrak{m}$, es decir, si existe un $\epsilon \in \mathcal{O}_1^*$ tal que $r\epsilon^{-1} \equiv^* 1$ (mód $\mathfrak{m}$). Por lo tanto el número de elementos del núcleo es igual al del conjunto

$$A = \{r \in \mathbb{Z} \mid 0 < r < m,\ (r, m) = 1,\ r \equiv^* \epsilon \text{ (mód } \mathfrak{m}) \text{ para un } \epsilon \in \mathcal{O}_1^*\}.$$

Ahora observamos que

$$\mathcal{O}_\mathfrak{m}^* = \{\epsilon \in \mathcal{O}_1^* \mid \epsilon \equiv^* r \text{ (mód } \mathfrak{m}) \text{ para un } r \in \mathbb{Z},\ (r, m) = 1,\ r > 0\}.$$

En efecto, si $\epsilon \in \mathcal{O}_\mathfrak{m}^*$ entonces es de la forma $\epsilon = u + vm\alpha$ (con la notación de [2.24]), luego $\epsilon \equiv u$ (mód $\mathfrak{m}$). Se cumple $(m, u) = 1$, porque si no ϵ no sería una unidad. Tomamos $r > 0$ tal que $r \equiv u$ (mód m). Tenemos $(r, m) = 1$. Si $\infty \mid \mathfrak{m}$ se cumple $e \equiv^* 1$ (mód ∞) por definición de $\mathcal{O}_\mathfrak{m}^*$, luego $\epsilon/r \equiv^* 1$ (mód ∞) y, en consecuencia, $\epsilon \equiv^* r$ (mód $\mathfrak{m}$). Recíprocamente, si $\epsilon \equiv^* r$ (mód $\mathfrak{m}$) con $r > 0$,

entonces $\epsilon = u + v\alpha$ y $m \mid u - r + v\alpha$, de donde $m \mid v$ y, por lo tanto, $\epsilon \in \mathcal{O}_m^*$. Si además $\infty \mid \mathfrak{m}$ tenemos que $\epsilon \equiv^* r \equiv^* 1 \pmod{\infty}$, luego $\epsilon \in \mathcal{O}_\mathfrak{m}^*$.

Como $U_\mathfrak{m} = \{\epsilon \in \mathcal{O}_1^* \mid \epsilon \equiv^* 1 \pmod{\mathfrak{m}}\}$, ahora es obvio que $U_\mathfrak{m} \leq \mathcal{O}_\mathfrak{m}^*$.

Consideremos el homomorfismo $\mathcal{O}_\mathfrak{m}^*/U_\mathfrak{m} \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$ dado por $[\epsilon] \mapsto [r]$, con $\epsilon \equiv^* r \pmod{m}$, $r > 0$. Es claro que está bien definido y es inyectivo, así como que la imagen tiene el mismo número de elementos que A. ∎

Aplicando ahora 5.8 obtenemos la generalización anunciada de [4.17]:

Teorema 11.7 *Sea k un cuerpo cuadrático $m > 0$ un número natural y $\mathfrak{m} = m$ o bien $\mathfrak{m} = m\infty$. Entonces*

$$|I(\mathfrak{m}) : H_\mathfrak{m}| = \frac{\Phi(\mathfrak{m})}{\phi(m)\,|\mathcal{O}_1^* : \mathcal{O}_\mathfrak{m}^*|}\, h,$$

donde ϕ es la función de Euler, Φ es la función de Euler de k y h el número de clases de k.

La fracción a la izquierda de h es en realidad un número natural, pues el grupo de clases de k es un cociente del grupo de clases de cualquiera de sus órdenes.

Grupos diédricos Vamos a necesitar algunos hechos elementales de la teoría de grupos. Si $n > 2$ se define el *grupo diédrico* de orden $2n$ como el subgrupo del grupo de permutaciones de n elementos generado por

$$\sigma = (1, \ldots, n), \qquad \text{y} \qquad \tau = (1, n)(2, n-1)(3, n-2)\cdots$$

Lo representaremos por $D_{2n} = \langle \sigma, \tau \rangle$. Es obvio que σ tiene orden n, τ tiene orden 2 y $\sigma^\tau = \sigma^{-1}$. De aquí se sigue que $\langle \sigma \rangle \trianglelefteq D_{2n}$, y es fácil ver que $\langle \sigma \rangle \cap \langle \tau \rangle = 1$ (tenemos que σ y τ no conmutan, luego $\tau \notin \langle \sigma \rangle$). En consecuencia, $D_{2n} = \langle \sigma \rangle\, \langle \tau \rangle$ tiene $2n$ elementos.

Ahora veamos que si p es un primo impar, todo grupo de orden $2p$ es cíclico o diédrico. En efecto, sea G un grupo de orden $2p$. Por el teorema de Sylow, G tiene un subgrupo N de orden p y otro H de orden 2. Ambos son cíclicos, $N = \langle \sigma \rangle$ y $H = \langle \tau \rangle$. Como N tiene índice 2 es normal, luego $\sigma^\tau = \sigma^i$ para cierto i. Como τ tiene orden 2, al volver a conjugar queda $\sigma = \sigma^{i^2}$, luego $p \mid i^2 - 1 = (p-1)(p+1)$. Esto da $\sigma^\tau = \sigma$ o $\sigma^\tau = \sigma^{-1}$.

Ciertamente $G = NH$ (basta comparar los órdenes), luego $G = \langle \sigma, \tau \rangle$. Si $\sigma^\tau = \sigma$ entonces G es abeliano, luego cíclico. Si $\sigma^\tau = \sigma^{-1}$ ya es fácil construir un isomorfismo entre G y D_{2p}. De hecho, un elemento cualquiera de G (o de D_{2p}) se expresa de forma única como nh, con $n \in N$, $h \in H$, y el producto en ambos casos viene dado por

$$nh\, n'h' = n(n')^{h-1}\, h^{-1}h' = n(n')^h\, hh',$$

donde $(n')^h$ es $n'^{\pm 1}$ según si $h = 1$ o $h = \tau$. Esto prueba que la estructura de G es la de D_{2p}. ∎

Volviendo a los cuerpos numéricos, si k es un cuerpo cuadrático y K es una extensión de k de grado p (primo impar) tal que $K/\mathbb{Q}$ es normal, entonces $G(K/\mathbb{Q})$ ha de ser cíclico o diédrico. Concretamente, el grupo cíclico de orden p es $G(K/k) = \langle\sigma\rangle$ y, si τ induce la conjugación en k, entonces o bien $\sigma^\tau = \sigma$, en cuyo caso $G(K/\mathbb{Q})$ es cíclico, o bien $\sigma^\tau = \sigma^{-1}$, en cuyo caso es diédrico.

Según las observaciones previas al teorema 11.4, la acción de τ sobre $G(K/k)$ es, a través del isomorfismo de Artin, la misma que la de la conjugación en k sobre $I(\mathfrak{f})/H$, donde $\mathfrak{f}$ es el conductor de K/k y H es el grupo de clases. Por lo tanto, si C es cualquier clase no trivial de $I(\mathfrak{f})/H$, el grupo $G(K/\mathbb{Q})$ será cíclico o diédrico según si $C' = C$ o $C' = C^{-1}$, donde el apóstrofo indica la conjugación en k.

El teorema siguiente ayuda a localizar los cuerpos de clases de los grupos $H_\mathfrak{m}$ en algunos casos.

Teorema 11.8 *Sea K/k una extensión de cuerpos numéricos, donde k es cuadrático y K es normal sobre $\mathbb{Q}$. Supongamos que $|K : k| = p$, primo impar. Sea $\mathfrak{f}$ el conductor de K/k y H el grupo de clases.*

a) Si $G(K/\mathbb{Q})$ es diédrico, entonces $H_{f\infty} \le H$, donde f es la parte finita de $\mathfrak{f}$ si ésta es racional, o bien su norma si no lo es.

b) Si $G(K/\mathbb{Q})$ es cíclico entonces H no contiene ningún grupo $H_{f\infty}$ para ningún f.

Demostración: a) Hay que probar que todos los ideales (a), con a entero están en H, pero obviamente $[(a)]' = [(a)]$ (el apóstrofo denota la conjugación) y, por las consideraciones anteriores, $[(a)]' = [(a)]^{-1}$. Esto prueba que $[(a)] = 1$.

b) Supongamos que $H_{f\infty} \le H$ para un cierto f, pero que $G(K/\mathbb{Q})$ es cíclico. Entonces el isomorfismo de Artin, junto con el teorema de Dirichlet, nos da que existe un primo racional q cuyo grado de inercia en K es $2p$. Más aún, existen infinitos primos en estas condiciones, por lo que podemos tomar q primo con f.

En particular q se conserva primo en k, pero entonces $(q) \in H_{f\infty} \le H$, luego q se escinde en K, lo cual es imposible. ∎

Ejemplo Vamos a calcular el cuerpo de clases del grupo H_6 correspondiente al cuerpo cuadrático $k = \mathbb{Q}\big(\sqrt{-3}\,\big)$.

Si lo llamamos K, podemos calcular el grado $|K : k|$ mediante el teorema 11.7. Puesto que 2 es primo en k y 3 se ramifica, tenemos que $\Phi(2) = 3$, $\Phi(3) = 6$. Por otra parte $|\mathcal{O}_1^* : \mathcal{O}_6^*| = 3$ (se trata de un grupo de orden 6 sobre uno de orden 2). Por último, el número de clases de k es $h = 1$. luego concluimos que K tiene grado 3 sobre k.

Sabemos que K ha de ser una extensión de Galois de $\mathbb{Q}$ y, por el teorema anterior, su grupo de Galois ha de ser diédrico (en este caso, el grupo completo de las permutaciones de tres elementos). Esto nos lleva a pensar en un cuerpo de la forma $K = \mathbb{Q}\big(\sqrt{-3}, \sqrt[3]{m}\,\big)$. Los cálculos del capítulo anterior muestran que

si tomamos $m = 2$ entonces el conductor de K es $\mathfrak{f} = 6$, con lo que el teorema anterior implica que H_6 está contenido en su grupo de clases. Comparando los órdenes obtenemos la igualdad. Así pues, $H_6 \leftrightarrow \mathbb{Q}\big(\sqrt{-3}, \sqrt[3]{2}\big)$. ∎

11.4 Géneros

La teoría de géneros de Gauss tiene una interpretación muy interesante en términos de cuerpos de clases. Consideremos el orden $\mathcal{O}_m$ de índice m en un cuerpo cuadrático k y su grupo de clases estrictas $H = I(m\infty)/H_{m\infty}$. Según el teorema de duplicación de Gauss [9.19], el grupo de géneros de $\mathcal{O}_m$ es el grupo $G = H/G_1$, donde el género principal G_1 está formado por los cuadrados de las clases de H. En nuestro contexto resulta más natural tomar esto como definición. Alternativamente, podemos considerar que

$$P_{m\infty} \le H_{m\infty} \le G_1 \le I(m\infty),$$

con lo que el género principal es un grupo de ideales módulo $m\infty$. Llamaremos *cuerpo de géneros* de $\mathcal{O}_m$ al cuerpo de clases de G_1. Notar que si el grupo de clases estrictas de k tiene todos sus elementos de orden 2, entonces coincide con su grupo de géneros, luego el cuerpo de géneros de (el orden maximal de) k es el cuerpo de clases estrictas de Hilbert de k.

Teorema 11.9 *Sea $\mathcal{O}_m$ el orden de índice m de un cuerpo cuadrático k. Sea $K_{m\infty}$ su cuerpo de clases estrictas y K_g su cuerpo de géneros. Entonces K_g es la mayor extensión abeliana de $\mathbb{Q}$ contenida en $K_{m\infty}$.*

Demostración: Llamemos K_g a la mayor extensión abeliana de $\mathbb{Q}$ contenida en $K_{m\infty}$ y probemos que se trata del cuerpo de géneros de $\mathcal{O}_m$. Puesto que $k \subset K_g \subset K_{m\infty}$, podemos considerar el grupo de clases G_1 de K_g módulo $m\,\infty$. Como $m\,\infty$ es invariante por los automorfismos de k, podemos aplicar el teorema 11.4 y concluir que $G_1/H_{m\infty}$ está generado por las clases $C\tau(C)^{-1}$, con $C \in I(m\infty)/H_{m\infty}$ y $\tau \in G(k/\mathbb{Q})$.

Si $\tau = 1$ entonces $C\tau(C)^{-1} = 1$. La otra posibilidad es que τ sea la conjugación en k y entonces, si $C = [\mathfrak{a}]$, se cumple $C\tau(C) = [\mathfrak{a}\tau(\mathfrak{a})] = [\mathrm{N}(\mathfrak{a})] = 1$ (pues las clases de los enteros están en $H_{m\infty}$). Así pues, $\tau(C)^{-1} = C$ y $C\tau(C)^{-1} = C^2$. Por lo tanto $G_1/H_{m\infty}$ está generado por los cuadrados de $I(m\infty)/H_{m\infty}$, luego G_1 es el género principal. ∎

Ahora vamos a construir explícitamente los cuerpos de géneros. Dividiremos la construcción en varios pasos. En los razonamientos que siguen $k = \mathbb{Q}\big(\sqrt{d}\big)$ será un cuerpo cuadrático y K_g el cuerpo de géneros del orden $\mathcal{O}_m$. Llamaremos Δ al discriminante de k y $D = m^2\Delta$ al discriminante de $\mathcal{O}_m$.

1) *Un cuerpo cuadrático $\mathbb{Q}\big(\sqrt{d'}\big)$ está contenido en K_g si y sólo si $m\infty$ es admisible para la extensión $k\big(\sqrt{d'}\big)/k$.*

En efecto, si se da la inclusión es obvio que $m\infty$ ha de ser admisible para la extensión. Recíprocamente, si $m\infty$ es admisible, entonces $k\big(\sqrt{d'}\big)$ tiene un

grupo de clases H módulo $m\infty$. Basta probar que $H_{m\infty} \le H$, pues entonces $k\big(\sqrt{d'}\,\big) \subset K_{m\infty}$ y, como la extensión $k\big(\sqrt{d'}\,\big)/\mathbb{Q}$ es abeliana, se cumple de hecho que $k\big(\sqrt{d'}\,\big) \subset K_g$.

Ahora bien, basta ver que $H_{m\infty}/P_{m\infty} \le H/P_{m\infty}$, y las clases del primer grupo son las de la forma $[(n)]$, donde $n \in \mathbb{Z}$ es primo con m. Entonces

$$\left(\frac{k\big(\sqrt{d'}\,\big)/k}{n}\right) = \left(\frac{k\big(\sqrt{d'}\,\big)/\mathbb{Q}}{\mathrm{N}(n)}\right) = \left(\frac{k\big(\sqrt{d'}\,\big)/\mathbb{Q}}{n}\right)^2 = 1,$$

pues el grupo de Galois $G\big(k\big(\sqrt{d'}\,\big)/\mathbb{Q}\big)$ es de tipo $C_2 \times C_2$ (salvo si $d = d'$, en cuyo caso es de tipo C_2).

Notemos que, según el teorema 10.35, (la parte finita de) el conductor de la extensión $k\big(\sqrt{d'}\,\big)/k$ es su discriminante. Si lo llamamos Δ', la condición necesaria y suficiente para que $\mathbb{Q}\big(\sqrt{d'}\,\big) \subset K_g$ es simplemente que $\Delta' \mid m$.

2) *Sea p un primo impar tal que $p \mid D$ y escojamos el signo adecuado para que $\pm p \equiv 1$ (mód 4). Entonces $\mathbb{Q}\big(\sqrt{\pm p}\,\big) \subset K_g$.*

En efecto, según la fórmula obtenida en el ejemplo 1 de la sección 10.6, el discriminante Δ' de la extensión $k\big(\sqrt{d'}\,\big)/k$ es

$$\Delta' = \begin{cases} \sqrt{\frac{p\cdot(\Delta/p)}{\Delta}} &= 1 \quad \text{si } p \mid \Delta, \\ \sqrt{\frac{p\cdot p\Delta}{\Delta}} &= p \quad \text{si } p \nmid \Delta. \end{cases}$$

En cualquier caso $\Delta' \mid m$.

3) *Se cumple $\mathbb{Q}(i) \subset K_g$ si y sólo si $2 \mid D$ y $D/4 \equiv 0, -1$ (mód 4).*

Es una comprobación rutinaria que no requiere sino distinguir los casos necesarios. Llamemos Δ' al discriminante de la extensión $k(i)/k$. Lo calcularemos en cada caso aplicando siempre la fórmula del ejemplo 1 de la sección 10.6.

Ante todo notemos que si $2 \nmid D$, entonces $d \equiv 1$ (mód 4) y $2 \nmid m$. Por consiguiente

$$\Delta' = \sqrt{\frac{4\cdot 4d}{d}} = 2 \nmid m,$$

luego por 1) tenemos que $\mathbb{Q}(i)$ no está contenido en K_g.

Así, la condición $2 \mid D$ es necesaria para que pueda cumplirse $\mathbb{Q}(i) \subset K_g$. Basta, pues, suponer que $2 \mid D$ (y entonces de hecho $4 \mid D$) y probar que la inclusión se da sólo cuando el resto de $D/4$ módulo 4 es 0 o -1.

- Si $D/4 \equiv 0$ (mód 4) entonces $4^2 \mid m^2\Delta$, luego $2 \mid m^2$, luego $2 \mid m$.

  Si $2 \mid d$ entonces $\Delta' = 2 \mid m$, si $2 \nmid d$ pero $2 \mid \Delta$ entonces $\Delta' = 1 \mid m$ y si $2 \nmid \Delta$ entonces $\Delta' = 4$, pero $4^2 \mid m^2$, luego $4 \mid m$.

- Si $D/4 \equiv -1$ (mód 4) entonces necesariamente $d \equiv -1$ (mód 4), con lo que $\Delta' = 1 \mid m$.

- Si $D/4 \equiv 1 \pmod 4$ entonces $d \equiv 1 \pmod 4$ y $\Delta' = 4 \nmid m$.
- Si $D/4 \equiv 2 \pmod 4$ entonces $2 \mid d$ y $\Delta' = 2 \nmid m$.

Similarmente se demuestra:

4) $\mathbb{Q}(\sqrt{2}) \subset K_g$ *si y sólo si* $2 \mid D$ *y* $D/4 \equiv 0, 2 \pmod 8$.

5) $\mathbb{Q}(\sqrt{-2}) \subset K_g$ *si y sólo si* $2 \mid D$ *y* $D/4 \equiv 0, 6 \pmod 8$.

Ahora ya podemos probar:

Teorema 11.10 *Sea $k = \mathbb{Q}(\sqrt{d})$ un cuerpo cuadrático y sea K_g el cuerpo de géneros de su orden $\mathcal{O}_m$. Sea D el discriminante de $\mathcal{O}_m$. Entonces K_g es la adjunción a $\mathbb{Q}$ de los números $\sqrt{p}$, donde p recorre los primos impares que dividen a D (tomados con el signo adecuado para que $p \equiv 1 \pmod 4$) y los valores $p = -1$, $p = 2$, $p = -2$ en los casos consignados en la tabla siguiente (sólo si $2 \mid D$):*

$D/4 \pmod 8$	p
$0, 3, 4, 7$	-1
$0, 2$	2
$0, 6$	-2

Demostración: Llamemos K al cuerpo construido según el enunciado. Los razonamientos anteriores prueban que $K \subset K_g$. Más aún, sabemos que cada uno de los cuerpos $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{-2})$ está contenido en K_g si y sólo si está contenido en K:

Veamos ahora que $k \subset K$. En efecto, si $d \equiv 1 \pmod 4$ podemos factorizar $d = p_1 \cdots p_r$ ajustando los signos de los primos para que $p_i \equiv 1 \pmod 4$. Como cada $\mathbb{Q}(\sqrt{p_1}) \subset K$, también $k = \mathbb{Q}(\sqrt{d}) \subset k$. Si $d \equiv -1 \pmod 4$ podemos hacer lo mismo con $-d$ y concluir que $\mathbb{Q}(\sqrt{-d}) \subset K$, pero claramente se cumple $D/4 = m^2 d \equiv 0, -1 \pmod 4$, con lo que $\mathbb{Q}(i) \subset K$ y por consiguiente $k = \mathbb{Q}(\sqrt{d}) \subset K$. Si $2 \mid d$ y $d/2 \equiv 1 \pmod 4$, entonces $D/8 = m^2 d \equiv 0, 1 \pmod 4$, luego $D/4 \equiv 0, 2 \pmod 8$ y así $\mathbb{Q}(\sqrt{2}) \subset K$. Ahora es fácil concluir como antes que $k \subset K$. Si $d/2 \equiv -1 \pmod 4$ razonamos igual, con la única diferencia de que ahora $\mathbb{Q}(\sqrt{-2}) \subset K$.

El grupo de Galois $G(K_g/k)$ es isomorfo al grupo de géneros de $\mathcal{O}_m$, luego es producto de grupos cíclicos de orden 2. Si fuera $K \neq K_g$, entonces el grupo $G(K_g/K)$ sería no trivial y contendría un subgrupo U de orden 2. Viendo a $G(K_g/k)$ como espacio vectorial sobre el cuerpo de dos elementos, el subespacio U tiene un complemento, es decir, existe un subgrupo V de modo que $G(K_g/k) = UV$ y $U \cap V = 1$. Sea E el cuerpo fijado por V. De este modo, E es una extensión cuadrática de k contenida en K_g y tal que $E \cap K = k$. Veamos que esto es imposible.

El hecho de que $E \subset K_g$ implica que la extensión $E/\mathbb{Q}$ es abeliana. El grupo $G(E/\mathbb{Q})$ puede ser de tipo C_4 o bien $C_2 \times C_2$. En el primer caso, el teorema de Dirichlet nos da que existen infinitos primos racionales p con grado de inercia 4 en E (los pertenecientes a una clase que genere el grupo de clases de E en $\mathbb{Q}$).

En particular podemos tomar uno tal que $p \nmid m$. Entonces p es primo en k y $(p) \in H_{m\infty}$, pero esto implica que p se escinde completamente en $K_{m\infty}$, luego también en K_g y en E, lo cual es absurdo.

Consideremos ahora el caso en que el grupo de Galois $G(E/\mathbb{Q})$ es de tipo $C_2 \times C_2$. Entonces $E = \mathbb{Q}\big(\sqrt{d}, \sqrt{d'}\big)$, con lo que obtenemos un cuerpo $k' = \mathbb{Q}\big(\sqrt{d'}\big)$ tal que $k' \subset K_g$ pero $k' \not\subset K$.

Llamemos Δ al discriminante de k, Δ' al de k' y Δ'' al de $\mathbb{Q}\big(\sqrt{dd'}\big)$. Entonces, el paso 1) anterior nos da que

$$\sqrt{\frac{\Delta'\Delta''}{\Delta}} \mid m, \quad \text{luego} \quad \Delta' \mid m^2\Delta = D.$$

Esto implica que si un primo impar p cumple $p \mid d'$, entonces $\mathbb{Q}\big(\sqrt{\pm p}\big) \subset K$. A su vez, de aquí se sigue que uno de los cuerpos $\mathbb{Q}(i)$, $\mathbb{Q}\big(\sqrt{2}\big)$ o $\mathbb{Q}\big(\sqrt{-2}\big)$ está contenido en K_g pero no en K, lo cual ya sabemos que es imposible. ∎

Los cuerpos $\mathbb{Q}\big(\sqrt{p}\big)$ con los que hemos construido el cuerpo de géneros tienen discriminantes primos entre sí excepto si aparecen los tres cuerpos $\mathbb{Q}(i)$, $\mathbb{Q}\big(\sqrt{2}\big)$ o $\mathbb{Q}\big(\sqrt{-2}\big)$ (únicamente en el caso $D/4 \equiv 0 \pmod 8$). Es claro entonces que $|K_g : \mathbb{Q}| = 2^m$, donde m es el número de primos que dividen al discriminante D (más 1 si $D/4 \equiv 1 \pmod 8$ y menos 1 si $D/4 \equiv 1, 5 \pmod 8$).

Por consiguiente, el número de géneros es $|K_g : k| = 2^{m-1}$. Además ahora es fácil introducir los caracteres a partir de los cuales Gauss definió los géneros. Como era de esperar, éstos están contenidos en el símbolo de Artin de la extensión K_g/k:

Para cada primo impar $p \mid D$ definimos el carácter $\chi_p : I(m\infty) \longrightarrow \{\pm 1\}$ mediante

$$\left(\frac{K_g/k}{\mathfrak{a}}\right)\big(\sqrt{\pm p}\big) = \chi_p(\mathfrak{a})\sqrt{\pm p},$$

donde el signo es el que hace $\pm p \equiv 1 \pmod 4$.

Es claro que χ_p es un carácter que contiene en su núcleo al género principal, luego induce un carácter en el grupo de géneros.

Si $p = 2$ y $D/4 \not\equiv 0, 1, 5 \pmod 8$ entonces K_g contiene a uno solo de los cuerpos $\mathbb{Q}(i)$, $\mathbb{Q}\big(\sqrt{2}\big)$ o $\mathbb{Q}\big(\sqrt{-2}\big)$ y podemos definir igualmente un carácter χ_2. Si $D/4 \equiv 0 \pmod 8$ tenemos tres caracteres χ_{21}, χ_{22}, χ_{23}.

El automorfismo $\left(\frac{K_g/k}{\mathfrak{a}}\right)$ está completamente determinado por los caracteres de $\mathfrak{a}$, luego dos ideales pertenecen al mismo género si y sólo si tienen los mismos caracteres.

Si $p \mid D$ y el carácter χ_p se calcula a partir de $\sqrt{p_0}$ (es decir, $p_0 = \pm p$ o $p_0 = -1$), entonces, para todo ideal fraccional $\mathfrak{a} \in I(m\infty)$ cuya norma no sea divisible entre p se cumple

$$\begin{aligned}\left(\frac{K_g/k}{\mathfrak{a}}\right)\big(\sqrt{p_0}\big) &= \left(\frac{k\big(\sqrt{p_0}\big)/k}{\mathfrak{a}}\right)\big(\sqrt{p_0}\big) = \left(\frac{\mathbb{Q}\big(\sqrt{p_0}\big)/\mathbb{Q}}{\mathrm{N}(\mathfrak{a})}\right)\big(\sqrt{p_0}\big)\\ &= \psi_p(\mathrm{N}(\mathfrak{a}))\sqrt{p_0},\end{aligned}$$

donde ψ_p es el carácter del cuerpo cuadrático $\mathbb{Q}\big(\sqrt{p_0}\big)$. Así $\chi_p(\mathfrak{a}) = \psi_p(\mathrm{N}(\mathfrak{a}))$.

Ahora es fácil ver que los caracteres que acabamos de definir son los mismos que definimos en el capitulo [IX]. De hecho, ahora ya es fácil probar todos los resultados sobre los géneros que probamos allí por otros medios.

Por ejemplo, notemos que podemos descomponer $d = p_0p_1\cdots p_m$, donde los primos p_i (elegidos con el signo adecuado) cumplen $p_i \equiv 1 \pmod 4$ salvo quizá p_0, que puede ser también -1 o ± 2. En cualquier caso se cumple que $\mathbb{Q}\big(\sqrt{p_i}\big) \subset K_g$ (el argumento está detallado en la prueba del teorema anterior, cuando hemos visto que $k \subset K$). A los caracteres correspondientes a los números p_i los llamaremos *caracteres fundamentales* del grupo de géneros. Es fácil ver que los caracteres fundamentales son los caracteres χ_p tales que $p \mid \Delta$ (entendiendo que si hay tres caracteres asociados al 2 sólo uno de ellos es fundamental).

De aquí se sigue la relación que liga a los caracteres, pues los símbolos de Artin han de fijar a $\sqrt{d}$, lo cual se traduce en que

$$\prod_{p|\Delta} \chi_p(\mathfrak{a}) = 1, \quad \text{para todo } \mathfrak{a} \in I(m\infty).$$

En otras palabras, el número de caracteres fundamentales negativos de un género ha de ser par. Otra restricción obvia es que si hay tres caracteres asociados al 2, su producto ha de ser 1. Teniendo en cuenta el número de géneros, es claro que no puede haber más restricciones.

Ejercicio: Dar una prueba sencilla de que si dos ideales tienen la misma norma (prima con el discriminante D) entonces son del mismo género.

11.5 Cálculo de cuerpos de clases

Vamos a abordar finalmente el problema del cálculo explícito de cuerpos de clases sobre cuerpos distintos de $\mathbb{Q}$. Como ya hemos comentado en varias ocasiones, se trata de un problema técnico muy complejo. Nosotros nos limitaremos a ver algunos resultados, mayoritariamente ejemplos, en el caso en que el cuerpo base es un cuerpo cuadrático.

En primer lugar nos ocupamos del cálculo del cuerpo de clases de Hilbert. Ante todo observamos que si el grupo de clases estrictas tiene todos sus elementos de orden 2, es decir, si es producto de grupos cíclicos de orden 2, entonces el grupo de clases coincide con el grupo de géneros y el problema lo resuelve el teorema 11.10.

Los mínimos cuerpos imaginarios cuyo grupo de clases de Hilbert no es de esta forma son $\mathbb{Q}\big(\sqrt{-14}\big)$ y $\mathbb{Q}\big(\sqrt{-17}\big)$, con $h = 4$, y $\mathbb{Q}\big(\sqrt{-21}\big)$, con $h = 3$. Entre los cuerpos reales el menor ejemplo es $\mathbb{Q}\big(\sqrt{34}\big)$ (cuyo grupo de clases estrictas tiene orden 4). El cuerpo de clases de $\mathbb{Q}\big(\sqrt{-21}\big)$ lo calculamos ya al final de la sección 11.1. Para calcular el cuerpo correspondiente a los otros ejemplos nos apoyaremos en un resultado general que deducimos a su vez de otro más general aún.

Teorema 11.11 *Si $K/\mathbb{Q}$ es una extensión de Galois entonces el grupo $G(K/\mathbb{Q})$ está generado por los grupos de inercia de los primos de K ramificados sobre $\mathbb{Q}$.*

DEMOSTRACIÓN: Sea H el subgrupo de $G(K/\mathbb{Q})$ generado por los grupos de inercia de los primos ramificados de K. Sea k el cuerpo fijado por H. Sea $\mathfrak{p}$ un primo en k, sea p el primo racional divisible entre $\mathfrak{p}$ y sea $\mathfrak{P}$ un divisor primo de $\mathfrak{p}$ en K. Sea F el cuerpo fijado por el grupo de inercia de $\mathfrak{P}$. Este grupo de inercia está contenido en H (si $\mathfrak{P}$ no es ramificado el grupo de inercia es trivial), luego $k \subset F$. Entonces el primo de F divisible entre $\mathfrak{P}$ es no ramificado sobre $\mathbb{Q}$, luego $\mathfrak{p}$ también lo es. En definitiva, ningún primo $\mathfrak{p}$ de k se ramifica sobre $\mathbb{Q}$. El discriminante de la extensión $k/\mathbb{Q}$ es igual a 1, pero el teorema de Minkowski [4.13] implica entonces que $k = \mathbb{Q}$, luego $G(K/\mathbb{Q}) = H$. ∎

En particular tenemos:

Teorema 11.12 *Sea $\mathbb{Q} \subset k \subset K$ una cadena de extensiones de modo que las tres sean de Galois. Supongamos que $|k : \mathbb{Q}| = p$ es primo y que la extensión K/k es no ramificada (en los primos finitos). Entonces $G(K/\mathbb{Q})$ está generado por los elementos de orden p y existe un grupo $H \leq G(K/\mathbb{Q})$ de manera que $G(K/\mathbb{Q}) = G(K/k)H$.*

DEMOSTRACIÓN: Si $\mathfrak{p}$ es un primo de K ramificado sobre $\mathbb{Q}$ entonces su índice de ramificación es $e = p$ (pues la ramificación se ha de producir en el tramo $k/\mathbb{Q}$), luego su grupo de inercia tiene orden p. Por el teorema anterior $G(K/\mathbb{Q})$ está generado por los elementos de estos grupos de inercia, todos de orden p.

Como $G(K/k) < G(K/\mathbb{Q})$, algún automorfismo σ de orden p ha de quedar fuera de $G(K/k)$, y el grupo $H = \langle\sigma\rangle$ cumple lo pedido. ∎

De este modo, si K es el cuerpo de clases de Hilbert estrictas de un cuerpo cuadrático k, entonces el grupo $G(K/\mathbb{Q})$ está generado por los automorfismos de orden 2.

Ejemplo Vamos a calcular el cuerpo de clases de Hilbert estrictas del cuerpo $k = \mathbb{Q}(\sqrt{34})$.

Se comprueba que el número de clases es $h = 2$, pero la unidad fundamental tiene norma positiva, por lo que el número de clases estrictas es $h' = 4$. De este modo, buscamos un cuerpo K de grado 8 sobre $\mathbb{Q}$. Sabemos que la extensión $K/\mathbb{Q}$ es de Galois y que el grupo $G(K/\mathbb{Q})$ está generado por los elementos de orden 2. Por otra parte K contiene al cuerpo de géneros $K_g = \mathbb{Q}(\sqrt{2}, \sqrt{17})$, que tiene grado 4 sobre $\mathbb{Q}$. Esto implica que el grupo de clases de K no coincide con el grupo de géneros, por lo que no puede ser de tipo $C_2 \times C_2$. Por consiguiente es cíclico. Además K_g es la mayor extensión abeliana de $\mathbb{Q}$ contenida en K, luego el grupo $G(K/\mathbb{Q})$ no es abeliano.

La teoría de grupos nos enseña[1] que todo grupo no abeliano de orden 8 es

[1] Usamos esto únicamente a nivel heurístico, para localizar el cuerpo K. No obstante, una vez lo hayamos encontrado, la prueba de que efectivamente se trata del cuerpo de clases que buscamos no se apoyará en estos razonamientos previos. De hecho ni siquiera es necesario el teorema anterior.

isomorfo al grupo diédrico D_4 o bien al grupo cuaternio Q_8, del que no hemos hablado, pero que tampoco nos va a hacer falta, pues este grupo tiene un único elemento de orden 2, de modo que no puede ser nuestro grupo de Galois. En definitiva, $G(K/\mathbb{Q}) \cong D_4$.

Recordemos que el grupo D_4 está generado por dos elementos σ y τ, de modo que σ tiene orden 4 y τ tiene orden 2. Además $\sigma^\tau = \sigma^{-1}$. Sus ocho elementos pueden expresarse en la forma

$$D_4 = \{1, \quad \sigma, \quad \sigma^2, \quad \sigma^3, \quad \sigma\tau, \quad \sigma^2\tau, \quad \sigma^3\tau\}.$$

De entre ellos, sólo σ y σ^3 tienen orden 4 y los restantes (aparte del neutro) tienen todos orden 2. De este modo, $G(K/\mathbb{Q})$ tiene un único subgrupo cíclico de orden 4, que necesariamente ha de ser $G(K/k)$, ya que éste es isomorfo al grupo de clases de k y ya hemos visto que es cíclico.

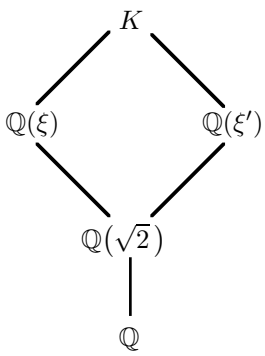
De este modo, si $G(K/k) = \langle\sigma\rangle$, necesariamente $G(K/K_g) = \langle\sigma^2\rangle$.

Los otros dos cuerpos cuadráticos $\mathbb{Q}(\sqrt{2}\,)$ y $\mathbb{Q}(\sqrt{17}\,)$ se corresponden con grupos de tipo $C_2 \times C_2$. Puesto que cada uno de estos grupos tiene tres subgrupos, cada cuerpo ha de estar contenido exactamente en tres cuerpos de grado cuatro, uno de los cuales es K_g. Por simplicidad vamos a estudiar únicamente el caso de $\mathbb{Q}(\sqrt{2}\,)$, si bien todo lo que digamos vale igualmente para $\mathbb{Q}(\sqrt{17}\,)$.

No perdemos generalidad si suponemos que el grupo de los $\mathbb{Q}(\sqrt{2}\,)$-automorfismos de K es $\langle\sigma^2, \tau\rangle$. Los subgrupos $\langle\tau\rangle$ y $\langle\sigma^2\tau\rangle$ no son normales en $G(K/\mathbb{Q})$. Más aún, son conjugados, pues

$$\tau^\sigma = \sigma^3\tau\sigma = \sigma^3\sigma^\tau\tau = \sigma^3\sigma^{-1}\tau = \sigma^2\tau.$$

Por lo tanto $\mathbb{Q}(\sqrt{2}\,)$ está contenido en dos cuerpos conjugados de grado 4. Si ξ es un elemento primitivo para uno de ellos, el otro tendrá por elemento primitivo a un conjugado ξ'. En definitiva tenemos la estructura que indica el diagrama.



Es claro que en estas condiciones $K = \mathbb{Q}(\xi, \xi')$. Equivalentemente, $\mathbb{Q}$ es el cuerpo de escisión del polinomio mínimo de ξ (que es el mismo que el de ξ'). Para determinar $\mathbb{Q}(\xi)$ calcularemos primero su discriminante.

Puesto que la extensión K/k es no ramificada, su discriminante es 1 y el teorema 3.24 nos da que

$$\Delta_K = \Delta_k^4 = 2^{12} \cdot 17^4.$$

De aquí se sigue por el mismo teorema que el discriminante de la extensión $K/\mathbb{Q}(\sqrt{2}\,)$ ha de ser 17^2 (aquí usamos que el discriminante ha de ser invariante por automorfismos de k). En particular, los únicos primos de $\mathbb{Q}(\sqrt{2}\,)$ que pueden ramificarse en K —y por consiguiente en $\mathbb{Q}(\xi)$— son los divisores de 17. Concretamente

$$17 = (5 + 2\sqrt{2}\,)(5 - 2\sqrt{2}\,).$$

Sabemos que $\sqrt{17} \in K$, luego resulta razonable conjeturar que $\sqrt{5+2\sqrt{2}}$ y $\sqrt{5-2\sqrt{2}}$ han de estar también en K. Más aún, si tomamos estos números como ξ y ξ' tenemos garantizado que los divisores de 17 se ramifican en un cuerpo intermedio cada uno, y por consiguiente ambos se ramifican en K.

No obstante esto no funciona, y podemos saber a priori que no puede funcionar. En efecto, el cuerpo de clases estrictas de Hilbert de k no coincide con el cuerpo de clases no estrictas (éste último tiene grado 2 sobre k) y, desde el punto de vista aritmético, la diferencia entre ambos es únicamente que ∞ puede ramificarse en K pero no en el cuerpo de clases no estrictas. Por consiguiente ∞ debe ramificarse en K, es decir, K ha de ser un cuerpo complejo. Esto se soluciona modificando la factorización del 17, que también puede expresarse en la forma

$$17 = \big(-5-2\sqrt{2}\big)\big(-5+2\sqrt{2}\big).$$

Definimos $\xi = \sqrt{-5-2\sqrt{2}}$ y $\xi' = \sqrt{-5+2\sqrt{2}}$. De este modo $K = \mathbb{Q}(\xi,\xi')$ es un cuerpo complejo y vamos a probar que es el cuerpo que buscamos.

En realidad todo se reduce a probar que el discriminante de la extensión $\mathbb{Q}(\xi)/\mathbb{Q}\big(\sqrt{2}\big)$ es exactamente $-5-2\sqrt{2}$, pues entonces el de $\mathbb{Q}(\xi')/\mathbb{Q}\big(\sqrt{2}\big)$ tendrá que ser $-5+2\sqrt{2}$ (aplicando un automorfismo) y podremos aplicar el teorema 3.25 para concluir que el discriminante de $K/\mathbb{Q}\big(\sqrt{2}\big)$ es 17^2, e invirtiendo los razonamientos anteriores llegamos a que el discriminante de K/k es 1.

Por lo demás, es claro que $\sqrt{17} = \xi\xi' \in K$, luego también $\mathbb{Q}\big(\sqrt{34}\big) \in K$ y por consiguiente K/k es una extensión de grado 4 no ramificada, es decir, K es el cuerpo de clases de Hilbert estrictas de k.

Ahora bien, el discriminante $\Delta[\xi]$ es 4ξ, pero un simple tanteo nos lleva a encontrar el número

$$\alpha = \frac{1+\sqrt{2}+\xi}{2},$$

que es un entero de $\mathbb{Q}(\xi)$ (su norma y su traza son enteras) y

$$\Delta[\alpha] = (\alpha-\alpha')^2 = \xi^2 = -5-2\sqrt{2}.$$

Tal α no existiría si hubiéramos tomado como ξ el número $\sqrt{5+2\sqrt{2}}$. De hecho teníamos cuatro posibilidades para ξ, correspondientes a las dos factorizaciones de 17 que hemos considerado más las dos que resultan de multiplicar los factores por $\pm(1+\sqrt{2})$ (la unidad fundamental de $\mathbb{Q}\big(\sqrt{2}\big)$). La única válida es la que hemos adoptado.

Para concluir observamos que el polinomio mínimo de ξ es x^4+10x^2+17, luego podemos enunciar nuestro resultado de la forma siguiente:

> *El cuerpo de clases de Hilbert estrictas de $\mathbb{Q}\big(\sqrt{34}\big)$ es el cuerpo de escisión del polinomio x^4+10x^2+17.*

■

Como ya hemos comentado, gran parte de los razonamientos que hemos empleado en este ejemplo han servido para identificar el cuerpo de clases que buscábamos pero, una vez encontrado, no hacen falta para justificar que ciertamente es el cuerpo que buscamos. Para mostrarlo más claramente calculamos ahora el cuerpo de clases de Hilbert de $\mathbb{Q}\big(\sqrt{-14}\big)$ suprimiendo toda la primera parte, lógicamente innecesaria.

Ejemplo *El cuerpo de clases de Hilbert de $k_2 = \mathbb{Q}\big(\sqrt{-14}\big)$ es el cuerpo de escisión del polinomio $x^4 + 2x^2 - 7$.*

En efecto, Sea ξ una raíz de este polinomio. Por ejemplo $\xi = \sqrt{-1+2\sqrt{2}}$. Es fácil ver que

$$\alpha = \frac{1+\sqrt{2}+\xi}{2}$$

es un entero (su norma y su traza en la extensión $\mathbb{Q}(\xi)/\mathbb{Q}\big(\sqrt{2}\big)$ son enteras). Claramente

$$\Delta[\alpha] = (\alpha - \alpha')^2 = \xi^2 = -1 + 2\sqrt{2}.$$

El discriminante de $\mathbb{Q}(\xi)/\mathbb{Q}\big(\sqrt{2}\big)$ divide a este discriminante y, como obviamente $-1+2\sqrt{2}$ es un primo ramificado en $\mathbb{Q}(\xi)$, concluimos que $-1+2\sqrt{2}$ es el discriminante de la extensión.

Sea $\xi' = \sqrt{-1-2\sqrt{2}}$. Es claro que ξ' es conjugado de ξ sobre $\mathbb{Q}$, luego las extensiones $\mathbb{Q}(\xi)$ y $\mathbb{Q}(\xi')$ son isomorfas y el isomorfismo intercambia ξ con ξ'. Además envía $\sqrt{2}$ a $-\sqrt{2}$, luego deja fijo al cuerpo $\mathbb{Q}\big(\sqrt{2}\big)$ y el discriminante de $\mathbb{Q}(\xi')/\mathbb{Q}\big(\sqrt{2}\big)$ es $-1-2\sqrt{2}$. En particular vemos que $\mathbb{Q}(\xi) \neq \mathbb{Q}(\xi')$.

Sea $K_8 = \mathbb{Q}(\xi, \xi')$, el cuerpo de escisión del polinomio dado. El teorema 3.25 nos da que el discriminante de $K_8/\mathbb{Q}\big(\sqrt{2}\big)$ es

$$\Delta_{8/2} = (-1+2\sqrt{2})^2(-1-2\sqrt{2})^2 = 7^2,$$

y por 3.24 el discriminante de $K_8/\mathbb{Q}$ es $\Delta_{8/1} = 2^{12}\cdot 7^4$.

El cuerpo K_8 contiene a $\xi\xi' = \sqrt{-7}$, luego también a $k_2 = \mathbb{Q}\big(\sqrt{-14}\big)$, y el teorema 3.24 nos permite concluir que $\Delta_{8/2} = 1$. Por lo tanto la extensión K_8/k_2 es no ramificada y obviamente abeliana. Como tiene el mismo grado que la extensión de Hilbert, concluimos que K_8 es el cuerpo de clases de Hilbert del cuerpo k_2. ∎

Ejemplo Vamos a calcular los primeros cuerpos de clases sobre $k = \mathbb{Q}\big(\sqrt{5}\big)$. Es conocido que k tiene factorización única y que una unidad fundamental es

$$\epsilon = \frac{1+\sqrt{5}}{2}.$$

La norma de ϵ es -1, con lo que $h_1 = h_\infty = 1$. El cuerpo k tiene dos divisores arquimedianos reales. Digamos que ∞_1 es el asociado a la identidad e ∞_2 es el asociado a la conjugación. De este modo, $\alpha \equiv 1 \pmod{\infty_1}$ si y sólo si $\alpha > 0$ y $\alpha \equiv 1 \pmod{\infty_2}$ si y sólo si $\alpha' > 0$.

En primer lugar calcularemos los órdenes de los grupos radiales mediante el teorema 11.7. Para ello necesitamos investigar las unidades de k. Sabemos que son de la forma $\pm\epsilon^m$. He aquí las primeras potencias de ϵ:

$$\epsilon^2 = 1+\epsilon, \quad \epsilon^3 = 1+2\epsilon, \quad \epsilon^4 = 2+3\epsilon, \quad \epsilon^5 = 3+5\epsilon, \quad \epsilon^6 = 5+8\epsilon.$$

El primo racional 2 sigue siendo primo en k, luego el primer grupo radial a investigar es $H(2\infty)$. Es fácil ver que $\Phi(2) = 3$, luego $\Phi(2\infty) = 12$. Por otra parte vemos que $\epsilon^3 \equiv 1 \pmod 2$, pero $\epsilon^3 \not\equiv 1 \pmod{\infty_2}$ (tiene norma negativa y es positivo, luego el conjugado es negativo). Así pues, la mínima potencia de ϵ que es congruente con 1 módulo 2∞ es ϵ^6, pero no $-\epsilon^6$, luego el índice $|U_1 : U_{2\infty}|$ es 12 (el grupo U_1 es $C_2 \times \mathbb{Z}$ y $U_{2\infty}$ es $1 \times 6\mathbb{Z}$, luego el cociente tiene orden 12). El teorema 11.7 nos da que $h_{2\infty} = 1$ y no hay más que hacer.

El 3 también se conserva primo en k, luego el grupo siguiente es $H(3\infty)$. Claramente $\Phi(3\infty) = 32$. Ahora tenemos que $\epsilon^4 \equiv -1 \pmod 3$, por lo que $\epsilon^8 \equiv 1 \pmod 3$ y el exponente es el mínimo posible. De hecho $\epsilon^8 \equiv 1 \pmod{3\infty}$ luego se cumple $|U_1 : U_{3\infty}| = 16$ y, en consecuencia. $h_{3\infty} = 2$.

El cuerpo radial asociado es una extensión de grado 2 de k cuyo conductor, o sea, su discriminante relativo, es 3. Es natural pensar en $K = \mathbb{Q}\big(\sqrt{5}, \sqrt{-3}\big)$. Efectivamente, los resultados del ejemplo 1 de la sección 10.6 confirman que el conductor es 3∞.

Hemos probado que $H(3\infty) \leftrightarrow \mathbb{Q}\big(\sqrt{5}, \sqrt{-3}\big)$. Como el conductor no es 3, concluimos que $h_3 = h_{3\infty_1} = h_{3\infty_2} = 1$.

El divisor siguiente es 4∞. Por una parte $\Phi(4\infty) = 48$. Por otra $\epsilon^6 \equiv 1 \pmod{4\infty}$, luego $|U_1 : U_{4\infty}| = 12$, y así $h_{4\infty} = 4$.

Si investigamos un poco más podemos obtener incluso la estructura de $H(4\infty)$. Para ello vemos que $h_{4\infty_1} = h_{4\infty_2} = 24/12 = 2$, mientras que $h_4 = 12/12 = 1$.

Esto significa que los grupos $H(4\infty_1)$ y $H(4\infty_2)$ son distintos, pues si coincidieran el conductor de su cuerpo de clases dividiría a $4\infty_1$ y a $4\infty_2$, luego a 4, pero entonces el cuerpo de clases sería el cuerpo radial de 4, que es k.

Resulta, pues, que el grupo radial de 4∞ tiene al menos dos subgrupos de orden 2, luego es isomorfo a $C_2 \times C_2$. Los cuerpos radiales de $4\infty_1$ y $4\infty_2$ tienen grado cuatro sobre $\mathbb{Q}$, pero no son normales, pues la conjugación en k intercambia los divisores infinitos, luego se extiende a un isomorfismo entre los cuerpos radiales.

Busquemos estos cuerpos. Han de ser de la forma $K = k\big(\sqrt{\alpha}\big)$ para un cierto a $\alpha \in k$. El discriminante de K/k es la parte finita del conductor, o sea, 4, luego el diferente es 2. En cualquier caso, el polinomio mínimo de $\sqrt{\alpha}$ es $x^2 - \alpha$, luego el diferente divide a 2. La forma de conseguir que sea exactamente 2 es tomar como α una unidad de k, con lo que $\sqrt{\alpha}$ también será una unidad.

Consideremos $K = k(\epsilon)$. Por lo que acabamos de ver, el diferente de K/k es 1 o 2, pero no puede ser 1 porque entonces K/k sería no ramificada, pero k no tiene extensiones abelianas no ramificadas, ya que su número de clases estrictas es 1. El cuerpo K tiene cuatro monomorfismos en $\mathbb{C}$. Dos de ellos son automorfismos, los del grupo $G(K/k)$, que extienden a la identidad de k. Esto

significa que ∞_1 se escinde en K en dos factores reales. Por el contrario, la conjugación de k se extiende a dos monomorfismos complejos, cuya imagen es el cuerpo $k(\sqrt{\epsilon'})$. Esto quiere decir que ∞_2 se ramifica.

Así pues, K tiene tres primos arquimedianos, y la factorización de ∞ es

$$\infty = \infty_{11}\,\infty_{12}\,\infty_{21}^2.$$

Consecuentemente, el conductor de K/k es $4\infty_2$. Además hemos encontrado el cuerpo $k(\sqrt{\epsilon'})$, que obviamente tiene conductor $4\infty_1$ y es otro de los cuerpos radiales buscados.

Como $H(4\infty) = H(4\infty_1) \cap H(4\infty_2)$, el cuerpo de clases de $H(4\infty)$ es el producto de los grupos de clases de estos dos cuerpos: $H(4\infty) \leftrightarrow k(\sqrt{\epsilon}, \sqrt{\epsilon'})$.

Nos falta localizar el tercer subcuerpo de $k(\sqrt{\epsilon}, \sqrt{\epsilon'})$, pero es claro que $\sqrt{\epsilon}\,\sqrt{\epsilon'} = i$, luego dicho cuerpo es $k(i)$. En resumen, la situación es:

Cuerpo	Conductor	$G(K/k)$
$k(\sqrt{\epsilon}\,, \sqrt{\epsilon'})$	4∞	C_4
$k(\sqrt{5}, \sqrt{\epsilon'})$	$4\infty_1$	C_2
$k(\sqrt{\epsilon}, \sqrt{\epsilon})$	$4\infty_2$	C_2
$k(\sqrt{\epsilon}, i)$	4∞	C_2
$\mathbb{Q}(\sqrt{5})$	1	1

El divisor siguiente es $\sqrt{5}$. Es claro que $\Phi(\sqrt{5}\infty) = 16$. Aparentemente la menor unidad congruente con un entero módulo $\sqrt{5}$ es $\epsilon^5 = 3 + 5\epsilon$, pero esto es erróneo. Notemos que $2\epsilon = 1 + \sqrt{5}$, luego $2\epsilon \equiv 1 \pmod{\sqrt{5}}$. El inverso de 2 módulo 5 es 3, por lo que

$$\epsilon \equiv 3 \pmod{\sqrt{5}}, \quad \epsilon^2 \equiv -1 \pmod{\sqrt{5}}, \quad \epsilon^4 \equiv 1 \pmod{\sqrt{5}}.$$

De aquí se concluye que $|U_1 : U_{\sqrt{5}\infty}| = 8$ y, por consiguiente, $h_\infty = 2$. Buscamos un cuerpo K de grado cuatro sobre $\mathbb{Q}$, de Galois (porque ∞ es invariante) y cuyo discriminante relativo es $\sqrt{5}$. Un cálculo sencillo nos da que el discriminante sobre $\mathbb{Q}$ ha de ser 5^3 y esto nos lleva al quinto cuerpo ciclotómico.

Por último señalamos que $h_{5\infty} = h_{6\infty} = 2$, luego $H(5\infty) = H(\sqrt{5}\infty)$ y $H(6\infty) = H(3\infty)$. ∎

Ejemplo Para terminar calcularemos los primeros cuerpos de clases sobre $k = \mathbb{Q}(\sqrt{-3})$. Las diferencias principales respecto al ejemplo anterior son que ahora los primos infinitos son irrelevantes y que sólo tenemos seis unidades: ± 1, $\pm\zeta$, $\pm\zeta^2$, donde

$$\zeta = \frac{-1 + \sqrt{3}}{2}.$$

Como antes, el número de clases es 1.

En general, $(\zeta - 1) = (\zeta^2 - 1) = (\sqrt{-3})$, por lo que ζ y ζ^2 sólo pertenecen a un grupo de unidades $U_\mathfrak{m}$ cuando $\mathfrak{m} = \sqrt{-3}$. Así mismo, $(-1 - 1) = (2)$, luego -1 sólo está en $U_\mathfrak{m}$ cuando $\mathfrak{m} = 2$ y por último $(-\zeta - 1) = (-\zeta^2 - 1) = (1)$, por

lo que $-\zeta$ y $-\zeta^2$ no pertenecen a ningún grupo $U_\mathfrak{m}$ (siempre suponiendo que $\mathfrak{m} \neq 1$).

En resumen, $|U_1| = 6$, $|U_2| = 2$, $|U_{\sqrt{-3}}| = 3$ y $|U_\mathfrak{m}| = 1$ en cualquier otro caso.

Por otro lado, un primo racional p se escinde en k si y sólo si $p \equiv 1$ (mód 3), se conserva si y sólo si $p \equiv -1$ (mód 3) y se ramifica si y sólo si $p = 3$.

Con todos estos datos es pura rutina calcular los órdenes $h_\mathfrak{m}$ de los grupos radiales. En particular $h_1 = h_2 = h_{\sqrt{-3}} = h_3 = 1$. He aquí una tabla con los casos siguientes, que ya no son triviales. El primer cuerpo de cada bloque es el cuerpo radial de su conductor.

Cuerpo	Conductor	$G(K/k)$
$\mathbb{Q}(\sqrt{-3}, i)$	4	C_2
$\mathbb{Q}\big(\sqrt{-3}\,\big)$	1	1
$\mathbb{Q}(e^{2\pi i/15})$	5	C_4
$\mathbb{Q}\big(\sqrt{-3}\,\sqrt{5}\big)$	5	C_2
$\mathbb{Q}\big(\sqrt{-3}\,\big)$	1	1
$\mathbb{Q}\big(\sqrt{-3}, \sqrt[3]{2}\big)$	6	C_3
$\mathbb{Q}\big(\sqrt{-3}\,\big)$	1	1
$\mathbb{Q}(e^{2\pi i/21})$	7	C_6
$\mathbb{Q}(\cos(2\pi i/21)$	7	C_3
$\mathbb{Q}\big(\sqrt{-3}, \sqrt{-7}\big)$	7	C_2
$\mathbb{Q}\big(\sqrt{-3}\,\big)$	1	1

Observar que 7 no es primo en k, sino que se escinde en dos factores, pero los cuerpos radiales asociados a sus divisores coinciden con k.

La tabla anterior se construye sin excesiva imaginación. Por ejemplo, para llegar hasta el cuerpo radial asociado a 7 partimos de que $h_7 = 6$, por lo que buscamos una extensión K_{12}/k_2 abeliana de grado 6. El grupo de Galois es necesariamente cíclico, luego tiene un subgrupo de orden 2 y otro de orden 3, correspondientes a dos cuerpos intermedios K_6 y K_4. Puesto que los divisores de 7 no son conductores de ningún cuerpo, los conductores de K_4 y K_6 son iguales a 7. Como son extensiones cíclicas, podemos concluir que $\Delta_{4/2} = 7$ y $\Delta_{6/2} = 7^2$. El grado de ramificación en K_{12} de los divisores de 7 en k_2 ha de ser 6 (múltiplo de 2 y 3) y, como la ramificación es dominada, esto nos da el discriminante $\Delta_{12/2} = 7^5$, y de aquí que $\Delta_{12/1} = 3^6 7^{10}$.

Por otro lado el cuerpo K_4 es fácil de calcular: ha de ser una extensión cuadrática de k_2 con discriminante 7, lo que nos lleva inmediatamente al cuerpo $\mathbb{Q}\big(\sqrt{-3}, \sqrt{-7}\,\big)$. Además sabemos que $K_{12}/\mathbb{Q}$ es normal (porque 7 es invariante). Con todos estos datos el cuerpo ciclotómico queda perfectamente perfilado.

De todos modos, hay que advertir que esto es sólo un ejemplo de cómo se puede obtener información que nos permita conjeturar cuál es el cuerpo radial de un divisor dado, pero nada de esto hace falta para probar que, por ejemplo en este caso, el cuerpo radial de 7 es el vigesimoprimer cuerpo ciclotómico. Si aceptamos la conjetura, lo único que hay que hacer es calcular $h_7 = 6$ y comprobar que el conductor del cuerpo es 7. ∎

11.6 Formas cuadráticas

La teoría de cuerpos de clases permite mejorar los resultados de Gauss sobre representación de números (especialmente primos) por formas cuadráticas binarias. La teoría básica está desarrollada en el capítulo [VI]. El problema general es determinar los enteros n que pueden expresarse en la forma $n = f(x, y)$, donde x e y son enteros y $f(x, y) = ax^2 + bxy + cy^2$ es una forma cuadrática binaria con coeficientes enteros. El discriminante de f es el entero $D = b^2 - 4ac$. Si $D \neq 0$ hay un único orden cuadrático $\mathcal{O}_m$ (correspondiente a un cierto cuerpo cuadrático k) con discriminante $D = m^2\Delta$ (donde Δ es el discriminante de k).

En la sección [6.2] definimos la equivalencia estricta de formas (de modo que dos formas estrictamente equivalentes representan a los mismos enteros) y probamos que las clases de equivalencia estricta de formas cuadráticas de discriminante D están en correspondencia biunívoca[2] con las clases de similitud estricta de los módulos cuyo anillo de coeficientes es $\mathcal{O}_m$. Explícitamente, si (α, β) es una base orientada de un módulo M (en el sentido de [6.5]), la clase de formas asociada a la clase de similitud estricta de M es la clase equivalencia estricta de la forma $f(x, y) = \mathrm{N}(\alpha x + \beta y)/\mathrm{N}(M)$.

En la sección [6.3] probamos que el grupo de clases de similitud estricta de los módulos del orden $\mathcal{O}_m$ es isomorfo al grupo de clases estrictas de $\mathcal{O}_m$, y en la sección 11.3 hemos visto que este grupo es isomorfo al grupo de clases $I(m\infty)/H_{m\infty}$ de k.

Para tratar con ejemplos concretos debemos explicitar la correspondencia entre ideales y formas a través de todos estos isomorfismos. Partimos de un ideal $\mathfrak{a} \in I(m\infty)$. Según el teorema [6.9] se puede expresar en la forma

$$\mathfrak{a} = k\,\langle a, b + \omega\rangle\,, \quad \text{con } a, b, k \in \mathbb{Z}, \quad a \mid \mathrm{N}(b + \omega), \quad \mathrm{N}(\mathfrak{a}) = k^2 a.$$

Entonces es fácil comprobar que $\mathfrak{a} \cap \mathcal{O}_m = k\,\langle a, mb + m\omega\rangle$. Éste es el módulo de $\mathcal{O}_m$ cuya clase de similitud estricta se corresponde con la de $\mathfrak{a}$. La forma cuadrática asociada a este módulo es

$$f(x, y) = k^2\,\frac{\mathrm{N}\big(ax + (mb + m\omega)y\big)}{\mathrm{N}(\mathfrak{a})}.$$

[2]Hay que restringirse a formas primitivas y, si $D < 0$, definidas positivas, pero esto no supone pérdida alguna de generalidad.

Ejemplo Vamos a calcular la correspondencia entre formas e ideales para el discriminante $D = -56$. El cuerpo cuadrático es $\mathbb{Q}\big(\sqrt{-14}\,\big)$ y $m = 1$. El grupo de ideales es simplemente el grupo de clases I/P, cuyo orden es $h = 4$. El teorema [4.14] nos da que toda clase contiene un ideal de norma menor o igual que 4. Los únicos ideales en estas condiciones son 1, 2, el divisor primo de 2 y los divisores primos de 3. Podemos descartar el 2 porque da lugar a la misma clase que el 1, luego nos quedan exactamente cuatro clases, que han de ser distintos. Los representantes son:

$$\begin{aligned} 1 &= \langle 1, \sqrt{-14}\,\rangle, \\ \mathfrak{p} &= \big(2, \sqrt{-14}\,\big) = \langle 2, \sqrt{-14}\,\rangle, \\ \mathfrak{q} &= \big(3, 1+\sqrt{-14}\,\big) = \langle 3, 1+\sqrt{-14}\,\rangle, \\ \mathfrak{q}' &= \big(3, -1+\sqrt{-14}\,\big) = \langle 3, -1+\sqrt{-14}\,\rangle. \end{aligned}$$

Hemos usado [3.16] y [6.9]. Por ejemplo, $\langle 3, 1+\sqrt{-14}\,\rangle$ es un ideal de norma 3, luego ha de ser $\big(3, 1+\sqrt{-14}\,\big)$. Las formas asociadas son

$$x^2 + 14y^2, \quad 2x^2 + 7u^2, \quad 3x^2 + 2xy + 5y^2, \quad 3x^2 - 2xy + 5y^2.$$

Toda forma cuadrática de discriminante -56 es estrictamente equivalente a una de estas cuatro. Observar que las dos últimas son equivalentes a través del cambio de variables (de discriminante -1) $(x, y) \mapsto (-x, y)$, luego representan a los mismos enteros. Las demás no son equivalentes, como es fácil ver. ∎

El resultado básico sobre representación de números por formas cuadráticas es el teorema [6.14], que reenunciamos aquí en una versión ligeramente distinta:

Teorema 11.13 *Si una clase de formas cuadráticas de discriminante $m^2\Delta$ se corresponde con una clase C de $I(m\infty)/H_{m\infty}$ y n es un número primo con m, entonces n está representado por las formas de dicha clase si y sólo si C^{-1} contiene un ideal de norma n.*

La hipótesis $(m, n) = 1$ hace falta al considerar clases en $I(m\infty)/H_{m\infty}$ y no en el grupo de clases de similitud de módulos del orden $\mathcal{O}_m$, tal y como se hace en [6.14]: si $(n, m) = 1$ las clases de los ideales de norma n en el grupo de clases de $\mathcal{O}_m$ se corresponden con las clases de los ideales de norma n en $I(m\infty)/H_{m\infty}$ a través del isomorfismo entre estos grupos.

De aquí se sigue en particular que un número n primo con m está representado por una forma de discriminante $D = m^2\Delta$ si y sólo si k (el cuerpo cuadrático de discriminante Δ) tiene un ideal de norma n. Una versión en términos más prácticos de este mismo hecho es el teorema [9.30].

Para el caso de números primos tenemos una condición muy simple: p (primo con D) es representable por una forma de discriminante D si y sólo si se escinde en k. Esto depende sólo del resto de p módulo Δ.

Ejercicio: Probar que los primos representables por una de las cuatro formas del ejemplo anterior son, además de 2 y 7, los que cumplen

$$p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \text{ (mód } 56).$$

La teoría de los géneros nos proporciona una distinción más fina. Si un entero n (primo con D) es representable por una forma de discriminante D, lo será concretamente por una forma de género G si y sólo si G $(= G^{-1})$ contiene un ideal de norma n. Esta condición depende sólo del resto de n módulo D. La teoría de cuerpos de clases lo muestra de la forma más clara:

Sea K_g el cuerpo de géneros del orden de discriminante D. Sea $\sigma = \left(\frac{K_g/k}{G}\right)$. Entonces n está representado por una forma de género G si y sólo si $\left(\frac{K_g/\mathbb{Q}}{n}\right) = \sigma$.

En efecto, si n está representado por una forma de género G existe un ideal $\mathfrak{a}$ de norma n tal que

$$\left(\frac{K_g/k}{\mathfrak{a}}\right) = \left(\frac{K_g/\mathbb{Q}}{n}\right) = \sigma.$$

Recíprocamente, si $\left(\frac{K_g/\mathbb{Q}}{n}\right) = \sigma$, el ideal $\mathfrak{a}$ de norma n que existe por hipótesis ha de cumplir $\left(\frac{K_g/k}{\mathfrak{a}}\right) = \sigma$, luego es de género G.

La condición $\left(\frac{K_g/\mathbb{Q}}{n}\right) = \sigma$ depende sólo del resto de n módulo cualquier divisor admisible para la extensión $K_g/\mathbb{Q}$. En particular depende del resto de n módulo D.

Ejercicio: Probar que un entero n (primo con D) no puede estar representado por formas de dos géneros distintos.

Ejemplo Continuando nuestro estudio de las formas de determinante -56, el género principal, que es el grupo de los cuadrados del grupo de clases, está formado por $[1]$ y $[\mathfrak{p}]$ (las clases $[\mathfrak{q}]$ y $[\mathfrak{q}']$ son mutuamente inversas, pues su producto es $[3] = [1]$, luego tienen orden 4).

El cuerpo de géneros es $K_g = \mathbb{Q}\big(\sqrt{2}, \sqrt{-7}\big)$. El isomorfismo de Artin de la extensión K_g/k transforma el género principal en la identidad y el otro género en el automorfismo σ determinado por $\sigma\big(\sqrt{2}\big) = -\sqrt{2}$, $\sigma\big(\sqrt{-7}\big) = -\sqrt{-7}$.

Así, si n es un entero representable por una forma de discriminante -56 (es decir, si existe un ideal $\mathfrak{a}$ en $k = \mathbb{Q}\big(\sqrt{-14}\big)$ de norma n) lo será por una de las dos formas $x^2 + 14y^2$ o $2x^2 + 7u^2$, si y sólo si

$$\left(\frac{K_g/\mathbb{Q}}{n}\right) = \left(\frac{K_g/K}{\mathfrak{a}}\right) = 1,$$

mientras que será representable por $3x^2 + 2xy + 5y^2$ si y sólo si $\left(\frac{K_g/\mathbb{Q}}{n}\right) = \sigma$.

La primera condición equivale a que

$$\left(\frac{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}{n}\right) = 1 \quad \text{y} \quad \left(\frac{\mathbb{Q}(\sqrt{-7})/\mathbb{Q}}{n}\right) = 1,$$

y la segunda a que estos símbolos de Artin sean las conjugaciones de los cuerpos $\mathbb{Q}(\sqrt{2}\,)$ y $\mathbb{Q}(\sqrt{-7}\,)$ respectivamente. Ahora bien, recordemos que

$$\left(\frac{\mathbb{Q}(\sqrt{2}\,)/\mathbb{Q}}{n}\right)(\sqrt{2}\,) = \psi_2(n)\sqrt{2}, \qquad \left(\frac{\mathbb{Q}(\sqrt{-7}\,)/\mathbb{Q}}{n}\right)(\sqrt{-7}\,) = \psi_{-7}(n)\sqrt{-7},$$

donde ψ_2 y ψ_{-7} son los caracteres de los cuerpos correspondientes, que son fáciles de calcular. Concretamente, n estará representado por una de las dos formas del género principal si y sólo si

$$n \equiv \pm 1 \text{ (mód 8)} \qquad \text{y} \qquad n \equiv 1, 2, 4 \text{ (mód 7)}, \tag{11.1}$$

y estará representado por la forma $3x^2 + 2xy + 5y^2$ si y sólo si

$$n \equiv \pm 3 \text{ (mód 8)} \qquad \text{y} \qquad n \equiv 3, 5, 6 \text{ (mód 7)}. \tag{11.2}$$

Todo esto suponiendo que n sea de hecho representable por una forma de discriminante -56. Puesto que se ha de dar uno de los dos casos y ambos son excluyentes, en realidad sólo es necesario verificar una de las dos condiciones de cada uno de ellos.

Para los números primos la condición de representabilidad por una forma de discriminante -56 puede unirse a las condiciones anteriores, de modo que es fácil concluir que los primos p representables por una de las dos formas del género principal son los que cumplen

$$p \equiv 1, 9, 15, 23, 25, 39 \text{ (mód 56)} \tag{11.3}$$

además de 2 y 7 (representables por $2x^2 + 7y^2$), mientras que los primos representables por $3x^2 + 2xy + 5y^2$ son los que cumplen

$$p \equiv 3, 5, 13, 19, 27, 45 \text{ (mód 56)}. \tag{11.4}$$

Podríamos haber llegado a esta conclusión de forma mecánica utilizando los caracteres que determinan los géneros y sus propiedades, pero nuestra intención era enfatizar la interpretación algebraica que proporciona la teoría de cuerpos de clases. ∎

Las condiciones (11.1) y (11.2) son ejemplos concretos de lo que hemos probado antes en general: la representabilidad de un entero n por las formas de un género G de discriminante D (supuesto que n es primo con D y que es representable por una forma de discriminante D) depende únicamente de su resto módulo D. También sabemos en general que la representación de un primo $p \nmid D$ por una forma de género G (sin suponer a priori que es representable por una forma de discriminante D) depende de condiciones del tipo de (11.3) y (11.4).

Observemos que hemos resuelto completamente el problema de cuándo un entero n (primo con -56) es representable por la forma $3x^2 + 2xy + 5y^2$. La solución es especialmente simple (11.4) para el caso de los primos. La razón por la que hemos llegado a una respuesta tan simple es que todas las clases del

género de esta forma son equivalentes entre sí. No tenemos un criterio similar para distinguir los primos representables por x^2+14y^2 de los representables por $2x^2+7u^2$. La teoría de cuerpos de clases nos permite probar que no existe tal criterio, que las congruencias no determinan los números que puede representar una familia de formas cuadráticas más allá de lo que permite la teoría de los géneros. Explícitamente:

Teorema 11.14 *Sea $\mathcal{F}$ una familia de formas cuadráticas de discriminante D tales que existe un número natural r con la propiedad de que la representabilidad de un primo $p \nmid r$ por una forma de $\mathcal{F}$ depende sólo de su resto módulo r. Entonces el conjunto de todas las formas equivalentes a las de $\mathcal{F}$ es unión de géneros.*

Demostración: Podemos suponer que $\mathcal{F}$ es unión de clases de equivalencia de formas de discriminante D. En particular es unión de clases de equivalencia estricta. Sea $\mathcal{O}_m$ el orden cuadrático de discriminante D, correspondiente al cuerpo cuadrático k. Llamemos C a la unión de todas las clases de similitud estricta de ideales del grupo de clases de $\mathcal{O}_m$ que se corresponden con las clases de equivalencia estricta de las formas cuadráticas de $\mathcal{F}$. Hemos de probar que C es unión de géneros.

Supongamos que un primo racional $p \nmid D$ es escinde en k, o sea, $p = \mathfrak{p}_1\mathfrak{p}_2$. Si la clase de equivalencia estricta de formas asociada a $[\mathfrak{p}_1]$ es la clase de la forma $ax^2+bxy+cy^2$, entonces la clase asociada a $[\mathfrak{p}_2]$ es la de $ax^2-bxy+cy^2$. Estas formas no tienen por qué ser estrictamente equivalentes, pero obviamente son equivalentes, luego una está en $\mathcal{F}$ si y sólo si lo está la otra. Consecuentemente $[\mathfrak{p}_1] \in C$ si y sólo si $[\mathfrak{p}_2] \in C$.

Sea D el conjunto de las clases del grupo de unidades U_r correspondientes a los primos representables por formas de $\mathcal{F}$. De la hipótesis se sigue que $[\mathfrak{p}_1] \in C$ si y sólo si $[p] \in D$.

En efecto, si $[p] \in D$ entonces una forma de $\mathcal{F}$ representa a p. Por el teorema 11.13, la inversa de su clase de similitud estricta asociada contiene a $\mathfrak{p}_1$ o a $\mathfrak{p}_2$, pero las clases $[\mathfrak{p}_1]$ y $[\mathfrak{p}_2]$ son mutuamente inversas, ya que $[p] = 1$, luego una de las dos clases $[\mathfrak{p}_i]$ está en C y, según hemos visto, la otra también. Recíprocamente, si $[\mathfrak{p}_1] \in C$ entonces las formas asociadas a $[\mathfrak{p}_2]$ representan a p, luego $[p] \in D$.

Notemos ahora que las hipótesis permiten sustituir r por cualquier múltiplo suyo, por lo que podemos exigir que $r\infty$ sea admisible para k. Sea $C_{r\infty}$ el cuerpo ciclotómico de orden r y $K_{m\infty}$ el cuerpo de clases de $\mathcal{O}_m$. Ambos son extensiones abelianas de k. Sea $\mathfrak{m}$ un divisor de k múltiplo de r y admisible para las extensiones $K_{m\infty}/k$ y $C_{r\infty}/k$. Sean H y H' los grupos de clases módulo $\mathfrak{m}$ de estos cuerpos. Así podemos considerar que $C \subset I(\mathfrak{m})/H$. Sean

$$T^* = \left(\frac{C_{r\infty}/\mathbb{Q}}{D}\right), \qquad T = T^* \cap G(C_{r\infty}/k).$$

Si $\mathfrak{p}_1 \in I(\mathfrak{m})$ es un primo de norma prima, se cumple

$$[\mathfrak{p}_1] \in C \iff [\mathrm{N}(\mathfrak{p}_1)] \in D \iff \left(\frac{C_{r\infty}/\mathbb{Q}}{\mathrm{N}(\mathfrak{p}_1)}\right) \in T^* \iff \left(\frac{C_{r\infty}/k}{\mathfrak{p}_1}\right) \in T.$$

La clave está en que la primera condición depende sólo de la clase de $\mathfrak{p}_1$ módulo H, mientras que la última depende de la clase de $\mathfrak{p}_1$ módulo H'. De aquí vamos a deducir que C es unión de clases módulo H'. En efecto, consideremos dos clases $\mathfrak{p}_1\,P_\mathfrak{m}$ y $\mathfrak{p}_2\,P_\mathfrak{m}$ (por el teorema de Dirichlet —ver la nota posterior— toda clase módulo $P_\mathfrak{m}$ tiene un representante primo de norma prima). Si ambas clases están contenidas en una misma clase módulo H' y la primera está contenida en C, entonces las equivalencias anteriores prueban que la segunda también lo está.

Así pues, C es unión de clases módulo H y módulo H'. Claramente entonces C es unión de clases módulo HH', pero $HH' \leftrightarrow L = K_{m\infty} \cap C_{r\infty}$, y L es una extensión abeliana de $\mathbb{Q}$ contenida en $K_{m\infty}$. Por lo tanto L está contenido en el cuerpo de géneros y HH' contiene al género principal G_1 de $\mathcal{O}_m$. De este modo C es unión de clases módulo G_1, es decir, es unión de géneros. ∎

Ejemplo Pese a este resultado, vamos a ver que la teoría de cuerpos de clases nos permite separar los primos representados por la forma principal $x^2 + 14y^2$ de los representados por $2x^2 + 7y^2$. Para ello hemos de considerar el cuerpo del orden de discriminante -56 en lugar del cuerpo de géneros. Puesto que el orden es maximal, se trata del cuerpo de clases de Hilbert de $\mathbb{Q}\big(\sqrt{-14}\,\big)$. Lo hemos calculado en la sección anterior. Es el cuerpo de escisión del polinomio $x^4 + 2x^2 - 7$, es decir, $K = \mathbb{Q}(\xi, \xi')$, con $\xi = \sqrt{-1 + 2\sqrt{2}}$, $\xi' = \sqrt{-1 - 2\sqrt{2}}$.

Teniendo en cuenta que la clase principal del grupo de clases $I(56)/P_{56}$ es su propia inversa, el teorema 11.13 nos da que un primo $p \nmid 56$ está representado por la forma principal $x^2 + 14y^2$ si y sólo si la clase P_{56} contiene un ideal $\mathfrak{p}$ de norma p. Esto equivale a que p tenga un divisor $\mathfrak{p}$ en k (de norma p) que se escinda completamente en K o, lo que es lo mismo, a que p se escinda completamente en K.

Claramente un primo p se escinde completamente en K si y sólo si se escinde completamente en $\mathbb{Q}(\xi)$ y en $\mathbb{Q}(\xi')$, pero como ambos cuerpos son isomorfos, p se escinde completamente en uno si y sólo si se escinde completamente en el otro. En resumen, un primo p es de la forma $p = x^2 + 14y^2$ si y sólo si se escinde completamente en $\mathbb{Q}(\xi)$. Vamos a desarrollar esta condición.

Tenemos calculado que el discriminante de $\mathbb{Q}(\xi)/\mathbb{Q}\big(\sqrt{2}\,\big)$ es $-1 + 2\sqrt{2}$, luego el teorema 3.24 nos da que el discriminante de $\mathbb{Q}(\xi)$ es $\Delta = -2^6 \cdot 7$ (el signo no es relevante, pero se sigue de 3.19).

Por otra parte,

$$\Delta[\xi] = \mathrm{N}(4\xi^3 + 4\xi) = 2^8\,\mathrm{N}(\xi)\,\mathrm{N}(\xi^2 + 1) = -2^8 \cdot 7\,\mathrm{N}\big(2\sqrt{2}\,\big) = -2^{14} \cdot 7.$$

Así pues, $\mathrm{índ}\,\xi = 16$. El teorema [3.16] nos da que un primo $p \neq 2$ se escinde completamente en $\mathbb{Q}(\xi)$ si y sólo si el polinomio $x^4 + 2x^2 - 7$ se escinde (completamente) módulo p.

Ahora usamos que una condición necesaria para que p esté representado por la forma principal es (11.3). En particular se ha de cumplir $p \equiv \pm 1$ (mód 8) y así 2 es un resto cuadrático módulo p. Tomemos $u^2 \equiv 2$ (mód p). Entonces

$$x^2 + 2x - 7 \equiv \big(x - (-1 + 2u)\big)\big(x - (-1 - 2u)\big) \text{ (mód } p),$$

luego

$$x^4 + 2x^2 - 7 \equiv \big(x^2 - (-1+2u)\big)\big(x^2 - (-1-2u)\big) \text{ (mód } p). \tag{11.5}$$

Por otra parte, $(-1+2u)(-1-2u) \equiv -1$ (mód p) y, por la ley de reciprocidad cuadrática,

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = 1,$$

ya que (11.3) implica que $p \equiv 1, 2, 4$ (mód 7).

Esto implica que $-1+2u$ es un resto cuadrático módulo p si y sólo si lo es $-1-2u$, luego (11.5) muestra que el polinomio x^4+2x-7 se escinde o no tiene raíces módulo p. En resumen tenemos el resultado siguiente:

Un primo p es de la forma $p = x^2 + 14y^2$ si y sólo si cumple

$$p \equiv 1, 9, 15, 23, 25, 39 \text{ (mód } 56)$$

y $m^4 + 2m^2 - 7 \equiv 0$ (mód p) para cierto entero m.

En la práctica la última condición se comprueba más fácilmente en la forma

$$(m^2+1)^2 \equiv 8 \text{ (mód } p),$$

pues así basta encontrar un u tal que $u^2 \equiv 8$ (mód p) (que siempre existe si p cumple 11.3) y decidir si $\pm u - 1$ es o no un resto cuadrático módulo p. ∎

Ejemplo Esbozamos ahora el caso que se obtiene a partir del ejemplo visto al final de la sección 11.1. Consideramos las formas de discriminante -23. Hay tres clases de equivalencia, en correspondencia con las clases de similitud estricta de ideales de $\mathbb{Q}\big(\sqrt{-23}\,\big)$. La clase principal se corresponde con la forma principal $x^2+xy+6y^2$, los ideales divisores de 2 son $\big\langle 2, \big(1+\sqrt{-23}\big)/2\big\rangle$ y $\big\langle 2, \big(-1+\sqrt{-23}\big)/2\big\rangle$, que se corresponden con $2x^2+xy+3y^2$ y $2x^2-xy+3y^2$. Por el teorema [6.18] estas tres formas determinan las tres clases de equivalencia estricta. No obstante las dos últimas son equivalentes entre sí.

Así pues, toda forma cuadrática de discriminante -23 es equivalente a una de las formas

$$x^2+xy+6y^2, \qquad 2x^2+xy+3y^2.$$

Los primos representables por una de estas formas son el 23 y los que cumplen

$$p \equiv 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \text{ (mód } 23).$$

Los de la forma $p = x^2+xy+6y^2$ son el 23 y los que cumplen además que $m^3 - m - 1 \equiv 0$ (mód p) para cierto entero m. ∎

Ejemplo Consideremos las formas de discriminante $D = -108 = 6^2(-3)$. Están asociadas al orden $\mathcal{O}_6$ de $k = \mathbb{Q}\big(\sqrt{-3}\,\big)$. Según el teorema 11.7, el número de clases es $\Phi(6)/6 = 3$.

El ideal 1 se corresponde con la forma principal $x^2 + 27y^2$. Para calcular las otras dos formas representantes de las clases de equivalencia necesitamos partir de ideales de $\mathbb{Q}\big(\sqrt{-3}\,\big)$ de norma prima con 6. El menor posible es 5 pero, como se conserva primo, se corresponde con el ideal (5) de $\mathcal{O}_6$, que es principal, luego su forma asociada es equivalente a la forma principal que ya tenemos. Los candidatos siguientes son los divisores de 7 que, como fácilmente se comprueba, son $7 = (7, 2+\omega)(7, -3+\omega)$, donde $\omega = \big(1+\sqrt{-3}\,\big)/2$.

Usando como es habitual el teorema [6.9] vemos que

$$(7, 2+\omega) = \langle 7, 2+\omega\rangle \mapsto \langle 7, 12+6\omega\rangle = \langle 7, -2+6\omega\rangle\,,$$

(el último cambio de base sólo nos hará pasar de una forma cuadrática a otra similar más sencilla). La forma asociada es $7x^2 + 2xy + 4y^2$.

Así mismo, la forma asociada al ideal conjugado es $7x^2 - 2xy + 4y^2$. Intercambiando las variables en estos dos últimos casos obtenemos las formas

$$x^2 + 27y^2, \qquad 4x^2 + 2xy + 7y^2, \qquad 4x^2 - 2xy + 7y^2,$$

que por el teorema [6.18] representan tres clases distintas de equivalencia estricta, luego toda forma cuadrática de discriminante -108 es estrictamente equivalente a una de estas tres. Como las dos últimas son equivalentes, todo primo representable por una forma de discriminante -108 es de la forma $p = x^2+27y^2$ o bien $p = 4x^2 + 2xy + 7y^2$.

Los primos que cumplen esto son los dados por $p \equiv 1$ (mód 3). Para separar los representados por cada forma hemos de considerar el cuerpo de clases de $\mathcal{O}_6$. En el ejemplo visto al final de de la sección 11.3 hemos probado que este cuerpo no es sino $K = \mathbb{Q}\big(\sqrt{-3}, \sqrt[3]{2}\,\big)$.

Consecuentemente, un primo $p \equiv 1$ (mód 3) es de la forma $p = x^2 + 27y^2$ si y sólo si sus divisores primos $\mathfrak{p}$ en k están en la clase principal de $I(6)/H_6$, si y sólo si $\mathfrak{p}$ se escinde completamente en K, si y sólo si p se escinde completamente en K, si y sólo si p se escinde completamente en $\mathbb{Q}\big(\sqrt[3]{2}\big)$. Según la tabla [3.2] esto ocurre si y sólo si $m^3 \equiv 2$ (mód p) para cierto entero m. En resumen:

> *Un primo p es de la forma $p = x^2 + 27y^2$ si y sólo si $p \equiv 1$* (mód 3) *y 2 es un resto cúbico módulo p.*

■

Ejercicio: Demostrar que un primo es de la forma $p = x^2 + xy + 61y^2$ si y sólo si $p \equiv 1$ (mód 3) y 3 es un resto cúbico módulo p.

Ejercicio: Probar que toda forma de discriminante 136 es equivalente a una de las formas

$$x^2 - 34y^2, \qquad 34x^2 - y^2, \qquad 3x^2 + 2xy - 11y^2.$$

Determinar los primos que representa cada una de ellas.

Capítulo XII

Extensiones infinitas

Vamos a terminar de perfilar los resultados básicos de la teoría de cuerpos de clases con el estudio de las extensiones infinitas de $\mathbb{Q}$ y de los cuerpos $\mathbb{Q}_p$. La idea básica es que las propiedades de consistencia del símbolo de Artin permiten definir un único isomorfismo entre un cociente del grupo de elementos ideales y el grupo de Galois de la mayor extensión abeliana de un cuerpo numérico (o p-ádico) dado, de modo que los isomorfismos de Artin para las extensiones finitas se obtienen de éste por restricción. Esto produce una simplificación técnica de la teoría y permite una visión más clara de la misma. Antes de entrar en ello debemos generalizar la teoría de Galois al caso de extensiones infinitas.

12.1 Extensiones infinitas de Galois

Los conceptos de separabilidad y normalidad de una extensión de cuerpos están definidos incluso para extensiones de grado infinito. En efecto: una extensión K/k es separable si es algebraica y todo elemento de K es raíz simple de su polinomio mínimo sobre k. Obviamente una extensión K/k es separable si y sólo si lo son todas las extensiones finitas intermedias L/k.

Ejercicio: Probar que si $k \subset K \subset L$ es una cadena de cuerpos, entonces L/k es separable si y sólo si lo son K/k y L/K.

Llamaremos *clausura separable* de un cuerpo k (fijada una clausura algebraica K) al cuerpo K_s formado por todos los elementos de K separables sobre k. Es inmediato probar que dos clausuras separables cualesquiera de k son k-isomorfas.

Una extensión K/k es normal si es algebraica y todo polinomio irreducible de $k[x]$ con una raíz en K se escinde en $K[x]$. Esto equivale a que K se obtenga de k por adjunción de todas las raíces de un conjunto (no necesariamente finito) de polinomios de $k[x]$. En efecto: si K/k es normal entonces K es la adjunción a k de las raíces de todos los polinomios de $k[x]$ que se escinden en $K[x]$ y, recíprocamente, si $K = k(A)$, donde A es una unión de conjuntos completos de raíces de polinomios de $k[x]$, dado cualquier polinomio irreducible de $k[x]$ con

una raíz α en K, se cumplirá que $\alpha = p(\alpha_1, \ldots, \alpha_n)$, donde p es un polinomio de $k[x_1, \ldots, x_n]$ y $\alpha_1, \ldots, \alpha_n \in A$. Multiplicando todos los polinomios mínimos en $k[x]$ de estos elementos obtenemos un único polinomio tal que si B es el conjunto de todas sus raíces, entonces $B \subset A$, luego $\alpha \in k(B) \subset K$ y la extensión $k(B)/k$ es finita y normal, luego el polinomio de partida se escinde en $k(B)[x]$, luego también en $K[x]$.

A partir de aquí se prueba sin dificultad que las extensiones normales tienen en general las mismas propiedades que las extensiones normales finitas. Por ejemplo, si tenemos una cadena $k \subset L \subset K$ de manera que L/k es normal, todo k-monomorfismo σ de K en una clausura algebraica cumple $\sigma[L] = L$ (ya que si $\alpha \in L$ entonces $\sigma(\alpha)$ es otra raíz del polinomio mínimo de α, luego está en L). De aquí que si $k \subset L \subset K$ con K/k normal entonces todo k-isomorfismo $\sigma : L \longrightarrow \sigma[L]$ se extiende a un k-automorfismo de K (pues se extiende a una clausura algebraica de K y al restringir a K resulta un automorfismo). En particular, si K/k es normal, dos elementos de K son conjugados respecto a k (son raíces del mismo polinomio mínimo) si y sólo si hay un k-automorfismo de K que transforma uno en otro.

Una extensión K/k es de Galois si es normal y separable. Por ejemplo, si k es un cuerpo cualquiera y K es su clausura separable (su clausura algebraica si k es perfecto), entonces la extensión K/k es de Galois (pues todo polinomio de $k[x]$ se escinde en $K[x]$).

Dada una extensión K/k, su grupo de Galois $G(K/k)$ es el formado por todos los k-automorfismos de K. A cada subgrupo $H \leq G(K/k)$ le podemos asociar su cuerpo fijado

$$L = F(H) = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ para todo } \sigma \in H\},$$

de modo que $k \subset L \subset K$, y a cada cuerpo intermedio $k \subset L \subset K$ le podemos asociar el grupo $H = G(K/L) \leq G(K/k)$.

Exactamente igual que en el caso finito se prueba que una extensión K/k es de Galois si y sólo si k es el cuerpo fijado por $G(K/k)$. En particular, si F es dicho cuerpo, la extensión K/F siempre es de Galois.[1]

En extensiones infinitas de Galois no es cierto que la correspondencia $H \leftrightarrow L$ sea biyectiva. Esto fue descubierto por Dedekind, pero Krull definió una topología en el grupo de Galois y probó que los cuerpos intermedios se corresponden biunívocamente con los subgrupos cerrados. Esto es lo que vamos a probar a continuación.

Definición 12.1 Sea K un cuerpo. Consideremos el conjunto K^K de todas las aplicaciones de K en K. Podemos verlo como el producto cartesiano de K por sí mismo tantas veces como elementos tiene K. Consideraremos a K como

[1] Recordemos la prueba: si $\alpha \in K$ y $\alpha_1, \ldots, \alpha_n$ son todas las raíces (distintas) en K del polinomio mínimo de α en $k[x]$, entonces el polinomio $(x-\alpha_1)\cdots(x-\alpha_n)$ es fijado por $G(K/k)$, luego es el polinomio mínimo de α en $F[x]$, luego se escinde en $K[x]$ y α es separable. Así pues K/F es de Galois. Si K/k es de Galois y $\alpha \in F$ entonces $\alpha \in k$, pues en caso contrario el polinomio mínimo de α en k tiene otra raíz distinta de α (por la separabilidad), luego hay un elemento de $G(K/k)$ que no deja fijo a α.

espacio topológico discreto y a K^K como espacio topológico con la topología producto.

Una base de K es la formada por los conjuntos $\{\alpha\}$ con $\alpha \in K$, y ésta induce a su vez la base de K^K formada por los conjuntos

$$X(\{\alpha_\beta\}_{\beta\in B}) = \{f \in K^K \mid f(\beta) = \alpha_\beta \text{ para } \beta \in B\},$$

donde $B \subset K$ es finito y $\alpha_\beta \in K$ para cada $\beta \in B$.

Es decir, $X(\{\alpha_\beta\}_{\beta\in B})$ es el conjunto de los elementos f del producto cuya componente β pertenece al abierto básico $\{\alpha_\beta\}$ de K. Estos conjuntos se pueden representar de una forma equivalente más sencilla:

$$X(g, B) = \{f \in K^K \mid f(\beta) = g(\beta) \text{ para } \beta \in B\},$$

donde $B \subset K$ es finito y $g \in K^K$.

Observar que los abiertos $X(g, B)$ son también cerrados, pues son el producto de los cerrados $\{\alpha_\beta\}$ en las componentes de B por el cerrado K en las componentes restantes. Así pues, K^K es lo que se llama un espacio *cero-dimensional* tiene una base formada por conjuntos abiertos y cerrados (el nombre se debe a que entonces los únicos subespacios conexos son los puntos).

El conjunto $\mathrm{Aut}(K)$ de todos los automorfismos de K está contenido en K^K. Definimos la *topología finita* en $\mathrm{Aut}(K)$ como la topología inducida desde K^K, es decir, la que tiene por base a los conjuntos de la forma

$$W_\sigma(B) = \{\tau \in \mathrm{Aut}(K) \mid \tau(\beta) = \sigma(\beta) \text{ para } \beta \in B\},$$

donde $B \subset K$ es finito y $\sigma \in \mathrm{Aut}(K)$.

Observar que si $\sigma \in \mathrm{Aut}(K)$, los conjuntos $W_\sigma(B)$ constituyen una base de entornos de σ. En efecto, si $\sigma \in W_\tau(B)$, entonces $\sigma \in W_\sigma(B) \subset W_\tau(B)$.

Teorema 12.2 *Si K es un cuerpo, su grupo de automorfismos es un grupo topológico (de Hausdorff) cero-dimensional con la topología finita.*

Demostración: Basta ver que la aplicación $\mathrm{Aut}(K)\times\mathrm{Aut}(K) \longrightarrow \mathrm{Aut}(K)$ dada por $(\sigma, \tau) \mapsto \sigma^{-1}\tau$ es continua. Para ello basta probar que, para todo par (σ, τ), la imagen de $W_1(\sigma^{-1}[B]) \times W_\tau(\sigma^{-1}[B])$ está contenida en $W_{\sigma^{-1}\tau}(B)$.

Si $(\phi, \psi) \in W_1(\sigma^{-1}[B]) \times W_\tau(\sigma^{-1}[B])$ y $\beta \in B$, entonces $\sigma^{-1}(\beta) \in \sigma^{-1}[B]$, luego $\phi(\sigma^{-1}(\beta)) = \beta$ y por consiguiente $\phi^{-1}(\beta) = \sigma^{-1}(\beta)$. Además

$$\psi(\phi^{-1}(\beta)) = \psi(\sigma^{-1}(\beta)) = \tau(\sigma^{-1}(\beta)).$$

Así pues, $(\phi^{-1}\psi)(\beta) = (\sigma^{-1}\tau)(\beta)$, luego $\phi^{-1}\psi \in W_{\sigma^{-1}\tau}(B)$. ∎

Definición 12.3 Sea K/k una extensión de cuerpos. Llamaremos *topología de Krull* a la topología del grupo de Galois $G(K/k)$ inducida por la topología finita de $\mathrm{Aut}(K)$.

Claramente $G(K/k)$ es un grupo topológico cero-dimensional con dicha topología. Más aún, las aplicaciones $G(K/k) \longrightarrow K$ dadas por $\sigma \mapsto \sigma(\beta)$ para cada $\beta \in K$ son continuas cuando en K consideramos la topología discreta (pues son las restricciones de las proyecciones en K^K).

Teorema 12.4 *Si K/k es una extensión algebraica, entonces $G(K/k)$ es un grupo topológico compacto cero-dimensional.*

DEMOSTRACIÓN: Para cada $\beta \in K$, sea C_β el conjunto de las raíces en K del polinomio mínimo de β en $k[x]$. Entonces $C = \prod_{\beta\in K} C_\beta$ es compacto (pues cada C_β es finito).

Si $\sigma \in G(K/k)$ es obvio que $\sigma(\beta) \in C_\beta$ para todo $\beta \in K$, luego $G(K/k) \subset C$. Basta probar que $G(K/k)$ es cerrado en K^K.

Tomemos $\phi \in \overline{G(K/k)}$. Para cada α, $\beta \in K$ y $\gamma \in k$ tomamos $B = \{\alpha, \beta, \alpha+\beta, \alpha\beta, \gamma\}$. Existe un $\sigma \in G(K/k) \cap X(\phi, B)$. Claramente

$$\phi(\alpha+\beta) = \sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta) = \phi(\alpha) + \phi(\beta),$$

$$\phi(\alpha\beta) = \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \phi(\alpha)\phi(\beta),$$

$$\phi(\gamma) = \sigma(\gamma) = \gamma,$$

con lo que $\phi \in G(K/k)$. ∎

El teorema siguiente nos conecta las extensiones finitas con las infinitas y nos permitirá aplicar los resultados de la teoría de extensiones finitas de Galois para probar los análogos en extensiones infinitas.

Teorema 12.5 *Sea K/k una extensión algebraica. Entonces una base de entornos abiertos de 1 en $G(K/k)$ está formada por los grupos $G(K/L)$, donde L varía en los cuerpos intermedios $k \subset L \subset K$ tales que la extensión L/k es finita. Si la extensión K/k es normal podemos considerar únicamente extensiones finitas normales L/k.*

DEMOSTRACIÓN: Es una consecuencia inmediata de que si $B \subset K$ es un conjunto finito, entonces $W_1(B) \cap G(K/k) = G\big(K/k(B)\big)$, junto con el hecho de que los cuerpos $k(B)$ recorren todos los cuerpos intermedios finitos sobre k.

Si K/k es normal, toda extensión intermedia finita L/k está contenida en una extensión intermedia finita normal L'/k, y claramente $G(K/L') \leq G(K/L)$, luego las extensiones finitas normales son por sí solas una base de entornos del neutro. ∎

Observar que si $k \subset L \subset K$ y K/k es una extensión algebraica, la topología de $G(K/L)$ es claramente la topología inducida desde $G(K/k)$. En particular $G(K/L)$ es cerrado en $G(K/k)$. Hemos de probar que, recíprocamente, si H es un subgrupo cerrado de $G(K/k)$ entonces H es el grupo de automorfismos de una extensión intermedia K/L.

Teorema 12.6 *Sea K/k una extensión algebraica y H un subgrupo de $G(K/k)$. Sea F el cuerpo fijado por H. Entonces $G(K/F) = \overline{H}$.*

DEMOSTRACIÓN: Obviamente $H \leq G(K/F)$, y como éste es cerrado, de hecho $\overline{H} \leq G(K/F)$. Para probar la otra inclusión veamos algunos hechos previos. Ante todo, sabemos que K/F es una extensión de Galois. Tomemos un cuerpo intermedio $F \subset L \subset K$ tal que L/F sea finita de Galois. Consideremos el homomorfismo $f : H \longrightarrow G(L/F)$ dado por $f(\sigma) = \sigma|_L$. Veamos que es suprayectivo.

Si $f[H] \neq G(L/F)$, entonces $F \neq F(f[H])$ (por el teorema de Galois para extensiones finitas). Sea $\alpha \in F(f[H])$ de manera que $\alpha \notin F$. Por definición de F existe un $\sigma \in H$ tal que $\sigma(\alpha) \neq \alpha$, pero por la elección de α ha de ser $\sigma|_L(\alpha) = \alpha$, contradicción.

Veamos ya la inclusión buscada. Tomamos $\sigma \in G(K/F)$ y hemos de probar que está en $\overline{H}$. Un entorno básico de σ es $\sigma G(K/L)$, donde L es un cuerpo en las condiciones anteriores. Basta ver que este entorno corta a H, pero según lo visto existe un $\tau \in H$ tal que $\tau|_L = \sigma|_L$, con lo que $\sigma G(K/L) = \tau G(K/L)$ y así $\tau \in H \cap \sigma G(K/L) \neq \varnothing$. ∎

Con esto tenemos el teorema fundamental:

Teorema 12.7 (Teorema de Krull) *Sea K/k una extensión de Galois.*

a) Las correspondencias $L \mapsto G(K/L)$ y $H \mapsto F(H)$ son mutuamente inversas y biyectan los cuerpos intermedios de K/k con los subgrupos cerrados de $G(K/k)$.

b) Si $H = G(K/L)$, entonces L/k es normal si y sólo si H es un subgrupo normal de $G(K/k)$, y en tal caso la aplicación $G(K/k) \longrightarrow G(L/k)$ dada por $\sigma \mapsto \sigma|_L$ es un epimorfismo continuo cuyo núcleo es $G(K/L)$, e induce un isomorfismo topológico $G(K/k)/G(K/L) \cong G(L/k)$.

c) La correspondencia $H \leftrightarrow L$ invierte las inclusiones, luego transforma supremos en ínfimos e ínfimos en supremos (los ínfimos son intersecciones, el supremo de una familia de cuerpos es su producto y el supremo de una familia de grupos es la clausura del grupo generado por la unión).

DEMOSTRACIÓN: a) Si $G(K/L) = G(K/L')$, como ambas extensiones son de Galois,

$$L = F(G(K/L)) = F(G(K/L')) = L'.$$

Esto prueba que la aplicación $L \mapsto G(K/L)$ es inyectiva. Por el teorema anterior es suprayectiva, luego es biyectiva y su inversa es $H \mapsto F(H)$, también por el teorema anterior.

b) La prueba es idéntica a la del caso finito. Respecto a la continuidad, basta probar que la restricción es continua como aplicación $G(K/k) \mapsto L^L$, para lo cual a su vez basta ver que la composición con cada proyección $f \mapsto f(\alpha)$ es continua para todo $\alpha \in L$, pero esto da la proyección $\sigma \mapsto \sigma(\alpha)$, que es ciertamente continua. La aplicación cociente es un homeomorfismo porque los grupos son compactos.

c) es evidente. ∎

Por último observamos que en la correspondencia de Galois las extensiones finitas de k se corresponden con los subgrupos abiertos (luego cerrados) de $G(K/k)$. Si extendemos la correspondencia a todos los subgrupos de $G(K/k)$, vemos que se cumple $F(H) = k$ si y sólo si $\overline{H} = G(K/k)$, es decir, si y sólo si H es denso.

Dejamos a cargo del lector los teoremas restantes que se cumplen en el caso finito y cuya prueba en el caso general no presenta diferencia alguna.

Ejercicio: Probar que el cardinal de un grupo de Galois es finito o bien es $2^{\aleph_0}$, por lo que en el caso infinito siempre hay subgrupos (numerables) que no son cerrados.

12.2 El isomorfismo de Artin para extensiones infinitas

Observar que, en general, todo cuerpo k tiene una máxima extensión abeliana A, es decir, una extensión abeliana que contiene a cualquier otra extensión abeliana de k en una clausura algebraica prefijada K. Concretamente, A es el cuerpo fijado por la clausura del subgrupo derivado de $G(K/k)$, y es la unión de todas las extensiones abelianas finitas de k.

Definición 12.8 Consideremos un cuerpo numérico o p-ádico k. Sea J el grupo de elementos ideales de k (entendiendo que $J = k^*$ en el caso p-ádico). Sea A la máxima extensión abeliana de k. Sea $\alpha \in J$. Para cada $\beta \in A$ existe una extensión abeliana finita L de k tal que $\beta \in L$. Por las propiedades del símbolo de Artin es claro que el valor

$$\left(\frac{k}{\alpha}\right)(\beta) = \left(\frac{L/k}{\alpha}\right)(\beta) \in A$$

no depende de la elección de L.

La aplicación (k/α) definida de este modo es un k-automorfismo de A al que llamaremos *símbolo de Artin* de α. Más aún, la aplicación $\omega : J \longrightarrow G(A/k)$ dada por $\omega(\alpha) = (k/\alpha)$ es un homomorfismo de grupos al que llamaremos *homomorfismo de Artin* de k.

En el caso global es obvio que k^* está en el núcleo del homomorfismo de Artin, por lo que podemos considerar a éste definido sobre el grupo de clases $\omega : C \longrightarrow G(A/k)$.

Teorema 12.9 *Sea k un cuerpo numérico. Entonces el homomorfismo de Artin $\omega : C \longrightarrow G(A/k)$ es continuo y suprayectivo. Más aún, si consideramos la factorización $C = \mathbb{R}^+ \times C^0$ se cumple que $\mathbb{R}^+$ está contenido en el núcleo de ω y, por lo tanto, la restricción $\omega : C^0 \longrightarrow G(A/k)$ también es suprayectiva.*

Demostración: Veamos primero la continuidad. Un entorno de 1 en $G(A/k)$ es un grupo $G(A/K)$, donde K/k es una extensión (abeliana) finita.

Su antiimagen por ω es el núcleo del homomorfismo de Artin $C \longrightarrow G(K/k)$, que es el grupo de normas $\mathrm{N}[C_K]$, que es abierto.

Si $\alpha \in \mathbb{R}^+$ y $\beta \in A$, existe una extensión finita L/k tal que $\beta \in L$. Sea $n = |L : k|$. Entonces

$$\left(\frac{k}{\alpha}\right)(\beta) = \left(\frac{L/k}{\alpha}\right)(\beta) = \left(\frac{L/k}{\sqrt[n]{\alpha}}\right)^n (\beta) = 1,$$

luego $\mathbb{R}^+$ está en el núcleo de ω.

Si $\beta \in A$, $\beta \notin k$, sea L/k una extensión finita tal que $\beta \in L$. Por la suprayectividad del homomorfismo de Artin para extensiones finitas existe un $\alpha \in C$ tal que

$$\left(\frac{L/k}{\alpha}\right)(\beta) \neq \beta.$$

Por lo tanto $(k/\alpha)(\beta) \neq \beta$, con lo que hemos probado que el cuerpo fijado por (k/C) es k. Esto significa que (k/C) es denso en $G(A/k)$, pero $(k/C) = (k/C^0)$ y C^0 es compacto, luego (k/C) es cerrado. Así pues, $(k/C) = G(A/k)$. ∎

Evidentemente, un elemento ideal $\alpha \in C$ está el núcleo del homomorfismo de Artin si y sólo si α está en el núcleo de cada homomorfismo de Artin de cada extensión finita L/k, es decir, si y sólo si α está en todos los grupos de normas $\mathrm{N}[C_L]$.

Definición 12.10 Sea k un cuerpo numérico. Llamaremos grupo de *normas universales* de k a la intersección D_k de todos los grupos de normas $\mathrm{N}[C_L]$ para todas las extensiones abelianas finitas L/k.

De este modo, el homomorfismo de Artin induce un isomorfismo topológico $C/D \cong G(A/k)$, y el teorema de Galois nos da una biyección entre los subgrupos cerrados de C que contienen a D y las extensiones abelianas de k.

Si K/k es una extensión abeliana finita, entonces su grupo asociado es precisamente el grupo de normas $\mathrm{N}[C_K]$, o sea, el grupo de clases de K. Por lo tanto la biyección que acabamos de establecer extiende a la que ya teníamos entre extensiones finitas y grupos abiertos. Si un grupo H se corresponde con una extensión K por esta correspondencia, diremos igualmente que K es el cuerpo de clases de H, o que H es el grupo de clases de K.

Sigue siendo cierto que la correspondencia $H \leftrightarrow K$ invierte inclusiones, etc.

Conviene observar que en realidad las normas universales de k son normas para todas las extensiones finitas de k, no necesariamente abelianas. Ello es consecuencia inmediata del hecho siguiente:

Teorema 12.11 *Sea K/k una extensión finita de cuerpos numéricos. Entonces el grupo de normas $\mathrm{N}_k^K[C_K]$ es el grupo de clases de la mayor extensión abeliana de k contenida en K.*

Demostración: Por 6.19 sabemos que $H = \mathrm{N}_k^K[C_K]$ es un subgrupo abierto de C_k. Sea L el cuerpo de clases de H. Para cada $b \in C_K$ tenemos

que $\mathrm{N}_k^K(\beta) \in H$, luego

$$1 = \left(\frac{L/k}{\mathrm{N}_k^K(b)}\right) = \left(\frac{LK/K}{b}\right)\Big|_L,$$

con lo que el grupo de clases de LK/K es todo C_K, es decir, $LK = K$ y, por lo tanto, $L \subset K$.

Si A/k es una extensión abeliana tal que $L \subset A \subset K$ entonces

$$H = \mathrm{N}[C_K] \leq \mathrm{N}[C_A] \leq \mathrm{N}[C_L] = H,$$

luego $\mathrm{N}[C_A] = \mathrm{N}[C_L]$ y por la unicidad de los cuerpos de clases $A = L$. ∎

Así pues, si K/k es una extensión finita de cuerpos numéricos y A es la mayor extensión abeliana de k contenida en K, se cumple que $\mathrm{N}_k^K[C_K] = \mathrm{N}_k^A[C_A]$, por lo que el grupo de normas universales de k está formado por los elementos de C_k que son normas para todas las extensiones finitas de k, tal y como afirmábamos. Incidentalmente tenemos así una prueba algebraica que de la segunda desigualdad fundamental es cierta para extensiones finitas cualesquiera de cuerpos numéricos, no necesariamente abelianas:

$$|C_k : \mathrm{N}_k^K[C_K]| \;\big|\; |K : k|.$$

En el capítulo 9 dimos una prueba analítica de este hecho.

El lector puede probar el resultado análogo al teorema anterior para cuerpos p-ádicos. La única dificultad adicional es que hay que probar que el índice del grupo de normas es finito. Para ello se puede cambiar K por su clausura normal sobre k, entonces la extensión K/k es resoluble, con lo que podemos tomar una cadena de extensiones abelianas intermedias en las que el índice del grupo de normas es igual al grado. De la finitud de estos índices se deduce la del índice total (en el capítulo 10 hemos probado esto mismo por un argumento más complicado, ver los párrafos previos al teorema 10.25).

A continuación vamos a dar dos caracterizaciones internas del grupo D, es decir, que dependan sólo de la estructura del grupo C y no de las extensiones de k. La primera será topológica y la segunda algebraica.

Teorema 12.12 *Sea k un cuerpo numérico. Entonces el grupo de normas universales de k es la componente conexa de 1 en el grupo de clases de elementos ideales.*

Demostración: Llamemos $X \leq C$ a la componente conexa de 1. Es claro que X está contenida en todos los subgrupos abiertos, luego $X \leq D$ (observar que todo subgrupo abierto de C es el grupo de normas de su cuerpo de clases).

Para probar la otra inclusión tomamos una clase $[\alpha] \in D$. Es fácil ver que la componente conexa de 1 en J es el producto Y de los intervalos $]0, +\infty[$ en los cuerpos $k_\mathfrak{p}$ con $\mathfrak{p}$ arquimediano real por los grupos $k_\mathfrak{p}^*$ con $\mathfrak{p}$ arquimediano complejo. Para probar este teorema nos basta con el hecho obvio de que Y es un subgrupo conexo de J.

Un entorno básico de 1 en J es de la forma

$$V = \prod_{\mathfrak{p}} W_{\mathfrak{m}}(\mathfrak{p}) \times \prod_{\mathfrak{q}} B_{\mathfrak{q}},$$

donde $\mathfrak{m}$ es un divisor de k, el índice $\mathfrak{p}$ varía entre los primos no arquimedianos, $\mathfrak{q}$ varía entre los primos arquimedianos y $B_{\mathfrak{q}}$ es una bola abierta de centro 1 y radio menor que 1 en $k_{\mathfrak{q}}$.

El grupo $W_{\mathfrak{m}}k^*/k^*$ es abierto, luego contiene a D y por lo tanto a $[\alpha]$. Así pues, existe un $\beta \in k^*$ tal que $\alpha\beta \in W_{\mathfrak{m}}$. Sea $\gamma \in J$ tal que sus componentes no arquimedianas sean iguales a 1 y sus componentes arquimedianas sean números reales positivos suficientemente pequeños como para que $(\alpha\beta)^{-1}\gamma \in V$. Claramente $\gamma \in Y$, con lo que $\alpha\beta V \cap Y \neq \varnothing$.

Por lo tanto $[\alpha]p[V] \cap p[Y] \neq \varnothing$, donde $p : J \longrightarrow C$ es la proyección. Como los conjuntos $p[V]$ forman una base de entornos de 1 en C, esto demuestra que $[\alpha]$ está en la clausura de $p[Y]$, pero Y es conexo, luego $p[Y]$ también, luego su clausura también, luego está contenida en D y así $[\alpha] \in D$. ∎

Teorema 12.13 *Sea k un cuerpo numérico.*

a) El grupo D de las normas universales es divisible, es decir, para todo $a \in D$ y todo entero n existe un $b \in D$ de manera que $a = b^n$.

b) Una clase de elementos ideales $a \in C$ es una norma universal si y sólo si es infinitamente divisible, es decir, si para todo entero n existe un $b \in C$ tal que $a = b^n$.

Demostración: Sólo hay que probar a), pues de aquí se sigue una implicación de b) y la otra es el argumento usado en el teorema 12.9 para probar que los elementos de $\mathbb{R}^+$ son normas universales.

Para probar a) veamos primero lo siguiente:

> (∗) *Si $n > 1$ es un número natural, k contiene las raíces n-simas de la unidad y a es una norma universal, entonces existe un $b \in C$ tal que $a = b^n$.*

Tomemos un conjunto finito E de primos de k que cumpla las hipótesis del teorema 8.5. Consideramos el grupo

$$D_1 = \prod_{\mathfrak{p}\in E} k_{\mathfrak{p}}^{*n} \times \prod_{\mathfrak{p}\in P\setminus E} U_{\mathfrak{p}},$$

que es de la forma (7.11) tomando $E_1 = \varnothing$, $E_2 = E$. El teorema 8.5 nos da que k^*D_1 es un grupo de clases, luego $D \leq k^*D_1/k^*$ y por consiguiente $a = [\alpha]$, con $\alpha \in D_1$. En particular, las componentes $\alpha_{\mathfrak{p}}$ con $\mathfrak{p} \in E$ son potencias n-simas. Vamos a probar que sucede lo mismo con las componentes restantes.

Tomemos para ello un conjunto finito E' de primos de k que contenga a E y consideremos el grupo

$$D' = \prod_{\mathfrak{p}\in E} k_{\mathfrak{p}}^{*n} \times \prod_{\mathfrak{p}\in E'\setminus E} U_{\mathfrak{p}}^n \times \prod_{\mathfrak{p}\in P\setminus E'} U_{\mathfrak{p}} \leq D_1.$$

Por el teorema 7.21 los grupos $U_\mathfrak{p}^n$ son abiertos en $k_\mathfrak{p}^*$, luego también lo son los grupos $k_\mathfrak{p}^{*n}$ (en el caso no arquimediano, pero en el caso arquimediano es trivial). Por consiguiente D' es abierto en J_k, luego k^*D' también, y es un grupo de clases. Esto significa que el grupo de normas universales D está contenido en k^*D'/k^*, luego $a = [\beta]$, con $\beta \in D'$. A su vez esto implica que existe un $\gamma \in k^*$ tal que $\alpha = \gamma\beta$.

Más concretamente, $\gamma \in k^* \cap D_1$. Si probamos que $\Delta_1 = k^* \cap D_1 = k_E^n$ tendremos que las componentes $\alpha_\mathfrak{p}$ con $\mathfrak{p} \in E'$ serán potencias n-simas en $k_\mathfrak{p}^*$, pues lo serán tanto γ como las componentes de β. Puesto que E' es arbitrario, todas las componentes de α resultarán ser potencias n-simas y por consiguiente α también lo será.

La inclusión $k_E^n \le \Delta_1$ es evidente. Más aún, tenemos la relación (7.14), según la cual $|\Delta_1 : k_E^n| = |K_1 : k|$, donde K_1 es la extensión de Kummer asociada a Δ_1. Ahora bien, según el teorema 8.5, el grupo de clases de este cuerpo es $k^*\Delta_2$, donde $\Delta_2 = k^* \cap D_2 = J_E$. Pero entre las hipótesis de 8.5 (que estamos suponiendo) se encuentra que $k^*\Delta_2 = k^*J_E = J_k$, luego $K_1 = k$ y $\Delta_1 = k_E^n$.

Con esto tenemos demostrado $(*)$.

Ahora veamos que si K/k es una extensión finita, entonces $D_k = \mathrm{N}_k^K[D_K]$. La transitividad de las normas da inmediatamente que $\mathrm{N}_k^K[D_K] \le D_k$. Tomemos ahora $a \in D_k$. Como a es una norma para cualquier extensión finita (ver el comentario tras el teorema 12.11), existe un $b \in \mathrm{N}_{K/k}^{-1}(a)$, y entonces $\mathrm{N}_{K/k}^{-1}(a) = b\,\mathrm{N}_{K/k}^{-1}(1)$.

Teniendo en cuenta la definición de la norma de un elemento ideal, es claro que si α tiene norma 1 entonces $\alpha_\mathfrak{P}$ es una unidad para todo $\mathfrak{P}$ no arquimediano, luego $\|\alpha_\mathfrak{P}\|_\mathfrak{P} = 1$.

Respecto a las componentes arquimedianas, el producto de todas las normas $\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P})$ correspondientes a un mismo primo $\mathfrak{p}$ de k es igual a 1.

Si $\mathfrak{p}$ es complejo la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ es trivial y $\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P}) = \alpha_\mathfrak{P}$. Tomando módulos y elevando al cuadrado queda que el producto de todos los $\|\alpha_\mathfrak{P}\|_\mathfrak{P}$ (con $\mathfrak{P} \mid \mathfrak{p}$) es 1.

Si $\mathfrak{p}$ es real entonces $|\,\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P})| = |\alpha_\mathfrak{P}| = \|\alpha_\mathfrak{P}\|_\mathfrak{P}$ cuando el primo $\mathfrak{P}$ es real y $|\,\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P})| = |\alpha_\mathfrak{P}|^2 = \|\alpha_\mathfrak{P}\|_\mathfrak{P}$ cuando $\mathfrak{P}$ es complejo, luego llegamos a la misma conclusión.

La conclusión final es que $\|\alpha\| = 1$. Por lo tanto $\mathrm{N}_{K/k}^{-1}(1) \le C^0$ y consecuentemente $\mathrm{N}_{K/k}^{-1}(a) = b\,\mathrm{N}_{K/k}^{-1}(1)$ es compacto.

Para cada extensión finita L/K sea $X_L = \mathrm{N}_K^L[C_L] \cap \mathrm{N}_{K/k}^{-1}(a) \subset C_K$. Como a es la norma de un elemento de C_L, el conjunto X_L es un compacto no vacío.

Claramente, si $K \subset L \subset L'$, entonces $X_{L'} \subset X_L$. De aquí se sigue que la familia de conjuntos X_L tiene la propiedad de la intersección finita, luego su intersección es no vacía, es decir, existe un $c \in X_L$ para toda extensión finita L de K. Esto significa que c es una norma universal de K y $a = \mathrm{N}_k^K(c) \in \mathrm{N}_k^K[D_K]$.

Probamos finalmente a). Tomamos un $a \in D$ y un natural n (podemos suponer $n > 1$). Sea ζ una raíz n-sima primitiva de la unidad. Sea $K = k(\zeta)$ y $b \in D_K$ tal que $\mathrm{N}(b) = a$.

Si probamos que b tiene raíz n-sima en D_K tendremos que a tiene raíz n-sima en D_k, luego podemos suponer que $K = k$ y que k contiene una raíz n-sima primitiva de la unidad.

La afirmación $(*)$ nos da que a tiene una raíz n-sima en C_k, pero queremos que tenga raíz n-sima en D_k. Aplicaremos un argumento de compacidad similar al anterior. Para cada extensión finita de Galois K/k tenemos, usando $(*)$, que

$$D_k = \mathrm{N}_k^K[D_K] \leq \mathrm{N}_k^K[C_K^n] = \mathrm{N}_k^K[C_K]^n.$$

Sea $Y_K = \mathrm{N}_k^K[C_K] \cap a^{1/n}$, donde $a^{1/n}$ es el conjunto de todos los $b \in C_k$ tales que $b^n = a$. Es claro que todo b que cumpla esto cumple también que $\|b\| = \|a\|^{1/n}$, luego $a^{1/n}$ está contenido en $\|a\|^{1/n}C^0$, que es compacto. Así pues, los conjuntos Y_K son compactos no vacíos de C_k. La transitividad de las normas nos da que la familia tiene la propiedad de la intersección finita, y un b perteneciente a la intersección total es una norma universal tal que $b^n = a$. ∎

12.3 El homomorfismo de Artin local

El comportamiento del homomorfismo de Artin local para extensiones infinitas es distinto del que se podría suponer. Al contrario de lo que ocurre en el caso global, resulta que es inyectivo y no suprayectivo. Veámoslo.

Teorema 12.14 *Sea k un cuerpo p-ádico y A la mayor extensión abeliana de k. Entonces el homomorfismo de Artin $\omega : k^* \longrightarrow G(A/k)$ es inyectivo, continuo y su imagen es densa en el grupo de Galois.*

Demostración: El núcleo del homomorfismo es la intersección de todos los subgrupos abiertos de índice finito. Veamos que es trivial.

Un elemento $\alpha \in k^*$ distinto de 1 es de la forma $\alpha = \epsilon\pi^n$, donde ϵ es una unidad y π es un primo. Para un natural m suficientemente grande, o bien $\epsilon \notin U_m = 1 + \mathfrak{p}^m$ (si $\epsilon \neq 1$) o bien $\pi^n \notin \langle \pi^m \rangle$ (si $n \neq 0$), luego en cualquier caso $\alpha \notin H = U_m \langle \pi^m \rangle$, que es un subgrupo abierto de índice finito, luego α no está en el núcleo de ω.

El resto de la demostración consiste en usar los argumentos aprovechables del teorema 12.9. Podemos probar que la imagen es densa, pero no hay un argumento de compacidad con el que llegar a la suprayectividad. ∎

Así pues, en el caso local la única norma universal es 1. Tratemos de entender mejor cuál es el problema que impide la suprayectividad del homomorfismo de Artin. Tenemos que ω es inyectiva y continua, pero no es un homeomorfismo en su imagen. En efecto, si H es un subgrupo abierto en k^* de índice finito y K es su cuerpo de clases, entonces $\omega[H] = G(A/K) \cap \omega[k^*]$, luego ω biyecta los subgrupos abiertos de k^* de índice finito con los entornos básicos del neutro en $\omega[k^*]$. Esto implica la continuidad, pero para que ω fuera un homeomorfismo en su imagen haría falta que las imágenes de los subgrupos abiertos de índice infinito fueran también abiertas, y esto ya no es cierto. De hecho $\omega[k^*]$ no tiene subgrupos abiertos de índice infinito (porque, claramente, $G(A/k)$ no los tiene).

La topología que $G(A/k)$ induce en $\omega[k^*]$ admite una descripción muy simple en términos de la aritmética de k. Para probarlo, comenzamos por trasladarla a k^*.

Definición 12.15 Sea k un cuerpo p-ádico. Llamaremos *topología de clases* en k^* a la topología inducida por el monomorfismo $\omega : k^* \longrightarrow G(A/k)$, es decir, la formada por las antiimágenes de los abiertos de $\omega[k^*]$.

De este modo el homomorfismo de Artin es un isomorfismo topológico en su imagen cuando en k^* consideramos la topología de clases. Según hemos comentado, la topología de clases es distinta de la que veníamos considerando hasta ahora (la inducida por el valor absoluto) y que desde ahora llamaremos *topología p-ádica.* Más concretamente, una base de entornos del neutro para la topología de clases la forman los subgrupos abiertos p-ádicos de índice finito. Puesto que k^* tiene subgrupos abiertos p-ádicos de índice infinito (por ejemplo el grupo de unidades U) la topología de clases no coincide con la p-ádica.

Precisando aún más, la estructura de k^* con la topología p-ádica es clara: podemos factorizar $k^* = \langle\pi\rangle \times U$, donde π es un primo en k. El subgrupo $\langle\pi\rangle$ es discreto, U es compacto y k^* tiene la topología producto.

Si H es un entorno básico del neutro para la topología de clases (es decir, H es un subgrupo abierto p-ádico de índice finito), entonces $U \cap H$ es un subgrupo abierto (p-ádico) de U, luego todo abierto de U para la topología de clases es abierto para la topología p-ádica. Así pues, la identidad $U \longrightarrow U$ es continua cuando a la izquierda consideramos la topología p-ádica y a la derecha la topología de clases. Ahora bien, U es compacto con la topología p-ádica y una biyección continua en un compacto es un homeomorfismo. Concluimos que ambas topologías coinciden en U.

Esto ya no es cierto sobre $\langle\pi\rangle$: Si H es un entorno básico del neutro para la topología de clases, entonces $\langle\pi\rangle \cap H$ es un subgrupo abierto (p-ádico) de índice finito. Que sea abierto no significa nada, pues $\langle\pi\rangle$ es discreto, y que sea de índice finito quiere decir simplemente que no es trivial, pues $\langle\pi\rangle$ es isomorfo a $\mathbb{Z}$ como grupo y todos sus subgrupos no triviales tienen índice finito.

Recíprocamente, si H es un subgrupo no trivial de $\langle\pi\rangle$, entonces H es cerrado en k^* para la topología p-ádica[2], luego $H \times U$ también lo es, y este grupo tiene índice finito en k^*, luego es abierto para la topología p-ádica y por tanto también para la topología de clases. Además $H = \langle\pi\rangle \cap (H \times U)$, luego H es abierto en $\langle\pi\rangle$ para la topología de clases.

En resumen, los entornos básicos del neutro en $\langle\pi\rangle$ son los subgrupos no triviales.

Definición 12.16 Si G es un grupo cíclico infinito llamaremos *topología de los ideales* en G a aquella con la que G es un grupo topológico y una base de entornos abiertos de 1 la forman los subgrupos no triviales.

[2] H es cerrado en $\langle\pi\rangle$ y éste es cerrado en k^* porque es el núcleo de la proyección en U, que es continua porque la topología de k^* es la topología producto.

Recibe este nombre porque en el caso del grupo $\mathbb{Z}$ los entornos básicos de 0 son los ideales no nulos $m\mathbb{Z}$, para $m = 1, 2, \ldots$ No es difícil comprobar directamente que estas condiciones determinan una topología en $\mathbb{Z}$ compatible con la suma, pero nosotros no necesitamos hacerlo, pues la topología de los ideales es la inducida en $\mathbb{Z}$ por el isomorfismo $\mathbb{Z} \longrightarrow \langle\pi\rangle$ dado por $n \mapsto \pi^n$.

Ahora ya podemos describir la topología de clases de un cuerpo p-ádico:

Teorema 12.17 *Sea k un cuerpo p-ádico, sea U su grupo de unidades y π un primo en k. Entonces $k^* = \langle\pi\rangle \times U$, la topología de clases de k^* induce la topología de los ideales en $\langle\pi\rangle$, la topología p-ádica en U y coincide con el producto de ambas.*

Demostración: Sólo falta probar que la topología de clases es el producto de las topologías que induce en los factores. Un entorno de 1 para la topología de clases es un subgrupo H abierto p-ádico y de índice finito, pero entonces

$$\big(H \cap \langle\pi\rangle\big) \times (H \cap U) \leq H$$

es un entorno de 1 para la topología producto. Así pues, todo abierto para la topología de clases es abierto para la topología producto. Recíprocamente, un entorno básico de 1 para la topología producto es de la forma HK, donde H es un subgrupo no trivial de $\langle\pi\rangle$ y K es un subgrupo de U de índice finito y abierto para la topología p-ádica. Entonces HK es un subgrupo abierto para la topología p-ádica (porque contiene a K) y tiene índice finito, luego es abierto para la topología de clases. ∎

Para simplificar los razonamientos siguientes conviene probar que todos los grupos que estamos considerando son metrizables. Esto es consecuencia de un resultado general sobre grupos topológicos: un grupo es metrizable si y sólo si tiene una base numerable de entornos del neutro. Por completitud probaremos un caso particular de este resultado suficiente para nuestros fines.

Teorema 12.18 *Sea G un grupo topológico abeliano y sea $\{V_n\}_{n=1}^{\infty}$ una base de entornos de 1 formada por subgrupos abiertos. Entonces G es metrizable. Más aún, sustituyendo cada V_n por la intersección de los n primeros entornos podemos exigir que se den las inclusiones*

$$\cdots \leq V_4 \leq V_3 \leq V_2 \leq V_1 = G,$$

y entonces una métrica compatible con el producto en G es la dada por

$$d(u, v) = 1/m, \qquad \text{donde } m = \text{máx}\{n \in \mathbb{N} \mid u^{-1}v \in V_n\} \in [1, +\infty].$$

Demostración: Es claro que $d(u, v) = 0$ si y sólo si $u = v$, así como que $d(u, v) = d(v, u)$.

Sean ahora u, v, $w \in G$. Si dos de ellos coinciden, la desigualdad triangular se vuelve trivial. Supongamos que son distintos dos a dos. Sea $d(u, v) = 1/m$ y $d(v, w) = 1/m'$. Llamemos r al mínimo de m y m'.

Entonces $u^{-1}v \in V_m \subset V_r$ y $v^{-1}w \in V_{m'} \subset V_r$, y al multiplicar queda $u^{-1}w \in V_r$, con lo cual $d(u,w) \leq 1/r$. Por lo tanto

$$d(u,w) \leq 1/r = \max\{d(u,v), d(v,w)\} \leq d(u,v) + d(v,w).$$

También es evidente a partir de la definición que $d(uv,uw) = d(v,w)$, es decir, la distancia es invariante por traslaciones.

La bola abierta de centro 1 y radio $1/n$ es claramente V_{n+1}, luego la bola de centro u y radio $1/n$ es uV_{n+1}. Por lo tanto los conjuntos uV_n son una base de entornos abiertos de u tanto para la topología de G como para la métrica, lo que significa que ambas coinciden. ∎

Según hemos comentado, este teorema justifica que todos los grupos topológicos que estamos manejando son metrizables. Observar por ejemplo que toda extensión algebraica tiene grado numerable, luego tiene sólo una cantidad numerable de subextensiones finitas). Por lo tanto los grupos de Galois son todos metrizables. El grupo k^* con la topología de clases es metrizable porque es homeomorfo a un subgrupo de un grupo de Galois, que es metrizable.

En particular tiene sentido hablar de sucesiones de Cauchy o de completitud. En realidad sobre grupos topológicos podemos caracterizar las sucesiones de Cauchy sin hacer referencia a ninguna métrica en particular:

Una sucesión $\{x_n\}$ en un grupo topológico G es *de Cauchy* si para todo entorno V de 1 existe un natural n_0 tal que si m, $n \geq n_0$ entonces $x_m x_n^{-1} \in V$.

Es fácil ver que en las condiciones del teorema 12.18 una sucesión es de Cauchy en este sentido si y sólo si lo es respecto a la distancia que allí se construye. Sin embargo esta equivalencia muestra que la noción de sucesión de Cauchy depende únicamente de la topología del grupo (y de su estructura algebraica), pero no de la distancia particular que consideremos (siempre que ésta induzca la topología del grupo).

En general se prueba sin dificultad que toda sucesión convergente es de Cauchy, así como que si una sucesión de Cauchy tiene una subsucesión convergente, entonces toda ella es convergente (por ejemplo, si $\{x_n\}$ converge a x y V es un entorno de 1, la continuidad del producto nos da un entorno W de 1 tal que $WW \subset V$. Para n suficientemente grande $x_n \in Wx \cap xW^{-1}$, con lo que $x_m x_n^{-1} = x_m x^{-1} x x_n^{-1} \in WW \subset V$).

Un grupo topológico metrizable G es *completo* si toda sucesión de Cauchy en G es convergente. Es claro que si G es compacto entonces es completo (pues toda sucesión de Cauchy tiene una subsucesión convergente, luego es convergente).

Es fácil probar que todo grupo topológico abeliano tiene una única compleción salvo isomorfismo topológico, es decir, existe un único grupo topológico completo que lo contiene como subgrupo denso. En el caso metrizable la compleción puede construirse como el cociente del grupo de las sucesiones de Cauchy sobre el subgrupo de las sucesiones convergentes a 1. La unicidad se debe a que si C y D son dos compleciones de G, entonces todo elemento $x \in C$ es límite de una sucesión de Cauchy en G, la cual converge a un $f(x) \in D$ y es fácil ver que f está bien definida y es un isomorfismo topológico.

Si k es un cuerpo p-ádico y llamamos $\bar{k}^*$ a la compleción de k^* respecto a la topología de clases, lo que afirma el teorema 12.14 es que $\bar{k}^* = G(A/k)$ o, más precisamente, que el homomorfismo de Artin se extiende a un isomorfismo topológico $\omega : \bar{k}^* \longrightarrow G(A/k)$.

Si K es una extensión abeliana finita de k, sabemos que

$$\omega[\mathrm{N}[K]] = G(A/K) \cap \omega[k^*],$$

de donde al tomar clausuras queda $\omega[\overline{\mathrm{N}[K]}] = G(A/K)$ (la intersección de un denso con un abierto es densa en el abierto). La correspondencia

$$\overline{\mathrm{N}[K]} \leftrightarrow G(A/K) \leftrightarrow K$$

es obviamente una biyección entre los subgrupos abiertos de $\bar{k}^*$ y las extensiones abelianas finitas de k, que se extiende ahora a una biyección entre los subgrupos cerrados y las extensiones abelianas (finitas o infinitas) de k, en completo paralelismo con el caso global.

Respecto a la estructura de $\bar{k}^*$, tenemos el teorema siguiente:

Teorema 12.19 *Sea k un cuerpo p-ádico, sea π un primo en k y U su grupo de unidades. Entonces la clausura $\overline{\langle\pi\rangle}$ en $\bar{k}^*$ es la compleción de $\langle\pi\rangle$ respecto a la topología de ideales, se cumple que $\bar{k}^* = \overline{\langle\pi\rangle} \times U$ y que la topología de $\bar{k}^*$ es el producto de las topologías de los factores.*

Demostración: El subgrupo $\overline{\langle\pi\rangle}$ es completo, pues es cerrado en $\bar{k}^*$ y todo cerrado en un completo es completo. Trivialmente tiene a $\langle\pi\rangle$ como subconjunto denso, luego por la unicidad es la compleción de $\langle\pi\rangle$. Notar que de hecho es compacto, pues $\bar{k}^*$ es compacto (es homeomorfo a un grupo de Galois).

Por otra parte

$$\overline{\langle\pi\rangle} \cap U = \overline{\langle\pi\rangle} \cap k^* \cap U = \overline{\langle\pi\rangle}^{k^*} \cap U = \langle\pi\rangle \cap U = 1,$$

donde $\overline{\langle\pi\rangle}^{k^*}$ denota la clausura de $\langle\pi\rangle$ en k^*. Así pues, el producto $\overline{\langle\pi\rangle} \times U$ es ciertamente directo.

La identidad en $\overline{\langle\pi\rangle} \times U$ es continua cuando consideramos la topología producto como topología inicial y la topología inducida como topología final. Basta tomar sucesiones y usar la continuidad del producto. Como $\overline{\langle\pi\rangle} \times U$ es compacto (para la topología producto) la identidad es un homeomorfismo, luego ambas topologías coinciden.

En particular $\overline{\langle\pi\rangle} \times U$, al ser compacto, es cerrado en $\bar{k}^*$ y, como contiene a k^*, ha de ser todo $\bar{k}^*$. ∎

Esta factorización se traduce a través del isomorfismo de Artin en una factorización del grupo de Galois $G(A/k)$. Vamos a interpretarla.

El teorema 2.36 afirma que la correspondencia $K \mapsto \overline{K}$ (donde $\overline{K}$ es el cuerpo de restos de K) biyecta las extensiones no ramificadas de k con las extensiones finitas de $\overline{K}$. Por lo tanto hay exactamente una extensión no ramificada de

grado n para cada número natural $n > 0$, digamos K_n. Además sabemos que $G(K_n/k)$ es isomorfo a $G(\overline{K}_n/\overline{k})$. El isomorfismo asigna a cada $\sigma \in G(K_n/k)$ el automorfismo $\overline{\sigma} \in G(\overline{K}_n/\overline{k})$ dado por $\overline{\sigma}([\alpha]) = [\sigma(\alpha)]$.

El grupo $G(\overline{K}_n/\overline{k})$ es cíclico y está generado por el automorfismo de Frobenius $\sigma(u) = u^{p^f}$, donde p^f es el número de elementos de $\overline{k}$. El automorfismo de $G(K_n/k)$ que induce al automorfismo de Frobenius es el que en el capítulo IV llamábamos símbolo de Frobenius asociado al primo de K_n, pero, dado que los cuerpos p-ádicos tienen un único primo, la notación del capítulo IV nos queda ahora "demasiado grande". En su lugar, llamaremos *automorfismo canónico* de la extensión K_n/k al automorfismo $\sigma_{K_n/k}$ que induce el automorfismo de Frobenius en la extensión de cuerpos de restos.

Como la extensión K_n/k es no ramificada, todas las unidades de k son normas, luego el grupo de unidades U está en el núcleo del homomorfismo de Artin y el automorfismo

$$\left(\frac{K_n/k}{\pi}\right) \tag{12.1}$$

es el mismo para cualquier primo π de k. Más aún, π^n también está en el núcleo del homomorfismo de Artin, ya que su imagen es una potencia n-sima en el grupo $G(K_n/k)$, que tiene orden n. De aquí se sigue que el núcleo del homomorfismo de Artin es exactamente $\langle \pi^n \rangle \times U$ (pues ha de tener índice n en k^*).

Es fácil ver que (12.1) es el automorfismo canónico de K_n/k. Más aún, se cumple que

$$\left(\frac{K_n/k}{\pi}\right)(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}} \ (\text{mód } \mathfrak{p}), \quad \text{para todo } \alpha \text{ entero en } K_n, \tag{12.2}$$

donde $\mathfrak{p}$ es el primo de k.

En efecto, por el teorema 8.22 podemos representar $k = E_{\mathfrak{p}}$, $K_n = F_{\mathfrak{P}}$, donde F/E es una extensión abeliana de cuerpos numéricos. El primo $\mathfrak{P}$ es no ramificado sobre $\mathfrak{p}$ luego, por definición, el símbolo de Artin

$$\left(\frac{F/E}{\mathfrak{p}}\right) = \left(\frac{K_n/k}{\pi}\right)\Bigg|_F$$

está determinado por la relación (12.2), válida en principio para todo α entero en F y, por continuidad, para todo entero en K_n.

Ahora expresaremos estos hechos en términos de extensiones infinitas. Para ello llamaremos N al producto de todas las extensiones no ramificadas de k. Nos referiremos a este cuerpo como *la máxima extensión de k no ramificada.*

La unión de todos los ideales primos de todos los cuerpos K_n forma un ideal primo del anillo de enteros de N, por lo que tiene sentido igualmente el cuerpo de restos $\overline{N}$, que es una extensión algebraica de $\overline{k}$ que contiene a todas las extensiones finitas de $\overline{k}$, luego es una clausura algebraica de $\overline{k}$. Más

aún, $G(N/k) \cong G(\overline{N}/\overline{k})$. A cada $\sigma \in G(N/k)$ le corresponde el automorfismo $\overline{\sigma} \in G(\overline{N}/\overline{k})$ dado por $\overline{\sigma}([\alpha]) = [\sigma(\alpha)]$ (todo esto se prueba inmediatamente a partir de los resultados análogos para extensiones finitas). Los automorfismos canónicos $\sigma_{K_n/k}$ se extienden a un único automorfismo de N/k, al que llamaremos *automorfismo canónico* de k y lo representaremos por σ_k. Se caracteriza por que induce el *automorfismo de Frobenius* de $\overline{N}/\overline{k}$, dado por $\sigma(u) = u^{p^f}$, donde p^f es el número de elementos de $\overline{k}$.

Ahora es claro que si π es un primo en k entonces $(k/\pi) = \sigma_k$. La relación (12.2) nos permite caracterizar σ_k como el único automorfismo que cumple

$$\sigma_k(\alpha) \equiv \alpha^{\mathrm{N}\,\mathfrak{p}} \text{ (mód } \mathfrak{p}), \quad \text{para todo } \alpha \text{ entero en } N.$$

Por otra parte, si $\omega : k^* \longrightarrow G(A/k)$ es el homomorfismo de Artin, se cumple que $\omega[U] = G(A/N)$. En efecto, basta ver que $\omega[U] = G(A/N) \cap \omega[k^*]$, pues entonces $\omega[U]$ ha de ser denso en $G(A/N)$ y, como es compacto, ha de ser todo el grupo de Galois.

Obviamente, si $\alpha \in U$ entonces $\omega(\alpha)$ fija a todos los cuerpos K_n, luego fija a N. Recíprocamente, si $\omega(\alpha) \in G(A/N)$, entonces $\omega(\alpha)|_{K^n} = 1$, luego $\alpha \in \langle \pi^n \rangle \times U$ para todo n, luego $\alpha \in \overline{U}$.

Como consecuencia tenemos que $\overline{\langle \pi \rangle} \cong G(N/k)$. El isomorfismo está determinado por la asignación $\pi \mapsto \sigma_k$.

En resumen, la factorización que hemos encontrado del grupo de Galois $G(A/k)$ resulta ser $G(A/k) = G(A/N) \times \overline{\langle \sigma \rangle}$, donde $G(A/N) \cong U$, y σ está determinado módulo U por que $\sigma|_N = \sigma_k$.

Todavía podemos decir más. Vamos a determinar la estructura del grupo $\overline{\langle \sigma \rangle} \cong \overline{\langle \pi \rangle} \cong \overline{\mathbb{Z}}$, es decir, de la compleción de un grupo cíclico infinito cualquiera respecto a la topología de ideales.

Antes de entrar en ello conviene observar que tomando como k la extensión adecuada del cuerpo p-ádico $\mathbb{Q}_p$ adecuado podemos conseguir que $\overline{k}$ sea cualquier cuerpo finito (por el teorema 2.36 aplicado a $\mathbb{Q}_p$), luego hemos probado que si K es la clausura algebraica de un cuerpo finito k, entonces

$$\overline{\mathbb{Z}} \cong G(K/k).$$

El isomorfismo es topológico y puede construirse de modo que la imagen de 1 sea el automorfismo de Frobenius $u \mapsto u^{p^f}$, donde p^f es el número de elementos de k.

Teorema 12.20 *Sea k un cuerpo finito y K una clausura algebraica. Entonces*

$$G(K/k) \cong \overline{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p,$$

donde p recorre los primos finitos de $\mathbb{Z}$ y $\mathbb{Z}_p$ es el anillo de los enteros p-ádicos.

Demostración: Sea $X = \prod_p \mathbb{Z}_p$, que es claramente un grupo topológico compacto con la topología producto. En particular es completo. Podemos

considerar a $\mathbb{Z}$ como subgrupo de X identificando cada entero n con el elemento de X cuyas componentes son todas iguales a n.

Una base de entornos de 0 en un grupo $\mathbb{Z}_p$ la forman los ideales p^n, es decir, los enteros p-ádicos divisibles entre p^n. Por lo tanto una base de entornos de 0 en X está formada por los grupos W_m definidos como sigue: si $m = p_1^{r_1} \cdots p_n^{r_n}$, entonces W_m es el producto que en la componente p_i tiene al abierto p^{r_i} y en las componentes restantes tiene a todo $\mathbb{Z}_p$.

Notar que $W_m \cap \mathbb{Z} = m\mathbb{Z}$, luego la topología que X induce en $\mathbb{Z}$ es la topología de ideales. Veamos finalmente que $\mathbb{Z}$ es denso en X.

Un abierto básico de X es de la forma $u + W_m$, para cierto $u \in X$. Sea $m = p_1^{r_1} \cdots p_n^{r_n}$ la factorización de m en primos. Como $\mathbb{Z}$ es denso en $\mathbb{Z}_p$ existe un entero $c_i \in u_{p_i} + p^{r_i}$ y por el teorema chino del resto podemos tomar un entero $n \equiv c_i \pmod{p_i^{r_i}}$ para todo i, con lo que $n \in u_{p_i} + p^{r_i}$ y consecuentemente $n \in u + W_m$.

Todo esto implica que X es una compleción de $\mathbb{Z}$ para la topología de ideales, luego por la unicidad $\overline{\mathbb{Z}} \cong X$. ∎

Es de destacar que esta representación de nos da una estructura de anillo (con divisores de 0).

Ejercicio: Sea G un grupo topológico completo con una base de entornos del neutro formada por subgrupos abiertos (por ejemplo cualquier grupo de Galois). Probar que la aplicación $G \times \mathbb{Z} \longrightarrow G$ dada por $(g, n) \mapsto g^n$ se extiende a una única aplicación continua $G \times \overline{\mathbb{Z}} \longrightarrow G$ que seguiremos representando exponencialmente. Se cumple

$$g^{m+n} = g^m g^n, \qquad g^{mn} = (g^m)^n \qquad \text{para todo } g \in G,\ m, n \in \overline{\mathbb{Z}}.$$

La clausura en G del subgrupo generado por g es el subgrupo $\{g^m \mid m \in \overline{\mathbb{Z}}\}$.

Terminamos la sección con una caracterización sencilla del homomorfismo de Artin local. Es especialmente interesante porque hay muchas formas distintas de definir el homomorfismo de Artin. Este teorema justifica inmediatamente que todas dan lugar al mismo concepto.

Teorema 12.21 *Sea k un cuerpo p-ádico, sea A una extensión abeliana de k que contenga a la máxima extensión no ramificada de k, llamémosla N, y sea $\phi : k^* \longrightarrow G(A/k)$ un monomorfismo que cumpla las propiedades siguientes:*

a) Si $K \subset A$ es una extensión finita de k entonces todo $\alpha \in k^*$ cumple

$$\phi(\alpha) \in G(A/K) \quad \text{si y sólo si} \quad \alpha \in \mathrm{N}[K^*].$$

b) Para cada primo π de k se cumple que $\phi(\pi)|_N$ es el automorfismo canónico de k.

Entonces A es la máxima extensión abeliana de k y ϕ es el homomorfismo de Artin.

Demostración: Llamemos $\psi : k^* \longrightarrow G(A/k)$ la composición del homomorfismo de Artin con la restricción a A, que también cumple las propiedades

a) y b). Si probamos que $\phi = \psi$, en particular ψ será un monomorfismo, luego será el homomorfismo de Artin y, por consiguiente, A será la máxima extensión abeliana de k.

Sea π un primo en k^*. Sea K una extensión abeliana finita de k y llamemos $H = G(A/K)$. Entonces por a) sabemos que $\phi(\pi) \in H$ si y sólo si $\psi(\pi) \in H$. Como H es cerrado, esto equivale a que $\overline{\langle\phi(\pi)\rangle} \leq H$ si y sólo si $\overline{\langle\psi(\pi)\rangle} \leq H$.

Ahora bien, como toda extensión de k es la unión de las extensiones finitas intermedias, todo subgrupo cerrado de $G(A/k)$ es la intersección de todos los grupos $G(A/K)$ que lo contienen, luego concluimos que $\overline{\langle\phi(\pi)\rangle} = \overline{\langle\psi(\pi)\rangle}$.

Sabemos que el grupo de Galois de la máxima extensión abeliana $\mathbb{A}$ de k factoriza como $G(\mathbb{A}/k) = G(\mathbb{A}/N) \times \overline{\langle\omega(\pi)\rangle}$, luego $G(A/k) = G(A/N) \times \overline{\langle\phi(\pi)\rangle}$.

La propiedad b) implica $\phi(\pi)|_N = \psi(\pi)|_N$, luego $\overline{\phi(\pi)} = \psi(\pi)u$, para un cierto $u \in G(A/N)$. Así pues, $\psi(\pi)u \in \overline{\langle\phi(\pi)\rangle} = \overline{\langle\psi(\pi)\rangle}$ y en consecuencia $u \in \overline{\langle\psi(\pi)\rangle} \cap G(A/N) = 1$. Por lo tanto llegamos a que $\phi(\pi) = \psi(\pi)$, para todo primo π de k.

Si $\epsilon \in U$ entonces $\phi(\epsilon) = \phi(\epsilon\pi)\phi(\pi)^{-1} = \psi(\epsilon\pi)\psi(\pi)^{-1} = \psi(\epsilon)$. Esto prueba que ambas aplicaciones coinciden en $k^* = U \times \langle\pi\rangle$. ∎

12.4 La aritmética de las extensiones infinitas

Sin entrar en excesivos detalles, comentamos que la aritmética finita admite una generalización débil al caso de extensiones algebraicas cualesquiera de los cuerpos numéricos o p-ádicos. Todas las definiciones son las generalizaciones naturales del caso finito y todas las pruebas consisten en aplicar los resultados que se desea probar para un cuerpo K al caso de las extensiones finitas contenidas en K (para las que ya están probados).

Por ejemplo, si K es una extensión finita de $\mathbb{Q}$ y $\mathfrak{P}$ es un divisor primo de K (o sea, una clase de equivalencia de valores absolutos), la restricción de los valores absolutos de $\mathfrak{p}$ a cualquier subcuerpo k determinan un divisor $\mathfrak{p}$ de k, y en este sentido podemos decir que $\mathfrak{P}$ divide a $\mathfrak{p}$. En particular, si restringimos $\mathfrak{P}$ a todos los cuerpos numéricos contenidos en k y consideramos los valores absolutos canónicos asociados a los primos que obtenemos, vemos que éstos son consistentes, es decir, el valor absoluto de un $\alpha \in K$ no depende del cuerpo numérico que lo contenga, luego podemos definir el valor absoluto canónico de $\mathfrak{P}$ como la extensión de todos estos valores absolutos. Entonces un primo $\mathfrak{P}$ divide a un primo $\mathfrak{p}$ de un subcuerpo si y sólo si el valor absoluto canónico de $\mathfrak{P}$ extiende al de $\mathfrak{p}$.

En lugar de dar más detalles nos limitaremos a considerar las diferencias con el caso finito. Ante todo, el anillo E de los enteros algebraicos de un cuerpo K ya no es un dominio de Dedekind, luego si $\mathfrak{P}$ es un primo no arquimediano de K, aunque podemos asociarle un ideal primo de E (la unión de los ideales asociados a las restricciones de $\mathfrak{P}$ a los cuerpos numéricos contenidos en K), no podemos deducir de aquí que dicho primo induzca a su vez una valoración (discreta) en K. No obstante podemos conseguir tal valoración a partir del anillo local

$E_{\mathfrak{P}} = \{\alpha \in K \mid |\alpha|_{\mathfrak{P}} \leq 1\}$ y de su ideal maximal $\mathfrak{P} = \{\alpha \in K \mid |\alpha|_{\mathfrak{p}} < 1\}$. Pero ahora no podemos reconstruir $\mathfrak{P}$ a partir de la valoración $v_{\mathfrak{P}}$. De todos modos la localización es útil porque nos permite definir el cuerpo de restos $\overline{K} = E_{\mathfrak{P}}/\mathfrak{P}$.

Si k es un subcuerpo de K podemos considerar a $\overline{K}$ como extensión de $\overline{k}$ de forma natural, luego en particular $\overline{K}$ es una extensión algebraica de su cuerpo primo, y por lo tanto la extensión $\overline{K}/\overline{k}$ es abeliana. El grupo $G(\overline{K}/\overline{k})$ es el análogo infinito del grado de inercia.

Otra diferencia importante es que a la hora de localizar un cuerpo K en un primo $\mathfrak{P}$ no arquimediano no conviene tomar compleciones, pues las clausuras algebraicas de los cuerpos p-ádicos no son completas con su valor absoluto, por lo que al completar una extensión infinita no obtendríamos una extensión algebraica de $\mathbb{Q}_p$. En lugar de esto definimos el cuerpo local $K_{\mathfrak{P}}$ como la unión de todas las compleciones $k_{\mathfrak{p}}$, donde k varía en los cuerpos numéricos contenidos en K y $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$. De este modo $K_{\mathfrak{P}}$ es una extensión algebraica de $\mathbb{Q}_p$ que contiene a K como conjunto denso. Las relaciones entre los cuerpos locales y globales son esencialmente las mismas que en el caso finito.

Capítulo XIII

La ley de reciprocidad

La ley de reciprocidad cuadrática permite determinar fácilmente en qué casos tiene solución una congruencia del tipo $x^2 \equiv a \pmod{p}$. Resulta natural preguntarse si existen resultados similares que permitan resolver el problema análogo planteado por las congruencias $x^n \equiv a \pmod{p}$. Euler obtuvo varias conjeturas sobre el carácter cúbico y bicuadrático de 2, 3 y 5 (es decir, sobre los primos p para los que estos números son cubos o potencias cuartas módulo p). Por ejemplo, conjeturó que si $p \equiv 1 \pmod{3}$ entonces $x^3 \equiv 2 \pmod{p}$ si y sólo si p es de la forma $p = a^2 + 27b^2$ (es fácil ver que en el caso $p \equiv -1 \pmod{3}$ o $p = 3$ todo entero es un resto cúbico módulo p).

Gauss observó una diferencia fundamental con el caso $n = 2$, y es que $\mathbb{Q}$ contiene las raíces cuadradas de la unidad, pero no así las cúbicas o cuartas, lo que le hizo conjeturar que un resultado natural sobre restos cúbicos o cuadráticos requeriría considerar los cuerpos $\mathbb{Q}\big(\sqrt{-1}\,\big)$ y $\mathbb{Q}(i)$, es decir, los cuerpos ciclotómicos tercero y cuarto. Efectivamente, estudiando estos cuerpos logró conjeturar una ley de reciprocidad cúbica y una ley de reciprocidad bicuadrática de las que se deducían las conjeturas de Euler. De la primera logró demostrar unos casos particulares, lo que le permitió probar la conjetura de Euler sobre el carácter cúbico de 2; de la segunda dijo que la prueba pertenecía *"a los misterios de la aritmética superior"*. Precisamente el estudio que realizó del anillo $\mathbb{Z}[i]$ a raíz de la ley de reciprocidad bicuadrática fue el que motivó que ahora se llame enteros de Gauss a los números de la forma $a + bi$.

Jacobi reclamó haber demostrado la ley de reciprocidad cúbica en sus lecciones de 1837, pero la primera prueba publicada fue la de Ferdinand Gotthold Eisenstein, en 1844, a la edad de 21 años. A lo largo de ese mismo año Eisenstein publicó 25 artículos que contenían entre otras cosas varias pruebas de las leyes de reciprocidad cúbica y bicuadrática así como nuevas pruebas de la ley de reciprocidad cuadrática. En 1850 publico un caso particular bastante genérico de una ley de reciprocidad para potencias de orden primo. Gauss dijo de él que tenía un talento que la naturaleza sólo otorga a unos pocos cada siglo. Lamentablemente, Eisenstein murió a los 29 años de edad.

La búsqueda de leyes de reciprocidad generales se convirtió en uno de los

problemas más importantes de la teoría de números de la época, y a él contribuyeron grandes figuras como Kummer, que encontró aplicaciones al estudio del último teorema de Fermat.

En este capítulo obtendremos una ley de reciprocidad general, debida a Artin, de la que se deducen todos los casos de los que hemos hablado y muchos otros. El teorema [8.37] afirma que la ley de reciprocidad cuadrática equivale a que el producto de los símbolos de Hilbert sea igual a 1. Lo primero que haremos será generalizar la definición del símbolo de Hilbert para exponentes distintos de 2, probaremos la fórmula del producto y de ella deduciremos la ley de reciprocidad de Artin.

13.1 El símbolo de Hilbert

Definición 13.1 Sea $n \geq 2$ un número natural y k un cuerpo p-ádico que contenga una raíz n-sima primitiva de la unidad ζ. Para cada $\alpha \in k^*$ consideramos el símbolo de Artin $\sigma = (k/\alpha)$. Si $\beta \in k^*$ y $\sqrt[n]{\beta}$ es una raíz n-sima de β en una extensión de k, las raíces restantes son

$$\sqrt[n]{\beta}, \quad \sqrt[n]{\beta}\,\zeta, \quad \ldots, \sqrt[n]{\beta}\,\zeta^{n-1}.$$

Entonces $\sigma\big(\sqrt[n]{\beta}\big) = \sqrt[n]{\beta}\,\zeta^s$ para cierto s, luego

$$\frac{\sigma\big(\sqrt[n]{\beta}\,\zeta^i\big)}{\sqrt[n]{\beta}\,\zeta^i} = \zeta^s$$

no depende de i o, en otras palabras, el número $\sigma\big(\sqrt[n]{\beta}\big)/\sqrt[n]{\beta}$ es una raíz de la unidad que depende de α, y de β, pero no de la elección de $\sqrt[n]{\beta}$.

Definimos el *símbolo de Hilbert* de k como el dado por

$$(\alpha, \beta) = \frac{1}{\sqrt[n]{\beta}} \left(\frac{k}{\alpha}\right)\big(\sqrt[n]{\beta}\big).$$

De este modo, (α, β) es una raíz n-sima de la unidad, y este símbolo determina los símbolos de Artin de las extensiones $k\big(\sqrt[n]{\beta}\big)/k$:

$$\left(\frac{k\big(\sqrt[n]{\beta}\big)/k}{\alpha}\right)\big(\sqrt[n]{\beta}\big) = (\alpha, \beta)\sqrt[n]{\beta}.$$

Obviamente $(\alpha, \beta) = 1$ si y sólo si α está en el núcleo del homomorfismo de Artin de la extensión $k\big(\sqrt[n]{\beta}\big)/k$, es decir, si y sólo si α es una norma en dicha extensión.

En [8.24] definimos el símbolo de Hilbert para $n = 2$ y $k = \mathbb{Q}_p$, si bien la definición no se parece apenas a la que acabamos de dar. Aquélla era la definición de Hasse y ésta es (esencialmente) la dada por Hilbert. Veamos que son equivalentes:

Teorema 13.2 *Sea k un cuerpo p-ádico y $\beta \in k^*$. Sea $K = k\big(\sqrt{\beta}\,\big)$. Entonces, para cada $\alpha \in k^*$ se cumple*

$$\alpha \in \mathrm{N}[K^*] \quad \textit{si y sólo si} \quad \alpha x^2 + \beta y^2 = 1 \textit{ tiene solución en } k.$$

DEMOSTRACIÓN: Si $\beta \in k^2$ el teorema es trivial. Supongamos lo contrario, es decir, $K \neq k$. Un elemento cualquiera de K es de la forma $u + v\sqrt{\beta}$, con $u, v \in K$. Supongamos que $\alpha = \mathrm{N}\big(u + v\sqrt{\beta}\,\big) = u^2 - \beta v^2$. Si $u \neq 0$ entonces $\alpha + \beta v^2 = u^2$, luego $\alpha(1/u)^2 + \beta(v/u)^2 = 1$. Si $u = 0$ la ecuación $\alpha x^2 + \beta y^2 = 1$ equivale a $-v^2x^2 + y^2 = 1/\beta$, o sea, a $(y - vx)(y + vx) = 1/\beta$, y tiene por solución a cualquier solución del sistema $y - vx = 1$, $y + vx = 1/\beta$ (que es compatible porque $v \neq 0$).

Recíprocamente, si $\alpha x^2 + \beta y^2 = 1$, como $\beta \notin k^2$, ha de ser $x \neq 0$, y así $\alpha = \mathrm{N}\big(1/x + (y/x)\sqrt{\beta}\,\big)$. ∎

De este modo el teorema [8.25] nos da el comportamiento explícito de (α, β) en el caso $n = 2$ y $k = \mathbb{Q}_p$. Observar que el símbolo de Hilbert puede definirse también para $n = 2$ y $k = \mathbb{R}$, es decir, para $p = \infty$). Trivialmente, tanto la definición de Hasse [8.29] como la definición de Hilbert (formalmente análoga[1] a la definición 13.1) dan lugar al mismo concepto: $(\alpha, \beta) = 1$ si y sólo si $\alpha > 0$ o $\beta > 0$. Observar que para $n > 2$ el caso arquimediano carece de interés, pues para que un cuerpo completo k contenga las raíces n-simas de la unidad ha de ser $k = \mathbb{C}$, con lo que el símbolo de Hilbert se vuelve trivial.

Para probar las propiedades generales del símbolo de Hilbert necesitamos un resultado técnico:

Teorema 13.3 *Sea k un cuerpo que contenga una raíz n-sima primitiva de la unidad. Si $\beta \in k^*$ entonces $-\beta$ y $1 - \beta$ son normas de la extensión $k\big(\sqrt[n]{\beta}\,\big)/k$.*

DEMOSTRACIÓN: Sea $|k\big(\sqrt[n]{\beta}\,\big) : k| = d$. Observemos que

$$x^n - \beta = \prod_{i=0}^{n-1} \big(x - \zeta^i \sqrt[n]{\beta}\,\big).$$

Los factores no son necesariamente conjugados, pero podemos distribuirlos en r clases de conjugación con d factores cada una ($n = rd$). Al evaluar en 0 y en 1 tenemos $-\beta$ y $1 - \beta$ expresados como producto de r normas, luego son normas. ∎

Teorema 13.4 *Sea k un cuerpo p-ádico que contenga una raíz n-sima primitiva de la unidad. Se cumple:*

a) $(\alpha, \beta) = 1$ *si y sólo si* α *es una norma de* $k\big(\sqrt[n]{\beta}\,\big)/k$.

b) $(\alpha_1\alpha_2, \beta) = (\alpha_1, \beta)(\alpha_2, \beta)$.

c) $(\alpha, \beta_1\beta_2) = (\alpha, \beta_1)(\alpha, \beta_2)$.

[1] El símbolo de Artin $(\mathbb{R}/\alpha)$ se define como la identidad en $\mathbb{C}$ si $\alpha > 0$ y la conjugación compleja si $\alpha < 0$.

d) $(-\alpha,\alpha) = (1-\alpha,\alpha) = 1$.

e) $(\alpha,\beta) = (\beta,\alpha)^{-1}$.

f) $(\alpha,\beta) = (\alpha,\alpha+\beta)(\alpha+\beta,\beta)(-1,\alpha+\beta)$ *(supuesto que* $\alpha+\beta \neq 0$*).*

g) El símbolo (α,β) *es continuo en sus dos argumentos.*

DEMOSTRACIÓN: a), b) y c) son inmediatas. d) es consecuencia del teorema anterior.

e) Usando las propiedades anteriores tenemos

$$\begin{aligned}(\alpha,\beta)(\beta,\alpha) &= (\alpha,\beta)(-\beta,\beta)(-\alpha,\alpha)(\beta,\alpha) = (-\alpha\beta,\beta)(-\alpha\beta,\alpha)\\ &= (-\alpha\beta,\alpha\beta) = 1.\end{aligned}$$

f) Sea $\gamma = \alpha+\beta$. Entonces

$$1 = (1-\alpha\gamma^{-1},\alpha\gamma^{-1}) = (\beta\gamma^{-1},\alpha\gamma^{-1}) = (\beta,\alpha)(\beta,\gamma^{-1})(\gamma^{-1},\alpha)(\gamma^{-1},\gamma^{-1}).$$

Por otra parte, $(\gamma^{-1},\gamma^{-1}) = (-\gamma^{-1},\gamma^{-1})(-1,\gamma^{-1}) = (-1,\gamma^{-1})$, luego

$$1 = (\alpha,\beta)^{-1}(\gamma,\beta)(\alpha,\gamma)(-1,\gamma)^{-1} = (\alpha,\beta)^{-1}(\gamma,\beta)(\alpha,\gamma)((-1)^{-1},\gamma).$$

En consecuencia $(\alpha,\beta) = (\alpha,\alpha+\beta)(\alpha+\beta,\beta)(-1,\alpha+\beta)$.

g) El símbolo de Hilbert es continuo en el primer argumento porque, fijado β, el núcleo del homomorfismo $(\ ,\beta)$ es el grupo de normas de la extensión $k\big(\sqrt[n]{\beta}\big)/k$, que es abierto. La continuidad en el segundo argumento es consecuencia de la propiedad e). ∎

Si k es un cuerpo numérico que contiene una raíz n-sima primitiva de la unidad, para cada primo $\mathfrak{p}$ de k tenemos que $k \subset k_\mathfrak{p}$, luego podemos considerar el símbolo de Hilbert de $k_\mathfrak{p}$, al que representaremos por $(\alpha,\beta)_\mathfrak{p}$. Observar que si α, $\beta \in k^*$, entonces $(\alpha,\beta)_\mathfrak{p} = 1$ siempre que $\mathfrak{p}$ no divide ni a α ni a β ni a n. En efecto, en tal caso el primo $\mathfrak{p}$ no se ramifica en la extensión $k\big(\sqrt[n]{\beta}\big)/k$ (por el teorema 7.25) y α es una unidad en $k_\mathfrak{p}$, luego es una norma local y está en el núcleo del homomorfismo de Artin.

Teorema 13.5 (Fórmula del producto de Hilbert) *Sea* k *un cuerpo numérico que contenga una raíz* n*-sima primitiva de la unidad. Sean* α, $\beta \in k^*$. *Entonces*

$$\prod_\mathfrak{p} (\alpha,\beta)_\mathfrak{p} = 1,$$

donde $\mathfrak{p}$ *recorre todos los primos de* k.

DEMOSTRACIÓN: Según la observación precedente, a lo sumo un número finito de factores son distintos de 1, luego el producto está bien definido. Consideremos el símbolo de Artin local

$$\sigma_\mathfrak{p} = \left(\frac{k_\mathfrak{p}\big(\sqrt[n]{\beta}\big)/k_\mathfrak{p}}{\alpha}\right).$$

Los teoremas 8.13 y 8.24 nos dan la relación

$$\prod_{\mathfrak{p}}\sigma_{\mathfrak{p}} = \left(\frac{k(\sqrt[n]{\beta})/k}{\alpha}\right) = 1,$$

pues k^* está contenido en el núcleo del homomorfismo de Artin global. Hay que entender que todos los factores salvo a lo sumo un número finito de ellos son la identidad.

Para cada primo $\mathfrak{p}$ tenemos por definición que $(\alpha,\beta)_{\mathfrak{p}} = \sigma_{\mathfrak{p}}(\sqrt[n]{\beta})/\sqrt[n]{\beta}$. Si tomamos otro primo $\mathfrak{q}$ vemos que

$$\sigma_{\mathfrak{q}}\big(\sigma_{\mathfrak{p}}(\sqrt[n]{\beta})\big) = \sigma_{\mathfrak{q}}\big((\alpha,\beta)_{\mathfrak{p}}\sqrt[n]{\beta}\big) = (\alpha,\beta)_{\mathfrak{p}}\sigma_{\mathfrak{q}}(\sqrt[n]{\beta}) = (\alpha,\beta)_{\mathfrak{p}}(\alpha,\beta)_{\mathfrak{q}}\sqrt[n]{\beta},$$

es decir, $(\sigma_{\mathfrak{p}}\sigma_{\mathfrak{q}})(\sqrt[n]{\beta})/\sqrt[n]{\beta} = (\alpha,\beta)_{\mathfrak{p}}(\alpha,\beta)_{\mathfrak{q}}$. Repitiendo un número finito de veces llegamos a que

$$\prod_{\mathfrak{p}}(\alpha,\beta)_{\mathfrak{p}} = \frac{1}{\sqrt[n]{\beta}}\Big(\prod_{\mathfrak{p}}\sigma_{\mathfrak{p}}\Big)(\sqrt[n]{\beta}) = 1.$$

■

Como veremos en la sección siguiente, esta fórmula contiene en esencia la ley de reciprocidad n-sima.

13.2 El símbolo potencial

Vamos a definir el símbolo potencial n-simo, es decir, la generalización del símbolo de Legendre. Si k es un cuerpo numérico y $\mathfrak{p}$ es un primo no arquimediano en k, diremos que un entero α de k^* es un *resto potencial n-simo* módulo $\mathfrak{p}$ si existe un entero β de k tal que $\alpha \equiv \beta^n \pmod{\mathfrak{p}}$.

Trabajaremos en un cuerpo numérico k que contenga una raíz n-sima primitiva de la unidad ζ. Sea $\mathfrak{p}$ un primo no arquimediano en k que no divida a n, sea $\mathrm{N}\,\mathfrak{p} = m = p^f$ y sea $\overline{k}$ el cuerpo de restos módulo $\mathfrak{p}$. La primera observación que hacemos es que ζ sigue teniendo orden n módulo $\mathfrak{p}$, pues las potencias de ζ son todas las raíces del polinomio $x^n - 1$ y éste sigue siendo separable módulo $\mathfrak{p}$ (es primo con su derivada).

Consideramos el homomorfismo $f : \overline{k}^* \longrightarrow \overline{k}^*$ dado por $f(u) = u^n$. Su núcleo está formado por las n raíces n-simas de la unidad, luego su imagen tiene $(m-1)/n$ elementos, es decir, hay $(m-1)/n$ potencias n-simas módulo $\mathfrak{p}$.

Sea $g : \overline{k}^* \longrightarrow \overline{k}^*$ el homomorfismo dado por $g(u) = u^{(m-1)/n}$. Si a es un generador de $\overline{k}^*$ entonces $a^{(m-1)/n}$ es un generador de $g[\overline{k}^*]$, luego la imagen de g tiene n elementos. Como $u^{(m-1)/n}$ es una raíz n-sima de la unidad para todo u, vemos que la imagen de g es exactamente el grupo de las raíces n-simas de la unidad.

Por otra parte todas las potencias n-simas están en el núcleo de g y, como éste tiene $(m-1)/n$ elementos, resulta que el núcleo es exactamente el grupo de las potencias n-simas.

Esto prueba que si α en un entero de k no divisible entre $\mathfrak{p}$ entonces $\alpha^{(m-1)/n}$ es congruente módulo $\mathfrak{p}$ con una única raíz n-sima de la unidad. Además α es un resto potencial n-simo módulo $\mathfrak{p}$ si y sólo si dicha raíz es 1.

Definición 13.6 Sea k un cuerpo numérico que contenga una raíz n-sima primitiva de la unidad. Sea $\mathfrak{p}$ un primo no arquimediano de k que no divida a n. Para cada entero α de k no divisible entre $\mathfrak{p}$ llamaremos $(\alpha/\mathfrak{p})$ a la única raíz n-sima de la unidad tal que

$$\left(\frac{\alpha}{\mathfrak{p}}\right) \equiv \alpha^{(\mathrm{N}\,\mathfrak{p}-1)/n} \text{ (mód } \mathfrak{p}).$$

Los razonamientos precedentes prueban que $(\alpha/\mathfrak{p}) = 1$ si y sólo si α es un resto potencial n-simo módulo $\mathfrak{p}$. Además, si $\mathfrak{p} \nmid \alpha\beta$, se cumple la relación

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right).$$

Más aún, $(\alpha/\mathfrak{p})$ depende sólo del resto de α módulo $\mathfrak{p}$.

El símbolo potencial está estrechamente relacionado con el símbolo de Hilbert:

Teorema 13.7 *Sea k un cuerpo numérico que contenga una raíz n-sima primitiva de la unidad. Sea $\mathfrak{p}$ un primo no arquimediano en k que no divida a n. Si α es un entero de k primo con $\mathfrak{p}$ entonces*

$$(\beta, \alpha)_{\mathfrak{p}} = \left(\frac{\alpha}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(\beta)}.$$

Demostración: Como $\mathfrak{p}$ no divide ni a α ni a n, el teorema 7.25 nos da que $\mathfrak{p}$ no se ramifica en la extensión $k\big(\sqrt[n]{\alpha}\,\big)/k$, luego, si $\mathfrak{p}$ tiene multiplicidad 1 en π, el símbolo de Artin local

$$\sigma = \left(\frac{k_{\mathfrak{p}}\big(\sqrt[n]{\alpha}\,\big)/k}{\pi}\right)$$

verifica

$$\sigma\big(\sqrt[n]{\alpha}\,\big) \equiv \sqrt[n]{\alpha}^{\,\mathrm{N}\,\mathfrak{p}} \text{ (mód } \mathfrak{p}).$$

(Ver las observaciones tras el teorema de ramificación).

Por consiguiente

$$\frac{\sigma\big(\sqrt[n]{\alpha}\,\big)}{\sqrt[n]{\alpha}} \equiv \sqrt[n]{\alpha}^{\,\mathrm{N}\,\mathfrak{p}-1} \equiv \alpha^{(\mathrm{N}\,\mathfrak{p}-1)/n} \text{ (mód } \mathfrak{p})$$

y concluimos que $(\alpha/\mathfrak{p}) = (\pi, \alpha)_{\mathfrak{p}}$.

Como la extensión $k_\mathfrak{p}\big(\sqrt[n]{\alpha}\,\big)/k_\mathfrak{p}$ es no ramificada, las unidades son normas, y están en el núcleo del homomorfismo de Artin, es decir, si $\beta = \epsilon\pi^{v_\mathfrak{p}(\beta)}$, donde ϵ es una unidad, tenemos que

$$(\beta,\alpha)_\mathfrak{p} = (\pi,\alpha)_\mathfrak{p}^{v_\mathfrak{p}(\beta)} = \left(\frac{\alpha}{\mathfrak{p}}\right)^{v_\mathfrak{p}(\beta)}.$$

■

Equivalentemente, hemos probado que la relación entre el símbolo de Artin y el símbolo potencial es la siguiente:

$$\left(\frac{k\big(\sqrt[n]{\alpha}\,\big)/k}{\mathfrak{p}}\right)\big(\sqrt[n]{\alpha}\,\big) = \left(\frac{\alpha}{\mathfrak{p}}\right)\sqrt[n]{\alpha},$$

bajo las hipótesis $\mathfrak{p}\nmid\alpha$, $\mathfrak{p}\nmid n$.

De aquí se desprende un hecho no trivial: *el valor de* $(\alpha/\mathfrak{p})$ *depende únicamente de la clase de* $\mathfrak{p}$ *módulo el conductor de la extensión* $k\big(\sqrt[n]{\alpha}\,\big)/k$. En el caso $k=\mathbb{Q}$ y $n=2$ esto es una consecuencia importante de la ley de reciprocidad cuadrática, y por ello se puede ver a este resultado como una forma abstracta de la ley de reciprocidad. Notar que hemos llegado a él a partir de las propiedades básicas del símbolo de Artin, es decir, que es una consecuencia de la mera existencia del isomorfismo de Artin. Éste es el motivo por el que a veces se llama ley de reciprocidad a la existencia del isomorfismo de Artin.

Para enunciar la ley de reciprocidad propiamente dicha, necesitamos introducir un símbolo en el que no aparezcan ideales (para así poder intercambiar el "numerador" y el "denominador"). Se trata de la generalización natural del símbolo de Jacobi:

Definición 13.8 Sea k un cuerpo numérico que contenga una raíz n-sima primitiva de la unidad. Sean α y β enteros de k^* primos entre sí y de modo que β sea primo con n. Definimos

$$\left(\frac{\alpha}{\beta}\right) = \prod_\mathfrak{p}\left(\frac{\alpha}{\mathfrak{p}}\right)^{v_\mathfrak{p}(\beta)},$$

donde $\mathfrak{p}$ recorre los primos no arquimedianos de k. (Observar que en los casos en los que $(\alpha/\mathfrak{p})$ no está definido el exponente $v_\mathfrak{p}(\beta)$ es 0, luego se entiende que dichos factores valen 1.

La ley de reciprocidad n-sima es el comportamiento de $(\alpha/\beta)(\beta/\alpha)^{-1}$, donde α y β son enteros de k primos entre sí y primos con n.

De la definición misma del símbolo de Jacobi generalizado se desprende que

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{\mathfrak{p}\nmid n\infty}\left(\frac{\alpha}{\mathfrak{p}}\right)^{v_\mathfrak{p}(\beta)}\left(\frac{\beta}{\mathfrak{p}}\right)^{-v_\mathfrak{p}(\alpha)}.$$

Ahora bien, como α y β son primos entre sí, a lo sumo uno de los dos exponentes de cada factor es no nulo, luego al aplicar el teorema 13.7 obtenemos $(\beta,\alpha)_\mathfrak{p}$ (si el exponente no nulo es el primero), $(\alpha,\beta)_\mathfrak{p}^{-1} = (\beta,\alpha)_\mathfrak{p}$ (si es el segundo) y $(\beta,\alpha)_\mathfrak{p} = 1$ si ambos exponentes son nulos. En resumen:

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{\mathfrak{p}\nmid n\infty}(\beta,\alpha)_\mathfrak{p}.$$

Si α no es primo con n tenemos definido igualmente el símbolo (α/β), pero no el símbolo inverso. En particular, si α sólo es divisible entre primos que dividen a n (incluyendo el caso en que α es una unidad) tenemos, como antes,

$$\left(\frac{\alpha}{\beta}\right) = \prod_{\mathfrak{p}\nmid n\infty}\left(\frac{\alpha}{\mathfrak{p}}\right)^{v_\mathfrak{p}(\beta)} = \prod_{\mathfrak{p}\nmid n\infty}(\beta,\alpha)_\mathfrak{p}.$$

Estas fórmulas pueden parecer ya versiones generales de la ley de reciprocidad y las leyes complementarias, pero no es así. La ley de reciprocidad aparece realmente cuando transformamos estas fórmulas mediante la fórmula del producto de Hilbert:

Teorema 13.9 (Ley de reciprocidad de Artin) *Sea k un cuerpo numérico que contenga a una raíz n-sima primitiva de la unidad.*

a) Si α y β son enteros de k no nulos, primos entre sí y primos con n, entonces

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{\mathfrak{p}\mid n\infty}(\alpha,\beta)_\mathfrak{p}.$$

b) (Ley complementaria) Si α es un entero de k no nulo y divisible a lo sumo entre primos que dividen a n (admitiendo el caso de que sea una unidad) y β es un entero de k no nulo y primo con α y con n, entonces

$$\left(\frac{\alpha}{\beta}\right) = \prod_{\mathfrak{p}\mid n\infty}(\alpha,\beta)_\mathfrak{p}.$$

Veamos cómo se deduce de aquí la ley de reciprocidad cuadrática. Consideramos $k = \mathbb{Q}$ y $n = 2$. Tomamos dos enteros impares u, v primos entre sí que podemos suponer positivos. Entonces usando [8.25] obtenemos que

$$\left(\frac{u}{v}\right)\left(\frac{v}{u}\right)^{-1} = (u,v)_2(u,v)_\infty = (u,v)_2 = (-1)^{(u-1)(v-1)/4}.$$

Igualmente, si v es impar tenemos

$$\left(\frac{2}{v}\right) = (2,v)_2 = (-1)^{(v^2-1)/8}, \qquad \left(\frac{-1}{v}\right) = (-1,v)_2 = (-1)^{(v-1)/2}.$$

Reflexionemos un momento sobre lo que realmente afirma la ley de reciprocidad de Artin: El símbolo de Hilbert $(\alpha,\beta)_\mathfrak{p}$ se calcula a partir del isomorfismo de Artin de la extensión $k_\mathfrak{p}\big(\sqrt[n]{\beta}\big)/k_\mathfrak{p}$. El diferente de esta extensión divide a $n\sqrt[n]{\beta}^{n-1}$ luego, si n es primo con β y $\mathfrak{p}\mid n$, concluimos que $\mathcal{D}_\mathfrak{p}\mid n$ y, por lo tanto, el discriminante cumple $\Delta_\mathfrak{p}\mid n^n$. El teorema del conductor-discriminante nos da para el conductor la relación $\mathfrak{f}_\mathfrak{p}\mid n^n$. Por consiguiente, si $\alpha\equiv\alpha'\ (\text{mód } n^n)$ se cumple $(\alpha,\beta)_\mathfrak{p}=(\alpha',\beta)_\mathfrak{p}$ para todo primo $\mathfrak{p}\mid n$. Si exigimos además que $\alpha\equiv^*\alpha'\ (\text{mód } n^n\infty)$ la conclusión vale también para los primos arquimedianos. Por simetría todo es válido para β también, es decir:

> *Si α y β son enteros de k primos con n y primos entre sí, el valor de $(\alpha/\beta)(\beta/\alpha)^{-1}$ depende únicamente de los restos de α y β módulo $n^n\infty$.*

Así pues, para determinar explícitamente la relación entre dos símbolos potenciales inversos sólo hace falta evaluar un número finito de símbolos de Hilbert $(\alpha,\beta)_\mathfrak{p}$, luego el teorema de Artin nos permite obtener en cada caso una ley similar a la ley de reciprocidad cuadrática. Esto quedará más claro en las secciones siguientes. De momento añadamos que lo mismo es válido para la ley complementaria, aunque ahora el módulo a considerar puede ser mayor que n^n (notar que podemos exigir que $v_\mathfrak{p}(\beta)<n$).

13.3 La ley de reciprocidad cúbica

En esta sección k será el tercer cuerpo ciclotómico, es decir, $k=\mathbb{Q}\big(\sqrt{-3}\big)$. Sea ζ una raíz cúbica primitiva de la unidad y $\lambda=1-\zeta$ el divisor primo de 3 en k. Es conocido que k tiene factorización única. En principio, la ley de reciprocidad de Artin y la ley complementaria se reducen en este caso a las fórmulas

$$\left(\frac{\alpha}{\beta}\right) = (\alpha,\beta)_\lambda\left(\frac{\beta}{\alpha}\right),$$
$$\left(\frac{\alpha}{\beta}\right) = (\alpha,\beta)_\lambda,$$

donde en la primera fórmula α y β son enteros de k primos entre sí y primos con λ, mientras que en la segunda α no es divisible entre primos distintos de λ y β es primo con lambda.

Para obtener fórmulas explícitas hemos de evaluar los símbolos de Hilbert $(\alpha,\beta)_\lambda$. El primer paso será reducir el problema a un número finito de casos.

Teorema 13.10 *Si α y β son enteros de k primos con λ, entonces el valor del símbolo de Hilbert $(\alpha,\beta)_\lambda$ depende únicamente de los restos de α y β módulo λ^3. Si α no es divisible entre primos distintos de λ y β es primo con λ entonces $(\alpha,\beta)_\lambda$ depende únicamente de α y del resto de β módulo λ^4.*

DEMOSTRACIÓN: Basta probar que si $\alpha \equiv 1 \pmod{\lambda^3}$ y β es primo con λ entonces $(\alpha,\beta)_\lambda = 1$, y que si $\alpha \equiv 1 \pmod{\lambda^4}$ y β no es divisible entre primos distintos de λ entonces $(\alpha,\beta)_\lambda = 1$ (invertimos la notación en el segundo caso para llevar las dos pruebas simultáneamente).

Hemos de considerar el cuerpo $K = k_\lambda\big(\sqrt[3]{\beta}\,\big)$ y el símbolo de Artin

$$\sigma = \left(\frac{K/k_\lambda}{\alpha}\right).$$

En el segundo caso podemos suponer que la multiplicidad de λ en β es igual a 1 o 2, pues si eliminamos los cubos de β la extensión $k_\lambda\big(\sqrt[3]{\beta}\,\big)$ no varía. Más aún, podemos suponer que la multiplicidad es 1 pues, si es 2, entonces $K = k_\lambda\big(\sqrt[3]{\beta}\,\big) = k_\lambda\big(\sqrt[3]{\beta^2}\,\big)$ y eliminamos λ^3 de la última raíz.

El diferente de la extensión K/k_λ divide a $3\sqrt[3]{\beta^2}$, luego el discriminante divide a $\mathrm{N}(3\sqrt[3]{\beta^2}) = 27\,\mathrm{N}\big(\sqrt[3]{\beta}\,\big)^2 = \lambda^6$, λ^8 (según si estamos en el primer caso o el segundo). El teorema 10.35 nos da para el conductor la relación $\mathfrak{f} \mid \lambda^3$, λ^4, luego $\alpha \equiv 1 \pmod{\mathfrak{f}}$ y basta aplicar la definición de conductor. ∎

Hay $\Phi(\lambda^3) = 2\cdot 3^2 = 18$ clases de unidades módulo λ^3, luego tenemos reducida la ley de reciprocidad cúbica a $18\cdot 18 = 324$ casos (171 si consideramos la simetría). Afortunadamente, todavía podemos hacer una reducción considerable. Para empezar observemos que los elementos

$$\{\pm 1, \pm 2, \pm 4\} \times \{1, \zeta, \zeta^2\}.$$

son representantes de las clases de unidades módulo λ^3. En efecto, por una parte, dos enteros racionales son congruentes módulo λ^3 si y sólo si lo son módulo 9, luego las clases de ± 1, ± 2 y ± 4 son distintas dos a dos. Por otra parte, es claro que ζ tiene orden 3 módulo λ^3 (pues $\lambda^3 \nmid \zeta - 1 = \lambda$). Finalmente, ζ no es congruente con un entero racional módulo λ^3 o, de lo contrario, todos los enteros de k serían congruentes con enteros racionales módulo λ^3 y habría 9 clases de congruencia, en lugar de $\mathrm{N}(\lambda^3) = 27$. Por lo tanto los dos subgrupos que hemos localizado son distintos y su producto es directo.

Vamos a calcular los símbolos (ζ/β). Para ello observamos que éstos dependen únicamente del ideal generado por el "denominador", de modo que si multiplicamos β por una unidad de k el símbolo no se altera. Así pues, basta calcular, por ejemplo, $(\zeta/1) = 1$, $(\zeta/2) = \zeta^{(\mathrm{N}(2)-1)/3} = \zeta$ (aquí usamos que 2 es primo en k), y $(\zeta/4) = (\zeta/2)^2 = \zeta^2$. La tabla completa es, por consiguiente:

$\beta \pmod{\lambda^3}$	(ζ/β)
$\pm 1,\quad \pm\zeta,\quad \pm\zeta^2$	1
$\pm 2,\quad \pm 2\zeta,\quad \pm 2\zeta^2$	ζ
$\pm 4,\quad \pm 4\zeta,\quad \pm 4\zeta^2$	ζ^2

Puesto que -1 es un cubo, se cumple $(-1/\pi) = 1$ para todo primo π de k primo con λ, luego también $(-1/\beta) = 1$ para todo entero β de k primo con λ. En particular sabemos calcular (ϵ/β) para las seis unidades ϵ de k. Esto hace que

a la hora de manipular símbolos (α/β) podamos sustituir α y β por cualquiera de sus asociados (en el caso de β trivialmente). Ahora conviene observar que ζ tiene orden 3 módulo 3 (lo hemos visto módulo λ^3, pero el razonamiento vale igual módulo 3), luego $-\zeta$ tiene orden 6 módulo 3. Esto significa que las seis unidades de k son representantes de las seis clases de unidades módulo 3 o, dicho de otro modo, que, pasando a los asociados oportunos, siempre podemos tomar, por ejemplo, $\alpha \equiv \beta \equiv 1$ (mód 3).

Teorema 13.11 (Ley de reciprocidad cúbica) *Sean α y β enteros de k primos entre sí y primos con λ. Si $\alpha \equiv \beta \equiv 1$ (mód 3) entonces $(\alpha/\beta) = (\beta/\alpha)$.*

DEMOSTRACIÓN: Si $\alpha \equiv 1$ (mód 3), entonces $\alpha \equiv 1, -2, 4$ (mód λ^3), y lo mismo vale para β, luego basta probar el teorema cuando α y β toman estos tres valores. Podemos suponer obviamente que $\alpha \neq \beta$.

Por la ley de reciprocidad, lo que hemos de probar es que $(\alpha, \beta)_\lambda = 1$. Esto es trivial si uno de los argumentos es 1, luego sólo queda el caso $(-2, 4)_\lambda = 1$. Ahora bien, $(-2, 4)_\lambda = (-2, 2)_\lambda^2 = 1$ por la propiedad d) del teorema 13.4. ∎

Observar que, como $(-1, \beta) = 1$ para cualquier β (porque -1 es un cubo), la ley de reciprocidad vale igualmente si α o β es congruente con -1 (mód 3). En otras palabras, basta con que α y β sean congruentes con enteros racionales módulo 3.

Nos falta determinar el valor de (λ/α) cuando α es primo con λ. Por el teorema 13.10 basta considerar los 54 posibles restos de α módulo 9. Agrupados en bloques de 6 asociados quedan 9 clases a considerar, por ejemplo las que cumplen $\alpha \equiv 1$ (mód 3). Veremos que, debidamente elegidos, dos cálculos serán suficientes.

Por ejemplo, tomemos $\alpha = 1 - 3\zeta$. Como $\mathrm{N}(\alpha) = 13$, tenemos que α es primo y, por definición del símbolo potencial

$$\left(\frac{\lambda}{\alpha}\right) \equiv \lambda^4 = 9\zeta^2 \text{ (mód } 1 - 3\zeta)$$

y, como $9\zeta^2 - 1 = (3\zeta + 1)(3\zeta - 1)$, concluimos que $(\lambda/\alpha) = 1$.

Así pues, la clase de $1 - 3\zeta$ (o la de $1 + 6\zeta$) está en el núcleo del símbolo potencial (λ/α), luego también lo está su cuadrado (mód 9), que es $1 + 3\zeta$. En resumen, los números

$$\alpha = 1, \quad 1 + 3\zeta, \quad 1 + 6\zeta,$$

cumplen $(\lambda/\alpha) = 1$.

Ahora calculamos $(\lambda/2) \equiv \lambda = 1 - \zeta$ (mód 2), de donde $(\lambda/2) = \zeta^2$. Por consiguiente también $(\lambda/7) = (\lambda/-2) = \zeta^2$.

Con esto ya podemos completar la tabla siguiente:

α (mód 9)			(λ/α)
1	$1 + 3\zeta$	$1 + 6\zeta$	1
4	$4 + 3\zeta$	$4 + 6\zeta$	ζ
7	$7 + 3\zeta$	$7 + 6\zeta$	ζ^2

Tenemos la primera fila y el 7 de la última. La tercera fila sale de multiplicar la primera por 7. La segunda fila sale por exclusión o, alternativamente, obtenemos el 4 como el cuadrado de 7 y el resto de la fila multiplicando la tercera por 7.

Así tenemos completamente descrita la reciprocidad cúbica. A partir de ella podemos obtener resultados parciales sobre $\mathbb{Z}$. En primer lugar consideremos un primo racional $p \equiv 1 \pmod 3$. Sea π un divisor primo de p en k. Entonces $\mathrm{N}(\pi) = p$, luego el grado de inercia es $f = 1$. Esto implica que todo entero de k es congruente con un entero racional módulo p. Así pues, si n es un entero racional primo con p se cumple $(n/\pi) = 1$ si y sólo si existe un entero racional x tal que $x^3 \equiv n \pmod \pi$, lo que a su vez equivale a que existe un entero racional x tal que $x^3 \equiv n \pmod p$.

Si $p \equiv -1 \pmod 3$ entonces p es primo en k y la afirmación anterior es cierta trivialmente: por una parte $(n/p) = 1$ para todo entero racional n (del hecho de que n y p son invariantes por conjugación se sigue fácilmente que (n/p) también lo es); por otra parte todo entero racional n es un resto cúbico módulo p (ζ no es congruente con un entero módulo p, o de lo contrario todo entero de k lo sería, y no es el caso, luego $\mathbb{Z}/p\mathbb{Z}$ no contiene raíces primitivas de la unidad, luego la aplicación $x \mapsto x^3$ es inyectiva, y por consiguiente biyectiva).

Vemos, pues, que los símbolos potenciales sirven para decidir si un entero racional es un resto cúbico en cualquier $\mathbb{Z}/p\mathbb{Z}$.

Ejemplo Vamos a determinar el carácter cúbico de 17 módulo 31.

Como $31 \equiv 1 \pmod 3$ el problema no es trivial. Un divisor primo de 31 en k es $\pi = \zeta - 5$. Observemos que $\zeta - 5 \equiv \zeta + 1 = -\zeta^2 \pmod 3$, luego, multiplicando por $-\zeta$, se cumple $-\zeta^2 + 5\zeta = 6\zeta + 1 \equiv 1 \pmod 3$. Así:

$$\left(\frac{17}{\zeta-5}\right) = \left(\frac{3\zeta+2}{6\zeta+1}\right) = \left(\frac{6\zeta+1}{3\zeta+2}\right) = \left(\frac{-3}{3\zeta+2}\right) = \left(\frac{\zeta}{3\zeta+2}\right)^2 \left(\frac{\lambda}{3\zeta+2}\right)^2.$$

Ahora observamos que $3\zeta + 2 \equiv 3(\zeta - 1) + 5 \equiv 5 \pmod \lambda^3$, por lo que $(\zeta/3\zeta + 2) = \zeta^2$, y por otra parte $-(3\zeta + 2) \equiv 6z + 7 \pmod 9$, luego se cumple $(\lambda/3\zeta + 2) = \zeta^2$. En definitiva

$$\left(\frac{17}{\zeta-5}\right) = \zeta^2,$$

luego 17 no es un resto cúbico módulo 31. ∎

Ejemplo Vamos a calcular el carácter cúbico de 2 módulo 31.

Como antes:

$$\left(\frac{2}{\zeta-5}\right) = \left(\frac{2}{6\zeta+1}\right) = \left(\frac{6\zeta+1}{2}\right) = \left(\frac{1}{2}\right) = 1.$$

Por lo tanto 2 es un resto cúbico módulo 31. ∎

Ejemplo Al empezar el capítulo mencionamos una conjetura de Euler: si un primo p cumple $p \equiv 1 \pmod 3$ entonces 2 es un resto cúbico módulo p si y sólo si $p = a^2 + 27b^2$. Esto lo obtuvimos ya en el capítulo 11 a partir de la teoría de las formas cuadráticas. Ahora daremos una prueba basada en la reciprocidad cúbica.

Factorizamos $p = \pi\pi'$. Multiplicando por una unidad podemos exigir que $\pi \equiv 1 \pmod 3$. Entonces 2 es un resto cúbico módulo 3 si y sólo si $(2/\pi) = 1$. Por la ley de reciprocidad y la definición del símbolo potencial

$$\left(\frac{2}{\pi}\right) = \left(\frac{\pi}{2}\right) \equiv \pi \pmod 2,$$

luego 2 es un resto cúbico módulo p si y sólo si p es divisible entre un primo $\pi \equiv 1 \pmod 3$, $\pi \equiv 1 \pmod 2$.

En tal caso, $\pi = 6u+1+6v\zeta$ o, equivalentemente, $\pi = 6u+1-3v+3v\sqrt{-3}$. Haciendo $a = 6u + 1 - 3v$, $b = v$, concluimos que $p = \mathrm{N}(\pi) = a^2 + 27b^2$.

Recíprocamente, si $p = a^2 + 27b^2$, ciertamente $3 \nmid a$ y, eligiendo el signo, podemos exigir que $a \equiv 1 \pmod 3$. Entonces $\pi = a+3b+6b\zeta$ cumple $\mathrm{N}(\pi) = p$, $\pi \equiv a \equiv 1 \pmod 3$, $\pi \equiv a+b \equiv 1 \pmod 2$ (si a y b fueran ambos pares o ambos impares p sería par). ∎

Ejemplo Vamos a caracterizar los primos $p \equiv 1 \pmod 3$ módulo los cuales 3 es un resto cúbico.

Sea π un divisor primo de p en k, que podemos tomar $\pi \equiv 1 \pmod 3$. Se cumplirá que 3 es un resto cúbico módulo p si y sólo si

$$1 = \left(\frac{3}{\pi}\right) = \left(\frac{-3}{\pi}\right) = \left(\frac{\zeta}{\pi}\right)^2 \left(\frac{\lambda}{\pi}\right)^2.$$

COnsiderando los 9 restos posibles de π módulo 9 concluimos que esto ocurre si y sólo si $\pi \equiv 1, 4, 7 \pmod 9$, o sea, si y sólo si $\pi = a+9b\zeta$, con $a \equiv 1 \pmod 3$. Razonando como en el ejemplo anterior es fácil ver que esto sucede si y sólo si $p = a^2 - 9ab + 81b^2$ (equivalentemente, pasando a una forma reducida, si y sólo si $p = a^2 + ab + 61y^2$). ∎

13.4 La ley de reciprocidad bicuadrática

En esta sección $k = \mathbb{Q}(i)$. El anillo de los enteros de k es el anillo $\mathbb{Z}[i]$ de los enteros de Gauss, y es un dominio de factorización única. El primo divisor de 2 es $\lambda = 1 + i$. Tenemos cuatro unidades: ± 1, $\pm i$, que recorren las cuatro clases de unidades módulo λ^3, luego cada entero de Gauss tiene un único asociado que cumple $\alpha \equiv 1 \pmod{\lambda^3}$. Observemos que si $\alpha = a + bi$, entonces la condición $\alpha \equiv 1 \pmod{\lambda^3}$ equivale a que

$$\frac{a-1+bi}{2(1+i)} = \frac{a+b-1}{4} + \frac{b-a+1}{4}i \in \mathbb{Z}[i],$$

o sea, a que $a+b \equiv 1 \pmod 4$ y $b-a \equiv 1 \pmod 4$. Es fácil ver que a su vez esto equivale a que

$$a \equiv 1 \pmod 4 \text{ y } b \equiv 0 \pmod 4 \quad \text{o bien} \quad a \equiv -1 \pmod 4 \text{ y } b \equiv 2 \pmod 4.$$

Los símbolos potenciales de las unidades son fáciles de calcular: si π es un primo de Gauss:

$$\left(\frac{i}{\pi}\right) = i^{(\mathrm{N}(\pi)-1)/4}, \qquad \left(\frac{-1}{\pi}\right) = (-1)^{(\mathrm{N}(\pi)-1)/4}.$$

Si $\pi = a+bi \equiv 1 \pmod{\lambda^3}$ es fácil comprobar que $(\mathrm{N}(\pi)-1)/4$ y $(a-1)/2$ tienen la misma paridad, por lo que es más práctica la fórmula

$$\left(\frac{-1}{\pi}\right) = (-1)^{(a-1)/2}.$$

Teorema 13.12 *Si α y β son enteros de Gauss primos con 2 entonces el símbolo de Hilbert $(\alpha,\beta)_\lambda$ sólo depende de los restos de α y β módulo 16. El símbolo de Hilbert $(\alpha,\lambda)_\lambda$ sólo depende del resto de α módulo 8λ.*

Demostración: El diferente de la extensión $k_\lambda\big(\sqrt[4]{\beta}\big)/k_\lambda$ divide a $4\sqrt[4]{\beta}^3$. Si la extensión tiene grado 4 el discriminante divide a 4^4 y, por el teorema del conductor-discriminante, teniendo en cuenta que la extensión es cíclica, $\mathfrak{f}^2 \mid 4^4$ y así $\mathfrak{f} \mid 16$. Si la extensión es cuadrática o trivial se llega al mismo resultado.

Por lo tanto $(\alpha,\beta)-\lambda$ sólo depende del resto de α módulo 16. Por simetría lo mismo vale para β (ver más detalles en la prueba del teorema 13.10).

Si $\beta = \lambda$, la extensión $k_\lambda\big(\sqrt[4]{\lambda}\big)/k_\lambda$ es completamente ramificada y $\sqrt[4]{\lambda}$ es un divisor primo de λ. Por el teorema 3.11 tenemos que $\sqrt[4]{\lambda}$ genera el anillo de enteros de $k_\lambda\big(\sqrt[4]{\lambda}\big)$, luego por el teorema 3.8 el diferente es exactamente $4\sqrt[4]{\lambda}^3$ y el discriminante es $4^4\lambda^3$.

Por el mismo argumento, el discriminante de $k_\lambda\big(\sqrt{\lambda}\big)/k_\lambda$ es 4λ y por el teorema del conductor-discriminante 4λ es también el conductor de esta extensión intermedia. Al aplicar este mismo teorema a la extensión bicuadrática obtenemos la relación $4^4\lambda^3 = \mathfrak{f}^2 4\lambda$, de donde $\mathfrak{f} = 8\lambda$ y se concluye como en el primer caso. ∎

Para determinar la ley de reciprocidad bicuadrática tenemos $\Phi(16) = 27$ clases a considerar. Como podemos limitarnos a los enteros $\alpha \equiv 1 \pmod{\lambda^3}$, el número de clases se reduce a la cuarta parte: $2^5 = 32$. Identificando $a+bi = (a,b)$, un conjunto de representantes para las 32 clases es

$$\{1,5,9,13\} \times \{0,4,8,12\} \cup \{3,7,11,15\} \times \{2,6,10,14\}.$$

(Los 16 primeros cumplen $\alpha \equiv 1 \pmod 4$ y los restantes $\alpha \equiv -1+2i \pmod 4$, que son las condiciones necesarias y suficientes que hemos obtenido al principio de la sección.)

Teorema 13.13 (Ley de reciprocidad bicuadrática) *Si α y β son enteros de Gauss primos entre sí y $\alpha \equiv \beta \equiv 1$ (mód λ^3) entonces*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = (-1)^{\mathrm{N}(\alpha)-1)(\mathrm{N}(\beta)-1)/16}.$$

DEMOSTRACIÓN: Si $\alpha = a + bi$ y $\beta = c + di$, ya hemos comentado que $(\mathrm{N}(\alpha) - 1)/4$ tiene la misma paridad que $(a-1)/2$, luego el exponente del segundo miembro puede sustituirse por $(a-1)(c-1)/4$. Esto significa que $(\alpha/\beta) = (\beta/\alpha)$ si y sólo si uno de los dos argumentos es congruente con 1 módulo 4 y $(\alpha/\beta) = -(\beta/\alpha)$ si ambos son congruentes con $3 + 2i$. Esto es lo que en la práctica hay que comprobar.

El conjunto de las clases de unidades $\alpha \equiv 1$ (mód λ^3) módulo 16 es un grupo G de 32 elementos. El conjunto de las clases de unidades $\alpha \equiv 1$ (mód 4) es un subgrupo H de 16 elementos. Hemos de probar que $(\alpha, \beta)_\lambda = 1$ si uno de los argumentos está en H y $(\alpha, \beta)_\lambda = -1$ en caso contrario.

En primer lugar probaremos que el símbolo de Hilbert es trivial en H. Como no estamos dispuestos a calcular $16^2 = 256$ pares analizamos la estructura de H. Por ejemplo, vemos que

$$\langle [5] \rangle = \{[1], [5], [9], [13]\}, \quad \langle [5 + 4i] \rangle = \{[1], [5 + 4i], [9 + 8i], [13 + 12i]\}$$

y, como tienen intersección trivial, concluimos que $H = \langle [5], [5 + 4i] \rangle$, luego basta probar que el símbolo de Hilbert toma el valor 1 sobre los cuatro pares formados con estos dos generadores. Si α es cualquiera de ellos,

$$(\alpha, \alpha)_\lambda = (-\alpha, \alpha)_\lambda (-1, \alpha)_\lambda = \left(\frac{-1}{\alpha}\right) = (-1)^{(a+1)/2} = 1.$$

Sólo falta calcular $(5, 5 + 4i)_\lambda$. Para ello usamos el apartado f) de 13.4:

$$(5, 4i)_\lambda = (5, 5 + 4i)_\lambda (5 + 4i, 4i)_\lambda (-1, 5 + 4i)_\lambda. \tag{13.1}$$

Para calcular los símbolos que han aparecido podemos usar la ley complementaria:

$$(4i, 5)_\lambda = \left(\frac{4i}{5}\right) = \left(\frac{4i}{1 + 2i}\right)\left(\frac{4i}{1 - 2i}\right).$$

Por definición del símbolo potencial $(4i/1 + 2i) \equiv 4i$ (mód $1 + 2i$), de donde claramente $(4i/1 + 2i) = -i$. Del mismo modo $(4i/1 - 2i) = -i$, luego llegamos a que $(4i, 5)_\lambda = -1$. Por otra parte,

$$(4i, 5 + 4i)_\lambda = \left(\frac{4i}{5 + 4i}\right) \equiv (4i)^{10} \equiv -1 \text{ (mód } 5 + 4i),$$

luego $(4i, 5 + 4i)_\lambda = -1$. Finalmente, $(-1, 5 + 4i)_\lambda = (-1)^{(5-1)/2} = 1$.

Sustituyendo en (13.1) obtenemos $(5, 5 + 4i)_\lambda = 1$.

El paso siguiente es demostrar que $(\alpha, \beta)_\lambda = 1$ si $[\alpha] \in H$ y $[\beta] \notin H$.

Tomemos por ejemplo $\gamma = 3 + 2i$. Todo elemento de $G \setminus H$ es de la forma $[\beta\gamma]$, para un cierto $\beta \in H$. Hemos de probar que $(\alpha, \beta\gamma)_\lambda = 1$ para todas las clases $[\alpha]$, $[\beta] \in H$. Por la parte ya probada basta verlo para los pares $(\alpha, \gamma)_\lambda$, con $[\alpha] \in H$. Más aún, es fácil ver que $H = \langle [5], [\gamma^2] \rangle$, por lo que basta probar que $(5, \gamma)_\lambda = (\gamma^2, \gamma)_\lambda = 1$. Ahora bien,

$$(\gamma^2, \gamma)_\lambda = (\gamma, \gamma)_\lambda^2 = (-1, \gamma)_\lambda^2 = (\pm 1)^2 = 1.$$

Para calcular $(5, 3 + 2i)_\lambda$ usamos la misma técnica que antes:

$$(2 - 2i, 3 + 2i)_\lambda = (5, 3 + 2i)_\lambda (2 - 2i, 5)_\lambda (-1, 5)_\lambda,$$

$$(2 - 2i, 3 + 2i)_\lambda = \left(\frac{2 - 2i}{3 + 2i}\right) \equiv (2 - 2i)^3 \equiv -5 \equiv -3 - 3i \pmod{3 + 2i},$$

de donde $(2 - 2i, 3 + 2i)_\lambda = -i$. Por otra parte

$$(2 - 2i, 5)_\lambda = \left(\frac{2 - 2i}{5}\right) = \left(\frac{2 - 2i}{1 + 2i}\right)\left(\frac{2 - 2i}{1 - 2i}\right).$$

Por definición de los símbolos potenciales

$$\left(\frac{2 - 2i}{1 + 2i}\right) \equiv 2 - 2i \pmod{1 + 2i}, \qquad \left(\frac{2 - 2i}{1 - 2i}\right) \equiv 2 - 2i \pmod{1 - 2i},$$

luego

$$\left(\frac{2 - 2i}{1 + 2i}\right) = -i, \qquad \left(\frac{2 - 2i}{1 - 2i}\right) = 1.$$

Así mismo

$$(-1, 5)_\lambda = \left(\frac{-1}{1 + 2i}\right)\left(\frac{-1}{1 - 2i}\right) = 1.$$

De estos cálculos se sigue que $(5, 3 + 2i)_\lambda = 1$.

Para terminar hay que probar que $(\alpha, \beta)_\lambda = -1$ si $[\alpha]$, $[\beta] \notin H$. Equivalentemente, hay que ver que $(\alpha\gamma, \beta\gamma)_\lambda = -1$ si $[\alpha]$, $[\beta] \in H$. Por la parte ya probada esto se reduce a probar que $(\gamma, \gamma)_\lambda = -1$ y, en efecto:

$$(\gamma, \gamma)_\lambda = (-1, \gamma)_\lambda = \left(\frac{-1}{3 + 2i}\right) = -1.$$

■

Nos falta calcular (λ/α). Hemos de considerar las $\Phi(8\lambda)/4 = 8$ clases módulo 8λ de unidades $\alpha \equiv 1 \pmod{\lambda^3}$. El resultado es el que muestra la tabla siguiente:

$\alpha \pmod{8\lambda}$				(λ/α)
1	$7 + 2i$	$5 + 4i$	$11 + 6i$	1
5	$11 + 2i$	$9 + 4i$	$15 + 6i$	i
9	$15 + 2i$	$13 + 4i$	$3 + 6i$	-1
13	$3 + 2i$	$1 + 4i$	$7 + 6i$	$-i$

Sólo es necesario calcular dos símbolos potenciales, a saber, $(\lambda/5) = i$, $(\lambda/7+2i) = 1$. Sus potencias nos dan la primera columna y la primera fila respectivamente. El resto de la tabla se completa por multiplicatividad.

Eisenstein encontró la expresión siguiente para la ley complementaria: Si $\alpha = a + bi \equiv 1 \pmod{\lambda^3}$ entonces

$$\left(\frac{\lambda}{\alpha}\right) = i^{(a-b-b^2-1)/4}.$$

Para probarla basta comprobar que el miembro derecho depende sólo del resto de α módulo 8λ (o sea, que toma el mismo valor si sustituimos (a,b) por $(a+8k, b\pm 8k)$) y que la igualdad se cumple en los 16 casos de la tabla.

Ejercicio: Comprobar que si $\alpha = a + bi \equiv 1 \pmod{\lambda^3}$ entonces $(2/\alpha) = i^{-b/2}$.

Al igual que la reciprocidad cúbica, la reciprocidad bicuadrática tiene reflejos en $\mathbb{Z}$. Si un primo p cumple $p \equiv -1 \pmod 4$ entonces los restos bicuadráticos módulo p coinciden con los restos cuadráticos. En efecto, p se conserva primo en $\mathbb{Z}[i]$, luego i no es congruente con un entero racional módulo p (en caso contrario $\mathbb{Z}[i]/(p)$ tendría p elementos). Por lo tanto $\mathbb{Z}/p\mathbb{Z}$ no contiene raíces bicuadráticas de la unidad. El núcleo del homomorfismo $x \mapsto x^4$ (en $(\mathbb{Z}/p\mathbb{Z})^*$) tiene dos elementos, luego la mitad exactamente de las clases de $(\mathbb{Z}/p\mathbb{Z})^*$ son restos bicuadráticos. Lo mismo es cierto para los restos cuadráticos y, como todo resto bicuadrático es un resto cuadrático, concluimos que un entero racional es un resto bicuadrático módulo p si y sólo si es un resto cuadrático.[2]

Por otra parte, si $p \equiv 1 \pmod 4$ y π es un primo de Gauss que lo divida, es claro que un entero racional n es una potencia cuarta en $\mathbb{Z}/p\mathbb{Z}$ si y sólo si $(n/\pi) = 1$, por lo que la reciprocidad bicuadrática puede usarse para decidir si se da el caso.

Ejemplo Probar que 31 es un resto bicuadrático módulo 41.

Un divisor primo de 41 es $5+4i$. Así pues, hemos de calcular

$$\begin{aligned}
\left(\frac{31}{5+4i}\right) &= \left(\frac{6-20i}{5+4i}\right) = -\left(\frac{5+4i}{3-10i}\right) = -\left(\frac{8-6i}{3-10i}\right) = -i\left(\frac{4-3i}{3-10i}\right)\\
&= -\left(\frac{-3-4i}{3-10i}\right) = -\left(\frac{3-10i}{-3-4i}\right) = -\left(\frac{6-6i}{-3-4i}\right)\\
&= -\left(\frac{3}{-3-4i}\right) = -\left(\frac{-3}{-3-4i}\right) = -\left(\frac{-3-4i}{-3}\right) = -\left(\frac{-4i}{-3}\right)\\
&= -\left(\frac{-1}{-3}\right)\left(\frac{2}{-3}\right)^2\left(\frac{i}{-3}\right) = 1.
\end{aligned}$$

■

[2]Por otra parte, todo entero racional n es la potencia cuarta módulo p de un entero de k. En efecto, el grupo multiplicativo módulo p en k es un grupo cíclico de p^2-1 elementos. Si g es un generador, entonces $(\mathbb{Z}/p\mathbb{Z})^*$ está generado por g^{p+1} y, como $4 \mid p+1$, todos sus elementos son potencias cuartas. Por lo tanto el símbolo bicuadrático toma siempre el valor 1 sobre los enteros racionales.

Ejemplo Sea $p \equiv 1 \pmod 8$. Entonces $p = A^2 + B^2$, con A, $B \in \mathbb{Z}$. Probar que 2 es un resto bicuadrático módulo p si y sólo si $AB \equiv 0 \pmod 8$.

La condición $AB \equiv 0 \pmod 8$ no se altera si intercambiamos A y B o si cambiamos los signos. Por lo tanto podemos suponer que A es impar y, más aún, que $A \equiv 1 \pmod 4$. Entonces $A^2 \equiv 1 \pmod 8$, luego $B^2 \equiv 0 \pmod 8$ y $B \equiv 0 \pmod 4$. Esto implica que $\pi = A + Bi \equiv 1 \pmod{\lambda^3}$. Ahora basta observar que

$$(2/\pi) = i^{-B/2} = (-1)^{B/4} = (-1)^{AB/4}.$$

■

Capítulo XIV

Cohomología de grupos

En los próximos capítulos presentaremos un nuevo enfoque de la teoría de cuerpos de clases, basado en las técnicas de la cohomología de grupos que aquí introducimos. Aunque se trata de un punto de vista mucho más abstracto, su interés reside fundamentalmente en que permite construir la teoría local independientemente de la teoría global, clarifica la relación entre ambas y permite trabajar en un marco más amplio, de modo que los resultados son aplicables a otros cuerpos distintos de los cuerpos numéricos y los cuerpos p-ádicos.

14.1 Preliminares al álgebra homológica

Recogemos aquí los resultados algebraicos que vamos a necesitar en lo sucesivo. Comencemos con unas observaciones generales sobre anillos y módulos:

Todos los anillos que consideraremos serán unitarios, aunque no necesariamente conmutativos. Todos los homomorfismos de anillos cumplirán por definición que $f(1) = 1$.

Recordemos que si un anillo A no es conmutativo hay dos clases de A-módulos: izquierdos y derechos, según que el producto escalar sea de la forma $A \times M \longrightarrow M$ o de la forma $M \times A \longrightarrow M$.

Si el anillo A es conmutativo todo A-módulo izquierdo se convierte en un A-módulo derecho (y viceversa) estableciendo que $ma = am$, para todo $a \in A$ y todo $m \in M$. Si A no es conmutativo este cambio hace que se cumplan todos los axiomas de módulo derecho excepto la propiedad asociativa, que quedaría en la forma $(ma)b = m(ba)$.

Si A y B son anillos un A-B-bimódulo M es un A-módulo izquierdo que es a la vez un B-módulo derecho y además cumple $(am)b = a(mb)$ para todo $a \in A$, $b \in B$, $m \in M$.

Productos tensoriales El producto tensorial de módulos es un concepto que aparece en numerosas ramas del álgebra moderna, especialmente en el álgebra multilineal. Aquí probaremos los únicos resultados que necesitamos para desarrollar la cohomología de grupos.

Definición 14.1 Sea A un anillo, M un A-módulo derecho y N un A-módulo izquierdo. Sea L un grupo abeliano libre con base $M \times N$. Llamaremos *producto tensorial* de M por N al grupo cociente de L sobre el subgrupo generado por los elementos de la forma

$$\begin{array}{ll} (m_1+m_2,n)-(m_1,n)-(m_2,n), & m_1,m_2\in M, n\in N,\\ (m,n_1+n_2)-(m,n_1)-(m,n_2), & m\in M, n_1,n_2\in N,\\ (ma,n)-(m,an), & m\in M, n\in N, a\in A. \end{array}$$

Lo representaremos por $M \otimes_A N$. Así mismo, la clase de equivalencia del par (m,n) en $M \otimes_A N$ la representaremos por $m \otimes n$ (el símbolo $\otimes$ se lee "tensor").

Así pues, $M \otimes_A N$ es un grupo abeliano generado por los elementos $m \otimes n$, que obviamente cumplen las relaciones

$$\begin{array}{ll} (m_1+m_2)\otimes n = m_1\otimes n + m_2\otimes n, & m_1,m_2\in M, n\in N,\\ m\otimes (n_1+n_2) = m\otimes n_1 + m\otimes n_2, & m\in M, n_1,n_2\in N,\\ ma\otimes n = m\otimes an, & m\in M, n\in N, a\in A. \end{array}$$

Es claro que el producto tensorial está unívocamente determinado salvo isomorfismo. En particular no depende de la elección del grupo libre con el que se construye. De todos modos, esto lo obtendremos explícitamente en breve. Observar que un elemento genérico de $M \otimes_A N$ no es de la forma $m \otimes n$, sino una suma finita de elementos de esta forma.

Una consecuencia inmediata de las igualdades anteriores es que $0 \otimes n = m \otimes 0 = 0$ (por ejemplo $0 \otimes n = (0+0) \otimes n = 0 \otimes n + 0 \otimes n$, luego $0 \otimes n = 0$).

En las condiciones de la definición anterior, si G es un grupo abeliano, una aplicación $f : M \times N \longrightarrow G$ es *balanceada* si cumple

$$\begin{array}{ll} f(m_1+m_2,n) = f(m_1,n) + f(m_2,n), & m_1,m_2\in M, n\in N,\\ f(m,n_1+n_2) = f(m,n_1) + f(m,n_2), & m\in M, n_1,n_2\in N,\\ f(ma,n) = f(m,an). & m\in M, n\in N, a\in A. \end{array}$$

Obviamente, la aplicación $i : M \times N \longrightarrow M \otimes_A N$ dada por $i(m,n) = m \otimes n$ es balanceada. Se llama *aplicación balanceada canónica.*

El teorema siguiente caracteriza a los productos tensoriales.

Teorema 14.2 *Sea A un anillo, M un A-módulo derecho, N un A-módulo izquierdo, G un grupo abeliano y $f : M \times N \longrightarrow G$ una aplicación balanceada. Entonces existe un único homomorfismo $g : M \otimes_A N \longrightarrow G$ tal que $g(m \otimes n) = f(m,n)$ para todo $m \in M$, $n \in N$.*

Demostración: Si $M \otimes_A N = L/R$ según la definición, como $M \times N$ es una base de L tenemos que f se extiende a un homomorfismo $f^* : L \longrightarrow G$ y del hecho de que f es balanceada se sigue inmediatamente que R está contenido en el núcleo de f^* (sus generadores lo están). En consecuencia la aplicación $g([x]) = f^*(x)$ está bien definida y es un homomorfismo de grupos. En particular $g(m \otimes n) = f^*(m,n) = f(m,n)$.

Como los tensores $m \otimes n$ generan el producto $M \otimes_A N$, dos homomorfismos que coincidan sobre ellos son iguales, luego g es único. ∎

En particular dos productos tensoriales $(M \otimes_A N)_1$ y $(M \otimes_A N)_2$ cumplen el teorema anterior, y las respectivas aplicaciones balanceadas canónicas se extienden a dos homomorfismos entre ellos mutuamente inversos, luego ambos grupos son isomorfos.

En la práctica usaremos la misma notación para las aplicaciones balanceadas y los homomorfismos que inducen. Este es un buen momento para notar que los productos tensoriales pueden ser más extraños de lo que podría pensarse:

Si A es un grupo abeliano finito, entonces $A \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ pues, si A tiene n elementos, para todo $r \in \mathbb{Q}$ se cumple

$$a \otimes r = a \otimes n(r/n) = an \otimes (r/n) = 0 \otimes (r/n) = 0.$$

Veamos ahora cómo convertir en módulos a los productos tensoriales.

Teorema 14.3 *Sean dos anillos A y B, sea M un A-B-bimódulo y N un B-módulo izquierdo. Entonces $M \otimes_B N$ se convierte en un A-módulo izquierdo mediante una operación caracterizada por la relación $a(m \otimes n) = (am) \otimes n$, para $a \in A$, $m \in M$, $n \in N$.*

Demostración: Dado $a \in A$, el teorema anterior nos permite construir un homomorfismo $f_a : M \otimes_B N \longrightarrow M \otimes_B N$ determinado por $f_a(m \otimes n) = (am) \otimes n$.

Para cada $x \in M \otimes_B N$ definimos $ax = f_a(x)$. Así tenemos definida una ley externa sobre $M \otimes_B N$ que evidentemente distribuye a la suma. Esta distributividad reduce la comprobación de los axiomas restantes al caso de tensores $m \otimes n$, donde la comprobación es inmediata. Por ejemplo:

$$a\Big(b\sum_{i=1}^{r} m_i \otimes n_i\Big) = \sum_{i=1}^{r} a(b(m_i \otimes n_i)) = \sum_{i=1}^{r} (ab)m_i \otimes n_i = (ab)\sum_{i=1}^{r} m_i \otimes n_i.$$

Este mismo tipo de razonamiento justifica la unicidad de la operación externa. ∎

Dejamos al lector el enunciado y la demostración de un teorema similar que confiera a $M \otimes_B N$ una estructura de módulo derecho. Más aún, si M es un A-B–bimódulo y N es un B-C-bimódulo entonces $M \otimes_B N$ es un A-C-bimódulo.

Observar que todo B-módulo izquierdo es un B-$\mathbb{Z}$-bimódulo y todo A-módulo derecho es un $\mathbb{Z}$-A–bimódulo, luego no perdemos generalidad si trabajamos sólo con bimódulos, ya que particularizando a $\mathbb{Z}$ todo vale para módulos izquierdos o derechos. La prueba del teorema siguiente es inmediata:

Teorema 14.4 *Sean tres anillos A, B, C, sea M un A-B-bimódulo y N un B-C-bimódulo. Entonces la aplicación canónica $i : M \times N \longrightarrow M \otimes_B N$ es bilineal, o sea, cumple $i(am, nc) = ai(m, n)c$. Además, toda aplicación bilineal y balanceada $f : M \times N \longrightarrow R$ en un A-C-bimódulo R induce un único homomorfismo de bimódulos de $M \otimes_B N$ en R tal que $g(m \otimes n) = f(m, n)$.*

Este teorema justifica la definición siguiente:

Definición 14.5 Sean tres anillos A, B, C, sean M, M' dos A-B-bimódulos y N, N' dos B-C-bimódulos. Sea $f : M \longrightarrow M'$ un homomorfismo de A-B-bimódulos y $g : N \longrightarrow N'$ un homomorfismo de B-C-bimódulos. Llamaremos $f \otimes g : M \otimes_B N \longrightarrow M' \otimes_B N'$ al (único) homomorfismo de A-C-módulos determinado por $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

Ahora nos ocupamos de las propiedades algebraicas de los productos tensoriales. En primer lugar la asociatividad. Para abreviar no indicaremos explícitamente los anillos sobre los que están definidos los módulos cuando se pueda deducir del contexto. Así mismo sobrentenderemos que las letras A, B, C, D denotan anillos y las letras M, N, R, S, módulos.

Teorema 14.6 *Se cumple* $(M \otimes_B N) \otimes_C R \cong M \otimes_B (N \otimes_C R)$ *(isomorfismo de A-D-bimódulos). El isomorfismo hace corresponder los tensores* $(m \otimes n) \otimes r$ *y* $m \otimes (n \otimes r)$.

Demostración: Para cada $r \in R$ sea $f_r : M \otimes_B N \longrightarrow M \otimes_B (N \otimes_C R)$ el homomorfismo de A-módulos determinado por $f_r(m \otimes n) = m \otimes (n \otimes r)$. La aplicación $(M \otimes_B N) \times R \longrightarrow M \otimes_B (N \otimes_C R)$ dada por $(x, r) \mapsto f_r(x)$ es balanceada, luego induce un homomorfismo de grupos

$$f : (M \otimes_B N) \otimes_C R \longrightarrow M \otimes_B (N \otimes_C R)$$

que cumple $f((m \otimes n) \otimes r) = f_r(m \otimes n) = m \otimes (n \otimes r)$.

De igual modo se construye un homomorfismo en sentido contrario que claramente es el inverso de éste, luego f es en realidad un isomorfismo de grupos, y obviamente también de A-D-bimódulos. ∎

Consecuentemente podemos suprimir los paréntesis y hablar del producto tensorial $M \otimes_B N \otimes_C R$, generado por los tensores de la forma $m \otimes n \otimes r$. Más en general, el número de factores puede ser cualquiera. Los teoremas siguientes se demuestran sin dificultad de forma similar al anterior:

Teorema 14.7 *Se cumple* $A \otimes_A N \cong N$ *(isomorfismo de A-B-bimódulos). El isomorfismo hace corresponder los tensores* $1 \otimes n$ *y* n. *Así mismo* $M \otimes_B B \cong M$.

Teorema 14.8 *Se cumple*

$$\Big(\bigoplus_{i\in I} M_i\Big) \otimes_B N \cong \bigoplus_{i\in I} (M_i \otimes_B N),$$

$$M \otimes_B \Big(\bigoplus_{i\in I} N_i\Big) \cong \bigoplus_{i\in I} (M \otimes_B N_i).$$

Ahora veremos que la estructura de los productos tensoriales de módulos libres es muy sencilla y dista mucho del comportamiento patológico del ejemplo que poníamos más arriba. Son estos productos tensoriales los que realmente nos van a interesar. Notemos en primeramente que un A-módulo libre es una suma directa de copias de A y, como A es un A-A-bimódulo, todo A-módulo libre tiene estructura de A-A-bimódulo.

Teorema 14.9 *Si M y N son B-módulos libres con bases $\{u_i\}$ y $\{v_j\}$ entonces el producto $M \otimes_B N$ es un B-módulo libre de base $\{u_i \otimes v_j\}$.*

DEMOSTRACIÓN: Tenemos que $M = \bigoplus_i \langle u_i\rangle$ y $N = \bigoplus_j \langle v_j\rangle$, luego por el teorema anterior $M \otimes_B N \cong \bigoplus_{i,j}(\langle u_i\rangle \otimes_B \langle v_j\rangle)$.

Además $\langle u_i\rangle \otimes_B \langle v_j\rangle \cong B \otimes_B B \cong B$ y el isomorfismo hace corresponder el tensor $u_i \otimes v_j$ con 1. Así pues, $M \otimes_B N \cong \bigoplus_{i,j} B$, y los tensores $\{u_i \otimes v_j\}$ se corresponden con la base canónica del último módulo, luego son una base de $M \otimes_B N$. ∎

A menudo consideraremos productos tensoriales donde sólo uno de los factores es libre, pero en este caso tenemos un teorema similar al anterior:

Teorema 14.10 *Si M es un B-módulo y N es un B-módulo libre de base $\{v_i\}$, todo elemento de $M \otimes_B N$ se expresa de forma única como $\sum_i m_i \otimes v_i$, con $m_i \in M$. (La expresión es única salvo sumandos con $m_i = 0$).*

DEMOSTRACIÓN: De forma análoga al caso anterior vemos que

$$M \otimes_B N \cong \bigoplus_i (M \otimes_B \langle v_i\rangle),$$

con $M \otimes_B \langle v_i\rangle \cong M \otimes_B B \cong M$, luego $M \otimes_B N \cong \bigoplus_i M$, donde el isomorfismo hace corresponder $m \otimes v_i$ con m (en el i-ésimo sumando). La unicidad que hay que probar es la de la suma directa traspasada a $M \otimes_B N$ a través de este isomorfismo. ∎

Grupos de homomorfismos El grupo de homomorfismos entre dos módulos dados desempeña en el álgebra homológica un papel "dual" —en cierto sentido— al concepto de producto tensorial. De momento nos limitamos a definirlos y a introducir las aplicaciones naturales que los conectan.

Definición 14.11 Sean M y N dos A-módulos (izquierdos o derechos). Llamaremos $\mathrm{Hom}_A(M,N)$ al grupo de los homomorfismos $f : M \longrightarrow N$ (con la suma definida puntualmente).

Las leyes distributivas siguientes se demuestran sin dificultad alguna:

$$\mathrm{Hom}_A\Big(\bigoplus_{i\in I} M_i, N\Big) \cong \prod_{i\in I} \mathrm{Hom}_A(M_i, N),$$

$$\mathrm{Hom}_A\Big(M, \prod_{i\in I} N_i\Big) \cong \prod_{i\in I} \mathrm{Hom}_A(M, N_i).$$

Así mismo $\mathrm{Hom}_A(A, M) \cong M$ (con el isomorfismo dado por $i(f) = f(1)$).

Si $\alpha : M' \longrightarrow M$ es un homomorfismo de módulos definimos

$$\alpha^{\#} : \mathrm{Hom}_A(M,N) \longrightarrow \mathrm{Hom}_A(M',N)$$

como la aplicación dada por $\alpha^{\#}(f) = \alpha \circ f$.

Análogamente, si $\alpha : N \longrightarrow N'$ definimos

$$\alpha_\# : \mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_A(M, N')$$

como la aplicación dada por $\alpha_\#(f) = f \circ \alpha$. Es sencillo comprobar que estas aplicaciones son homomorfismos de grupos, así como que

$$(\alpha \circ \beta)^\# = \beta^\# \circ \alpha^\#, \quad (\alpha \circ \beta)_\# = \alpha_\# \circ \beta_\#, \quad \alpha_\# \circ \beta^\# = \beta^\# \circ \alpha_\#.$$

Sucesiones exactas La noción de sucesión exacta está en la base del álgebra homológica, pues los resultados fundamentales se expresan en términos de éstas. La definición es muy simple:

Definición 14.12 Una cadena de homomorfismos de módulos

$$\cdots \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} R \longrightarrow \cdots$$

es *exacta* en N si cumple $\mathrm{Im}\,\alpha = \mathrm{N}(\beta)$. La sucesión completa es *exacta* si lo es en todos sus módulos.

Notar que una sucesión $0 \longrightarrow M \xrightarrow{\alpha} N$ es exacta en M si y sólo si α es inyectiva, mientras que una sucesión $M \xrightarrow{\beta} N \longrightarrow 0$ es exacta en N si y sólo si α es suprayectiva.

Una porción importante de la cohomología de grupos consiste en demostrar la existencia de ciertas sucesiones exactas. De momento estudiaremos algunas circunstancias en que se conserva la exactitud de una sucesión al transformarla con productos tensoriales o con módulos de homomorfismos.

Teorema 14.13 *Si $N \xrightarrow{\alpha} R \xrightarrow{\beta} S \longrightarrow 0$ es una sucesión exacta de B-C-módulos y M es un A-B-bimódulo, entonces*

$$M \otimes_B N \xrightarrow{1\otimes\alpha} M \otimes_B R \xrightarrow{1\otimes\beta} M \otimes_B S \longrightarrow 0$$

es una sucesión exacta de A-C-módulos. (Similarmente si se multiplica por la derecha).

Demostración: Lo único que no es inmediato es que $\mathrm{N}(1\otimes\beta) \leq \mathrm{Im}(1\otimes\alpha)$. Sea $H = \mathrm{Im}(1 \otimes \alpha)$. Puesto que $H \leq \mathrm{N}(1 \otimes \beta)$, la aplicación $1 \otimes \beta$ induce un homomorfismo $\phi : (M \otimes_B R)/H \longrightarrow M \otimes_B S$ que cumple $\phi([m \otimes r]) = m \otimes \beta(r)$.

Por otra parte la aplicación balanceada $(m, \beta(r)) \mapsto [m \otimes r]$ está bien definida e induce una inversa para ϕ, luego ϕ es un isomorfismo y, por consiguiente, $\mathrm{N}(1 \otimes \beta)/H = 0$. ∎

Ahora probamos el resultado análogo para grupos de homomorfismos:

Teorema 14.14 *Si $0 \longrightarrow N \xrightarrow{\alpha} R \xrightarrow{\beta} S \longrightarrow 0$ es una sucesión exacta de A-módulos entonces las sucesiones*

$$0 \longrightarrow \mathrm{Hom}_A(M, N) \xrightarrow{\alpha_\#} \mathrm{Hom}_A(M, R) \xrightarrow{\beta_\#} \mathrm{Hom}_A(M, S),$$

$$0 \longrightarrow \mathrm{Hom}_A(S,M) \xrightarrow{\beta^\#} \mathrm{Hom}_A(R,M) \xrightarrow{\alpha^\#} \mathrm{Hom}_A(N,M),$$

son sucesiones exactas de grupos.

DEMOSTRACIÓN: Claramente $\alpha_\#$ es inyectiva y $\operatorname{Im}\alpha_\# \leq \mathrm{N}(\beta_\#)$. Tomemos $f \in \mathrm{N}(\beta_\#)$. Entonces $f \circ \beta = 0$, luego $\beta(f(m)) = 0$ para todo $m \in M$, luego $f[M] \leq \mathrm{N}(\beta) = \operatorname{Im}\alpha$. Como α es inyectiva existe $g \in \mathrm{Hom}_A(M,N)$ tal que $\alpha_\#(g) = f$ (concretamente, $g = f \circ \alpha^{-1}$). Así, $\mathrm{N}(\beta_\#) = \operatorname{Im}\alpha_\#$.

Claramente $\beta^\#$ es inyectiva y $\operatorname{Im}\beta^\# \leq \mathrm{N}(\alpha^\#)$. Sea $f \in \mathrm{N}(\alpha^\#)$. Como $\alpha \circ \beta = 0$ y β es suprayectiva podemos definir $g \in \mathrm{Hom}_A(S,M)$ mediante $g(s) = f(\beta^{-1}(s))$ y así $f = \beta^\#(g)$. ∎

Los teoremas anteriores no son ciertos para sucesiones exactas más largas, ni siquiera si añadimos una flecha nula. Ahora daremos condiciones suficientes para que se conserve la exactitud en este último caso.

Teorema 14.15 *Si* $0 \longrightarrow N \xrightarrow{\alpha} R \xrightarrow{\beta} S \longrightarrow 0$ *es una sucesión exacta de módulos y se cumple una de estas condiciones:*

a) $\operatorname{Im}\alpha$ *está complementada en* R*,*

b) M *es un* B*-módulo libre,*

entonces también es exacta la sucesión

$$0 \longrightarrow M \otimes_B N \xrightarrow{1\otimes\alpha} M \otimes_B R \xrightarrow{1\otimes\beta} M \otimes_B S \longrightarrow 0.$$

DEMOSTRACIÓN: Basta probar que $1 \otimes \alpha$ es inyectiva. Si $R = \operatorname{Im}\alpha \oplus R'$, entonces $M \otimes_B N \xrightarrow{1\otimes\alpha} M \otimes_B \operatorname{Im}\alpha$ es un isomorfismo y

$$M \otimes_B \operatorname{Im} a \subset (M \otimes_B \operatorname{Im}\alpha) \oplus (M \otimes_B R') \cong M \otimes_B R.$$

Es claro que la composición de $1\otimes\alpha$ con el último isomorfismo es $1\otimes\alpha$ como aplicación entre $M \otimes_B N$ y$M \otimes_B R$, luego es inyectiva.

Si M es libre entonces $M \cong \bigoplus_{i\in I} B$ y por lo tanto

$$M \otimes_B N \cong \bigoplus_{i\in I}(B \otimes_B N) \cong \bigoplus_{i\in I} N, \quad M \otimes_B R \cong \bigoplus_{i\in I}(B \otimes_B R) \cong \bigoplus_{i\in I} R.$$

Si componemos estos isomorfismos con $1 \otimes \alpha$ obtenemos la aplicación

$$\bigoplus_{i\in I} \alpha : \bigoplus_{i\in I} N \longrightarrow \bigoplus_{i\in I} R,$$

que claramente es inyectiva, luego $1 \otimes \alpha$ también lo es. ∎

La prueba del teorema siguiente es análoga a la que acabamos de ver.

Teorema 14.16 *Si* $0 \longrightarrow N \xrightarrow{\alpha} R \xrightarrow{\beta} S \longrightarrow 0$ *es una sucesión exacta de módulos y* M *es libre entonces también es exacta la sucesión*

$$0 \longrightarrow \mathrm{Hom}_A(M,N) \xrightarrow{\alpha_\#} \mathrm{Hom}_A(M,R) \xrightarrow{\beta_\#} \mathrm{Hom}_A(M,S) \longrightarrow 0.$$

Anillos de grupos La conexión de todos estos conceptos con la teoría de cuerpos se lleva a cabo esencialmente a través de los anillos de grupos. Vamos a ver que a cada grupo finito G le podemos asociar un anillo $\mathbb{Z}[G]$, de modo que los cuerpos y los grupos de elementos ideales se convierten de forma natural en $\mathbb{Z}[G]$-módulos, donde G es un grupo de Galois.

Definición 14.17 Sea G un grupo. Llamaremos $\mathbb{Z}[G]$ al $\mathbb{Z}$-módulo libre de base G, es decir, cada elemento de $\mathbb{Z}[G]$ se expresa de forma única como

$$\sum_{\sigma\in G} n_\sigma\sigma, \qquad n_\sigma \in \mathbb{Z}.$$

Para cada $\tau \in G$ consideramos el automorfismo de $\mathbb{Z}[G]$ dado por

$$p_\tau\Big(\sum_{\sigma\in G} n_\sigma\sigma\Big) = \sum_{\sigma\in G} n_\sigma\tau\sigma.$$

En particular si $\sigma \in G$ tenemos $p_\tau(\sigma) = \tau\sigma$. Para cada $s = \sum_{\sigma\in G} n_\sigma\sigma \in \mathbb{Z}[G]$ consideramos el endomorfismo de $\mathbb{Z}[G]$ dado por

$$p_s(t) = \sum_{\sigma\in G} n_\sigma p_\sigma(t).$$

Notar que si $\tau \in G$ entonces

$$p_s(\tau) = \sum_{\sigma\in G} n_\sigma\sigma\tau.$$

Para cada s, $t \in \mathbb{Z}[G]$ definimos $st = p_s(t)$. Es claro que este producto extiende al producto de G, distribuye las sumas por la derecha y que los elementos de G distribuyen las sumas por la izquierda. Con estos datos es fácil ver que $\mathbb{Z}[G]$ es un anillo. También es claro que el producto es la única extensión posible del producto en G que confiere a $\mathbb{Z}[G]$ estructura de anillo.

A $\mathbb{Z}[G]$ se le llama *anillo del grupo* G. A los $\mathbb{Z}[G]$-módulos los llamaremos simplemente *G-módulos.* Un *G-homomorfismo* será un homomorfismo de G-módulos.

Recordemos de 7.4 que una acción de un grupo G sobre un grupo M es un homomorfismo de G en el grupo de los automorfismos de M. En lo sucesivo sólo nos va a interesar el caso en que M es un grupo abeliano. Es fácil ver que una acción de G sobre M determina y está determinada por una aplicación $M \times G \longrightarrow M$ que satisfaga las condiciones

a) $(m + n)\sigma = m\sigma + n\sigma$,

b) $m(\sigma\tau) = (m\sigma)\tau$,

c) $m1 = m$.

Dada la acción, basta definir $m\sigma = \sigma(m)$ y, dada una aplicación en estas condiciones, se comprueba inmediatamente que las aplicaciones $f_\sigma(m) = m\sigma$ son automorfismos de M y que la aplicación $\sigma \mapsto f_\sigma$ es un homomorfismo de grupos. Por este motivo, a una aplicación $M \times G \longrightarrow M$ que cumpla estas condiciones se le llama también una *acción* de G sobre M.

Si un grupo G actúa sobre un grupo abeliano M, entonces M se convierte en un G-módulo derecho mediante la ley externa dada por

$$m\Big(\sum_{\sigma\in G} n_\sigma\sigma\Big) = \sum_{\sigma\in G} n_\sigma\sigma(m).$$

Notar que esta ley externa extiende a la acción de G sobre M (y es la única extensión posible que convierte a M en un G-módulo). Recíprocamente, si M es un G-módulo derecho entonces la restricción de la ley externa a $M \times G$ es una acción de G sobre M.

Similarmente, es fácil ver que para determinar una estructura de G-módulo izquierdo en un grupo abeliano M basta especificar una aplicación $G\times M \longrightarrow M$ que verifique:

a) $\sigma(m+n) = \sigma m + \sigma n$,

b) $(\sigma\tau)m = \sigma(\tau m)$,

c) $1m = m$.

La aplicación $\sigma \mapsto \sigma^{-1}$ se extiende por linealidad a un único isomorfismo de grupos $i : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]$ al que llamaremos *inversión.* Es fácil ver que $i(st) = i(t)i(s)$.

De aquí se sigue que todo G-módulo izquierdo M se pueda considerar como G-módulo derecho mediante $ms = i(s)m$, y viceversa, por lo que en general será irrelevante el carácter izquierdo o derecho de los G-módulos. No obstante hay que tener presente que en general M no es un bimódulo con estas operaciones.

Observar que el propio $\mathbb{Z}[G]$ admite entonces dos estructuras de G-módulo izquierdo: (1) el producto usual y (2) $st = t\,i(s)$. No obstante la aplicación i es un isomorfismo de G-módulos izquierdos:

$$i(s^{(1)}t) = i(t)^{(1)}i(s) = s^{(2)}i(s),$$

luego normalmente no importará la estructura considerada.

Todo G-módulo es obviamente un $\mathbb{Z}$-módulo. Adoptaremos el convenio de que los símbolos $\otimes_G$ y Hom_G harán referencia al anillo $\mathbb{Z}[G]$, mientras que $\otimes$ y Hom harán referencia a $\mathbb{Z}$.

Módulos duales En este apartado G será un grupo finito.

Definición 14.18 Si A es un G-módulo entonces $A^* = \mathrm{Hom}(A, \mathbb{Z})$ se convierte en un G-módulo con la operación dada por

$$(\sigma f)(a) = f(a\sigma), \qquad \sigma \in G, f \in A^*, a \in A.$$

El G-módulo A^* recibe el nombre de *módulo dual* de A. Todo G-homomorfismo $\phi : A \longrightarrow B$ induce un *homomorfismo dual* $\phi^* : B^* \longrightarrow A^*$ dado por $\phi^*(f) = \phi \circ f$. Es claro que $(\phi \circ \psi)^* = \psi^* \circ \phi^*$.

Vamos a probar que todo G-módulo libre de rango finito es isomorfo a su bidual. En general, si A es un G-módulo y $a \in A$ definimos $x_a \in A^{**}$ mediante $x_a(f) = f(a)$. Es fácil comprobar que la aplicación $A \longrightarrow A^{**}$ dada por $a \mapsto x_a$ es un G-monomorfismo.

Si ahora suponemos que A es G-libre de rango finito y $\{v_1, \ldots, v_n\}$ es una G-base, entonces es claro que $\{\sigma v_i\}$ es una $\mathbb{Z}$-base de A (donde σ varía en G). Sea $\alpha_i \in A^*$ el homomorfismo determinado por

$$\alpha_i(\sigma v_j) = \begin{cases} 1 & \text{si } \sigma = 1,\ i = j, \\ 0 & \text{en otro caso.} \end{cases} \tag{14.1}$$

Se cumple que $\{\alpha_1, \ldots, \alpha_n\}$ es una G-base de A^*, pues si $\alpha \in A^*$ y llamamos $n_{\sigma i} = \alpha(\sigma v_i)$, entonces

$$\Big(\sum_{i,\sigma}(n_{\sigma i}\sigma)\alpha_i\Big)(\tau v_j) = \sum_{i,\sigma} n_{\sigma i}(\sigma\alpha_i)(\tau v_j) = \sum_{i,\sigma} n_{\sigma i}\alpha_i(\sigma^{-1}\tau v_j) = n_{\tau j} = \alpha(\tau v_j).$$

Así pues, $\alpha = \sum_{i,\sigma}(n_{\sigma i}\sigma)\alpha_i$, lo que prueba que $\{\alpha_i\}$ es un sistema generador de A^*. Así mismo, si $\sum_{i,\sigma}(n_{\sigma i}\sigma)\alpha_i = 0$, al hacerlo actuar sobre τv_j concluimos que $n_{\tau j} = 0$, luego $\{\alpha_i\}$ es libre.

La base $\{\alpha_1, \ldots, \alpha_n\}$ dada por (14.1) se llama *base dual* de $\{v_1, \ldots, v_n\}$.

Sea ahora $\{\beta_1, \ldots, \beta_n\}$ la base dual de $\{\alpha_1, \ldots, \alpha_n\}$. Entonces $\beta_i(\sigma\alpha_j) = 1$ si y sólo si $\sigma = 1$, $i = j$, si y sólo si $x_{v_i}(\sigma\alpha_j) = (\sigma\alpha_j)(v_i) = \alpha_j(\sigma^{-1}v_i) = 1$, y en caso contrario se cumple $\beta_i(\sigma\alpha_j) = 0 = x_{v_i}(\sigma\alpha_j)$. Por lo tanto $\beta_i = x_{v_i}$, luego la base bidual de $\{v_1, \ldots, v_n\}$ es precisamente $\{x_{v_1}, \ldots, x_{v_n}\}$. Esto implica que el monomorfismo $a \mapsto x_a$ es en este caso un isomorfismo.

Notar que hemos probado que el módulo dual de un G-módulo libre de rango finito es también libre y del mismo rango. También hay que destacar que tenemos un isomorfismo canónico entre A y su bidual, pero no entre A y su dual.

Otra observación sencilla es que si $\phi : A \longrightarrow B$ es un G-homomorfismo, el diagrama siguiente es conmutativo:

$$\begin{array}{ccc} A^{**} & \xrightarrow{\phi^{**}} & B^{**} \\ \uparrow & & \uparrow \\ A & \xrightarrow{\phi} & B \end{array}$$

Las flechas verticales representan a los isomorfismos canónicos entre los módulos y sus biduales.

El teorema siguiente tiene gran importancia porque, según veremos, de él se desprende que la homología y la cohomología de grupos finitos, que en principio serían dos teorías distintas, resultan ser de hecho teorías equivalentes.

Teorema 14.19 *Sea G un grupo finito, A un G-módulo y C un G-módulo libre de rango finito. Entonces $A \otimes_G C \cong \mathrm{Hom}_G(C^*, A)$.*

DEMOSTRACIÓN: Para cada $(a, c) \in A \times C$ definimos $f_{a,c} \in \mathrm{Hom}_G(C^*, A)$ mediante

$$f_{a,c}(g) = \sum_{\sigma \in G} g(\sigma c)\sigma a.$$

Claramente $f_{\tau a,\tau c} = f_{a,c}$, pero esto equivale a que $f_{a\tau,c} = f_{\tau^{-1}a,\tau^{-1}\tau c} = f_{a,\tau c}$, luego la aplicación $(a, c) \mapsto f_{a,c}$ es balanceada y, por consiguiente, induce un homomorfismo de grupos $F : A \otimes_G C \longrightarrow \mathrm{Hom}_G(C^*, A)$.

Si $\{c_i\}$ es una base de C y $\{g_i\}$ es su base dual, para todo $f \in \mathrm{Hom}_G(C^*, A)$ se cumple

$$F\Big(\sum_i a_i \otimes c_i\Big)(g_j) = \sum_i f_{a,c_i}(g_j) = \sum_i \sum_{\sigma \in G} g_j(\sigma c_i)\sigma a_i = a_j,$$

luego $f = F\Big(\sum_i a_i \otimes c_i\Big)$ si y sólo si $f(g_i) = a_i$. El teorema 14.10 implica que F es un isomorfismo. ∎

Notar que el homomorfismo F que hemos construido en la prueba puede definirse aunque C no sea libre.

La última observación que vamos a necesitar es que si consideramos a $\mathbb{Z}$ como G-módulo trivial, es decir, $\sigma n = n$ para todo $\sigma \in G$ y todo $n \in \mathbb{Z}$, entonces $\mathbb{Z}^* \cong \mathbb{Z}$. El isomorfismo viene dado por $f \mapsto f(1)$.

14.2 Homología y cohomología de grupos

En esta sección introducimos los conceptos básicos de la cohomología de grupos. Básicamente vamos a asociar una familia de grupos de homología y de cohomología a cada G-módulo A. En el caso en que el grupo G sea finito los grupos de homología serán esencialmente los mismos que los grupos de cohomología. Tan pronto como sea posible ampliaremos este esbozo de nuestros objetivos.

Complejos En primer lugar introducimos la noción de complejo (y, más en general, la de módulo graduado) de modo que todo complejo tiene asociados unos grupos de homología (o de cohomología). Después veremos como asociar un cierto complejo a cada G-módulo A, de modo que los grupos de homología o de cohomología de A serán los asociados a dicho complejo.

Definición 14.20 Sea G un grupo. Un *G-módulo graduado* es una suma directa de G-módulos $C = \bigoplus_{n\in\mathbb{Z}} C_n$. Los elementos de cada G-submódulo C_n se llaman elementos *homogéneos* de grado n. Un *submódulo graduado* de C es un módulo $D = \bigoplus_{n\in\mathbb{Z}} D_n$, donde $D_n = C_n \cap D$.

Un *homomorfismo graduado* $f : C \longrightarrow D$ (de grado d) es un G-homomorfismo tal que $f_n = f|_{C_n} : C_n \longrightarrow D_{n+d}$ para todo entero n.

Un *complejo* es un par $\mathcal{C} = (\bigoplus_{n\in\mathbb{Z}} C_n, \partial)$, donde ∂ es un homomorfismo de grado -1 tal que $\partial\circ\partial = 0$. Entonces tenemos

$$\cdots \longrightarrow C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \longrightarrow \cdots$$

de manera que $\partial_{n+1}\circ\partial_n = 0$.

Recíprocamente, una sucesión de homomorfismos y módulos en estas condiciones determina un complejo. El homomorfismo ∂ se llama *operador frontera* del complejo. Los elementos de C_n se llaman *cadenas* de dimensión n. Los elementos de $Z_n = \mathrm{N}(\partial_n)$ se llaman *ciclos* de dimensión n. Los elementos de $F_n = \operatorname{Im}\partial_{n+1}$ se llaman *fronteras* de dimensión n. La condición $\partial_{n+1}\circ\partial_n = 0$ implica que $F_n \le Z_n$.

El módulo $H_n(\mathcal{C}) = Z_n/F_n$ se llama *grupo de homología* de dimensión n. Dos ciclos son *homólogos* si pertenecen a la misma clase de homología.

Un *homomorfismo de complejos* $\phi : \mathcal{C} \longrightarrow \mathcal{C}'$ es un homomorfismo de grado 0 tal que $\phi\circ\partial' = \partial\circ\phi$ o, equivalentemente, tal que los diagramas siguientes conmutan:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \phi_{n+1}} & & \downarrow{\scriptstyle \phi_n} & & \downarrow{\scriptstyle \phi_{n-1}} & & \\
\cdots & \longrightarrow & C'_{n+1} & \xrightarrow[\partial'_{n+1}]{} & C'_n & \xrightarrow[\partial'_n]{} & C'_{n-1} & \longrightarrow & \cdots
\end{array}$$

Es claro que ϕ envía ciclos a ciclos y fronteras a fronteras, luego induce homomorfismos $\overline{\phi}_n : H_n(\mathcal{C}) \longrightarrow H_n(\mathcal{C}')$. Si ϕ es un isomorfismo los homomorfismos inducidos también lo son.

También es inmediato que la composición de homomorfismos de complejos es un homomorfismo de complejos, así como que $\overline{\phi_n\circ\psi_n} = \overline{\phi}_n\circ\overline{\psi}_n$.

Un *complejo inverso* se define análogamente a un complejo, pero con un operador ∂ de grado 1 en lugar de -1. Entonces el operador se llama *operador cofrontera* y hablamos de *cocadenas, cociclos, cofronteras y grupos de cohomología.* Además usaremos superíndices en lugar de subíndices. En principio hablaremos únicamente de homología, pues es claro que todo hecho en torno a homología de complejos tiene su traducción inmediata a cohomología de complejos inversos.

Homotopía Nuestro propósito es asignar a cada grupo finito G un complejo con ciertas características, entre ellas que todos sus grupos de homología sean triviales. A partir de éste y de un G-módulo A obtendremos dos nuevos complejos: uno con los módulos $A \otimes_G C_n$ y el otro (inverso) con $\mathrm{Hom}_G(C_n, A)$. Los grupos de homología del primero los representaremos mediante $H_n(G, A)$ y los grupos de cohomología del segundo mediante $H^n(G, A)$. En realidad los complejos que vamos a construir no van a estar unívocamente determinados, sino que dos cualesquiera de ellos serán equivalentes en un sentido que implica que sus grupos de homología serán isomorfos. Vamos a definir este tipo de equivalencia.

Diremos que dos homomorfismos de complejos $\phi,\ \psi : \mathcal{C} \longrightarrow \mathcal{C}'$ son *homotópicos,* y lo representaremos por $\phi \approx \psi$, si existe un homomorfismo de complejos $\Delta : \mathcal{C} \longrightarrow \mathcal{C}'$ de grado 1 tal que $\phi - \psi = \Delta\partial' + \partial\Delta$ o, equivalentemente, tal que $\phi_n - \psi_n = \Delta_n\partial'_{n+1} + \partial_n\Delta_{n+1}$.

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & & \searrow^{\Delta_n} & \downarrow{\scriptstyle \phi_n-\psi_n} & \swarrow_{\Delta_{n-1}} & & & \\
\cdots & \longrightarrow & C'_{n+1} & \xrightarrow[\partial'_{n+1}]{} & C'_n & \xrightarrow[\partial'_n]{} & C'_{n-1} & \longrightarrow & \cdots
\end{array}$$

Entonces $\phi - \psi$ envía ciclos de dimensión n a fronteras de dimensión n, por lo que se cumple $\overline{\phi}_n = \overline{\psi}_n$ para todo entero n. Diremos que Δ es una *homotopía* entre ϕ y ψ.

Dos complejos $\mathcal{C}$ y $\mathcal{C}'$ son *equivalentes* si existen homomorfismos $\phi : \mathcal{C} \longrightarrow \mathcal{C}'$ y $\psi : \mathcal{C}' \longrightarrow \mathcal{C}$ tales que $\phi \circ \psi \approx 1$ y $\psi \circ \phi \approx 1$. Es claro entonces que $H_n(\mathcal{C}) \cong H_n(\mathcal{C}')$ para todo entero n.

Resoluciones completas Nos ocupamos ahora del problema de asociar un complejo a cada grupo finito. Primeramente trataremos lo tocante a la unicidad, y más específicamente a la unicidad de la parte no negativa de los complejos. Para ello conviene dar la definición siguiente:

Definición 14.21 Un *complejo reducido* sobre un grupo G es un complejo de la forma

$$\cdots \longrightarrow C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0,$$

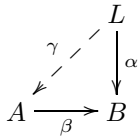
donde $\mathbb{Z}$ tiene estructura de G-módulo trivial y todos los módulos a su derecha son nulos.

Un complejo reducido es *acíclico* si es una sucesión exacta. Un complejo reducido es *libre* si todos sus módulos excepto $\mathbb{Z}$ son G-libres.

Cuando hablemos un homomorfismo entre complejos reducidos entenderemos que restringido a $\mathbb{Z}$ es la identidad.

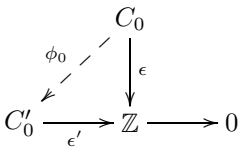
Teorema 14.22 *Sea $\mathcal{C}$ un complejo reducido libre sobre un grupo G y $\mathcal{C}'$ un complejo reducido acíclico. Entonces existe un homomorfismo $\phi : \mathcal{C} \longrightarrow \mathcal{C}'$ y dos cualesquiera son homotópicos.*

DEMOSTRACIÓN: Para construir el homomorfismo conviene hacer una observación general. Consideremos tres G-módulos L, A, B, donde L es libre, y dos G-homomorfismos α y β como indica la figura siguiente y de modo que $\operatorname{Im}\alpha \subset \operatorname{Im}\beta$:



Entonces existe un homomorfismo γ que hace el diagrama conmutativo. En efecto, tomamos una base X de L. Para cada $x \in X$ definimos $\gamma(x)$ como una antiimagen por β de $\alpha(x)$ y extendemos la aplicación por linealidad. Así $\beta(\gamma(x)) = \alpha(x)$ para todo $x \in X$ y, en consecuencia, para todo $x \in L$. Esto se llama *propiedad proyectiva* de los módulos libres.

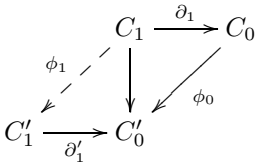
Aplicamos este hecho al caso



Por hipótesis la línea inferior es exacta, luego ϵ' es suprayectivo y C_0 es libre. Así pues, existe un homomorfismo ϕ_0 que hace conmutativo el diagrama, es decir, $\phi_0\epsilon' = \epsilon$. Por lo tanto $\partial_1\phi_0\epsilon' = \partial_1\epsilon = 0$ y, por la exactitud de la sucesión

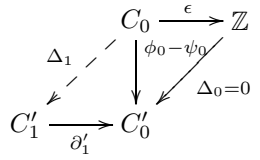
$$C_1' \xrightarrow{\partial_1'} C_0' \xrightarrow{\epsilon'} \mathbb{Z} \longrightarrow 0, \tag{14.2}$$

tenemos que $\operatorname{Im}(\partial_1\phi_0) \subset \operatorname{N}(\epsilon') = \operatorname{Im}\partial_1'$, luego podemos aplicar la propiedad proyectiva al diagrama



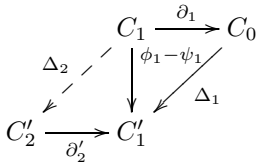
lo que nos da un G-homomorfismo ϕ_1 tal que $\phi_1\partial_1' = \partial_1\phi_0$. Repitiendo el proceso obtenemos un homomorfismo $\phi : \mathcal{C} \longrightarrow \mathcal{C}'$.

Supongamos ahora que tenemos dos homomorfismos ϕ, $\psi : \mathcal{C} \longrightarrow \mathcal{C}'$. Entonces $(\phi_0 - \psi_0)\epsilon' = \epsilon - \epsilon = 0$, luego por la exactitud de la sucesión (14.2) tenemos que $\operatorname{Im}(\phi_0 - \psi_0) \subset \operatorname{N}(\epsilon') = \operatorname{Im}\partial_1'$. Aplicamos la propiedad proyectiva al diagrama



y obtenemos un homomorfismo Δ_1 tal que $\phi_0 - \psi_0 = \epsilon\Delta_0 + \Delta_1\partial_1'$ (donde, por definición, $\Delta_0 = 0$).

Por lo tanto $(\phi_1 - \psi_1 - \partial_1\Delta_1)\partial_1' = \partial_1(\phi_0 - \psi_0) - \partial_1\Delta_1\partial_1' = 0$, y de aquí se concluye que $\mathrm{Im}(\phi_1 - \psi_1 - \partial_1\Delta_1) \subset \mathrm{N}(\partial_1') = \mathrm{Im}\,\partial_2'$ y podemos repetir el proceso con el diagrama



Continuando de este modo obtenemos una homotopía entre los dos homomorfismos. ∎

Definición 14.23 Una *resolución* de un grupo G es un complejo reducido libre y acíclico. Dos resoluciones cualesquiera $\mathcal{C}$ y $\mathcal{C}'$ de un grupo G son equivalentes, pues por la primera parte del teorema anterior existen homomorfismos de complejos $\phi : \mathcal{C} \longrightarrow C'$ y $\psi : \mathcal{C}' \longrightarrow \mathcal{C}$, y por la segunda los homomorfismos $\phi\psi$ y la identidad 1 han de ser homotópicos, y así mismo $\psi\phi \approx 1$.

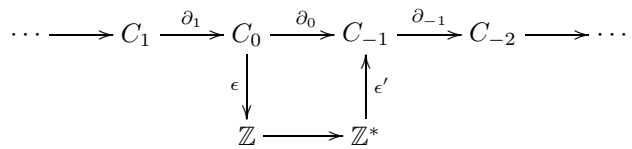
Pronto probaremos que todo grupo tiene una resolución, pero antes consideremos una resolución de un grupo finito G, que será de la forma

$$\cdots \longrightarrow C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

Supongamos además que todos los G-módulos tienen rango finito. Entonces podemos formar la sucesión de módulos y homomorfismos duales:

$$0 \longrightarrow \mathbb{Z}^* \xrightarrow{\epsilon^*} C_0^* \xrightarrow{\partial_1^*} C_1^* \longrightarrow \cdots$$

Recordemos que al final de la sección anterior mostramos un isomorfismo canónico entre $\mathbb{Z}$ y $\mathbb{Z}^*$. Llamamos ∂_0 a la composición de ϵ con este isomorfismo y con ϵ^*, llamamos así mismo $C_{-1} = C_0^*$, $C_{-2} = C_1^*$, etc. y renombramos consecuentemente a las aplicaciones duales. El resultado es un complejo

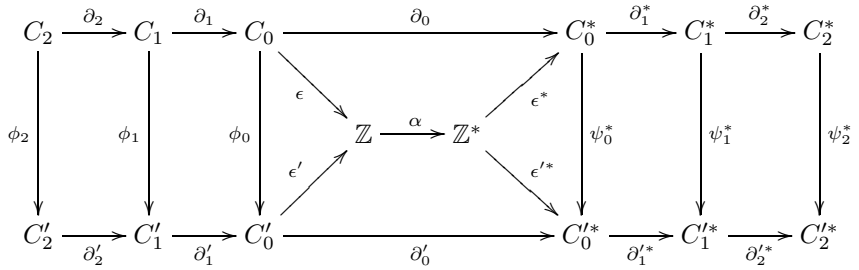


A todo complejo construido de esta forma lo llamaremos *resolución completa* del grupo G.

Teorema 14.24 *Todo grupo finito G tiene una resolución completa, cualquiera de ellas es una sucesión exacta y sus módulos son G-libres. Dos resoluciones completas de un mismo grupo son equivalentes.*

DEMOSTRACIÓN: En cuanto a la existencia basta probar que todo grupo tiene una resolución reducida formada por G-módulos libres de rango finito. Esto es consecuencia inmediata de que todo módulo finitamente generado es imagen homomorfa de un módulo libre de rango finito. En efecto, partimos de $\mathbb{Z}$ como G-módulo trivial, que es finitamente generado. Existe un G-módulo libre C_0 y un epimorfismo $\epsilon : C_0 \longrightarrow \mathbb{Z}$. Ahora consideramos el submódulo $\mathrm{N}(\epsilon)$. Como G es finito $\mathbb{Z}[G]$ es un $\mathbb{Z}$-módulo libre de rango finito, luego lo mismo le ocurre a C_0, luego $\mathrm{N}(\epsilon)$ es un $\mathbb{Z}$-módulo finitamente generado, luego también un G-módulo finitamente generado. Por consiguiente existe un G-módulo libre de rango finito C_1 junto con un epimorfismo $\partial_1 : C_1 \longrightarrow \mathrm{N}(\epsilon) \subset C_0$, etc. De este modo obtenemos la resolución buscada.

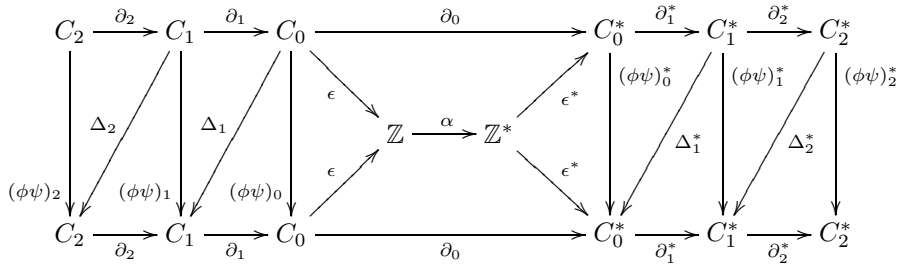
Supongamos que tenemos dos resoluciones completas de G, construidas a partir de dos resoluciones reducidas $\mathcal{C}$ y $\mathcal{C}'$. El teorema 14.22 nos da dos homomorfismos $\phi : \mathcal{C} \longrightarrow \mathcal{C}'$ y $\psi : \mathcal{C}' \longrightarrow \mathcal{C}$, a partir de los cuales podemos construir el homomorfismo siguiente entre las resoluciones completas asociadas:



Para probar que ciertamente es un homomorfismo de complejos hay que ver que todos los cuadrados son conmutativos. En realidad sólo hay que probarlo para el diagrama central. Ahora bien:

$$\phi_0\partial'_0 = \phi_0\epsilon'\alpha\epsilon'^* = \epsilon\alpha\epsilon'^* = \epsilon\alpha\epsilon^*\psi_0^* = \partial_0\psi_0^*.$$

Intercambiando los papeles de ϕ y ψ obtenemos un homomorfismo en sentido opuesto. Si componemos ambos homomorfismos y consideramos la homotopía entre $\phi\psi$ y 1 dada por el teorema 14.22 tenemos



Es claro que Δ así extendida (tomando $\Delta_0 = 0$) es una homotopía para el homomorfismo extendido y la identidad. Igualmente sucede para la composición inversa.

Los módulos duales de módulos libres son libres, luego las resoluciones completas son libres. Falta probar que son exactas. Toda resolución completa para un grupo G lo es también para el grupo trivial 1 (pues $\mathbb{Z}[G]$ es un $\mathbb{Z} = \mathbb{Z}[1]$-módulo libre). Una resolución para el grupo trivial es por ejemplo

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0,$$

donde ϵ es la identidad (pues en este caso $\mathbb{Z}$ es libre). Por consiguiente una resolución completa del grupo trivial es

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}^* & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & & & \downarrow{\scriptstyle \epsilon} & & \uparrow{\scriptstyle \epsilon'} & & & & \\ & & & & \mathbb{Z} & \longrightarrow & \mathbb{Z}^* & & & & \end{array} \tag{14.3}$$

Este complejo es, pues, equivalente a cualquier resolución completa de G, luego sus grupos de homología son isomorfos, pero los de este último complejo son todos triviales, luego los de cualquier otro también lo son, pero esto significa que la sucesión es exacta. ∎

Grupos de homología y cohomología Finalmente estamos en condiciones de definir los grupos de homología y cohomología de un G-módulo A. Para ello construimos, como habíamos anunciado, dos complejos (uno directo y otro inverso) a partir de A y de una resolución completa de G.

Definición 14.25 Sea G un grupo finito y A un G-módulo. Si $\mathcal{C}$ es un complejo de G-módulos definimos los complejos de $\mathbb{Z}$-módulos (= 1-módulos) $A \otimes_G \mathcal{C}$ y $\mathrm{Hom}_G(\mathcal{C}, A)$ mediante

$$\cdots \longrightarrow A \otimes_G C_{n+1} \xrightarrow{1\otimes\partial_{n+1}} A \otimes_G C_n \xrightarrow{1\otimes\partial_n} A \otimes_G C_{n-1} \longrightarrow \cdots$$

$$\cdots \longrightarrow \mathrm{Hom}_G(C_{n-1}, A) \xrightarrow{\partial_n^\#} \mathrm{Hom}_G(C_n, A) \xrightarrow{\partial_{n+1}^\#} \mathrm{Hom}_G(C_{n+1}, A) \longrightarrow \cdots$$

En el segundo caso convendremos en que el módulo n-simo es $\mathrm{Hom}_G(C_n, A)$, luego se trata de un complejo inverso cuyo n-simo operador cofrontera viene dado por $\partial^n = \partial_{n+1}^\#$. En el primer caso tenemos de forma natural que el módulo n-simo es $A \otimes_G C_n$ y $\partial_n = 1 \otimes \partial_n$.

Todo homomorfismo graduado $f : \mathcal{C} \longrightarrow \mathcal{C}'$ induce homomorfismos graduados

$$1 \otimes f : A \otimes_G \mathcal{C} \longrightarrow A \otimes_G \mathcal{C}' \quad \text{y} \quad f^\# : \mathrm{Hom}_G(\mathcal{C}, A) \longrightarrow \mathrm{Hom}_G(\mathcal{C}', A).$$

Se conservan todas las composiciones, de modo que si f es un homomorfismo de complejos o una homotopía entre homomorfismos de complejos, lo mismo sucede con los homomorfismos inducidos.

Si f es un homomorfismo de complejos definimos los homomorfismos de grupos

$$f_{*n} = \overline{1 \otimes f_n} : H_n(A \otimes_G \mathcal{C}) \longrightarrow H_n(A \otimes_G \mathcal{C}'),$$

$$f^{*n} = \overline{f_n^\#} : H^n(\mathrm{Hom}_G(\mathcal{C}', A)) \longrightarrow H^n(\mathrm{Hom}_G(\mathcal{C}, A)).$$

Es inmediato que $(fg)_* = f_* g_*$, $(fg)^* = f^* g^*$. Así mismo, si $f, g : \mathcal{C} \longrightarrow \mathcal{C}'$ son homotópicos ya hemos dicho que $1 \otimes f \approx 1 \otimes g$ y $f^\# \approx g^\#$, luego $f_* = g_*$ y $f^* = g^*$.

En particular tenemos que si $\mathcal{C}$ y $\mathcal{C}'$ son complejos equivalentes entonces

$$H_n(A \otimes_G \mathcal{C}) \cong H_n(A \otimes_G \mathcal{C}') \quad \text{y} \quad H^n(\mathrm{Hom}_G(\mathcal{C}, A)) \cong H^n(\mathrm{Hom}_G(\mathcal{C}', A)).$$

Esto nos permite definir los *grupos de homología y cohomología* de G y A como

$$H_n(G, A) = H_n(A \otimes_G \mathcal{C}), \qquad H^n(G, A) = H^n(\mathrm{Hom}_G(\mathcal{C}, A)), \qquad n \in \mathbb{Z},$$

donde $\mathcal{C}$ es cualquier resolución completa de G. Tenemos que estos grupos están unívocamente determinados por G y A salvo isomorfismo. Con más precisión, si los calculamos a partir de dos resoluciones distintas de G, todos los homomorfismos entre ellas inducen un mismo isomorfismo entre los grupos de (co)homología, al que llamaremos *isomorfismo natural* entre ambas construcciones.

El teorema siguiente muestra que la sucesión de grupos de homología es la misma que la de los grupos de cohomología pero en orden inverso, por lo que podemos limitarnos a estudiar una de ellas. En la práctica nos centraremos en la sucesión de cohomología.

Teorema 14.26 *Sea G un grupo finito y A un G-módulo. Entonces para todo $n \in \mathbb{Z}$ se cumple $H_n(G, A) \cong H^{-(n+1)}(G, A)$.*

Demostración: La prueba descansa esencialmente en el teorema 14.19, pero hay que prestar atención a los convenios que hemos adoptado en la numeración de los complejos.

Fijemos una resolución completa $\mathcal{C}$ de G y consideremos el diagrama siguiente:

$$\begin{array}{ccc} A \otimes_G C_n & \xrightarrow{1\otimes\partial_n} & A \otimes_G C_{n-1} \\ \downarrow & & \downarrow \\ \mathrm{Hom}_G(C_n^*, A) & \xrightarrow{(\partial_n^*)^\#} & \mathrm{Hom}_G(C_{n-1}^*, A) \end{array}$$

Las flechas verticales son los isomorfismos construidos en 14.19. Una comprobación rutinaria muestra que el diagrama conmuta. Si $n > 0$ la fila superior es un segmento del complejo $A \otimes_G \mathcal{C}$ (correspondiente a los índices n y $n-1$) y la fila inferior es un segmento del complejo $\mathrm{Hom}_G(\mathcal{C}, A)$ (correspondiente a los índices $-(n+1)$ y $-n$).

Para índices negativos el módulo C_n^* es el bidual del módulo de $\mathcal{C}$ de índice $-(n+1)$. El isomorfismo canónico entre ambos permite sustituir dicha fila inferior por otra análoga que contenga a los módulos de $\mathcal{C}$ en lugar de a sus biduales.

En conclusión tenemos un isomorfismo entre $A \otimes_G \mathcal{C}$ y $\mathrm{Hom}_G(\mathcal{C}, A)$, pero considerando al segundo como complejo directo (no inverso) cuyo grupo n-simo es el de índice $-(n+1)$ según la ordenación usual. Por lo tanto $H_n(G, A) = H^{-(n+1)}(G, A)$. ∎

Concluimos esta sección con algunos ejemplos sencillos. Ante todo recordemos que, según vimos en la prueba del teorema 14.24 una resolución completa $\mathcal{C}$ del grupo trivial es la dada por (14.3).

Como consecuencia, si A es un grupo abeliano cualquiera (un 1–módulo) entonces el complejo $A \otimes_1 \mathcal{C}$ tiene todos sus módulos triviales excepto los de índices 0 y -1, que son ambos isomorfos a A, y la aplicación que los conecta es un isomorfismo. En particular la sucesión es exacta. Con esto y el teorema anterior queda probado lo siguiente:

Teorema 14.27 *Si A es un grupo abeliano entonces $H_n(1, A) = H^n(1, A) = 0$ para todo $n \in \mathbb{Z}$.*

Veamos una generalización útil de este teorema:

Definición 14.28 Un G-módulo A es *regular* o *inducido* si $A \cong B \otimes \mathbb{Z}[G]$ para un cierto grupo abeliano B.

En tal caso, si $\mathcal{C}$ es una resolución completa de G es fácil comprobar los siguientes isomorfismos de complejos:

$$A \otimes_G \mathcal{C} \cong (B \otimes \mathbb{Z}[G]) \otimes_G \mathcal{C} \cong B \otimes (\mathbb{Z}[G] \otimes_G \mathcal{C}) \cong B \otimes \mathcal{C}.$$

Pero $\mathcal{C}$ es también una resolución completa del grupo trivial 1 y, viéndolo así, concluimos que $H_n(G, A) = H_n(A \otimes_G \mathcal{C}) = H_n(B \otimes_1 \mathcal{C}) = H_n(1, B) = 0$. Por lo tanto tenemos:

Teorema 14.29 *Si A es un G-módulo regular $H_n(G, A) = H^n(G, A) = 0$ para todo $n \in \mathbb{Z}$.*

Ejemplo Si L es un G-módulo libre entonces es regular: basta tomar como B el subgrupo generado por una G-base de L, y es claro que $L = B \otimes \mathbb{Z}[G]$ (el isomorfismo hace corresponder $b\sigma$ con $b \otimes \sigma$). Por lo tanto todos los grupos $H^n(G, L)$ y $H_n(G, L)$ son triviales. ∎

Ejemplo Si K/k es una extensión finita de Galois y G es su grupo de Galois, es claro que podemos considerar al grupo aditivo K^+ como G-módulo de forma natural. El teorema de la base normal afirma que existe un $a \in K$ de manera que $\{a\sigma \mid \sigma \in G\}$ es una k-base de K. Esto nos da un isomorfismo de G-módulos $K^+ \cong k^+ \otimes \mathbb{Z}[G]$. Concretamente, el isomorfismo hace corresponder cada $\sum_{\sigma \in G} \alpha_\sigma(a\sigma)$ con $\sum_{\sigma \in G} \alpha_\sigma \otimes \sigma$. Por lo tanto concluimos que $H_n(G, K^+) = H^n(G, K^+) = 0$ para todo $n \in \mathbb{Z}$. ∎

En relación con las extensiones de Galois, los grupos de cohomología que nos van a interesar son los correspondientes al grupo multiplicativo K^*, que también es un G-módulo de forma natural. Estos grupos de cohomología ya no son triviales en general.

Definición 14.30 Si K/k es una extensión finita de Galois se definen los *grupos de homología y cohomología de Galois* de la extensión como

$$H_n(K/k) = H_n(G, K^*), \qquad H^n(K/k) = H^n(G, K^*).$$

Por último conviene comentar que originalmente se definieron independientemente las sucesiones de homología y cohomología de un G-módulo A para índices no negativos exclusivamente (considerando resoluciones reducidas en lugar de resoluciones completas). En tal caso el grupo G no necesita ser finito. La posibilidad de enlazar ambas sucesiones de grupos en una sola es una característica exclusiva de los grupos finitos (gracias a las propiedades de los módulos duales), y se debe a Tate. La relación entre la cohomología de Tate (o la homología, que es equivalente) y la homología y cohomología tradicionales es la descrita en el teorema 14.26, con la salvedad de que el grupo $H^0(G, A)$ es distinto según si se calcula con resoluciones reducidas o con resoluciones completas.

14.3 Las sucesiones exactas de homología y cohomología

Antes de dar más detalles sobre los grupos de cohomología demostraremos un teorema general que tiene gran importancia en la teoría y no requiere de más técnicas que las que hemos venido manejando hasta ahora. Comenzamos con un resultado auxiliar.

Teorema 14.31 *Consideremos el siguiente diagrama conmutativo de G-módulos y supongamos que sus filas son exactas.*

$$\begin{array}{ccccccccc} & & Z_1' & \xrightarrow{\phi'} & Z_2' & \xrightarrow{\psi'} & Z_3' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \partial_1} & & \downarrow{\scriptstyle \partial_2} & & \downarrow{\scriptstyle \partial_3} & & \\ 0 & \longrightarrow & Z_1 & \xrightarrow[\phi]{} & Z_2 & \xrightarrow[\psi]{} & Z_3 & & \end{array}$$

Entonces existe un homomorfismo de G-módulos $\delta_* : \mathrm{N}(\partial_3) \longrightarrow Z_1/\operatorname{Im}\partial_1$ tal que la sucesión

$$N(\partial_1) \xrightarrow{\phi''} \mathrm{N}(\partial_2) \xrightarrow{\psi''} \mathrm{N}(\partial_3) \xrightarrow{\delta_*} Z_1/\operatorname{Im}\partial_1 \xrightarrow{\bar\phi} Z_2/\operatorname{Im}\partial_2 \xrightarrow{\bar\psi} Z_3/\operatorname{Im}\partial_3$$

es exacta, donde ϕ'' y ψ'' son las restricciones de ϕ' y ψ' a $\mathrm{N}(\partial_1)$ y $\mathrm{N}(\partial_2)$ y $\bar\phi$, $\bar\psi$ son los homomorfismos inducidos de forma natural.

Demostración: Es fácil comprobar que las aplicaciones ϕ'', ψ'', $\bar\phi$ y $\bar\psi$ están bien definidas, así como la exactitud de la sucesión en $\mathrm{N}(\partial_2)$ y $Z_2/\operatorname{Im}\partial_2$.

Para definir δ_* tomamos $c'_3 \in \mathrm{N}(\partial_3)$. Entonces existe $c'_2 \in Z'_2$ tal que $c'_3 = \psi'(c'_2)$. Como $\psi(\partial_2(c'_2)) = \partial_3(\psi'(c'_2)) = \partial_3(c'_3) = 0$, existe un $c_1 \in Z_1$ tal que $\phi(c_1) = \partial_2(c'_2)$.

Es claro que c'_2 es único módulo $\mathrm{N}(\psi') = \operatorname{Im}\phi'$, luego $\partial_2(c'_2)$ es único módulo $\phi[\operatorname{Im}\partial_1]$, luego c_1 es único módulo $\operatorname{Im}\partial_1$.

Por lo tanto podemos definir $\delta_*(c'_3) = c_1 + \operatorname{Im}\partial_1$. Es claro que, así definido, es un homomorfismo de G-módulos. (Observar que en definitiva δ_* se calcula eligiendo una antiimagen por ψ', su imagen por ∂_2 y una antiimagen por ψ.)

Es claro que $\operatorname{Im}\psi'' \subset \mathrm{N}(\delta_*)$. Si $c'_3 \in \mathrm{N}(\delta_*)$ entonces $c_1 = \partial_1(c'_1)$, para un cierto $c'_1 \in Z'_1$, luego $\partial_2(c'_2) = \phi(c_1) = \phi(\partial_1(c'_1)) = \partial_2(\phi'(c'_1))$, con lo que $c'_2 - \phi'(c'_1) \in \mathrm{N}(\partial_2)$ y así

$$c'_3 = \psi'(c'_2) = \psi'\big(c'_2 - \phi'(c'_1)\big) + \psi'\big(\phi'(c'_1)\big) = \psi'\big(c'_2 - \phi'(c'_1)\big) \in \operatorname{Im}\psi''.$$

También es claro que $\operatorname{Im}\delta_* \subset \mathrm{N}(\bar{\phi})$. Si $c_1 + \operatorname{Im}\partial_1 \in \mathrm{N}(\bar{\phi})$ entonces tenemos que $\phi(c_1) \in \operatorname{Im}\partial_2$, digamos $\phi(c_1) = \partial_2(c'_2)$, con $c'_2 \in Z'_2$. Sea $c'_3 = \psi'(c'_2)$. Es claro que $c'_3 \in \mathrm{N}(\partial_3)$ y por construcción $\delta_*(c'_3) = c_1 + \operatorname{Im}\partial_1$, luego concluimos que $c_1 + \operatorname{Im}\partial_1 \in \operatorname{Im}\delta_*$. ∎

De aquí deducimos:

Teorema 14.32 *Si* $0 \longrightarrow \mathcal{A} \xrightarrow{\phi} \mathcal{B} \xrightarrow{\psi} \mathcal{C} \longrightarrow 0$ *es una sucesión exacta de complejos de G-módulos entonces existen homomorfismos de G-módulos*

$$\delta_{*n} : H_n(\mathcal{C}) \longrightarrow H_{n-1}(\mathcal{A})$$

tales que la sucesión siguiente es exacta:

$$\cdots \longrightarrow H_n(\mathcal{A}) \xrightarrow{\overline{\phi_n}} H_n(\mathcal{B}) \xrightarrow{\overline{\psi_n}} H_n(\mathcal{C}) \xrightarrow{\delta_{*n}} H_{n-1}(\mathcal{A}) \xrightarrow{\overline{\phi_{n-1}}} H_{n-1}(\mathcal{B}) \longrightarrow \cdots$$

Demostración: La hipótesis significa que las sucesiones

$$0 \longrightarrow C_n(\mathcal{A}) \xrightarrow{\phi_n} C_n(\mathcal{B}) \xrightarrow{\psi_n} C_n(\mathcal{C}) \longrightarrow 0,$$

son exactas para todo $n \in \mathbb{Z}$.

Basta comprobar que el diagrama siguiente se encuentra en las hipótesis del teorema anterior.

$$\begin{array}{ccccccccc}
 & & C_n(\mathcal{A})/F_n(\mathcal{A}) & \xrightarrow{\phi_n} & C_n(\mathcal{B})/F_n(\mathcal{B}) & \xrightarrow{\psi_n} & C_n(\mathcal{C})/F_n(\mathcal{C}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial_n} & & \\
0 & \longrightarrow & Z_{n-1}(\mathcal{A}) & \xrightarrow{\phi_{n-1}} & Z_{n-1}(\mathcal{B}) & \xrightarrow{\psi_{n-1}} & Z_{n-1}(\mathcal{C}) & &
\end{array}$$

(donde Z y F representan los grupos de ciclos y fronteras de los complejos.)

Ciertamente la fila superior está bien definida, ψ_n es suprayectiva y se cumple $\operatorname{Im}\phi_n \subset \mathrm{N}(\psi_n)$.

Si $\psi_n(u + F_n(\mathcal{B})) = 0$ entonces $\psi_n(u) \in F_n(\mathcal{C})$, luego $\psi_n(u) = \partial_{n-1}(v)$, para un cierto $v \in C_{n-1}(\mathcal{C})$, que a su vez es de la forma $v = \psi_{n-1}(w)$ con $w \in C_{n-1}(\mathcal{B})$. Así pues, $\psi_n(u) = \partial_{n-1}(\psi_{n-1}(w)) = \psi_n(\partial_{n-1}(w))$, con lo que $u - \partial_{n-1}(w) \in \mathrm{N}(\psi_n)$. Por consiguiente existe un $x \in C_n(\mathcal{A})$ tal que $u - \partial_{n-1}(w) = \phi_n(x)$, luego $u + F_n(\mathcal{B}) = \phi_n(x + F_n(\mathcal{A}))$.

Esto prueba la exactitud de la fila superior. Es obvio que el diagrama conmuta, que ϕ_{n-1} es inyectiva y que $\operatorname{Im}\phi_{n-1} \subset \mathrm{N}(\psi_{n-1})$.

Supongamos por último que $x \in \mathrm{N}(\psi_{n-1})$. Entonces $x = \phi_{n-1}(y)$ para un $y \in C_{n-1}(\mathcal{A})$ y hay que probar que $y \in Z_{n-1}(\mathcal{A})$. Ahora bien, $\phi_{n-2}(\partial_{n-1}(y)) = \partial_{n-1}(\phi_{n-1}(y)) = \partial_{n-1}(x) = 0$ (pues x es un ciclo). Como ϕ_{n-2} es inyectiva resulta que $\partial_{n-1}(y) = 0$, luego y es un ciclo. ∎

Los homomorfismos δ_{*n} reciben el nombre de *homomorfismos de conexión* de la sucesión exacta dada. Conviene recordar cómo actúa: dado un ciclo de $\mathcal{C}$ de dimensión $n-1$, tomamos cualquier antiimagen por ψ, calculamos la frontera de ésta, calculamos su antiimagen por ϕ y la clase del ciclo resultante es la imagen por δ_{*n} de la clase del ciclo de partida.

Naturalmente el teorema anterior es igualmente válido para el caso de complejos inversos. Con esto estamos en condiciones de probar el objetivo de esta sección.

Teorema 14.33 *Sea G un grupo finito y $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ una sucesión exacta de G-módulos. Entonces existen homomorfismos de grupos*

$$\delta_{*n} : H_n(G, C) \longrightarrow H_{n-1}(G, A),$$

$$\delta^{*n} : H^n(G, C) \longrightarrow H^{n-1}(G, A),$$

(homomorfismos de conexión) tales que las sucesiones siguientes son exactas:

$$\cdots \xrightarrow{\alpha_*} H_n(G, B) \xrightarrow{\beta_*} H_n(G, C) \xrightarrow{\delta_*} H_{n-1}(G, A) \xrightarrow{\alpha_*} H_{n-1}(G, B) \xrightarrow{\beta_*} \cdots$$

$$\cdots \xrightarrow{\alpha^*} H^{n-1}(G, B) \xrightarrow{\beta^*} H^{n-1}(G, C) \xrightarrow{\delta^*} H^n(G, A) \xrightarrow{\alpha^*} H^n(G, B) \xrightarrow{\beta^*} \cdots$$

donde $\alpha_* = \overline{\alpha \otimes 1}$, $\alpha^* = \overline{\alpha_\#}$, e igualmente con β.

Demostración: Sea $\mathcal{C}$ una resolución completa de G. Como sus módulos son libres, los teoremas 14.15 y 14.16 implican la exactitud de las sucesiones de complejos

$$0 \longrightarrow A \otimes_G \mathcal{C} \xrightarrow{\alpha\otimes 1} B \otimes_G \mathcal{C} \xrightarrow{\beta\otimes 1} C \otimes_G \mathcal{C} \longrightarrow 0$$

y

$$0 \longrightarrow \mathrm{Hom}_G(\mathcal{C}, A) \xrightarrow{\alpha_\#} \mathrm{Hom}_G(\mathcal{C}, B) \xrightarrow{\beta_\#} \mathrm{Hom}_G(\mathcal{C}, C) \longrightarrow 0.$$

Ahora basta aplicar el teorema anterior. ∎

Los homomorfismos de conexión actúan del siguiente modo: dada una clase de (co)homología de C, para calcular su imagen por δ se escoge un (co)ciclo

representante, se escoge una antiimagen de éste por β, se calcula su (co)frontera y se escoge una antiimagen de ésta por α. La clase del (co)ciclo obtenido es la imagen buscada.

También es importante notar que las aplicaciones inducidas son independientes de la resolución con que calculamos los grupos de (co)homología, en el sentido de que si tenemos dos resoluciones $\mathcal{C}$, $\mathcal{C}'$ y $u : \mathcal{C}' \longrightarrow \mathcal{C}$ es un homomorfismo entre ellas que induce isomorfismos u^* entre los grupos de cohomología (por ejemplo) entonces se cumple $\alpha^* u^* = u^* \alpha^*$, pues ambos actúan como $(\alpha^* u^*)([f]) = [uf\alpha]$, para todo cociclo $f \in \mathrm{Hom}_G(C_n, A)$. Lo mismo es válido para β y vamos a ver que también para δ.

En efecto, para calcular $\delta^*([f])$, donde $f \in \mathrm{Hom}_G(C_n, C)$ es un cociclo, elegimos un $g \in \mathrm{Hom}_G(C_n, B)$ de modo que $g\beta = f$ y luego $h \in \mathrm{Hom}_G(C_{n+1}, A)$ tal que $h\alpha = \partial g$, y entonces $\delta^*([f]) = [h]$. Pero también tenemos $ug\beta = f$ y $uh\alpha = u\partial g = \partial ug$, es decir,

$$\delta^*(u^*([f])) = \delta^*([uf]) = [uh] = u^*([h]) = u^*(\delta^*([f]).$$

Los mismos argumentos valen para los homomorfismos entre grupos de homología.

Como aplicación demostraremos un sencillo resultado que resulta útil con frecuencia en demostraciones por inducción.

Teorema 14.34 (Reducción regular) *Sea G un grupo finito y A un G-módulo. Entonces existen G-módulos A^+ y A^- tales que para todo $S \leq G$ y todo entero n se cumple*

$$H^n(S, A^+) \cong H^{n+1}(S, A), \qquad H^n(S, A^-) \cong H^{n-1}(S, A).$$

Demostración: Notar que todo G-módulo es un S-módulo de forma natural. Consideramos el módulo regular $B = A \otimes \mathbb{Z}[G]$, y las sucesiones exactas

$$0 \longrightarrow A^- \longrightarrow B \longrightarrow A \longrightarrow 0,$$

$$0 \longrightarrow A \longrightarrow B \longrightarrow A^+ \longrightarrow 0,$$

determinadas por el epimorfismo $a \otimes \sigma \mapsto a$ y el monomorfismo $a \mapsto \sum_\sigma a\sigma^{-1} \otimes \sigma$, respectivamente.

Observar que $\mathbb{Z}[G]$ es un S-módulo libre (una base es, por ejemplo, un conjunto de representantes de las clases a derecha módulo S). Por lo tanto $\mathbb{Z}[G]$ es S-regular y B también. Según el teorema 14.29 todos los grupos $H^n(S, B)$ son triviales, luego la sucesión de cohomología asociada a la primera sucesión exacta es de la forma

$$0 \longrightarrow H^{n-1}(S, A) \xrightarrow{\delta^*} H^n(S, A^-) \longrightarrow 0,$$

luego los homomorfismos de conexión son isomorfismos. Similarmente se razona con la segunda sucesión exacta. ∎

14.4 Cálculo de grupos de cohomología

El primer paso para calcular los grupos de cohomología de un grupo finito G es obtener una resolución completa. Nos ocupamos en primer lugar de los grupos cíclicos, donde el problema es especialmente simple y no por ello menos importante en la teoría.

La resolución monomial Sea $G = \langle\sigma\rangle$ un grupo cíclico de orden n. Para construir una resolución reducida de G partimos del G-módulo trivial $\mathbb{Z}$. Hemos de definir un epimorfismo ϵ de un G-módulo libre C_0 en $\mathbb{Z}$. Puesto que $\mathbb{Z}$ está generado por 1, podemos tomar un G-módulo libre de rango 1, digamos $C_0 = \langle u_0\rangle$ y definir $\epsilon : C_0 \longrightarrow \mathbb{Z}$ mediante $\epsilon(u_0) = 1$.

Ahora hemos de calcular el núcleo de ϵ y definir un epimorfismo de otro G-módulo libre C_1 sobre dicho núcleo. Es claro que $u_0(\sigma - 1) \in \mathrm{N}(\epsilon)$, pues $\epsilon(u_0(\sigma-1)) = 1(\sigma-1) = 1-1 = 0$. Vamos a probar que $\mathrm{N}(\epsilon) = \langle u_0(\sigma-1)\rangle$.

Un elemento arbitrario de C_0 es de la forma $c = u_0 \sum_{i=0}^{n-1} m_i\sigma^i$, y claramente $c \in \mathrm{N}(\epsilon)$ si y sólo si

$$\epsilon(c) = \sum_{i=0}^{n-1} m_i = 0.$$

Por otra parte, la ecuación

$$u_0(\sigma-1)\sum_{i=0}^{n-1} x_i\sigma^i = u_0\sum_{i=0}^{n-1} m_i\sigma^i$$

equivale al sistema

$$m_0 = x_{n-1} - x_0,\ m_1 = x_0 - x_1,\ m_2 = x_1 - x_2,\ \ldots, m_{n-1} = x_{n-2} - x_{n-1},$$

que a su vez es equivalente a

$$x_0 = x_{n-1} - m_0,\ x_1 = x_{n-1} - (m_0 + m_1),\ \ldots,\ x_{n-1} = x_{n-1} - \sum_{i=0}^{n-1} m_i.$$

La última ecuación es contradictoria salvo si $\epsilon(c) = 0$, en cuyo caso cualquier valor de x_{n-1} determina una solución del sistema.

Así pues, si $\epsilon(c) = 0$ entonces $c = u_0(\sigma-1)x$, para un cierto $x \in \mathbb{Z}[G]$, luego en efecto $\mathrm{N}(\epsilon) = \langle u_0(\sigma-1)\rangle$. Consecuentemente podemos tomar un G-módulo libre de rango 1, digamos $C_1 = \langle u_1\rangle$ y definir $\partial_1 : C_1 \longrightarrow C_0$ mediante $\partial_1(u_1) = u_0(\sigma-1)$.

Ahora,

$$\partial_1\Big(u_1\sum_{i=0}^{n-1} m_i\sigma^i\Big) = u_0(\sigma-1)\sum_{i=0}^{n-1} m_i\sigma^i$$

$$= u_0\big((m_{n-2} - m_{n-1})\sigma^{n-1} + \cdots + (m_0 - m_1)\sigma + (m_{n-1} - m_0)\big),$$

luego los elementos de $\mathrm{N}(\partial_1)$ son los de la forma $u_1 mT$, donde

$$T = \sum_{i=0}^{n-1} \sigma^i \in \mathbb{Z}[G].$$

Esto nos lleva a definir $C_2 = \langle u_2 \rangle$ y $\partial_2 : C_2 \longrightarrow C_1$ mediante $\partial_2(u_2) = u_1 T$. Para el paso siguiente observamos que $T\sigma = T$, luego

$$\partial_2\Big(u_2 \sum_{i=0}^{n-1} m_i \sigma^i\Big) = u_1 T \sum_{i=0}^{n-1} m_i \sigma^i = u_1 \sum_{i=0}^{n-1} m_i T = 0 \text{ si y sólo si } \sum_{i=0}^{n-1} m_i = 0.$$

Éste es el mismo caso de antes, luego sabemos que $\mathrm{N}(\partial_2) = \langle u_2(\sigma - 1) \rangle$.

Con esto entramos en un proceso cíclico. En general definimos $C_n = \langle u_n \rangle$ como un G-módulo libre de rango 1 y establecemos que

$$\partial_{2n+1}(u_{2n+1}) = u_{2n}(\sigma - 1), \qquad \partial_{2n}(u_{2n}) = u_{2n-1} T. \tag{14.4}$$

Con estas definiciones y la ya dada para ϵ tenemos una resolución reducida de G. Ahora estudiaremos su resolución completa asociada. Sea u_n^* la base dual de u_n. Vamos a determinar $\partial_0(u_0)$. Éste se calcula pasando primero a $\epsilon(u_0) = 1$, luego a la imagen de 1 en $\mathbb{Z}^*$ a través del isomorfismo canónico, que es la aplicación identidad, a la que también representaremos por 1; finalmente $\partial_0(u_0) = \epsilon^*(1) \in C_0^*$. Para determinarlo hay que tener presente que $\partial_0(u_0)$ no es un G-homomorfismo, luego no está determinado por el valor que toma en u_0, sino por los valores que toma sobre la $\mathbb{Z}$-base $u_0\sigma^i$. Así pues

$$\partial_0(u_0)(u_0\sigma^i) = \epsilon^*(1)(u_0\sigma^i) = 1(\epsilon(u_0\sigma^i)) = 1.$$

Por otra parte,

$$(u_0^*\sigma^j)(u_0\sigma^i) = u_0^*(\sigma^j u_0 \sigma^i) = u_0^*(u_0\sigma^{i-j}) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

(Recordar que la acción de G en los módulos duales está definida como $(\sigma f)(u) = f(u\sigma)$ o, equivalentemente, $(f\sigma)(u) = f(\sigma u)$, donde $\sigma u = u\sigma^{-1}$.)

Por lo tanto concluimos que

$$\partial_0(u_0) = \sum_{i=0}^{n-1} u_0^*\sigma^i = u_0^* T.$$

Si llamamos $u_{-1} = u_0^*$ tenemos que la fórmula (14.4) vale para $2n = 0$.

La aplicación ∂_{-1} es la dual de ∂_1. En general tenemos que

$$(\partial_{-(2n+1)} u_{2n}^*)(u_{2n+1}\sigma^i) = (\partial_{2n+1}^* u_{2n}^*)(u_{2n+1}\sigma^i) = u_{2n}^*(\partial_{2n+1} u_{2n+1}\sigma^i)$$

$$= u_{2n}^*(u_{2n}(\sigma - 1)\sigma^i) = u_{2n+1}^*(u_{2n+1}(\sigma - 1)\sigma^i) = ((\sigma - 1)u_{2n+1}^*)(u_{2n+1}\sigma^i)$$

$$= (u_{2n+1}^*(\sigma^{-1} - 1))(u_{2n+1}\sigma^i).$$

Por lo tanto

$$\partial_{-(2n+1)}u^*_{2n} = u^*_{2n+1}(\sigma^{-1} - 1)$$

y, del mismo modo,

$$\partial_{-2n}u^*_{2n-1} = u^*_{2n}T.$$

En particular $\partial_{-1}u_{-1} = \partial_{-1}u^*_0 = u^*_1(\sigma^{-1} - 1) = u^*_1(-\sigma^{-1})(\sigma - 1)$.

Así, si definimos $u_{-2} = u^*_1(-\sigma^{-1})$ seguimos teniendo una base de C_{-2} y la fórmula (14.4) vale para $2n + 1 = -1$.

Igualmente $\partial_{-2}u_{-2} = \partial_{-2}u^*_1(-\sigma^{-1}) = u^*_2T(-\sigma^{-1}) = u^*_2T$, y definimos $u_{-3} = u^*_2$. Siguiendo de este modo expresamos $C_n = \langle u_n\rangle$ de modo que (14.4) es válido para todo $n \in \mathbb{Z}$.

En particular, la aplicación dada por $\omega(u_n) = u_{n+2}$ es un isomorfismo de grado 2 del complejo $\mathcal{C}$ en sí mismo. Si A es un G-módulo, este isomorfismo induce otro análogo en el complejo $\mathrm{Hom}_G(\mathcal{C}, A)$, que a su vez nos da los isomorfismos $H^n(G, A) \cong H^{n+2}(G, A)$ para todo $n \in \mathbb{Z}$.

Consecuentemente sólo nos falta calcular los grupos $H^0(G, A)$ y $H^1(G, A)$. Para ello observamos que cada grupo $\mathrm{Hom}_G(C_n, A)$ es isomorfo a A mediante $f \mapsto f(u_n)$. A través de estos isomorfismos, los operadores cofrontera se convierten en

$$\partial^{2n+1}a = aT, \qquad \partial^{2n}a = a(\sigma - 1).$$

Por consiguiente, los cociclos de dimensión 0 son los elementos de A que cumplen $a(\sigma - 1) = 0$ o, equivalentemente, $a\sigma = a$, y las cofronteras son los elementos de la forma aT.

En general, si A es un G-módulo, definimos A^G como el submódulo formado por los elementos fijados por todos los elementos de G. Acabamos de probar que

$$H^{2n}(G, A) \cong A^G/AT.$$

Igualmente,

$$H^{2n+1}(G, A) \cong A_T/A(\sigma - 1),$$

donde $A_T = \{a \in A \mid aT = 0\}$. Comparar con (7.2).

Por ejemplo, si K/k es una extensión finita de Galois cíclica y A es el grupo aditivo de K, entonces $A^G = k$, $AT = \mathrm{Tr}[K]$, donde Tr es la traza de la extensión. Sabemos que los grupos de cohomología son triviales, luego concluimos que $\mathrm{Tr}[K] = k$, es decir, la traza es suprayectiva. Así mismo, concluimos que los elementos de K de traza nula son exactamente los de la forma $\sigma(a) - a$. Esto es parte del teorema 90 de Hilbert. La parte multiplicativa la obtendremos más adelante.

La resolución de G que hemos construido recibe el nombre de *resolución monomial.*

La resolución canónica Ahora construimos una resolución completa para un grupo finito arbitrario G, a la que llamaremos *resolución canónica.* Para

cada $n \geq 0$ definimos $C_n = \mathbb{Z}[G] \otimes \cdots \otimes \mathbb{Z}[G]$ ($n+1$ veces). Así C_n es un G-módulo libre y una base la forman los tensores

$$[\sigma_1, \ldots, \sigma_n] = \sigma_1 \otimes \cdots \otimes \sigma_n \otimes 1,$$

donde $\sigma_1, \ldots, \sigma_n$ varían en G. Convenimos en que $[\,] = 1$ es una base de C_0. Definimos los monomorfismos de grupos

$$D_n : C_n \longrightarrow C_{n+1} \qquad \text{y} \qquad E : \mathbb{Z} \longrightarrow C_0$$

mediante

$$D_n([\sigma_1, \ldots, \sigma_n]\sigma) = [\sigma_1, \ldots, \sigma_n, \sigma], \quad (D_0(\sigma) = [\sigma]), \quad E(1) = 1.$$

Con ayuda de estas aplicaciones podemos definir los G-homomorfismos

$$\epsilon : C_0 \longrightarrow \mathbb{Z} \qquad \text{y} \qquad \partial_n : C_n \longrightarrow C_{n-1}.$$

La aplicación ϵ es simplemente el epimorfismo dado por $\epsilon([\,]) = 1$. Las aplicaciones ∂_n vienen determinadas por las ecuaciones

$$\begin{aligned} &D_0\partial_1 + \epsilon E = 1, \\ &D_n\partial_{n+1} + \partial_n D_{n-1} = 1, \quad \text{para } n > 0. \end{aligned}$$

Como D_{n-1} es inyectivo e $\operatorname{Im} D_{n-1}$ contiene una base de C_n, es claro que estas fórmulas determinan a ∂_n. Más detalladamente, si suponemos definido ∂_n entonces

$$\begin{aligned} \partial_{n+1}([\sigma_1, \ldots, \sigma_{n+1}]) &= \partial_{n+1}(D_n([\sigma_1, \ldots, \sigma_n]\sigma_{n+1})) \\ &= (1 - \partial_n D_{n-1})([\sigma_1, \ldots, \sigma_n]\sigma_{n+1}) \\ &= [\sigma_1, \ldots, \sigma_n]\sigma_{n+1} - D_{n-1}(\partial_n([\sigma_1, \ldots, \sigma_n]\sigma_{n+1})). \end{aligned}$$

Definiendo así ∂_{n+1} sobre la base $[\sigma_1, \ldots, \sigma_{n+1}]$ es claro que se cumple la ecuación sobre los elementos de la $\mathbb{Z}$-base $[\sigma_1, \ldots, \sigma_n]\sigma_{n+1}$, y por linealidad se cumple para todos los elementos de C_n.

La sucesión $\cdots \longrightarrow C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$ es un complejo de G-módulos. Por ejemplo, vamos a probar que $\partial_{n+1}\partial_n = 0$ para $n > 1$ (los otros casos son similares). Suponemos como hipótesis inductiva que $\partial_n\partial_{n-1} = 0$. Entonces

$$D_n\partial_{n+1}\partial_n = (1 - \partial_n D_{n-1})\partial_n = \partial_n - \partial_n D_{n-1}\partial_n$$

$$= \partial_n - \partial_n(1 - \partial_{n-1}D_{n-2}) = \partial_n - \partial_n + \partial_n\partial_{n-1}D_{n-2} = 0 + 0 = 0.$$

Como $\operatorname{Im} D_n$ contiene una base de C_{n+1}, concluimos que $\partial_{n+1}\partial_n = 0$.

Si $u \in \mathrm{N}(\partial_n)$ entonces $u = \partial_{n+1}(D_n(u))$, luego $u \in \operatorname{Im}\partial_{n+1}$, para $n > 0$. Similarmente se prueba la exactitud en C_0 y por lo tanto el complejo es una resolución reducida de G, que a su vez determina una resolución completa.

Veamos cómo actúan explícitamente los primeros operadores frontera:

$$\begin{aligned}
\partial_1([\sigma_1]) &= \partial_1(D_0([\,]\sigma_1)) = [\,]\sigma_1 - E(\epsilon([\,]\sigma_1)) = \sigma_1 - 1.\\
\partial_2([\sigma_1,\sigma_2]) &= \partial_2(D_1([\sigma_1]\sigma_2)) = [\sigma_1]\sigma_2 - D_0(\partial_1([\sigma_1])\sigma_2)\\
&= [\sigma_1]\sigma_2 - D_0((\sigma_1-1)\sigma_2)\\
&= [\sigma_1]\sigma_2 - [\sigma_1\sigma_2] + [\sigma_2].\\
\partial_3([\sigma_1,\sigma_2,\sigma_3]) &= \partial_3(D_2([\sigma_1,\sigma_2]\sigma_3))\\
&= [\sigma_1,\sigma_2]\sigma_3 - D_1([\sigma_1]\sigma_2\sigma_3 - [\sigma_1\sigma_2]\sigma_3 + [\sigma_2]\sigma_3)\\
&= [\sigma_1,\sigma_2]\sigma_3 - [\sigma_1,\sigma_2\sigma_3] + [\sigma_1\sigma_2,\sigma_3] - [\sigma_2,\sigma_3].
\end{aligned}$$

En los C_{-n} consideramos la base dual $\langle\sigma_1,\dots,\sigma_{n-1}\rangle$ de $[\sigma_1,\dots,\sigma_{n-1}]$. Tenemos que $\epsilon([\,]) = 1$ y 1 se corresponde en $\mathbb{Z}^*$ con la identidad I, con lo que $\partial_0([\,])(\sigma) = \epsilon^*(I)(\sigma) = I(\epsilon(\sigma)) = 1$. Por lo tanto

$$\partial_0([\,]) = \langle\,\rangle\, T,$$

donde $T = \sum_{\sigma\in G}\sigma$. Similarmente

$$\begin{aligned}
\partial_{-1}\big(\langle\,\rangle\big)([\sigma_1]\sigma_2) &= \langle\,\rangle\,\big(\partial_1([\sigma_1]\sigma_2\big) = \langle\,\rangle\,([\,]\sigma_1\sigma_2) - \langle\,\rangle\,([\,]\sigma_2)\\
&= \Big(\sum_{\sigma\in G}\langle\sigma\rangle\,\sigma^{-1}\Big)\big([\sigma_1]\sigma_2\big)) - \sum_{\sigma\in G}\langle\sigma\rangle\,([\sigma_1]\sigma_2),
\end{aligned}$$

luego $\partial_{-1}\big(\langle\,\rangle\big) = \sum_{\sigma\in G}\langle\sigma\rangle\,(\sigma^{-1}-1)$.

De este modo podemos calcular cualquier operador frontera ∂_{-n}.

Si A es un G-módulo, las cocadenas de dimensión n de (G,A) son los elementos de $\mathrm{Hom}_G(C_n,A)$, pero éstos están determinados por sus imágenes sobre los elementos de la base de C_n, de la forma $[\sigma_1,\dots,\sigma_n]$ o $\langle\sigma_1,\dots,\sigma_{-n-1}\rangle$. Por lo tanto podemos identificar el grupo de cocadenas $C^n(G,A)$ con el grupo de funciones de n (o $-n-1$) variables de G en A (sumadas puntualmente). Específicamente, $C^0(G,A) = A$, y el operador cofrontera es

$$\partial^0(a)(\sigma) = a\partial_1\big([\sigma]\big) = a(\sigma-1) = a\sigma - a. \tag{14.5}$$

Por consiguiente el grupo de cociclos $Z^0(G,A)$ está formado por los elementos $a\in A$ tales que $a\sigma = a$ para todo $\sigma\in G$, es decir, con la notación introducida en la página 354, tenemos $Z^0(G,A) = A^G$.

Para calcular las cofronteras tomamos una cocadena de dimensión -1, que no es más que un $a\in A$ (identificado con el G-homomorfismo f_a que cumple $f_a\big(\langle\,\rangle\big) = a$) y calculamos

$$\partial^{-1}(a) = \partial^{-1}(f_a)\big([\,]\big) = f_a\big(\partial_0([\,])\big) = f_a\big(\langle\,\rangle\, T\big) = aT.$$

Concluimos que, como en el caso cíclico,[1]

$$H^0(G,A) = A^G/AT.$$

[1]En la teoría general, para grupos no necesariamente finitos, los grupos de cohomología se calculan a partir de resoluciones reducidas, con lo que $C^{-1} = 0$, $F^0(G,A) = 1$ y por lo tanto $H^0(G,A) = A^G$.

En particular, si consideramos a $\mathbb{Z}$ como G-módulo trivial y $|G| = n$ es fácil ver que

$$H^0(G,\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}. \tag{14.6}$$

También hemos probado que $Z^{-1}(G,A) = A_T = \{a \in A \mid aT = 0\}$ y, por otra parte, si $\{a_\sigma\}_\sigma$ es una cocadena de dimensión -2, se cumple

$$\begin{aligned}\partial^{-2}\big(\{a_\sigma\}\big) &= \{a_\sigma\}\big(\partial_{-1}(\langle\,\rangle)\big) = \{a_\sigma\}\Big(\sum_{\sigma\in G}\langle\sigma\rangle\,(\sigma^{-1}-1)\Big)\\ &= \sum_{\sigma\in G} a_\sigma(\sigma^{-1}-1),\end{aligned} \tag{14.7}$$

con lo que claramente las cofronteras de dimensión -1 son los elementos de A de la forma

$$\sum_{\sigma\in G} a_\sigma(\sigma-1), \qquad a_\sigma \in A.$$

Si llamamos I al subgrupo generado por los elementos $\sigma-1$ en $\mathbb{Z}[G]$ cuando σ varía en G, es claro que I es un ideal de $\mathbb{Z}[G]$ (pues $(\sigma-1)\tau = (\sigma\tau-1)-(\tau-1)$) y el grupo de cofronteras es AI. En definitiva

$$H^{-1}(G,A) = A_T/AI,$$

lo que generaliza al caso cíclico que hemos estudiado antes.[2] Claramente $\mathbb{Z}_T = 0$, luego

$$H^{-1}(G,\mathbb{Z}) = 0. \tag{14.8}$$

Observar que 1 más lo elementos $\sigma - 1$ con $\sigma \neq 1$ forman una $\mathbb{Z}$-base de $\mathbb{Z}[G]$, y la aplicación $\epsilon : \mathbb{Z}[G] \longrightarrow \mathbb{Z}$ del complejo reducido canónico asigna a cada elemento de $\mathbb{Z}[G]$ su coordenada en 1 en esta base, luego $I = \mathrm{N}(\epsilon)$. En particular la sucesión

$$0 \longrightarrow I \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0 \tag{14.9}$$

es exacta. Esta circunstancia nos permite calcular indirectamente el grupo $H^{-2}(G,\mathbb{Z})$. Teniendo en cuenta que los grupos de cohomología de $\mathbb{Z}[G]$ son triviales (por el teorema 14.29), la sucesión de cohomología asociada a la sucesión anterior es

$$H^{-2}(G,\mathbb{Z}[G]) = 0 \longrightarrow H^{-2}(G,\mathbb{Z}) \xrightarrow{\partial^*} H^{-1}(G,I) \longrightarrow 0 = H^{-1}(G,\mathbb{Z}[G]),$$

luego $H^{-2}(G,\mathbb{Z}) \cong H^{-1}(G,I) = I_T/I^2 = I/I^2$, pues I es el subgrupo generado por los elementos de la forma $\sigma - 1$ y todos ellos cumplen $(\sigma-1)T = 0$, luego $I_T = I$.

Ahora probamos que $I/I^2 \cong G/G'$. En efecto, la aplicación $\sigma \mapsto \sigma - 1 + I^2$ es un homomorfismo de G en I/I^2. Basta observar que

$$\sigma\tau - 1 = (\sigma-1) + (\tau-1) + (\sigma-1)(\tau-1).$$

[2]Es fácil ver que si $G = \langle\sigma\rangle$ entonces $I = (\sigma-1)$ y $AI = A(\sigma-1)$.

Este homomorfismo induce un otro en G/G'. Recíprocamente, el homomorfismo $\sigma - 1 \mapsto \sigma G'$ (extendido a I por linealidad) tiene a I^2 en su núcleo, pues

$$(\sigma-1)(\tau-1) = (\sigma\tau-1) - (\sigma-1) - (\tau-1) \mapsto \sigma\tau\sigma^{-1}\tau^{-1}G' = G'.$$

Así tenemos un homomorfismo $I/I^2 \longrightarrow G/G'$, que obviamente es el inverso del anterior, luego ambos son isomorfismos y en total concluimos que

$$H^{-2}(G,\mathbb{Z}) \cong G/G'.$$

Vamos a describir explícitamente este isomorfismo cuando consideramos $H^{-2}(G,\mathbb{Z})$ construido a partir de la resolución canónica. Sea $\sigma \in G$ y consideremos el cociclo de dimensión -2 dado por

$$f_\sigma\big(\langle\tau\rangle\big) = \begin{cases} 1 & \text{si } \tau = \sigma, \\ 0 & \text{si } \tau \neq \sigma. \end{cases} \tag{14.10}$$

Notar que según (14.7) toda cocadena de dimensión -2 es un cociclo. Podemos considerar también a f_σ como cocadena de $C^{-2}(G,\mathbb{Z}[G])$. La imagen de f_σ por la aplicación inducida por $\mathbb{Z}[G] \longrightarrow \mathbb{Z}$ es el propio f_σ. Éste es el primer paso en el cálculo de $\delta^*([f_\sigma])$. La fórmula (14.7) nos da ahora que $\partial^{-2}(f_\sigma) = \sigma^{-1} - 1$. Este mismo cociclo se puede considerar en $C^{-1}(G,I)$, y así $\delta^*([f_\sigma]) = [\sigma^{-1}-1]$.

Al componer con el isomorfismo $I/I^2 \longrightarrow G/G'$ llegamos a σ^{-1}. Por simplificar podemos aplicar también el automorfismo de G/G' dado por $\tau \mapsto \tau^{-1}$ y en total tenemos que un isomorfismo entre G/G' y $H^{-2}(G,\mathbb{Z})$ viene dado por $[\sigma] \mapsto [f_\sigma]$.

Para terminar esta sección describimos los grupos $H^1(G,A)$ y $H^2(G,A)$. Según la fórmula (14.5) las cofronteras de dimensión 1 son las cocadenas de la forma $\{a_\sigma\} = \{a\sigma - a\}$, para un $a \in A$. Para determinar los cociclos calculamos

$$\partial^1\big(\{a_\sigma\}\big)(\sigma,\tau) = \{a_\sigma\}\big(\partial_2([\sigma,\tau])\big) = \{a_\sigma\}([\sigma]\tau - [\sigma\tau] + [\tau]) = a_\sigma\tau - a_{\sigma\tau} + a_\tau.$$

Por lo tanto los cociclos de dimensión 1 son las aplicaciones $\{a_\sigma\}$ que verifican la ecuación $a_{\sigma\tau} = a_\sigma\tau + a_\tau$. En particular, si G actúa trivialmente sobre A, entonces el grupo de cociclos es $\mathrm{Hom}(G,A)$ y el grupo de cofronteras es trivial, luego

$$H^1(G,A) = \mathrm{Hom}(G,A) \qquad \text{(si la acción es trivial.)}$$

Notar que los homomorfismos de un grupo finito G en $\mathbb{Z}$ tienen imagen finita, luego trivial, y por lo tanto $H^1(G,\mathbb{Z}) = 0$.

Respecto a $H^2(G,A)$, acabamos de probar que las cofronteras de dimensión 2 son las cocadenas de la forma $\{a_{\sigma,\tau}\} = \{a_\sigma\tau - a_{\sigma\tau} + a_\tau\}$, donde $\{a_\sigma\}$ es cualquier cocadena de dimensión 1. Por otra parte,

$$\partial^2\big(\{a_{\sigma,\tau}\}\big)(\rho,\sigma,\tau) = \{a_{\sigma,\tau}\}\big(\partial_3([\rho,\sigma,\tau])\big)$$

$$= \{a_{\sigma,\tau}\}\big([\rho,\sigma]\tau - [\rho,\sigma\tau] + [\rho\sigma,\tau] - [\sigma,\tau]\big) = a_{\rho,\sigma}\tau - a_{\rho,\sigma\tau} + a_{\rho\sigma,\tau} - a_{\sigma,\tau},$$

luego los cociclos de dimensión 2 son las cocadenas que satisfacen la ecuación

$$a_{\rho,\sigma}\tau - a_{\rho,\sigma\tau} + a_{\rho\sigma,\tau} - a_{\sigma,\tau} = 0.$$

Cohomología de Galois Los cálculos anteriores muestran que si K/k es una extensión finita de Galois entonces $H^0(K/k) = k^*/\,\mathrm{N}[K^*]$, donde N es la norma de la extensión, y $H^{-1}(K/k)$ es el cociente del núcleo de la norma sobre el grupo generado por los elementos de la forma $u/\sigma(u)$ con $u \in K^*$ y $\sigma \in G(K/k)$. Si la extensión es cíclica y σ es un generador entonces este último grupo es simplemente el conjunto de todos los elementos de la forma $u/\sigma(u)$ (con σ fijo).

Observar que la operación en los grupos que acabamos de describir es multiplicativa y esto se debe esencialmente a que lo es la operación en K^*. En general conviene usar notación multiplicativa en todos los grupos de cohomología de Galois. Consecuentemente, si $a \in K^*$ y $\sigma \in G(K/k)$ escribiremos $\sigma(a) = a^\sigma$ en lugar de $a\sigma$.

El carácter de la cohomología de Galois viene marcado por el teorema siguiente:

Teorema 14.35 (Hilbert-Speiser) *Si K/k es una extensión finita de Galois entonces $H^1(K/k) = 1$.*

Demostración: La ecuación de los cociclos de dimensión 1 con notación multiplicativa se convierte en $a_{\sigma\tau} = a_\sigma^\tau a_\tau$. Dado este cociclo, el teorema de independencia de Dedekind afirma que $\sum_\sigma a_\sigma \sigma \neq 0$, luego existe un $u \in K^*$ tal que $b = \sum_\sigma a_\sigma \sigma(u) \neq 0$. Así pues

$$b^\tau a_\tau = \sum_\sigma a_\sigma^\tau u^{\sigma\tau} a_\tau = \sum_\sigma a_{\sigma\tau} u^{\sigma\tau} = b.$$

Si llamamos $c = b^{-1}$ la igualdad anterior se convierte en $a_\tau = c^\tau c^{-1}$, luego $\{a_\tau\}$ es una cofrontera. Puesto que los cociclos coinciden con las cofronteras, el grupo de cohomología es trivial. ∎

Si la extensión K/k es cíclica tenemos que $H^{-1}(K/k) \cong H^1(K/k) = 1$, luego un elemento $\alpha \in K$ cumple $\mathrm{N}(\alpha) = 1$ si y sólo si es de la forma $\alpha = \beta/\sigma(\beta)$, donde σ es un generador fijo del grupo de Galois y $\beta \in K^*$. Esto es el teorema 90 de Hilbert.

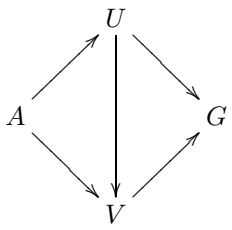
14.5 Extensiones de grupos

Terminamos el capítulo dando una interpretación del segundo grupo de cohomología. Dado un grupo U y un subgrupo normal abeliano A, tenemos que U actúa sobre A por conjugación y, como los elementos de A actúan trivialmente, es claro que también el cociente $G = U/A$ actúa sobre A. La teoría de extensiones de grupos trata de describir el grupo U a partir de los grupos A y G y de la acción de G sobre A. Conviene fijar estas ideas mediante la definición siguiente:

Definición 14.36 Una *extensión* de un grupo A por un grupo G es una sucesión exacta de grupos

$$0 \longrightarrow A \xrightarrow{i} U \xrightarrow{j} G \longrightarrow 0.$$

Dos extensiones $0 \longrightarrow U \longrightarrow G \longrightarrow 0$ y $0 \longrightarrow A \longrightarrow V \longrightarrow G \longrightarrow 0$ son *isomorfas* si existe un isomorfismo $U \longrightarrow V$ tal que los dos triángulos



son conmutativos.

Supongamos que U es una extensión de un grupo abeliano A por G (se entiende que con ciertos homomorfismos i, j). Entonces U actúa sobre $i[A]$ por conjugación y, como los elementos de $i[A]$ actúan trivialmente, es claro que $U/i[A]$ actúa de forma natural sobre $i[A]$. A través de los isomorfismos i (entre A e $i[A]$) y j (entre $U/i[A]$ y G) obtenemos una acción de G sobre A. Concretamente, si $j(u) = \sigma$ y $a \in A$ se cumple $i(a^\sigma) = i(a)^u$.

Así pues, cada extensión de un grupo abeliano A por un grupo G determina una acción de G sobre A, y es claro que extensiones isomorfas determinan la misma acción.

En el caso particular en que $A \trianglelefteq U$ y $U/A = G$, la acción de G sobre A es simplemente la inducida por la conjugación de U en A.

Una vez dadas las definiciones en general, cuando consideremos una extensión U de un grupo abeliano A por un grupo G identificaremos A con su imagen por i y a G con el cociente U/A, de modo que nos evitamos el engorro de explicitar en todo momento los homomorfismos i, j sin perder por ello generalidad.

Dada, pues, una extensión cualquiera $G = U/A$, elegimos para cada $\sigma \in G$ un elemento $u_\sigma \in U$ tal que $\sigma = [u_\sigma]$ (sin las identificaciones escribiríamos $j(u_\sigma) = \sigma$). Es importante tener presente que cuanto digamos va a depender de esta elección arbitraria, pero de nada más. Diremos que $\{u_\sigma\}$ es una *transversal* de la extensión. La acción de G sobre A es, en estos términos:

$$a^\sigma = u_\sigma^{-1} a u_\sigma.$$

Cada $u \in U$ se expresa de forma única como $u = u_\sigma a$, para un $\sigma \in G$ y un $a \in A$. Esto nos da una representación del conjunto U como $U = G \times A$, es decir, podemos identificar cada elemento $u = u_\sigma a$ de U con el par (σ, a) de $G \times A$. Ahora trataremos de expresar el producto de dos elementos de U en función de los pares que los representan.

Si $\sigma, \tau \in G$, entonces $[u_\sigma][u_\tau] = [u_{\sigma\tau}]$, luego hay un único elemento $a_{\sigma,\tau} \in A$ tal que

$$u_\sigma u_\tau = u_{\sigma\tau} a_{\sigma,\tau}. \tag{14.11}$$

En general, si $u = u_\sigma a$ y $v = u_\tau b$, entonces

$$uv = u_\sigma a u_\tau b = u_\sigma u_\tau a^\tau b = u_{\sigma\tau} a_{\sigma,\tau} a^\tau b.$$

En términos de la representación de U, esta igualdad se reescribe como

$$(\sigma, a)(\tau, b) = (\sigma\tau, a_{\sigma,\tau} a^\tau b), \tag{14.12}$$

y nos da el producto de U en términos de G, A, la acción de G sobre A y los elementos $a_{\sigma,\tau}$, los cuales determinan una cocadena de dimensión 2 de G sobre A. Más aún, la asociatividad del producto en U implica que se trata de un cociclo:

$$\begin{aligned} u_\rho(u_\sigma u_\tau) &= u_\rho u_{\sigma\tau} a_{\sigma,\tau} = u_{\rho\sigma\tau} a_{\rho,\sigma\tau} a_{\sigma,\tau}, \\ (u_\rho u_\sigma) u_\tau &= u_{\rho\sigma} a_{\rho,\sigma} u_\tau = u_{\rho\sigma} u_\tau a_{\rho,\sigma}^\tau = u_{\rho\sigma\tau} a_{\rho\sigma,\tau} a_{\rho,\sigma}^\tau. \end{aligned}$$

Igualando ambas expresiones llegamos a la relación de los cociclos:

$$a_{\rho,\sigma\tau} a_{\sigma,\tau} = a_{\rho\sigma,\tau} a_{\rho,\sigma}^\tau.$$

Hemos probado que toda extensión U de A por G determina un cociclo de dimensión 2 el cual, junto con el producto de A, el de G y la acción de G sobre A, determina completamente el producto de U.

Recíprocamente, si G es un grupo que actúa sobre un grupo abeliano A y $a_{\sigma,\tau}$ es un cociclo de dimensión 2 de G sobre A, podemos construir una extensión de A por G haciendo $U = G \times A$ y definiendo el producto mediante (14.12). La relación de los cociclos permite probar fácilmente que este producto es asociativo. Para encontrar el elemento neutro observamos que de la relación de los cociclos, haciendo $\sigma = \tau = 1$, se deduce que $a_{1,1} = a_{\rho,1}$ para todo $\rho \in G$, y si $\rho = \sigma = 1$ queda que $a_{1,\tau} = a_{1,1}^\tau$ para todo $\tau \in G$. Teniendo esto en cuenta es fácil probar que $(1, a_{1,1}^{-1})$ es el elemento neutro de U. La prueba de que existen inversos no tiene problemas.

La aplicación $j : U \longrightarrow G$ dada por $j(\sigma, a) = \sigma$ es un epimorfismo de grupos cuyo núcleo es $\overline{A} = \{(1, a) \mid a \in A\}$. La aplicación $i : A \longrightarrow U$ dada por $i(a) = (1, a_{1,1}^{-1} a)$ es un isomorfismo entre A y $\overline{A}$, luego U es una extensión de A por G. Más aún, la acción inicial de G sobre A coincide con la inducida por la extensión. Concretamente, es fácil ver que

$$(1, a_{1,1}^{-1} a)(\sigma, 1) = (\sigma, a^\sigma) = (\sigma, 1)(1, a_{1,1}^{-1} a^\sigma).$$

Si partimos de una extensión $U/A = G$, seleccionamos una transversal u_σ, con ella formamos un cociclo $a_{\sigma,\tau}$ y con éste construimos la extensión U^*, resulta que la extensión final es isomorfa a la inicial. El isomorfismo es $(\sigma, a) \mapsto u_\sigma a$ (observar que $u_1 = a_{1,1}$).

Recordemos que la definición del cociclo $a_{\sigma,\tau}$ a partir de la extensión de A por G depende de la elección de la transversal $\{u_\sigma\}$. Veamos qué ocurre si tomamos otra transversal $\{v_\sigma\}$. Entonces existen elementos $\{c_\sigma\}$ en A tales que

$v_\sigma = u_\sigma c_\sigma$. Tenemos así una cocadena de dimensión 1 de G en A. Sea $b_{\sigma,\tau}$ el cociclo determinado por $\{v_\sigma\}$. Entonces

$$\begin{aligned} u_{\sigma\tau}c_{\sigma\tau}b_{\sigma,\tau} &= v_{\sigma\tau}b_{\sigma,\tau} = v_\sigma v_\tau = u_\sigma c_\sigma u_\tau c_\tau \\ &= u_\sigma u_\tau c_\sigma^\tau c_\tau = u_{\sigma\tau}a_{\sigma,\tau}c_\sigma^\tau c_\tau, \end{aligned}$$

luego $b_{\sigma,\tau} = a_{\sigma,\tau}c_\sigma^\tau c_{\sigma\tau}^{-1} = a_{\sigma,\tau}\partial^1\big(\{c_\sigma\}\big)_{\sigma,\tau}$.

En consecuencia dos cociclos obtenidos a partir de dos transversales de una misma extensión son cohomólogos. Más aún, dos extensiones equivalentes determinan la misma clase de cohomología (si $f : U \longrightarrow V$ es un isomorfismo entre dos extensiones y $\{u_\sigma\}$ es una transversal en U, entonces $\{f(u_\sigma)\}$ es una transversal en V que determina el mismo cociclo).

De este modo, si un grupo G actúa sobre un grupo abeliano A, tenemos una biyección entre las extensiones de A por G (salvo isomorfismo) que inducen la acción dada y los elementos del grupo $H^2(G, A)$. La clase de cohomología trivial se corresponde con la extensión dada por $U = G \times A$ con el producto dado por

$$(\sigma, a)(\tau, b) = (\sigma\tau, a^\tau b).$$

Este grupo U se conoce como el *producto semidirecto* de G por A, y se representa por $G[A]$. Si la acción de G sobre A es trivial entonces el producto semidirecto es simplemente el producto directo o producto cartesiano.

Una propiedad que caracteriza al producto semidirecto de grupos es que la aplicación $G \longrightarrow G[A]$ dada por $\sigma \mapsto (\sigma, 1)$ es un monomorfismo de grupos, con lo que podemos considerar que $G \leq G[A]$ y, por supuesto, $A \trianglelefteq G[A]$. Decimos que esta propiedad caracteriza al producto en el sentido de que una extensión

$$0 \longrightarrow A \xrightarrow{i} U \xrightarrow{j} G \longrightarrow 0$$

es trivial (es decir, su clase de cohomología es trivial) si y sólo si existe un homomorfismo $e : G \longrightarrow U$ tal que $e \circ j = 1$ (basta tomar $u_\sigma = e(\sigma)$ y el cociclo que se obtiene es el trivial). En tal caso U es isomorfo al producto semidirecto $G[A]$ (mediante $(\sigma, a) \mapsto e(\sigma)i(a)$) y se dice que la extensión *se escinde.*

La correspondencia que hemos encontrado entre clases de extensiones y clases de cohomología permite justificar fácilmente un hecho sencillo pero útil: Siempre podemos elegir una transversal $\{u_\sigma\}$ con la propiedad de que $u_1 = 1$, con lo que $u_\sigma = u_\sigma u_1 = u_\sigma a_{\sigma,1}$, luego $a_{\sigma,1} = 1$ para todo $\sigma \in G$, y similarmente $a_{1,\sigma} = 1$. Por lo tanto toda clase de cohomología contiene un cociclo con esta condición adicional.

Estudiemos ahora el caso particular en que $G = \langle\sigma\rangle$ es un grupo cíclico de orden n. Entonces basta fijar un elemento $u \in U$ tal que $\sigma = [u]$ y una transversal de U/A la forman sus potencias $u_{\sigma^i} = u^i$, $i = 0, \ldots, n-1$.

El cociclo asociado viene dado por $u^i u^j = u^r a_{\sigma^i,\sigma^j}$, donde r es el resto de $i + j$ módulo n. Por lo tanto, si $0 \leq i, j < n$,

$$a_{\sigma^i,\sigma^j} = \begin{cases} 1 & \text{si } i + j < n, \\ u^n & \text{si } i + j \geq n. \end{cases} \tag{14.13}$$

Más aún el elemento $a = u^n \in A$ (porque n es el orden de U/A) y, como obviamente u conmuta con a, tenemos que $a^u = a$, es decir, $a^\sigma = a$, luego $a \in A^G$. En términos de a, el cociclo puede expresarse como

$$a_{\sigma^i,\sigma^j} = a^{[(i+j)/n]-[i/n]-[j/n]},$$

donde los corchetes denotan la parte entera.

Es fácil ver que cualquier cocadena definida de este modo a partir de un $a \in A^G$ es de hecho un cociclo. Si cambiamos u por otro representante $v = uc$, con $c \in A$, entonces

$$v^n = (uc)\cdots(uc) = u^n c^{1+\sigma+\cdots+\sigma^{n-1}} = u^n\,\mathrm{N}(c),$$

donde $\mathrm{N}(c) = c^T$ es la norma de c (la versión multiplicativa de la traza).

Así pues, dos elecciones distintas de u llevan a dos elementos de A^G cuyo cociente está en $\mathrm{N}[A]$ y, recíprocamente, los cociclos determinados por dos elementos a, b de A^G tales que $a = b\,\mathrm{N}(c)$, para un $c \in U$, corresponden a dos transversales de una misma extensión relacionadas por $v = uc$. Así tenemos una expresión explícita del isomorfismo $A^G/\,\mathrm{N}[A] \cong H^0(G,A) \cong H^2(G,A)$ dada por

$$[a] \mapsto [a^{[(i+j)/n]-[i/n]-[j/n]}]. \tag{14.14}$$

El isomorfismo inverso tiene una expresión mucho más simple, como veremos enseguida.

Definición 14.37 Sea G un grupo finito, A un G-módulo y $\{a_{\sigma,\tau}\}$ un cociclo de dimensión 2. Definimos

$$E\big(\{a_{\sigma,\tau}\}\big)(\sigma) = \prod_{\tau\in G} a_{\sigma,\tau} \in A.$$

Para todo $\rho \in G$ tenemos

$$E\big(\{a_{\sigma,\tau}\}\big)(\sigma)^\rho = \prod_{\tau\in G} a_{\sigma,\tau}^\rho = \prod_{\tau\in G} a_{\sigma,\tau}a_{\tau,\rho}a_{\sigma\tau,\rho}^{-1} = \prod_{\tau\in G} a_{\sigma,\tau}a_{\tau,\rho}a_{\tau,\rho}^{-1} = \prod_{\tau\in G} a_{\sigma,\tau},$$

luego $E\big(\{a_{\sigma,\tau}\}\big)(\sigma) \in A^G$.

Si cambiamos $\{a_{\sigma,\tau}\}$ por un cociclo cohomólogo $\{b_{\sigma,\tau}\}$, entonces tenemos la relación $b_{\sigma,\tau} = a_{\sigma,\tau}c_\sigma^\tau c_\tau c_{\sigma\tau}^{-1}$, luego

$$\begin{aligned} E\big(\{b_{\sigma,\tau}\}\big)(\sigma) &= E\big(\{a_{\sigma,\tau}\}\big)(\sigma)\prod_{\tau\in G} c_\sigma^\tau c_\tau c_{\sigma\tau}^{-1} = E\big(\{a_{\sigma,\tau}\}\big)(\sigma)\prod_{\tau\in G} c_\sigma^\tau c_\tau c_\tau^{-1} \\ &= E\big(\{a_{\sigma,\tau}\}\big)(\sigma)\prod_{\tau\in G} c_\sigma^\tau = E\big(\{a_{\sigma,\tau}\}\big)(\sigma)\,\mathrm{N}(c_\sigma). \end{aligned}$$

Así, si $x = \big[\{a_{\sigma,\tau}\}\big] \in H^2(G,A)$ podemos definir $E(x)(\sigma) \in A^G/\,\mathrm{N}[A]$ como $E\big(\{a_{\sigma,\tau}\}\big)(\sigma)$, que es independiente del cociclo elegido en la clase x.

La aplicación $E(x) : G \longrightarrow A^G/\,\mathrm{N}[A]$ se llama *aplicación de Nakayama* asociada a x, y es un homomorfismo de grupos. En efecto,

$$\begin{aligned} E(x)(\sigma\tau) &= \prod_{\rho\in G} a_{\sigma\tau,\rho}\,\mathrm{N}[A] = \prod_{\rho\in G} a_{\sigma,\tau\rho}a_{\tau,\rho}a_{\sigma,\tau}^{-\rho}\,\mathrm{N}[A] \\ &= \prod_{\rho\in G} a_{\sigma,\rho}a_{\tau,\rho}\,\mathrm{N}[A] = E(x)(\sigma)E(x)(\tau). \end{aligned}$$

También es obvio que si fijamos un $\sigma \in G$ la aplicación $x \mapsto E(x)(\sigma)$ es un homomorfismo de grupos.

Ahora volvamos al caso en que $G = \langle\sigma\rangle$ es un grupo cíclico de orden n y sea $a \in A^G$. Según hemos visto, a determina el cociclo (14.13). Si x es su clase de cohomología,

$$E(x)(\sigma) = \prod_{i=0}^{n-1} a_{\sigma,\sigma^i}\,\mathrm{N}[A] = a\,\mathrm{N}[A].$$

Esto demuestra que el homomorfismo $x \mapsto E(x)(\sigma)$ es el inverso del isomorfismo $[a] \mapsto x$.

Capítulo XV

Formaciones

En este capítulo mostraremos cómo se relaciona la cohomología de grupos que acabamos de introducir con la teoría de extensiones de cuerpos. Para tratar simultáneamente las extensiones globales (extensiones de cuerpos numéricos) y las locales (extensiones de cuerpos p-ádicos) introducimos la noción abstracta de formación. De hecho, al desarrollar la teoría de cuerpos de clases en el contexto general de las formaciones, no sólo recuperamos los dos casos que ya conocemos, sino que los resultados son aplicables a otros nuevos, como son las extensiones finitas de cuerpos métricos discretos localmente compactos arbitrarios.

15.1 Formaciones de cuerpos

La diferencia fundamental entre la teoría local y la teoría global de cuerpos de clases es que la primera depende de la cohomología de Galois, es decir, la derivada de la acción de los grupos de Galois sobre los grupos multiplicativos de los cuerpos p-ádicos, mientras que la segunda depende de la cohomología asociada a la acción de los grupos de Galois sobre los grupos de clases de elementos ideales.

Definición 15.1 Una *formación* es una terna $(G, \{G_K\}_{K\in S}, A)$ que cumpla las condiciones siguientes:

a) G es un grupo topológico compacto, $\{G_K\}_{K\in S}$ es la familia de los subgrupos abiertos de G (donde K varía en un conjunto de índices arbitrario S) y A es un G-módulo.

b) Los subgrupos $\{G_K\}$ forman una base de entornos de 1.

c) Si llamamos $A_K = A^{G_K}$ al subgrupo de los elementos fijados por G_K, entonces A es la unión de todos los grupos A_K.

Ejemplo Un caso particular de formación lo constituye cualquier grupo de automorfismos $G(L/k)$ de una extensión de Galois (quizá infinita) junto con el módulo $A = L^*$ y $G_K = G(A/K)$, para cada cuerpo intermedio $k \subset K \subset L$ de grado finito sobre k (y entonces $A_K = K^*$). Llamaremos *formaciones locales* a las formaciones de este tipo en las que el cuerpo base k sea un cuerpo métrico discreto localmente compacto. A estos cuerpos los llamaremos *cuerpos locales.*

■

Ejemplo Si $k \subset K$ son cuerpos numéricos, el teorema 6.14 nos da un isomorfismo topológico entre el grupo de elementos ideales J_k y el correspondiente J_K. Llamémosla $i_{k,K}$. Esto nos permite identificar a J_k con un subgrupo de J_K, en cuyo caso la aplicación $i_{k,K}$ pasa a ser la inclusión. Ahora necesitamos considerar a todas las aplicaciones $i_{k,K}$ como inclusiones, es decir, considerar que si $k \subset K$ entonces $J_k \leq J_K$. Para ello necesitamos considerar a todos los grupos J_K como subgrupos de un mismo grupo. Esto es un mero problema técnico que puede resolverse en general construyendo el llamado "límite inductivo" de los grupos $\{J_K\}_K$ junto con los monomorfismos $i_{k,K}$. En lugar de hacerlo así, mostraremos cómo construir este grupo en nuestro caso particular.

Sea $\mathbb{A}$ la clausura algebraica de $\mathbb{Q}$. Cada divisor primo $\mathfrak{p}$ de $\mathbb{A}$ determina (al restringir sus valores absolutos) un divisor primo $\mathfrak{p}_K$ en cada cuerpo numérico K. Definimos $\mathbb{A}_\mathfrak{p} = \bigcup_K K_{\mathfrak{p}_K}$, donde K recorre los cuerpos numéricos y cada compleción $K_{\mathfrak{p}_K}$ es la clausura de K en una compleción fija de $\mathbb{A}$ respecto a $\mathfrak{p}_K$. Sea $J^* = \prod_\mathfrak{p} \mathbb{A}_\mathfrak{p}^*$, donde $\mathfrak{p}$ recorre los divisores primos de A. Claramente J^* es un grupo abeliano con el producto definido componente a componente.

Para cada cuerpo numérico K sea $i_K : J_K \longrightarrow J^*$ el monomorfismo dado por $i_K(\alpha)_\mathfrak{p} = \tau_{\mathfrak{p},K}(\alpha_{\mathfrak{p}_K})$, donde $\tau_{\mathfrak{p},K} : K_{\mathfrak{p}_K} \longrightarrow \mathbb{A}_\mathfrak{p}$ es la única isometría que extiende a la identidad en K. Es fácil ver que si $k \subset K$ tenemos el diagrama conmutativo

$$\begin{array}{ccc} J_K & \xrightarrow{i_K} & J^* \\ {\scriptstyle i_{k,K}}\uparrow & \nearrow_{i_k} & \\ J_k & & \end{array}$$

En particular, si identificamos cada J_K con su imagen en J^* y $k \subset K$ resulta que $J_k \leq J_K$. Con esta identificación, definimos

$$J = \bigcup_K J_K.$$

De este modo tenemos los que buscábamos, un grupo abeliano J con la propiedad de que cada grupo J_K es canónicamente isomorfo a un subgrupo de J y, a través de estos isomorfismos, las aplicaciones $i_{k,K}$ se convierten en las inclusiones.

Consideremos ahora el grupo $G = G(\mathbb{A}/\mathbb{Q})$ y, para cada cuerpo numérico K, sea $G_K = G(\mathbb{A}/K)$. En las observaciones previas al teorema 6.22 vimos que todo isomorfismo $\sigma : K \longrightarrow K'$ entre dos cuerpos numéricos induce un

isomorfismo $\sigma : J_K \longrightarrow J_{K'}$. En particular, si fijamos $\sigma \in G$, las restricciones $\sigma|_K : K \longrightarrow \sigma[K]$ conmutan con las aplicaciones $i_{k,K}$, luego los isomorfismos i_K los transforman en isomorfismos consistentes entre los subgrupos de J, es decir, isomorfismos que se extienden a un único automorfismo $\sigma : J \longrightarrow J$. Es fácil ver la correspondencia entre los elementos de G y estos automorfismos de J determina una acción de G en J, con la que J resulta ser un G-módulo.

Para demostrar que $(G, \{G_K\}, J)$ es una formación sólo falta comprobar que J_K es el subgrupo de J fijado por G_K, con lo que se cumplirá la propiedad c) por la definición de J. Llamemos A_K a este subgrupo y observemos en general que si L/K es una extensión normal de cuerpos numéricos y $\sigma \in G_K$ entonces $\sigma[L] = L$ y $\sigma|_{J_L}$ (considerando $J_L \leq J$) se corresponde a través del isomorfismo i_L con el automorfismo inducido por $\sigma|_L$ en J_L (considerado según la definición del capítulo VI). En particular, si aplicamos esto a la extensión K/K concluimos que $J_K \leq A_K$. Recíprocamente, si $\alpha \in A_K$, podemos suponer que $\alpha \in J_L$, donde L es una extensión finita normal de K, y el teorema 6.22 nos da que $\alpha \in J_K$. ∎

Ejemplo Veamos finalmente que los grupos de clases de elementos ideales constituyen también una formación. Sea J el grupo de elementos ideales construido en el ejemplo anterior y consideremos el monomorfismo $\mathbb{A}^* \longrightarrow J$ que identifica cada $u \in \mathbb{A}^*$ con el elemento ideal de coordenadas iguales a u. De este modo, $\mathbb{A}^*$ es un G-submódulo de J. De hecho, la acción natural de G sobre $\mathbb{A}^*$ (recordemos que $G = G(\mathbb{A}/\mathbb{Q})$) coincide con la restricción de la acción sobre J. En particular, si K es un cuerpo numérico, tenemos que $\mathbb{A}^* \cap J_K = K^*$, pues la intersección está formada por los elementos de $\mathbb{A}^*$ fijados por G_K.

Consideremos el G-módulo cociente $G = J/\mathbb{A}^*$. La observación anterior implica que las aplicaciones $i_L : C_K \longrightarrow C$ definidas de forma natural (es decir, que llevan la clase de α a la clase de α) son monomorfismos, luego podemos considerar a los grupos C_K como subgrupos de C, de modo que si $k \subset K$ entonces $C_k \leq C_K$.

También es claro que C es la unión de todos los subgrupos C_K. Para probar que $(G, \{G_K\}_K, C)$ constituyen una formación sólo necesitamos demostrar que el subgrupo fijado por cada G_K es C_K (con esto generalizamos el teorema 6.24).

Una inclusión es inmediata. Supongamos que $[\alpha] \in C$ es fijado por G_K. Podemos tomar una extensión finita normal L de K tal que $\alpha \in J_L$. La hipótesis es que para todo $\sigma \in G_K$ se cumple $[\alpha] = [\sigma(\alpha)]$. En particular esto vale para todo $\sigma \in G(L/K)$, luego existe un $u_\sigma \in L^*$ tal que $\sigma(\alpha) = u_\sigma \alpha$. Si $\tau \in G(L/K)$, tenemos que

$$u_{\sigma\tau}\alpha = \sigma\tau(\alpha) = \tau(\sigma(\alpha)) = \tau(u_\sigma)\tau(\alpha) = u_\sigma^\tau u_\tau \alpha,$$

luego tenemos las relaciones $u_{\sigma\tau} = u_\sigma^\tau u_\tau$, que prueban que $\{u_\sigma\}$ es un 1-cociclo de L. Por el teorema de Hilbert-Speiser sabemos que $H^1(L/K) = 1$, luego $\{u_\sigma\}$ es una cofrontera, es decir, existe un $u \in L^*$ tal que $u_\sigma = u/\sigma(u)$ para todo $\sigma \in G(L/K)$. Esto significa que $\sigma(u\alpha) = u\alpha$ para todo $\sigma \in G(L/K)$, y obviamente esto vale para todo $\sigma \in G_K$, de donde $u\alpha \in J_K$ y $[\alpha] = [u\alpha] \in C_K$.

∎

En estos ejemplo, y de hecho en todos los de interés, la "suma" en el módulo A de una formación es un "producto", por lo que usaremos notación multiplicativa tanto para la suma en A como para los grupos de cohomología. Así mismo, en todos los casos de interés el grupo G de una formación será un grupo de Galois infinito, los índices K (que en la definición general son lógicamente superfluos) recorrerán extensiones finitas de un cuerpo base fijo k_0 y el grupo G_K será el grupo de los automorfismos que fijan al cuerpo K. Sin embargo, como muestran los ejemplos, el módulo A_K no será necesariamente el cuerpo K o su grupo multiplicativo.

Las definiciones siguientes están motivadas por los ejemplos anteriores, pero tienen sentido sobre una formación arbitraria: al grupo G lo llamaremos *grupo de Galois* de la formación, el módulo A será el *módulo* de la formación, a los índices K los llamaremos *cuerpos,* a los grupos A_K los llamaremos *niveles,* si k y K son dos cuerpos de la formación, diremos que k es un *subcuerpo* de K, o que K es una *extensión* de k si $G_K \leq G_k$, en cuyo caso $A_k \subset A_K$.

Si K/k es una extensión, su *grado* es el índice $|K : k| = |G_k : G_K|$, que es finito porque la compacidad implica la finitud de todos los índices $|G : G_K|$ (las clases módulo G_K forman un cubrimiento abierto de G). Diremos que una extensión K/k es *normal* si $G_K \trianglelefteq G_k$. Entonces el grupo cociente $G(K/k) = G_k/G_K$ actúa de forma natural sobre A_K. A este cociente lo llamaremos *grupo de Galois* de la extensión K/k. Es claro que A_k coincide con el subgrupo de A_K fijado por los elementos de $G(K/k)$. Una extensión normal es *resoluble, abeliana* o *cíclica* si lo es su grupo de Galois. Representaremos por $H^n(K/k)$ al n-simo grupo de cohomología de $G(K/k)$ sobre el módulo A_K. Si K es un cuerpo de la formación y $\sigma \in G$, definimos el *cuerpo conjugado* K^σ como el índice del grupo conjugado $G_{K^\sigma} = G_K^\sigma$. El *producto* de dos cuerpos K, L es el cuerpo determinado por $G_{KL} = G_K \cap G_L$.

Algunas propiedades sencillas de las extensiones de cuerpos se generalizan fácilmente a formaciones arbitrarias. Por ejemplo, si tenemos $k \subset L \subset K$ entonces $G(K/L) \leq G(K/k)$ y todo subgrupo de $G(K/k)$ es de esta forma (pues los subgrupos de G_k/G_K son de la forma H/G_K con $G_K \leq H \leq G_k$, y entonces H es abierto, luego $H = G_L$ para un cierto L). Por otra parte, si K/k es normal entonces K/L también lo es. Si L/k es normal entonces $G(L/k) \cong G(K/k) \,/\, G(K/L)$.

Observar que cada cuerpo K tiene un número finito de conjugados, pues dos elementos de G congruentes módulo G_K (por la derecha) dan lugar al mismo conjugado, luego el número de conjugados de K es a lo sumo $|G : G_K|$. De aquí se sigue que, dado un conjunto finito de extensiones de un mismo cuerpo k, existe una mínima extensión normal de k que las contiene a todas (la determinada por la intersección de todos los conjugados de todos los grupos asociados a las extensiones).

Un resultado elemental en el caso de extensiones de Galois y que no es cierto en general es que la correspondencia $G_K \mapsto A_K$ sea biyectiva, pero esto no tendrá ninguna relevancia.

Definimos una *formación de cuerpos* como una formación que satisfaga el

AXIOMA I: *Si K/k es una extensión normal, entonces $H^1(K/k) = 1$.*

El axioma I refleja una de las propiedades básicas de la cohomología de Galois (el teorema de Hilbert-Speiser), luego lo cumplen todas las formaciones descritas en el ejemplo 1. Sucede que las formaciones J y C de los grupos de elementos ideales y los grupos de clases de elementos ideales también son formaciones de cuerpos, pero aquí encontramos una primera diferencia entre la teoría local y la global: mientras el axioma I es un hecho sencillo en el caso local, en el caso global es un resultado muy profundo. En el capítulo VII probamos esencialmente que C cumple el

AXIOMA I′: *Si K/k es cíclica de grado primo, entonces $H^1(K/k) = 1$.*

No es evidente, pero luego demostraremos que el axioma I es equivalente al axioma I′. De momento interpretemos este último axioma. Para ello conviene introducir el

AXIOMA 0: *Si K/k es una extensión cíclica, se cumple*

$$h_2(K/k) = h_1(K,k)\,|K:k|, \tag{15.1}$$

donde $h_n(K/k)$ es el orden del grupo $H^n(K/k)$ (que de momento no sabemos que sea finito, esta hipótesis de finitud forma parte del axioma 0).

El AXIOMA 0′ es el axioma 0 para extensiones cíclicas de orden primo. Teniendo en cuenta la interpretación de los grupos de cohomología de los grupos cíclicos, la relación (15.1) equivale a

$$|A_k : \mathrm{N}[A_k]| = h_{-1}(K/k)\,|K:k|.$$

Esta relación implica, para extensiones cíclicas (de grado primo) la *primera desigualdad fundamental:* $|K:k| \;\big|\; |A_k : \mathrm{N}[A_k]|$ y, si una formación cumple el axioma 0′, entonces el axioma I′ equivale al

AXIOMA I″: *(segunda desigualdad fundamental)*

$$|A_k : \mathrm{N}[A_k]| \le |K:k| \qquad \text{para extensiones cíclicas de grado primo.}$$

El en capítulo VII demostramos la relación (7.7), que no es sino el axioma 0 para la formación C de los grupos de clases de elementos ideales. Después probamos la segunda desigualdad, luego ciertamente C satisface el axioma I′.

Admitiendo que C cumple el axioma I, es claro que J también lo cumple: si K/k es una extensión de cuerpos numéricos y $G = G(K/k)$, basta considerar la sucesión de cohomología derivada de la sucesión exacta

$$1 \longrightarrow K^* \longrightarrow J_K \longrightarrow C_K \longrightarrow 1$$

para concluir que $H^1(G, J_K) = 1$.

Debemos resaltar que todos los resultados a los que hemos hecho referencia están en el capítulo VII y no hemos necesitado nada sobre el isomorfismo de Artin. Sólo nos queda pendiente de prueba la equivalencia entre los axiomas I y I′. La veremos al principio de la sección 15.3, después de desarrollar un poco más la cohomología de grupos.

15.2 Restricción, transferencia e inflación

Sea G un grupo finito y S un subgrupo. Sea A un G-módulo. Entonces A es también un S-módulo de forma natural. Vamos a definir homomorfismos que relacionan los grupos de cohomología $H^n(G,A)$ con los grupos $H^n(S,A)$. Para ello nos apoyaremos en el concepto de traza, que introducimos a continuación. Recordemos que A^G es el submódulo de A formado por los elementos fijados por G.

Definición 15.2 En las condiciones anteriores, la *traza* $\mathrm{Tr}_S^G : A^S \longrightarrow A^G$ es la aplicación dada por

$$\mathrm{Tr}_S^G(a) = \sum_{i=1}^{r} a\sigma_i,$$

donde $\{\sigma_1, \ldots, \sigma_r\}$ es una transversal derecha de G/S, es decir, un conjunto de representantes de las clases a derecha de G módulo S.

La traza no depende de la elección de la transversal, pues cualquier otra es de la forma $\{s_1\sigma_1, \ldots, s_r\sigma_r\}$ con $s_i \in S$ y obviamente

$$\sum_{i=1}^{r} as_i\sigma_i = \sum_{i=1}^{r} a\sigma_i,$$

También es claro que $\mathrm{Tr}_S^G(a) \in A^G$, según afirmamos, pues $\sigma_i\sigma = s_i\sigma_{j_i}$, para un cierto $s_i \in S$ y un índice j_i; de modo que la correspondencia $i \mapsto j_i$ es biyectiva. Por lo tanto

$$\mathrm{Tr}_S^G(a)\sigma = \sum_{i=1}^{r} as_i\sigma_{j_i} = \sum_{i=1}^{r} a\sigma_{j_i} = \mathrm{Tr}_S^G(a)$$

Observar que si $S = 1$ entonces T_1^G es la multiplicación por la traza

$$T = \sum_{\sigma \in G} \sigma$$

que ya nos ha aparecido en el cálculo de grupos de cohomología.

Si tenemos $S \leq U \leq G$ se cumple la relación $\mathrm{Tr}_S^G = \mathrm{Tr}_S^U \mathrm{Tr}_U^G$. En efecto, si tomamos transversales derechas $\{\sigma_i\}$ y $\{u_j\}$ de G/U y U/S respectivamente, entonces $\{u_j\sigma_i\}$ es una transversal derecha de G/S, de donde

$$\mathrm{Tr}_S^G(a) = \sum_i \Big(\sum_j au_j\Big)\sigma_i = \sum_i \mathrm{Tr}_S^U(a)\sigma_i = \mathrm{Tr}_U^G(\mathrm{Tr}_S^U(a)).$$

Ejemplo El lector ya habrá observado que esta noción de traza generaliza a la usual en teoría de cuerpos. En efecto, si G es el grupo de Galois de una extensión K/k y A es el grupo aditivo de K, entonces $A^G = k$ y $L = A^S$ es el cuerpo fijado por S. La traza es precisamente la traza de L en k en el sentido usual. Si tomamos como módulo el grupo multiplicativo de K, entonces la traza que acabamos de definir es la norma en el sentido usual en la teoría de cuerpos. ∎

Veamos ahora el motivo por el que nos va a interesar la traza en esta sección. Consideremos dos G-módulos C y A. Definimos en $\mathrm{Hom}(C, A)$ la operación dada por $f^\sigma(c) = f(c\sigma^{-1})\sigma$, con la que se convierte en un G-módulo (observar que si $A = \mathbb{Z}$ tenemos la operación usual en el módulo dual C^*).

Se cumple que $f^\sigma = \sigma$ si y sólo si $f(c\sigma^{-1}) = f(c)\sigma^{-1}$ para todo $c \in C$, luego

$$\mathrm{Hom}(C, A)^S = \mathrm{Hom}_S(C, A).$$

Así pues, la traza transforma S-homomorfismos en G-homomorfismos. Concretamente, transforma un S-homomorfismo f en el G-homomorfismo

$$\mathrm{Tr}_S^G(f)(c) = \sum_{i=1}^{r} f(c\sigma_i^{-1})\sigma_i.$$

En particular, si f ya es un G-homomorfismo queda $\mathrm{Tr}_S^G(f)(c) = rf(c)$, es decir,

$$\mathrm{Tr}_S^G(f) = |G : S|f. \tag{15.2}$$

Ocupémonos ya del problema de relacionar los grupos de cohomología de un grupo G con los de un subgrupo S. Comenzamos observando que $\mathbb{Z}[G]$ es un S-módulo libre, pues cualquier transversal izquierda de G/S es una S-base. Consecuentemente, todo G-módulo libre es también un S-módulo libre (es suma directa de copias de $\mathbb{Z}[G]$, y cada una de ellas es suma directa de copias de $\mathbb{Z}[S]$). Esto implica que toda resolución reducida de G lo es también de S, y de aquí a su vez que toda resolución completa de G lo es también de S.

Consideremos ahora sendas resoluciones completas $\mathcal{C}(G)$ y $\mathcal{C}(S)$ de G y S. Ambas son resoluciones completas de S, luego son equivalentes. Con más precisión, sabemos que existen dos S-homomorfismos $u : \mathcal{C}(S)_0 \longrightarrow \mathcal{C}(G)_0$ y $v : \mathcal{C}(G)_0 \longrightarrow \mathcal{C}(S)_0$ entre las resoluciones reducidas, de modo que cualquier otro u' (resp. v') es homotópico a u (resp. v). Al extender u con el dual de v y viceversa obtenemos homomorfismos entre las resoluciones completas, de modo que si cambiamos u o v obtenemos homomorfismos homotópicos.

Si A es un G-módulo, el homomorfismo u induce un homomorfismo de complejos

$$\begin{array}{ccccccc}
\cdots & \longrightarrow & \mathrm{Hom}_G(C_{n-1}(G), A) & \xrightarrow{\partial^{n-1}} & \mathrm{Hom}_G(C_n(G), A) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle u_{n-1}^\#} & & \downarrow{\scriptstyle u_n^\#} & & \\
\cdots & \longrightarrow & \mathrm{Hom}_S(C_{n-1}(S), A) & \xrightarrow{\partial^{n-1}} & \mathrm{Hom}_S(C_n(S), A) & \longrightarrow & \cdots
\end{array}$$

(en principio deberíamos poner en la fila superior los grupos de S-homomorfismos, pero podemos restringir las aplicaciones a los subgrupos de G-homomorfismos). Si partimos de otros homomorfismos u' y v', la homotopía entre u y u' induce una homotopía entre $u^\#$ y $u'^\#$. Esto implica que los homomorfismos

$$\mathrm{Res}^n_{G,S} : H^n(G,A) \longrightarrow H^n(S,A)$$

inducidos por $u^\#$ no dependen de la elección de u y v.

La aplicación $\mathrm{Res}^n_{G,S}$ recibe el nombre de *restricción.* Es pura rutina comprobar que si partimos de resoluciones distintas obtenemos diagramas conmutativos para las restricciones y los isomorfismos entre los grupos de cohomología.

Por otra parte, el homomorfismo $v^\#$ transforma S-homomorfismos en S-homomorfismos, pero podemos conseguir G-homomorfismos aplicando la traza. Definimos las aplicaciones

$$\mathrm{V}^n_{S,G} : \mathrm{Hom}_S(C_n(S),A) \longrightarrow \mathrm{Hom}_G(C_n(G),A)$$

mediante

$$\mathrm{V}^n_{S,G}(f) = \mathrm{Tr}^G_S(v^\#_n(f)).$$

Es fácil ver que los diagramas siguientes conmutan, con lo que $\mathrm{V}_{S,G}$ es un homomorfismo de complejos.

$$\begin{array}{ccccccc}
\cdots & \longrightarrow & \mathrm{Hom}_G(C_{n-1}(G),A) & \xrightarrow{\partial^{n-1}} & \mathrm{Hom}_G(C_n(G),A) & \longrightarrow & \cdots \\
 & & \uparrow{\scriptstyle \mathrm{Tr}^G_S} & & \uparrow{\scriptstyle \mathrm{Tr}^G_S} & & \\
\cdots & \longrightarrow & \mathrm{Hom}_S(C_{n-1}(G),A) & \xrightarrow{\partial^{n-1}} & \mathrm{Hom}_S(C_n(G),A) & \longrightarrow & \cdots \\
 & & \uparrow{\scriptstyle v^\#_{n-1}} & & \uparrow{\scriptstyle v^\#_n} & & \\
\cdots & \longrightarrow & \mathrm{Hom}_S(C_{n-1}(S),A) & \xrightarrow{\partial^{n-1}} & \mathrm{Hom}_S(C_n(S),A) & \longrightarrow & \cdots
\end{array}$$

Así mismo, una homotopía entre v y otro homomorfismo da lugar a una homotopía entre el homomorfismo $\mathrm{V}_{S,G}$ y su análogo. Por lo tanto los homomorfismos inducidos no dependen de la elección de u, v. Los denominaremos *transferencias:*

$$\mathrm{V}^n_{S,G} : H^n(S,A) \longrightarrow H^n(G,A).$$

Como en el caso de las restricciones, un cambio en los complejos da lugar al diagrama conmutativo correspondiente.

Antes de continuar estudiando las restricciones y transferencias nos conviene calcular explícitamente homomorfismos u y v entre las resoluciones canónicas de $\mathbb{Z}[G]$ y $\mathbb{Z}[S]$. Basta determinar u_n y v_n para $n \geq 0$, pues los correspondientes a índices negativos son los duales de éstos.

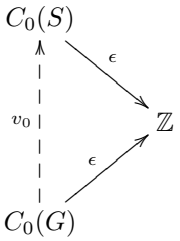
Como homomorfismo $u_n : C_n(S) \longrightarrow C_n(G)$ podemos tomar la inclusión, de modo que $u^\#$ es la restricción de $C_n(G)$ a $C_n(S)$ en el sentido usual para

aplicaciones, luego $\mathrm{Res}^n_{G,S}$ actúa sobre una clase de cohomología restringiendo sus cociclos a S.

Para obtener homomorfismos v_n aplicamos el proceso descrito en la prueba del teorema 14.22. Conviene introducir la siguiente notación: sea T una transversal izquierda de G sobre S, es decir, un sistema de representantes de las clases a izquierda de G módulo S. Entonces todo $\sigma \in G$ se expresa de forma única como $\sigma = \bar{\sigma}\tilde{\sigma}$, con $\bar{\sigma} \in T$, $\tilde{\sigma} \in S$. Además $\sigma\tau = \sigma\bar{\tau}\tilde{\tau} = \overline{\sigma\bar{\tau}}\,\widetilde{\sigma\bar{\tau}}\tilde{\tau}$, de donde

$$\overline{\sigma\tau} = \overline{\sigma\bar{\tau}}, \qquad \widetilde{\sigma\tau} = \widetilde{\sigma\bar{\tau}}\tilde{\tau}.$$

Partimos de $C_0(G) = \mathbb{Z}[G]$, $C_0(S) = \mathbb{Z}[S]$ y buscamos un homomorfismo v_0 que haga conmutativo el diagrama



Los homomorfismos ϵ vienen dados por $\epsilon(s) = 1$ y $\epsilon(\sigma) = 1$ respectivamente. Para obtener v_0 tomamos una S-base de $\mathbb{Z}[G]$, concretamente T, y para cada $\tau \in T$ calculamos $\epsilon(\tau) = 1$ y buscamos un elemento de $C_0(S)$ cuya imagen por ϵ sea 1. Por ejemplo 1. De este modo v_0 es el S-homomorfismo determinado por $v_0(\tau) = 1$ para cada $\tau \in T$. Claramente esto equivale a $v_0(\sigma) = \tilde{\sigma}$, para todo $\sigma \in G$. Ahora buscamos un v_1 que haga conmutativo el diagrama

$$\begin{array}{ccc} C_1(S) & \xrightarrow{\partial_1} & C_0(S) \\ {\scriptstyle v_1}\uparrow & & \uparrow{\scriptstyle v_0} \\ C_1(G) & \xrightarrow[\partial_1]{} & C_0(G) \end{array}$$

Para ello consideramos una S-base de $C_1(G)$, por ejemplo la formada por los elementos $[\sigma_1]\tau$, con $\sigma_1 \in G$, $\tau \in T$. Calculamos

$$v_0(\partial_1([\sigma_1]\tau)) = v_0(\partial_1([\sigma_1])\tau) = v_0((\sigma_1 - 1)\tau) = \widetilde{\sigma_1\tau} - 1$$

y hemos de encontrar un elemento de $C_1(S)$ cuya frontera sea $\widetilde{\sigma_1\tau} - 1$. Por ejemplo sirve $v_1([\sigma_1]\tau) = [\widetilde{\sigma_1\tau}]$. Es fácil ver entonces que

$$v_1([\sigma_1]\sigma_0) = [\widetilde{\sigma_1\bar{\sigma}_0}]\tilde{\sigma}_0, \qquad \text{para todo } \sigma_1, \sigma_0 \in G. \tag{15.3}$$

Similarmente se comprueba que

$$v_2([\sigma_2, \sigma_1]\sigma_0) = [\widetilde{\sigma_2\overline{\sigma_1\sigma_0}}, \widetilde{\sigma_1\bar{\sigma}_0}]\tilde{\sigma}_0, \qquad \text{para todo } \sigma_2, \sigma_1, \sigma_0 \in G. \tag{15.4}$$

Dejamos al lector enunciar y probar el caso general. ∎

Como aplicación calculamos los homomorfismos

$$\mathrm{Res}^{-2}_{G,S} : H^{-2}(G,\mathbb{Z}) \longrightarrow H^{-2}(G,\mathbb{Z}), \quad \mathrm{V}^{-2}_{S,G} : H^{-2}(S,\mathbb{Z}) \longrightarrow H^{-2}(G,\mathbb{Z}).$$

Más exactamente, calcularemos las aplicaciones en que se transforman a través de los isomorfismos $H^{-2}(G,\mathbb{Z}) \cong G/G'$ y $H^{-2}(S,\mathbb{Z}) \cong S/S'$ que describimos en el capítulo anterior.

Necesitamos el homomorfismo $u_{-2} : C_{-2}(S) \longrightarrow C_{-2}(G)$, que es el dual del homomorfismo $v_1 : C_1(G) \longrightarrow C_1(S)$, dado por (15.3). Mantenemos la notación empleada en esta fórmula, es decir, T es una transversal izquierda de G sobre S y $\sigma = \bar{\sigma}\tilde{\sigma}$, con $\bar{\sigma} \in T$ y $\tilde{\sigma} \in S$.

Ahora partimos de una clase $\sigma G' \in G/G'$, cuya clase de cohomología asociada es $[f_\sigma]$, donde

$$f_\sigma\big(\langle\tau\rangle\big) = \begin{cases} 1 & \text{si } \sigma = \tau, \\ 0 & \text{si } \sigma \neq \tau. \end{cases}$$

Entonces $\mathrm{Res}^{-2}_{G,S}(f_\sigma)\big(\langle s\rangle\big) = f_\sigma(v_1^*(\langle s\rangle))$. Sea

$$v_1^*\big(\langle s\rangle\big) = \sum_{\rho\in G} \langle\rho\rangle \Big(\sum_{\tau\in G} n_{\tau,\rho}\tau\Big).$$

Así

$$\mathrm{Res}^{-2}_{G,S}(f_\sigma)\big(\langle s\rangle\big) = \sum_{\rho\in G} f_\sigma\big(\langle\rho\rangle\big)\Big(\sum_{\tau\in G} n_{\tau,\rho}\tau\Big) = \sum_{\tau\in G} n_{\tau,\sigma}\tau = \sum_{\tau\in G} n_{\tau,\sigma}.$$

Al construir la base dual probamos que

$$n_{\tau,\sigma} = v_1^*\big(\langle s\rangle\big)([\sigma]\tau) = \langle s\rangle\,\big(v_1([\sigma]\tau)\big) = \langle s\rangle\,([\widetilde{\sigma\tau}]\tilde{\tau}).$$

Según la definición de base dual esta expresión es nula cuando $\tilde{\tau} \neq 1$ y si $\tau \in T$ entonces $n_{\tau,\sigma} = f_{\widetilde{\sigma\tau}}\big(\langle s\rangle\big)$. Consecuentemente

$$\mathrm{Res}^{-2}_{G,S}(f_\sigma)\big(\langle s\rangle\big) = \sum_{\tau\in T} f_{\widetilde{\sigma\tau}}\big(\langle s\rangle\big) = f_v\big(\langle s\rangle\big),$$

donde $v = \prod\limits_{\tau\in T} \widetilde{\sigma\tau}$. En conclusión, la imagen de $\sigma G'$ a través de los isomorfismos y la restricción es

$$V_{G,S}(\sigma G') = \prod_{\tau\in T} \widetilde{\sigma\tau} S'. \tag{15.5}$$

Esta aplicación es la *transferencia* en el sentido de la teoría de Grupos. Acabamos de probar la mitad del teorema siguiente:

Teorema 15.3 *Sea G un grupo finito y S un subgrupo de G. Entonces los diagramas siguientes son conmutativos:*

$$\begin{array}{ccc} H^{-2}(G,\mathbb{Z}) & \xrightarrow{\mathrm{Res}^{-2}_{G,S}} & H^{-2}(S,\mathbb{Z}) \\ \updownarrow & & \updownarrow \\ G/G' & \xrightarrow{V_{G,S}} & S/S' \end{array} \qquad \begin{array}{ccc} H^{-2}(S,\mathbb{Z}) & \xrightarrow{\mathrm{V}^{-2}_{S,G}} & H^{-2}(G,\mathbb{Z}) \\ \updownarrow & & \updownarrow \\ S/S' & \xrightarrow{\textit{inclusión}} & G/G' \end{array}$$

DEMOSTRACIÓN: Para probar la segunda afirmación necesitamos el homomorfismo $v_{-2} : C_{-2}(G) \longrightarrow C_{-2}(S)$, que es el S-homomorfismo dual de u_1. Podemos tomar como u_1 la inclusión. Entonces,

$$v_{-2}\big(\langle\sigma\rangle\,\tau\big) = u_1 \circ \langle\sigma\rangle\,\tau = \big(\langle\sigma\rangle\,\tau\big)|_{C_1(S)}.$$

Si s, $t \in S$ tenemos que

$$\big(\langle\sigma\rangle\,\tau\big)([s]t) = \begin{cases} 1 & \text{si } \sigma = s,\ \tau = t, \\ 0 & \text{en otro caso.} \end{cases}$$

Por consiguiente

$$\big(\langle\sigma\rangle\,\tau\big)|_{C_1(S)} = \begin{cases} \langle\sigma\rangle\,\tau & \text{si } \sigma,\ \tau \in S, \\ 0 & \text{en otro caso.} \end{cases}$$

Así pues, si $s \in S$ tenemos que

$$v_{-2}^{\#}(f_s)\big(\langle\sigma\rangle\,\tau\big) = f_s(v_{-2}(\langle\sigma\rangle\,\tau)) = \begin{cases} 1 & \text{si } \sigma = s,\ \tau \in S, \\ 0 & \text{en otro caso.} \end{cases}$$

Claramente entonces $v_{-2}^{\#}(f_s) = \sum\limits_{t\in S} \langle s\rangle\, t = \langle s\rangle\, T_S$, y de aquí se sigue que

$$\mathrm{V}_{S,G}^{-2}(f_s) = \mathrm{Tr}_S^G(v_{-2}^{\#}(f_s)) = \langle s\rangle\, T_G = f_s.$$

El resultado es ahora inmediato. ∎

Se puede definir la restricción y la transferencia sobre los grupos de homología, y el resultado análogo a este teorema afirma que la transferencia homológica sobre el grupo $H_1(G,\mathbb{Z}) \cong G/G'$ se corresponde con la transferencia de la teoría de grupos y la restricción se corresponde con la inclusión. De aquí procede el nombre de las transferencias homológica y cohomológica.

Por último vamos a usar la transferencia como auxiliar para obtener algunos resultados importantes sobre la restricción. Todos ellos serán consecuencias del teorema siguiente:

Teorema 15.4 *Sea G un grupo finito, S un subgrupo de G y A un G-módulo. Entonces $\mathrm{Res}_{G,S}^n \circ \mathrm{V}_{G,S}^n$ es la multiplicación por $|G : S|$.*

DEMOSTRACIÓN: Para los cálculos podemos tomar $\mathcal{C}(S) = \mathcal{C}(G)$ y los homomorfismos u, v iguales a la identidad. Entonces, usando (15.2),

$$\mathrm{V}_{S,G}^n(\mathrm{Res}_{G,S}^n([f])) = \mathrm{V}_{S,G}^n([f]) = [\mathrm{Tr}_S^G(f)] = [|G : S|f] = |G : S|[f].$$

∎

Por ejemplo, si $S = 1$ se cumple $H^n(S, A) = 0$, luego $\mathrm{Res}_{G,S}^n = 0$. Así pues, para todo $x \in H^n(G, A)$ se cumple $|G|x = 0$.

Sea $m = |G|$ y supongamos que la multiplicación por m es biyectiva en A. Entonces dicho automorfismo induce un automorfismo de cada grupo $H^n(G, A)$

que no es sino la multiplicación por m, luego concluimos que $H^n(G,A) = 0$ para todo n.

En particular si K es (el grupo aditivo de) un cuerpo se cumple que la multiplicación por cualquier natural m no nulo es biyectiva, luego $H^n(G,K) = 0$ para todo grupo finito G. Ya habíamos probado este hecho para el caso en que G es un grupo de Galois. La prueba que acabamos de encontrar no necesita el teorema de la base normal. Otra consecuencia que usaremos después es la siguiente:

Teorema 15.5 *Sea G un grupo finito y G_p un p-subgrupo de Sylow de G para cada primo p que divida a su orden. Si un $x \in H^n(G,A)$ cumple que su restricción a cada G_p es nula, entonces $x = 0$.*

DEMOSTRACIÓN: Si $|G| = p^{e_p} d_p$, entonces el teorema anterior implica que $d_p x = 0$. Como los números d_p son primos entre sí, existen enteros tales que $\sum_p m_p d_p = 1$, luego $x = 0$. ∎

Estudiamos ahora la cohomología de los grupos cociente. Sea, pues, G un grupo finito y S un subgrupo normal de G. Entonces A^S es un G-módulo, ya que $a\sigma s = as^{\sigma^{-1}}\sigma = a\sigma$. A su vez éste adquiere estructura de G/S-módulo de forma natural.

Consideremos resoluciones reducidas $\mathcal{C}(G)$ y $\mathcal{C}(G/S)$. Entonces $\mathcal{C}(G/S)$ es también un G-complejo con la operación dada por $x\sigma = x(\sigma S)$. Ahora no podemos asegurar que sea una resolución reducida, por lo que no podemos encontrar dos homomorfismos u, v con los que pasar a las resoluciones completas. Al menos sabemos que $\mathcal{C}(G/S)$ es acíclico, luego el teorema 14.22 nos da un homomorfismo $u : \mathcal{C}(G) \longrightarrow \mathcal{C}(G/S)$, y dos cualesquiera (que sobre $\mathbb{Z}$ sean la identidad) son homotópicos. A su vez u induce un homomorfismo

$$u^* : \mathrm{Hom}_{G/S}(\mathcal{C}(G/S), A^S) \longrightarrow \mathrm{Hom}_G(\mathcal{C}(G), A^S).$$

(Observar que aquí $\mathrm{Hom}_{G/S}$ equivale a Hom_G.)

Por otra parte, la inclusión $A^S \subset A$ induce un homomorfismo

$$\mathrm{Hom}_G(\mathcal{C}(G), A^S) \longrightarrow \mathrm{Hom}_G(\mathcal{C}(G), A),$$

que de hecho es también la inclusión. La composición de ambos es un homomorfismo de complejos que induce homomorfismos

$$\mathrm{Inf}^n_{G/S,G} : H^n(G/S, A^S) \longrightarrow H^n(G,A), \qquad n \geq 1,$$

a los que llamamos *inflaciones*. (Notar que para $n = 0$ no podemos garantizar que el homomorfismo que hemos construido respete la relación de cohomología.)

Por ejemplo, si consideramos las resoluciones canónicas de G y G/S, podemos tomar $u\big([\sigma_1,\dots,\sigma_n]\big) = [\sigma_1 S,\dots,\sigma_n S]$, y así $\mathrm{Inf}^n_{G/S,G}\big([f]\big) = [g]$, donde $g\big([\sigma_1,\dots,\sigma_n]\big) = f\big([\sigma_1 S,\dots,\sigma_n S]\big)$.

Al igual que ocurre con la restricción y la transferencia, también tiene interés estudiar la composición de la inflación seguida de la restricción. Comenzamos probando lo siguiente:

Teorema 15.6 *Sea G un grupo finito, $S \trianglelefteq G$ y A un G-módulo. Entonces*

$$\mathrm{Inf}^n_{G/S,G} \circ \mathrm{Res}^n_{G,S} = 0$$

Demostración: Consideramos las resoluciones canónicas de S, G y G/S. Entonces, si

$$\mathrm{Res}^n_{G,S}\big(\mathrm{Inf}^n_{G/S,G}([f])\big) = [g],$$

se cumple $g([s_1,\dots,s_n]) = f\big([s_1S,\dots,s_nS]\big) = f\big([S,\dots,S]\big)$.

Por otra parte podemos calcular $\mathrm{Inf}^n_{S/S,S}\big(\mathrm{Res}^n_{G/S,S/S}([f]\big) = [g']$ usando también las resoluciones canónicas, y tenemos igualmente que $g'\big([s_1,\dots,s_n]\big) = f\big([S,\dots,S]\big)$. Por lo tanto

$$\mathrm{Inf}^n_{G/S,G} \circ \mathrm{Res}^n_{G,S} = \mathrm{Res}^n_{G/S,S/S} \circ \mathrm{Inf}^n_{S/S,S},$$

y basta probar que $\mathrm{Res}^n_{G/S,S/S} = 0$, pero su imagen está en $H^n(S/S, A^S) = 0$. ∎

Para los grupos de cohomología de dimensión 1 podemos afirmar bastante más:

Teorema 15.7 *Sea G un grupo finito, $S \trianglelefteq G$ y A un G-módulo. Entonces la sucesión*

$$0 \longrightarrow H^1(G/S, A^S) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(S,A)$$

es exacta.

Demostración: Para probar la inyectividad de la inflación suponemos que $\mathrm{Inf}\big([f]\big) = [\partial a]$, para un cierto $a \in A$ (consideramos las resoluciones canónicas).

Entonces $f([\sigma S]) = (\partial a)\big([\sigma]\big) = a\sigma - a = a(\sigma S) - a$, para todo $\sigma \in G$. En particular si $s \in S$ tenemos $as - a = f\big([sS]\big) = 0$ (observar que la ecuación de los cociclos implica en general $f(1) = f(1\cdot 1) = f(1)1 + f(1) = f(1) + f(1)$, luego $f(1) = 0$). Por lo tanto $a \in A^S$ y hemos probado que $f = \partial a$, luego $[f] = 0$.

Teniendo en cuenta el teorema anterior sólo falta probar que el núcleo de la restricción está contenido en la imagen de la inflación.

Supongamos, pues, que $\mathrm{Res}\big([g]\big) = [\partial a]$, para un $a \in A$. Cambiando g por $g - \partial a$ podemos suponer que $g\big([s]\big) = 0$, para todo $s \in S$.

Entonces la ecuación de los cociclos nos da que

$$g\big([s\sigma]\big) = g\big([s]\big)\sigma + g\big([\sigma]\big) = g\big([\sigma]\big),$$

luego podemos definir $g^*\big([S\sigma]\big) = g\big([\sigma]\big)$. Además

$$g\big([\sigma]\big)s = g\big([\sigma s]\big) - g\big([s]\big) = g\big([s^{\sigma^{-1}}\sigma]\big) = g\big([\sigma]\big),$$

luego $g^*\big([S\sigma]\big) \in A^S$.

Por último, el hecho de que g sea un cociclo implica inmediatamente que g^* también lo es, y obviamente $\mathrm{Inf}\big([g^*]\big) = [g]$. ∎

Para establecer este teorema en dimensiones superiores necesitamos una hipótesis adicional. Antes necesitamos dos hechos auxiliares sencillos.

Teorema 15.8 *Sea G un grupo finito y $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ una sucesión exacta de G-módulos de manera que $H^1(G,A) = 0$. Entonces la sucesión de las restricciones $0 \longrightarrow A^G \xrightarrow{\alpha} B^G \xrightarrow{\beta} C^G \longrightarrow 0$ también es exacta.*

DEMOSTRACIÓN: Lo único que no es inmediato es la exactitud en C^G. Dado $c \in C^G$ existe un $b \in B$ tal que $\beta(b) = c$. Para cada $\sigma \in G$ tenemos que $\beta(b\sigma - b) = c\sigma - c = 0$, luego existe un $a_\sigma \in A$ tal que $\alpha(a_\sigma) = b\sigma - b$. La aplicación $\{a_\sigma\}$ es un cociclo, pues

$$\alpha(a_\sigma\tau - a_{\sigma\tau} + a_\tau) = (b\sigma - b)\tau - (b\sigma\tau - b) + (b\tau - b) = 0.$$

Por hipótesis existe un $a \in A$ tal que $a_\sigma = a\sigma - a$, para todo $\sigma \in G$, luego

$$b\sigma - b = \alpha(a)\sigma - \alpha(a),$$

de donde a su vez concluimos que $(b-\alpha(a))\sigma-(b-\alpha(a)) = 0$, y así $b-\alpha(a) \in B^G$. Por último notamos que $\beta(b - \alpha(a)) = \beta(b) = c$. ∎

Teorema 15.9 *Sea G un grupo finito, $S \trianglelefteq G$ y A un G-módulo regular. Entonces A^S es un G/S-módulo regular.*

DEMOSTRACIÓN: Recordemos que A es regular si $A \cong B \otimes \mathbb{Z}[G]$ para cierto grupo abeliano B. Podemos suponer que $A = B \otimes \mathbb{Z}[G]$. Entonces todo elemento de A se expresa de forma única como

$$\sum_{\sigma\in G} b_\sigma \otimes \sigma, \qquad b_\sigma \in B,$$

y es fácil ver que los elementos de A^S son los que cumplen $b_\sigma = b_{\sigma s}$ para todo $s \in S$ o, equivalentemente, llamando $T = \sum_{s\in S} s$, los elementos de B^S son los de la forma

$$\sum_{i=1}^{r} b_i \otimes \sigma_i T,$$

donde $\{\sigma_i\}$ es una transversal de G/S. La aplicación dada por

$$\sum_{i=1}^{r} b_i \otimes \sigma_i T \mapsto \sum_{i=1}^{r} b_i \otimes (\sigma_i S)$$

es un isomorfismo entre A^S y $B \otimes \mathbb{Z}[G/S]$. ∎

Teorema 15.10 *Sea G un grupo finito, $S \trianglelefteq G$, A un G-módulo y $n \geq 1$ un número natural tal que $H^i(S,A) = 0$ para $i = 1, \ldots, n-1$. Entonces la sucesión*

$$0 \longrightarrow H^n(G/S, A^S) \xrightarrow{\text{Inf}} H^n(G,A) \xrightarrow{\text{Res}} H^n(S,A)$$

es exacta.

DEMOSTRACIÓN: Lo probaremos por inducción sobre n (reducción regular). La prueba del teorema 14.34 nos da una sucesión exacta

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} A^+ \longrightarrow 0,$$

donde B es un G-módulo regular, de donde se siguen los isomorfismos

$$H^{i-1}(S, A^+) \cong H^i(S, A), \qquad H^{i-1}(G, A^+) \cong H^i(G, A), \quad \text{para todo } i.$$

En particular $H^i(S, A^+) = 0$ para $i = 1, \ldots, n-2$. El teorema 15.8 nos da la sucesión exacta de G/S-módulos

$$0 \longrightarrow A^S \xrightarrow{\phi} B`S \xrightarrow{\psi} (A^+)^S \longrightarrow 0,$$

y en virtud del teorema anterior $(A^+)^S$ es un G/S-módulo regular, luego también tenemos que

$$H^{i-1}(G/S, (A^+)^S) \cong H^i(G/S, A^S), \quad \text{para todo } i.$$

Consideremos el diagrama siguiente:

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{n-1}(G/S, (A^+)^S) & \xrightarrow{\text{Inf}} & H^{n-1}(G, A^+) & \xrightarrow{\text{Res}} & H^{n-1}(S, A^+) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^n(G/S, A^S) & \xrightarrow{\text{Inf}} & H^n(G, A) & \xrightarrow{\text{Res}} & H^n(S, A)
\end{array}$$

La fila superior es exacta por hipótesis de inducción. Hemos de probar que la inferior también lo es, para lo cual basta demostrar que el diagrama es conmutativo. Las flechas verticales son los isomorfismos dados por las aplicaciones de conexión en la sucesión exacta de cohomología. Recordemos que la imagen de un $[f] \in H^{n-1}(G/S, (A^+)^S)$ se calcula tomando una antiimagen de f por ψ^* (es decir, una cocadena g tal que $g \circ \psi = f$), calculando $p = \partial_n^*(g)$ y tomando una antiimagen q de p por ϕ^* (de modo que $q \circ \psi = p$). La imagen de $[f]$ es $[q]$.

Sea $u : \mathcal{C}(G) \longrightarrow \mathcal{C}(G/S)$ un homomorfismo entre resoluciones de G y G/S. Entonces la sucesión $u \circ g$, $u \circ p$, $u \circ q$ justifica que $\text{Inf}\big([q]\big) = [u \circ q]$ es la imagen de $\text{Inf}\big([f]\big) = [u \circ f]$ por la aplicación de conexión, es decir, $u \circ g \circ \psi = u \circ f$, $u \circ p = \partial_n^*(u \circ g)$ (porque u^* es un homomorfismo de complejos) y $u \circ q \circ \psi = u \circ p$. Esto nos da la conmutatividad del primer diagrama. El segundo se trata análogamente. ∎

15.3 Cohomología en formaciones de cuerpos

Los resultados de la sección anterior nos permiten profundizar en el estudio de la cohomología de las formaciones de cuerpos. Si $k \subset K \subset L$ es una cadena de cuerpos en una formación tal que L/k es normal, introducimos la notación

$$\text{Res}^n_{L/k,L/K} : H^n(L/k) \longrightarrow H^n(L/K), \quad \text{V}^n_{L/K,L/k} : H^n(L/K) \longrightarrow H^n(L/k)$$

para las restricciones y transferencias. Respecto a las inflaciones, observemos que si K/k también es normal tenemos el isomorfismo

$$G(K/k) \cong G(L/k) \,/\, G(L/K),$$

el submódulo de A_L fijado por $G(L/K)$ es A_K y las acciones de los dos grupos sobre A_K son equivalentes a través del isomorfismo. Esto significa que podemos sustituir en todo lugar las clases $(\sigma G_L)(G_K/G_L)$ por clases σG_K sin alterar por ello ningún resultado sobre inflaciones. En particular podemos considerar que las inflaciones son homomorfismos

$$\mathrm{Inf}^n_{K/k,L/k} : H^n(K/k) \longrightarrow H^n(L/k)$$

dados por $\mathrm{Inf}^n_{K/k,L/k}\big([f]\big) = [g]$, donde

$$\begin{aligned} g(\sigma_1 G_L, \dots, \sigma_n G_L) &= f\big((\sigma_1 G_L)(G_K/G_L), \dots, (\sigma_n G_L)(G_K/G_L)\big) \\ &= f(\sigma_1 G_K, \dots, \sigma_n G_K). \end{aligned}$$

Empezamos probando la afirmación que dejamos pendiente en la sección 15.1, es decir, la equivalencia entre los axiomas I y I′. Nos apoyaremos en la sucesión exacta

$$1 \longrightarrow H^1(L/K) \xrightarrow{\mathrm{Inf}} H^1(K/k) \xrightarrow{\mathrm{Res}} H^1(K/L)$$

que nos proporciona el teorema 15.7 para toda cadena de extensiones normales $k \subset L \subset K$ de una formación. Basta aplicar el teorema siguiente en el caso $m = 0$ y $r = 1$.

Teorema 15.11 *Consideremos una formación en la que para toda cadena de extensiones normales $k \subset L \subset K$ la sucesión*

$$H^r(L/K) \xrightarrow{Inf} H^r(K/k) \xrightarrow{Res} H^r(K/L)$$

es exacta (para un cierto $r \geq 1$). Entonces la relación $h_r(K/k) \,\big|\, |K : k|^m$ (para un $m \geq 0$ fijo) es válida para toda extensión normal K/k si y sólo si es válida para toda extensión cíclica de grado primo.

Demostración: Razonaremos por inducción sobre $|K : k|$. Supongamos que el teorema se cumple para extensiones de grado menor. Si el grado es primo la conclusión es la hipótesis. Si $|K : k|$ es potencia de primo (con exponente mayor que 1) entonces $G(K/k)$ contiene un subgrupo normal propio, que será de la forma $G(K/L)$.

Por la hipótesis sobre la sucesión exacta $h_r(K/k) \mid h_r(K/L)\, h_r(L/k)$. Las extensiones K/L y L/k tienen grados menores que $|K : k|$, luego por hipótesis de inducción

$$h_r(K/L) \,\big|\, |K : L|^m, \qquad h_r(L/k) \,\big|\, |L : k|^m.$$

La transitividad de grados implica obviamente que $h_r(K/k) \,\big|\, |K : k|^m$.

Finalmente, si $|K:k|$ no es potencia de primo tomamos un p-subgrupo de Sylow $G(K/L_p)$ de $G(K/k)$ para cada primo p que divida a dicho orden. El producto de las restricciones de $H^r(K/k)$ en $\prod_p H^r(K/L_p)$ es un monomorfismo por el teorema 15.5, luego resulta que $h_r(K/k) \mid \prod_p h_r(K/L_p)$ y por hipótesis de inducción $h_r(K/L_p) \,\big|\, |K:L_p|^m$. Así pues

$$h_r(K/k) \mid \prod_p |K:L_p|^m = |K:k|^m.$$

■

Con esto tenemos probado que la formación C de los grupos de clases de elementos ideales es una formación de cuerpos. Observemos ahora que el teorema 15.10 nos da que si $k \subset K \subset L$ es una cadena de extensiones normales en una formación de cuerpos, entonces tenemos la sucesión exacta

$$1 \longrightarrow H^2(K/k) \xrightarrow{\text{Inf}} H^2(L/k) \xrightarrow{\text{Res}} H^2(L/K). \tag{15.6}$$

En particular podemos identificar el segundo grupo de cohomología de K/k con un subgrupo del de L/k. Esto nos da la posibilidad de reunir todos los grupos de cohomología como subgrupos de un mismo grupo, es decir, construir un límite inductivo de los grupos $H^2(K/k)$ cuando K varía entre las extensiones normales de k. Veamos la construcción.

Definición 15.12 Sea $(G, \{G_K\}_{K\in S}, A)$ una formación de cuerpos y consideremos en A la topología discreta. Un *cociclo* de un cuerpo k es una aplicación continua $f : G_k \times G_k \longrightarrow A_k$ que cumpla la ecuación

$$f(\rho,\sigma)^\tau = f(\rho,\sigma\tau)f(\sigma,\tau)f(\rho\sigma,\tau)^{-1}.$$

Una *cocadena* en k es una aplicación continua $g : G_k \longrightarrow A_k$. Una *cofrontera* es un cociclo de la forma

$$f(\sigma,\tau) = g(\sigma)^\tau g(\tau) g(\sigma\tau)^{-1},$$

para una cierta cocadena g.

La continuidad de una cocadena equivale a que $g(\sigma)$ depende sólo de la clase de σ módulo un subgrupo normal abierto de G_k. En efecto, para cada $\sigma \in G_k$ existe un subgrupo abierto $H_\sigma \leq G_k$ tal que $\sigma \in H_\sigma\sigma \subset g^{-1}[\{g(\sigma)\}]$. La unión de estas clases $H_\sigma\sigma$ es todo G_k, luego por compacidad basta un número finito de ellas. Formando la intersección de los subgrupos H_σ correspondientes a dicha unión finita obtenemos un subgrupo abierto H con la propiedad de que si σ' y σ'' determinan la misma clase módulo H entonces ambos elementos están en la misma clase $H_\sigma\sigma$, luego $g(\sigma') = g(\sigma) = g(\sigma'')$.

Si N es la intersección de todos los conjugados de H en G_k, entonces N es un subgrupo normal abierto de G_k y dos elementos congruentes módulo N lo son módulo H, luego f depende sólo de las clases módulo N.

Recíprocamente, si g depende de las clases módulo un subgrupo N, entonces las antiimágenes de los elementos de A son vacías o uniones de clases módulo N, luego son abiertas, y por tanto g es continua.

Del mismo modo se justifica que la continuidad de un cociclo f equivale a que $f(\sigma,\tau)$ depende de la clase de σ y τ módulo un subgrupo normal abierto de G_k. Si K es una extensión normal de k, llamaremos cociclos de k módulo K a los cociclos de k que dependen sólo de las clases módulo G_K.

Observemos que existe una biyección entre los cociclos de k módulo K y los cociclos de dimensión 2 (en el sentido usual) del grupo $G(K/k) = G_k/G_K$ respecto a su acción sobre A_k. Esta biyección viene dada por

$$f(\sigma,\tau) = f(G_K\sigma, G_K\tau), \qquad \text{para } \sigma,\tau \in G_k.$$

(Notar que usamos el mismo nombre f para los cociclos correspondientes).

Del mismo modo podemos identificar las cocadenas de K/k con las cocadenas de k módulo K.

Ahora definimos el *grupo de Brauer* de k como el grupo cociente de los cociclos de k módulo las cofronteras, y lo representaremos por $H^2(*/k)$.

Es importante tener presente que no podemos aplicar a $H^2(*/k)$ la teoría de cohomología de grupos que hemos estudiado, pues G_k es infinito y además no estamos considerando todos sus cociclos (en el sentido de la cohomología), sino sólo los continuos. El grupo de Brauer sólo va a ser una forma de relacionar los grupos de cohomología de las distintas extensiones de k.

Como las cofronteras de K/k se corresponden claramente con las cofronteras de k módulo K, podemos definir inflación

$$\mathrm{Inf} : H^2(K/k) \longrightarrow H^2(*/k),$$

mediante $\mathrm{Inf}\big([f]\big) = [f]$. El teorema siguiente afirma en esencia que $H^2(*/k)$ es el límite inductivo de los grupos $H^2(K/k)$.

Teorema 15.13 *Sea k un cuerpo en una formación de cuerpos. Entonces*

a) La inflación $\mathrm{Inf} : H^2(K/k) \longrightarrow H^2(*/k)$ es un monomorfismo para cada extensión normal K de k.

b) Si identificamos cada grupo $H^2(K/k)$ con su imagen en el grupo de Brauer, entonces $H^2(*/k)$ es la unión de todos los subgrupos $H^2(K/k)$.

c) Si $k \subset K \subset L$ es una cadena de extensiones normales, entonces la inflación

$$\mathrm{Inf} : H^2(K/k) \longrightarrow H^2(L,k)$$

coincide con la inclusión.

d) Si $\phi_K : H^2(K/k) \longrightarrow G$ es una familia de homomorfismos de grupos tal que cuando $K \subset L$ entonces ϕ_L extiende a ϕ_K (o, equivalentemente, si conmutan con las inflaciones) entonces existe un único homomorfismo $\phi : H^2(*/k) \longrightarrow G$ que extiende a todos los homomorfismos ϕ_K .

DEMOSTRACIÓN: a) Supongamos que $[f] = 1$ en $H^2(*/k)$. Entonces f está determinado por una cocadena g de k, que por continuidad será una cocadena módulo L para una cierta extensión normal L/k. Podemos suponer que L contiene a K. Es claro que g determina una cocadena de L/k, de modo que la inflación $H^2(K/k) \longrightarrow H^2(L/k)$ envía $[f]$ a la clase de la cocadena determinada por g, es decir, $\mathrm{Inf}\big([f]\big) = 0$.

Como las inflaciones entre extensiones son inyectivas (en las formaciones de cuerpos), concluimos que $[f] = 0$.

b), c) y d) son inmediatos. ∎

Definición 15.14 Como caso particular del apartado d) del teorema anterior, para cada extensión K/k (no necesariamente normal) podemos definir las *restricciones* y *transferencias*

$$\mathrm{Res}_{k,K} : H^2(*/k) \longrightarrow H^2(*/K), \qquad \mathrm{V}_{K,k} : H^2(*/K) \longrightarrow H^2(*/k)$$

como las extensiones de las aplicaciones correspondientes entre los grupos de cohomología $H^2(L/k)$ y $H^2(L/K)$, donde L varía en las extensiones normales de k que contienen a K. Observar que no importa ignorar a las que no cumplen $K \subset L$ porque los grupos $H^2(L/k)$ cubren igualmente a $H^2(*/k)$, y eso es lo único que hace falta.

La comprobación de que las restricciones y transferencias conmutan con las inflaciones es mera rutina, usando las resoluciones canónicas. Para la restricción el argumento es sencillo, para la transferencia es más largo porque hay que aplicar la definición de la traza y la fórmula (15.4).

Del teorema 15.4 se sigue la relación $\mathrm{V}_{K,k}\big(\mathrm{Res}_{k,K}(x)\big) = |K : k|\, x$. Así mismo, teniendo en cuenta (15.6), es clara la exactitud de las sucesiones

$$1 \longrightarrow H^2(K/k) \xrightarrow{\mathrm{Inf}} H^2(*/k) \xrightarrow{\mathrm{Res}} H^2(*/K).$$

Resulta útil pensar en este hecho en los términos siguientes: Diremos que una clase $x \in H^2(*/k)$ *se escinde* en K cuando $\mathrm{Res}_{k,K}(x) = 1$. Entonces tenemos que $H^2(K/k)$ es isomorfo (o igual) al grupo de clases de $H^2(*/k)$ que se escinden en K.

15.4 El grupo de Brauer de una formación local

Recordemos que las formaciones locales son las constituidas por extensiones finitas de un cuerpo métrico discreto localmente compacto k. Vamos a obtener la estructura del grupo de Brauer de estas formaciones. Tan sólo vamos a necesitar lo que en el teorema 7.9 probamos para extensiones de cuerpos p-ádicos. Con las técnicas cohomológicas es relativamente fácil generalizarlo a cuerpos locales cualesquiera. Ante todo conviene modificar la notación que usábamos en el capítulo VII. Es claro que si G es un grupo cíclico y A es un G-módulo, los

grupos definidos en (7.2) son los grupos de cohomología de dimensión 0 y -1 o, equivalentemente, de dimensión 2 y 1. Por lo tanto, el cociente de Herbrand es el cociente de los órdenes de estos dos grupos. En lo sucesivo lo llamaremos $h_{2/1}(G, A)$.

Diremos que A es un G-módulo *topológico* si A es un grupo topológico y los isomorfismos inducidos por la acción de G son continuos. El resultado que buscamos se sigue del siguiente teorema técnico:

Teorema 15.15 *Sea A un G-módulo topológico completo y*

$$A = A_0 \supset A_1 \supset A_1 \supset \cdots$$

una sucesión de submódulos tal que todo entorno de 0 contiene un A_i. Si $H^n(G, A_i/A_{i+1}) = 0$ para todo i, entonces $H^n(G, A) = 0$.

Demostración: La sucesión $0 \longrightarrow A_{i+1} \longrightarrow A_i \longrightarrow A_i/A_{i+1} \longrightarrow 0$ da lugar a la sucesión exacta

$$H^n(G, A_{i+1}) \longrightarrow H^n(G, A_i) \longrightarrow H^n(G, A_i/A_{i+1}) = 0.$$

La suprayectividad de la primera aplicación (que no es sino la dada por $[f] \mapsto [f]$) implica que para todo cociclo f_i de A_i (de dimensión n) existe un cociclo f_{i+1} de A_{i+1} y una cocadena g_i de A_i (de dimensión $n-1$) de modo que $f_i - f_{i+1} = \partial^{n-1} g_i$. Partiendo de un cociclo arbitrario f_0 de A obtenemos sucesiones $\{f_i\}$ y $\{g_i\}$ tales que

$$\begin{aligned} f_0(x) - f_{i+1}(x) &= \partial^{n-1} g_0(x) + \cdots + \partial^{n-1} g_i(x) \\ &= g_0(\partial_n(x)) + \cdots + g_i(\partial_n(x)), \end{aligned} \tag{15.7}$$

para todo $x \in C_n$ (el grupo de cadenas de una resolución de G).

Si $y \in C_{n-1}$ tenemos que $g_i(y) \in A_i$, luego $\sum_{k=i}^{i+j} g_k(y) \in A_i$. Como todo entorno de 0 contiene un A_i, concluimos que la serie es una sucesión de Cauchy y, como A es completo, converge a un $g(y) = \sum_{k=0}^{\infty} g_i(y)$. La continuidad de las operaciones implica que g es un G-homomorfismo (o sea, una cocadena).

Por otra parte es claro también que $f_{i+1}(x)$ tiende a 0, luego tomando límites en (15.7) concluimos que $f_0(x) = g(\partial_n(x)) = \partial^{n-1} g(x)$, luego $[f_0] = 0$. ∎

De aquí deducimos:

Teorema 15.16 *Sea k un cuerpo local y K/k una extensión cíclica. Sea G el grupo de Galois y U el grupo de las unidades de K. Entonces $h_{2/1}(G, U) = 1$.*

Demostración: Sea $\{u^\sigma\}_{\sigma \in G}$ una base normal de K/k, sea E el anillo de enteros de k y π un primo de E. Definimos $V_0 = \sum_{\sigma \in G} E u^\sigma$ y $V_i = \pi^i V_0$.

Cada producto $u^\sigma u^\tau$ tiene una ciertas coordenadas en la base $\{u^\sigma\}_{\sigma \in G}$. Si cambiamos u por $\pi^k u$ para cierto k obtenemos una nueva base normal en la

que dichas coordenadas han sido multiplicadas por π^{2k}. Por lo tanto podemos exigir que todas ellas sean enteras y divisibles entre π. Esto se traduce en que $V_0V_0 \subset V_1$ y, más en general, $V_i^2 \subset V_{i+1}$. En particular V_0 es un anillo (no unitario).

La base $\{u^\sigma\}_{\sigma\in G}$ define una norma en K respecto a la cual V_0 es la bola unidad (la norma de un elemento de K es el supremo de los valores absolutos de sus coordenadas en la base dada). Puesto que todas las normas son equivalentes, V_0 es un entorno (abierto y cerrado) de 0 en K (para su topología dada, que no depende de la norma). Además V_0 está acotado, luego los módulos V_i resultan ser una base de entornos de 0.

Definimos ahora $A_i = 1+V_i$. Es claro que $A_i^2 \subset 1+V_i+V_i+V_i^2 \subset 1+V_i = A_i$, luego cada A_i es un G-submódulo de U. Además forman una base de entornos (abiertos) de 1. Como U es compacto, el cociente U/A_0 es finito, luego la relación (7.1) aplicada a la sucesión exacta

$$1 \longrightarrow A_0 \longrightarrow U \longrightarrow U/A_0 \longrightarrow 1$$

nos da que $h_{2/1}(G,U) = h_{2/1}(G,A_0)h_{2/1}(G,U/A_0) = h_{2/1}(G,A_0)$ (recordemos que los cocientes de Herbrand de los módulos finitos son triviales).

Para probar que el último cociente vale 1 es suficiente demostrar que todos los grupos de cohomología de A_0 son triviales, para lo cual aplicaremos el teorema anterior. Observar que A_0 es completo porque es compacto (es abierto y cerrado). Sólo hemos de probar que $H^n(G, A_i/A_{i+1}) = 1$ para todo n y todo i. A su vez basta probar que los módulos A_i/A_{i+1} son G-regulares.

Tenemos el G-isomorfismo $V_0/\pi V_0 \cong A_i/A_{i+1}$ dado por $[\alpha] \mapsto [1+\pi^i\alpha]$. La prueba es sencilla si tenemos en cuenta que

$$\frac{(1+\pi^i\alpha)(1+\pi^i\beta)}{1+\pi^i(\alpha+\beta)} = 1 + \frac{\pi^{2i}\alpha\beta}{1+\pi^i(\alpha+\beta)} \in A_{i+1}.$$

Para probar que el segundo sumando está en V_0 usamos el desarrollo en serie $(1+x)^{-1} = 1 - x + x^2 - x^3 + \cdots$ junto con el hecho de que V_0 es un anillo cerrado. Finalmente observamos que $V_0 = \sum_{\sigma\in G} Eu^\sigma$ y $\pi V_0 = \sum_{\sigma\in G} \pi E u^\sigma$, luego

$$V_0/\pi V_0 \cong \sum_{\sigma\in G} \big(E/(\pi)\big)u^\sigma \cong \sum_{\sigma\in G} \big(E/(\pi)\big) \otimes \sigma \cong \big(E/(\pi)\big) \otimes \mathbb{Z}[G].$$

■

Ahora ya es fácil generalizar 7.9. Dada una extensión cíclica K/k como en el teorema anterior, si π es un primo en K tenemos que $K^* = U \times \langle\pi\rangle$, y además U es un G-submódulo de K^*. Más aún, la acción de G sobre el cociente es $[\pi]^\sigma = [\pi^\sigma] = [\epsilon\pi] = [\pi]$, es decir, el cociente K^*/U es un G-módulo trivial. Equivalentemente, tenemos la sucesión exacta

$$1 \longrightarrow U \xrightarrow{i} K^* \xrightarrow{v} \mathbb{Z} \longrightarrow 0, \tag{15.8}$$

donde i es la inclusión y v la valoración en K^*.

Ahora es fácil probar el teorema siguiente. Notemos que el apartado a) afirma que las formaciones locales satisfacen el axioma 0.

Teorema 15.17 *Sea K/k una extensión cíclica de cuerpos locales. Sea e su índice de ramificación, G su grupo de Galois y U el grupo de unidades de K. Entonces*

a) $|H^2(K/k)| = |K : k|$.

b) $|H^n(G, U)| = e$ *para todo* $n \in \mathbb{Z}$.

Demostración: a) Aplicamos la relación (7.1) a la sucesión exacta (15.8) junto con el teorema anterior, que nos da

$$h_{2/1}(K/k) = h_{2/1}(G, \mathbb{Z}).$$

Por el teorema de Hilbert-Speiser el miembro izquierdo es $|H^2(K/k)|$, mientras que (14.6) y (14.8), junto con la periodicidad de la cohomología cíclica, nos dan que el miembro derecho es $|K : k|$.

b) De la sucesión (15.8) obtenemos la sucesión exacta de cohomología

$$0 \longrightarrow H^0(G, U) \longrightarrow H^0(K/k) \longrightarrow H^0(G, \mathbb{Z}) \longrightarrow H^1(G, U) \longrightarrow 1.$$

Además $H^0(K/k) = k^*/\,\mathrm{N}[K^*]$, $H^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ (donde $n = |K : k|$) y la aplicación que los conecta es la dada por $[\alpha] \mapsto [v(\alpha)]$. Es claro que la imagen de este homomorfismo es $e\mathbb{Z}/n\mathbb{Z}$, luego $|H^1(G, U)| = e$. Como $h_{2/1}(G, U) = 1$, también $|H^2(G, U)| = e$ y, por la periodicidad, lo mismo vale para todas las dimensiones. ∎

En el caso en que $e = 1$, la sucesión exacta que hemos considerado en la prueba se reduce a

$$1 \longrightarrow H^0(K/k) \longrightarrow H^0(G, \mathbb{Z}) \longrightarrow 0,$$

de donde concluimos el teorema siguiente:

Teorema 15.18 *Sea K/k una extensión no ramificada de cuerpos locales. Entonces $H^2(K/k) \cong k^*/\,\mathrm{N}[K^*] \cong \mathbb{Z}/n\mathbb{Z}$, donde $n = |K : k|$. El último isomorfismo viene dado por $[\alpha] \mapsto [v(\alpha)]$.*

Las extensiones no ramificadas son la clave para determinar la estructura de los grupos de Brauer locales. Recordemos que al final del capítulo anterior probamos que el isomorfismo $H^*(K/k) \cong k^*/\,\mathrm{N}[K^*]$ viene dado por $x \mapsto E(x)(\sigma)$, donde σ es cualquier generador del grupo $G(K/k)$. Veamos ahora que si en una cadena elegimos consistentemente los generadores, los isomorfismos satisfacen una relación de consistencia.

Teorema 15.19 *Sea $k \subset L \subset K$ una cadena de extensiones cíclicas de cuerpos locales. Sea $|K:k| = m$ y $|L:k| = n$. Fijemos un generador $G(K/k) = \langle\sigma\rangle$, con lo que $G(L/k) = \langle\sigma|_L\rangle$. Entonces el diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} H^2(K/k) & \xrightarrow{E(\cdot)(\sigma)} & k^*/\,\mathrm{N}[K^*] \\ \mathrm{Inf}\uparrow & & \uparrow \\ H^2(L/k) & \xrightarrow[E(\cdot)(\sigma|_L)]{} & k^*/\,\mathrm{N}[L^*] \end{array}$$

donde la flecha de la derecha es el homomorfismo dado por $[a] \mapsto [a^{m/n}]$.

Demostración: En términos de formaciones podemos considerar

$$G(K/k) = G_k/G_K = \langle\sigma G_K\rangle \quad \text{y} G(L/k) = G_k/G_L = \langle\sigma G_L\rangle$$

(donde G_k es el grupo de Galois de cualquier extensión de k que contenga a K).

Tomamos un $a \in k^*$, a cuya clase módulo $\mathrm{N}[L^*]$ le corresponde, de acuerdo con (14.14), la del cociclo dado por

$$f(\sigma^i G_L, \sigma^j G_L) = a^{[(i+j)/n]} \quad i,j = 0,\dots,n-1.$$

Su inflación es $f(\sigma^i G_K, \sigma^j G_K) = f(\sigma^i G_L, \sigma^j G_L)$, y a la clase de este cociclo le corresponde a su vez la clase

$$\prod_{i=0}^{m-1} f(\sigma G_L, \sigma^i G_L) = \prod_{i=0}^{n-1} f(\sigma G_L, \sigma^i G_L)^{m/n} = a^{m/n},$$

(pues $f(\sigma G_L, \sigma^i G_L)$ depende sólo de la clase de σ^i, luego del resto de i módulo n). ∎

El paso siguiente es notar que para las extensiones no ramificadas tenemos un criterio con que elegir los generadores de los grupos de Galois de modo que se pueda aplicar siempre el teorema anterior: basta tomar el *automorfismo canónico* que ya consideramos en el capítulo 12 para extensiones de cuerpos p-ádicos. Concretamente, si K/k es una extensión no ramificada de cuerpos locales, llamaremos $\sigma_{K/k}$ a la antiimagen por el isomorfismo descrito en el teorema 1.39 del automorfismo de Frobenius de la extensión $\overline{K}/\overline{k}$ de los cuerpos de restos. Equivalentemente, $\sigma_{K/k}$ es el único elemento de $G(K/k)$ que verifica la congruencia $\sigma_{K/k}(\alpha) \equiv \alpha^r \pmod{\mathfrak{p}}$, para todo entero α de K, donde $\mathfrak{p}$ es el ideal primo de k y r es el número de elementos de $\overline{k}$.

Es obvio que, en las condiciones del teorema anterior, $\sigma_{K/k}|_L = \sigma_{L/k}$, luego siempre tenemos la conmutatividad del diagrama indicado. Ahora consideramos el segundo isomorfismo del teorema 15.18, es decir, el inducido por la valoración de k. Obviamente obtenemos un diagrama conmutativo

$$\begin{array}{ccccc} H^2(K/k) & \longrightarrow & k^*/\,\mathrm{N}[K^*] & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ \uparrow & & \uparrow & & \uparrow \\ H^2(L/k) & \longrightarrow & k^*/\,\mathrm{N}[L^*] & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \end{array}$$

donde la flecha vertical derecha es el monomorfismo dado por $[u] \mapsto [mu/n]$.

Cuando consideramos los grupos de cohomología como subgrupos del grupo de Brauer de k, la flecha izquierda es simplemente la inclusión. Podemos transformar la flecha derecha en una inclusión si sumergimos cada grupo $\mathbb{Z}/n\mathbb{Z}$ en $\mathbb{Q}/\mathbb{Z}$ mediante el monomorfismo $[u] \mapsto [u/n]$. Así llegamos al diagrama

$$\begin{array}{ccccccc} H^2(K/k) & \longrightarrow & k^*/\,\mathrm{N}[K^*] & \longrightarrow & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \langle 1/m\rangle \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ H^2(L/k) & \longrightarrow & k^*/\,\mathrm{N}[L^*] & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \langle 1/n\rangle \end{array}$$

donde la última flecha corresponde a la aplicación $[1/n] \mapsto [1] \mapsto [m/n] \mapsto [1/n]$, es decir, a la inclusión.

Definición 15.20 Sea k un cuerpo local y sea A/k una extensión de Galois (quizá infinita) que determina una formación local. Llamaremos

$$\overline{H}^2(*/k) = \bigcup_T H^2(T/k),$$

donde T recorre las extensiones no ramificadas de k contenidas en A. Entonces $\overline{H}^2(*/k)$ es un subgrupo de $H^2(*/k)$ sobre el que tenemos definido el monomorfismo

$$\mathrm{Inv}_k : \overline{H}^2(*/k) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

determinado por la composición de los tres isomorfismos anteriores en cada grupo $H^2(T/k)$. Si $c \in \overline{H}^2(*/k)$, entonces $\mathrm{Inv}_k(c)$ se llama *invariante* de c. Explícitamente,

$$\mathrm{Inv}_k(c) = \frac{v_k(E(c)(\sigma_{T/k}))}{n} \ (\text{mód } 1),$$

donde T es cualquier extensión no ramificada de k tal que $c \in H^2(T/k)$, v_k es la valoración de k y $n = |T : k|$.

Vamos a probar que las formaciones locales verifican, bajo condiciones obvias, el

Axioma II′: *Para cada cuerpo k, existe un subgrupo $\overline{H}^2(*/k)$ de $H^2(*/k)$ y un monomorfismo* $\mathrm{Inv} : \overline{H}^2(*/k) \longrightarrow \mathbb{Q}/\mathbb{Z}$ *de modo que*

a) Si K/k es una extensión cualquiera $\mathrm{Res}_{k,K}[\overline{H}^2(*/k)] \subset \overline{H}^2(*/K)$ *y para todo $c \in \overline{H}^2(*/k)$ se verifica que*

$$\mathrm{Inv}_K(\mathrm{Res}_{k,K}(c)) = |K : k|\ \mathrm{Inv}_k(c).$$

b) Si existe una extensión K/k de grado n, entonces $\overline{H}^2(*/k)$ contiene un subgrupo (cíclico) de orden n

Las condiciones obvias a las que aludíamos se refieren a la parte b). Teniendo en cuenta que un cuerpo k admite extensiones no ramificadas de todos los órdenes, es obvio que esta parte se cumple si A contiene a todas las extensiones no ramificadas de k (en cuyo caso tenemos de hecho que $\overline{H}^2(*/k) \cong \mathbb{Q}/\mathbb{Z}$). Por ejemplo esto sucede si A es la clausura separable de k (en una clausura algebraica), si A es la mayor extensión abeliana de k o si A es la unión de todas las extensiones no ramificadas de k. Éstos son los principales casos de interés. Sin embargo la parte b) del axioma anterior puede satisfacerse en otras circunstancias, como por ejemplo si A es la unión de todas las extensiones de k de grado potencia de un primo prefijado. Observar también que todos los subgrupos finitos de $\mathbb{Q}/\mathbb{Z}$ son cíclicos, luego la hipótesis al respecto en la parte b) es superflua. El resto del axioma II′ se cumple siempre en las formaciones locales:

Teorema 15.21 *Toda extensión K/k en una formación local cumple la parte a) del axioma II′.*

Demostración: Si T es una extensión no ramificada de k, es claro que $\mathrm{Res}_{k,K}[H^2(T/k)] \subset H^2(KT/K)$ (si un cociclo de k depende de las clases módulo G_T, su restricción a G_K depende sólo de las clases módulo $G_K \cap G_T = G_{KT}$). Por lo tanto $\mathrm{Res}_{k,K}[\overline{H}^2(*/k)] \subset \overline{H}^2(*/K)$.

Supongamos ahora que la extensión K/k es no ramificada. En este caso basta probar la fórmula para clases $c \in H^2(T/k)$ donde $k \subset K \subset T$ (pues estos subgrupos cubren a todo el grupo $\overline{H}^2(*/k)$).

Sea $|T:k| = n$ y $|K:k| = m$. Es claro que $\sigma_{T/K} = (\sigma_{T/k})^m$ (a partir de la relación análoga entre los automorfismos de Frobenius de los cuerpos de restos).

Veamos primero el homomorfismo $k^*/\mathrm{N}[T^*] \longrightarrow K^*/\mathrm{N}[T^*]$ que se corresponde con la restricción a través de los isomorfismos canónicos que hemos fijado. Si $a \in k^*$, la clase de cohomología asociada a su clase es la del cociclo

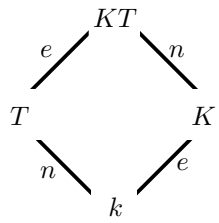
$$f(\sigma^i_{T/k}, \sigma^j_{T/k}) = a^{[(i+j)/n]}, \qquad i,j = 0,\dots,n-1.$$

Por otra parte, a la clase de su restricción le corresponde el elemento

$$\prod_{i=0}^{n/m-1} f(\sigma_{T/K}, \sigma^i_{T/K}) = \prod_{i=0}^{n/m-1} f(\sigma^m_{T/k}, \sigma^{mi}_{T/k}) = a.$$

Así pues, la aplicación correspondiente es la dada por $[a] \mapsto [a]$. Al componer con los isomorfismos inducidos por las valoraciones en k y en K (teniendo en cuenta que la segunda extiende a la primera debido a que K/k es no ramificada) obtenemos el homomorfismo $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/\frac{n}{m}\mathbb{Z}$ dado por $[u] \mapsto [u]$. Por último, al sumergir estos grupos en $\mathbb{Q}/\mathbb{Z}$ nos queda que $[1/n] \mapsto [1] \mapsto [1] \mapsto [m/n]$, luego se trata de la aplicación $[r] \mapsto m[r] = |K:k|\,[r]$, como queríamos probar.

En segundo lugar supongamos que la extensión K/k es totalmente ramificada, es decir, su grado de inercia es $f = 1$. Si T/k es cualquier extensión no ramificada (digamos de grado n) tenemos la situación siguiente:



Se cumple $|KT : K| = |T : k| = n$, pues n es el grado de inercia de toda la extensión KT/k (alternativamente, $T \cap K = k$, pues el grado de inercia y el índice de ramificación de $T \cap K$ sobre k son ambos iguales a 1). Como los cuerpos de restos de KT y K coinciden respectivamente con los de T y k es claro que $\sigma_{KT/K}|_T = \sigma_{T/k}$. Si consideramos los automorfismos de las extensiones como clases de automorfismos de una extensión mayor, esta igualdad se interpreta como que $\sigma_{KT/K} = \sigma G_{KT}$ y $\sigma_{T/k} = \sigma G_k$, para un mismo automorfismo σ.

Ahora, a un elemento $a \in k^*$ le corresponde el cociclo

$$f(\sigma^i_{KT/K}, \sigma^j_{KT/K}) = a^{[(i+j)/n]}, \qquad i, j = 0, \dots, n-1.$$

Su restricción es $f(\sigma^i_{T/k}, \sigma^j_{T/k}) = f(\sigma^i_{KT/K}, \sigma^j_{KT/K})$, y es claro que a ésta le corresponde de nuevo el elemento a. El resto es idéntico al caso anterior.

En el caso en que K/k es una extensión cualquiera consideramos el cuerpo de inercia E, de modo que la extensión E/k es no ramificada y la extensión K/E es totalmente ramificada. Es obvio que $\mathrm{Res}_{k,K} = \mathrm{Res}_{k,E} \circ \mathrm{Res}_{E,K}$, y la fórmula se deduce inmediatamente de los dos casos ya probados. ∎

Ahora estamos en condiciones de obtener la estructura de los grupos de Brauer locales. El resultado que vamos a obtener tiene un análogo en la teoría global, y sobre él descansa fuertemente la teoría de cuerpos de clases, por lo que conviene expresarlo axiomáticamente.

Definición 15.22 Una formación de cuerpos es una *formación de clases* si cumple el

Axioma II: *Para cada cuerpo k de la formación existe un monomorfismo $\mathrm{Inv}_k : H^2(*/k) \longrightarrow \mathbb{Q}/\mathbb{Z})$ de modo que*

a) Si K/k es una extensión normal de grado n entonces

$$\mathrm{Inv}_k[H^2(K/k)] = \langle 1/n \rangle\,.$$

b) Si K/k es una extensión cualquiera y $c \in H^2(*/k)$ entonces

$$\mathrm{Inv}_K(\mathrm{Res}_{k,K}(c)) = |K : k|\ \mathrm{Inv}_k(c).$$

Observar que ya no hablamos de subgrupos, sino de los propios grupos de Brauer. El hecho notable es el teorema siguiente:

Teorema 15.23 *Si una formación satisface los axiomas $0'$, I' (resp. I'') y II' entonces es una formación de clases.*

DEMOSTRACIÓN: Ya sabemos que se trata de una formación de cuerpos. Sólo hay que demostrar el axioma II.

Veamos en primer lugar que $\overline{H}^2(*/k) = H^2(*/k)$ para todo cuerpo k. Para ello basta ver que si K/k es cualquier extensión normal $H^2(K/k) \subset \overline{H}^2(*/k)$. Sea $n = |K : k|$. Por II′ b) tenemos que $\overline{H}^2(*/k)$ contiene un subgrupo cíclico T de orden n. Por II′ a) se cumple que

$$\mathrm{Inv}_K[\mathrm{Res}_{k,K}[T]] = n\ \mathrm{Inv}_k[T] = \mathrm{Inv}_k[T^n] = 0.$$

Como Inv_K es un monomorfismo concluimos que $\mathrm{Res}_{k,K}[T] = 1$ y de la exactitud de la sucesión

$$1 \longrightarrow H^2(K/k) \xrightarrow{\mathrm{Inf}} H^2(*/k) \xrightarrow{\mathrm{Res}} H^2(*/K)$$

deducimos que $T \subset H^2(K/k)$ (recordemos que la inflación es simplemente la inclusión).

El teorema 15.11, aplicado con $r = 2$, $m = 1$, nos da que $|H^2(K/k)| \leq |K : k|$ para toda extensión normal (pues para extensiones cíclicas de grado primo es una igualdad por los axiomas I y 0′). Así pues, tenemos que $|H^2(K/k)| \leq |T|$ y por consiguiente $H^2(K/k) = T \subset \overline{H}^2(*/k)$. En particular tenemos que $H^2(K/k)$ es un grupo cíclico de orden n, luego lo mismo le ocurre a su imagen por Inv_k. Terminamos la prueba notando que $\langle 1/n\rangle$ es el único subgrupo cíclico de orden n en $\mathbb{Q}/\mathbb{Z}$, luego se cumple también la parte a) del axioma II. ∎

Si particularizamos la prueba anterior al caso de las formaciones locales, lo que hemos demostrado es que, para cualquier extensión normal de grado n, el grupo $H^2(K/k)$ coincide con el grupo $H^2(T/k)$, donde T es la única extensión no ramificada de k de grado n.

15.5 Formaciones de clases

En esta sección estudiamos las propiedades comunes de las formaciones de clases que acabamos de introducir. Esencialmente, vamos a ver que en las formaciones de clases podemos seleccionar generadores canónicos de los grupos $H^2(K/k)$, con lo que obtendremos una serie de propiedades de consistencia. A su vez, esto nos permitirá redondear los resultados que hemos visto hasta ahora sobre la cohomología de las formaciones.

Definición 15.24 Si K/k es una extensión normal de grado n en una formación de clases, entonces el monomorfismo Inv_k biyecta $H^2(K/k)$ con $\langle[1/n]\rangle$. Llamaremos *clase fundamental* de la extensión a la clase $\xi_{K/k} \in H^2(K/k)$ tal que $\mathrm{Inv}_k(\xi_{K/k}) = [1/n]$. Así pues, $H^2(K/k) = \langle \xi_{K/k} \rangle$. A los cociclos de la clase fundamental los llamaremos *cociclos fundamentales.*

En primer lugar probamos:

Teorema 15.25 *Sea $k \subset K \subset L$ una cadena de extensiones en una formación de clases con L/k normal. Entonces* $\mathrm{Res}_{k,K}(\xi_{L/k}) = \xi_{L/K}$.

DEMOSTRACIÓN: Sea $n = |L : k|$ y $m = |L : K|$. Entonces $|K : k| = n/m$. En virtud del axioma II b) tenemos que

$$\mathrm{Inv}_K(\mathrm{Res}_{k,K}(\xi_{L/k})) = (n/m)\,\mathrm{Inv}_k(\xi_{L/k}) = (n/m)[1/n] = [1/m],$$

luego en efecto $\mathrm{Res}_{k,K}(\xi_{L/k}) = \xi_{L/K}$. ∎

Como aplicación tenemos el teorema siguiente, que mejora (15.6). La prueba es inmediata, sin más que tener en cuenta que las clases fundamentales generan los grupos de cohomología.

Teorema 15.26 *Sea $k \subset K \subset L$ una cadena de extensiones en una formación de clases con L/k normal. Entonces $\mathrm{Res}_{k,K}[H^2(L/k)] = H^2(L/K)$. En particular, si K/k es normal tenemos la sucesión exacta*

$$1 \longrightarrow H^2(K/k) \xrightarrow{Inf} H^2(L/k) \xrightarrow{Res} H^2(L/K) \longrightarrow 1.$$

Este teorema se traduce fácilmente a términos de los grupos de Brauer:

Teorema 15.27 *Sea K/k una extensión en una formación de clases. Entonces la restricción $\mathrm{Res}_{k,K} : H^2(*/k) \longrightarrow H^2(*/K)$ es suprayectiva. En particular si K/k es normal tenemos la sucesión exacta*

$$1 \longrightarrow H^2(K/k) \xrightarrow{Inf} H^2(*/k) \xrightarrow{Res} H^2(*/K) \longrightarrow 1.$$

También obtenemos información sobre las transferencias:

Teorema 15.28 *Sea K/k una extensión en una formación de clases. La transferencia $\mathrm{V}_{K,k} : H^2(*/K) \longrightarrow H^2(*/k)$ es un monomorfismo y además cumple*

$$\mathrm{Inv}_k(\mathrm{V}_{K,k}(x)) = \mathrm{Inv}_K(x).$$

DEMOSTRACIÓN: Para todo $y \in H^2(*/k)$ se cumple

$$\begin{aligned}\mathrm{Inv}_k(\mathrm{V}_{K,k}(\mathrm{Res}_{k,K}(y))) &= \mathrm{Inv}_k(|K : k|\, y) = |K : k|\ \mathrm{Inv}_k(y)\\ &= \mathrm{Inv}_K(\mathrm{Res}_{k,K}(y)).\end{aligned}$$

Como la restricción es suprayectiva, tenemos la fórmula del enunciado. El hecho de que la transferencia conserve invariantes implica que es inyectiva. ∎

Veamos otro resultado de consistencia sobre las clases fundamentales.

Teorema 15.29 *Sea $k \subset L \subset K$ una cadena de extensiones normales en una formación de clases. Si $|K : L| = m$ entonces $\xi_{L/k} = \xi_{K/k}^m$.*

DEMOSTRACIÓN: En efecto, si $|K : k| = n$ entonces

$$\mathrm{Inv}_k(\xi_{K/k}^m) = m\,\mathrm{Inv}_k(\xi_{K/k}) = m[1/(mn)] = [1/n],$$

luego $\xi_{K/k}^m = \xi_{L/k}$. ∎

Hay un último resultado de interés sobre conservación de invariantes, relacionado con unas aplicaciones cohomológicas de las que aún no hemos hablado y que introducimos ahora. Notemos ante todo que grupos de cohomología $H^n(G,A)$ se definen algebraicamente a partir de un G-módulo A. Es obvio entonces que si $\sigma : G \longrightarrow T$ y $\tau : A \longrightarrow B$ son isomorfismos de grupos tales que $\tau(ag) = \tau(a)\sigma(g)$, para todo $a \in A$, y todo $g \in G$, entonces $H^n(G,A) \cong H^n(T,B)$. Vamos a detallar cómo se llega a estos isomorfismos.

En primer lugar, todo T-módulo A se convierte en un G-módulo mediante $ag = a\sigma(g)$. Recíprocamente, todo G-módulo se convierte en T-módulo de modo que si repetimos el proceso obtenemos el módulo de partida. Es fácil ver que A es un T-módulo libre si y sólo si es un G-módulo libre, y todo homomorfismo de T-módulos es también un isomorfismo de G-módulos. A partir de aquí concluimos que toda resolución completa de T lo es también de G, y viceversa.

Así pues, si $\mathcal{C}$ es una resolución completa de G y $\mathcal{C}'$ es una resolución completa de T, existen homomorfismos $u : \mathcal{C} \longrightarrow \mathcal{C}'$ y $v : \mathcal{C}' \longrightarrow \mathcal{C}$ que inducen isomorfismos entre los grupos de homología (sus composiciones son homotópicas a la identidad). Que v sea un homomorfismo (de T-módulos) significa en este caso que $v(x\sigma(g)) = v(x)g$. De aquí obtenemos homomorfismos de complejos

$$\phi_r : \mathrm{Hom}_G(C_r, A) \longrightarrow \mathrm{Hom}_T(C'_r, B)$$

dados por $\phi_r(f)(x) = \tau(f(v(x)))$, y análogamente en sentido inverso. Sus composiciones son homotópicas a la identidad, por lo que inducen isomorfismos $(\sigma,\tau)_* : H^n(G,A) \longrightarrow H^n(T,B)$.

Es fácil ver que $(\sigma,\tau)_*$ no depende de la elección de v y que si cambiamos de resoluciones obtenemos un diagrama conmutativo con los isomorfismos naturales entre los grupos de cohomología.

Partamos ahora de un grupo G y de dos subgrupos $T \trianglelefteq S \leq G$. Sea A un G-módulo y, como es habitual, A^T será el submódulo formado por los elementos de A fijados por T. Entonces A^T es también un S/T-módulo de forma natural. Sea $\sigma \in G$. Entonces $T^\sigma \trianglelefteq S^\sigma \leq G$ y claramente la conjugación por σ induce un isomorfismo $S/T \longrightarrow S^\sigma/T^\sigma$. Así mismo la multiplicación por σ es un isomorfismo de A^T en A^{T^σ} y se cumple la relación $(a[s])\sigma = (a\sigma)[s]^\sigma$. Por consiguiente nos encontramos bajo las hipótesis anteriores.

Definición 15.30 Si G es un grupo finito, A es un G-módulo, $T \trianglelefteq S \leq G$ y $\sigma \in G$, definimos la *conjugación cohomológica*

$$\sigma_* : H^n(S/T, A^T) \longrightarrow H^n(S^\sigma/T^\sigma, A^{T^\sigma})$$

como la aplicación que acabamos de construir.

Estas aplicaciones conmutan con los isomorfismos naturales al cambiar de resolución. Si en particular consideramos la misma resolución para S/T y S^σ/T^σ entonces σ_* es la identidad. Si consideramos las resoluciones canónicas tenemos

$$\sigma_*(f)([[s_1^\sigma], \ldots, [s_n^\sigma]]) = f([[s_1], \ldots, [s_n]])^\sigma,$$

y análogamente para índices negativos con las bases duales $\langle [s_1^\sigma], \dots, [s_n^\sigma] \rangle$.

En particular si $T = 1$ tenemos $\sigma_* : H^n(S, A) \longrightarrow H^n(S^\sigma, A)$. Vamos a necesitar el teorema siguiente:

Teorema 15.31 *Sea G un grupo finito y A un G-módulo. Entonces para todo $\sigma \in G$ se cumple que la conjugación $\sigma_* : H^n(G, A) \longrightarrow H^n(G, A)$ es la identidad.*

DEMOSTRACIÓN: Por inducción sobre n. Para $n = 0$ es fácil probarlo. Basta tener en cuenta la igualdad $\sigma_*(f)([\,]) = f([\,])\sigma = f([\,])$ (pues $f([\,]) \in A^G$). Ahora (ver el teorema 14.34) consideramos el diagrama:

$$\begin{array}{ccc} H^n(G, A^+) & \xrightarrow{\delta^*} & H^{n+1}(G, A) \\ \downarrow{\scriptstyle \sigma_*} & & \downarrow{\scriptstyle \sigma_*} \\ H^n(G, A^+) & \xrightarrow{\delta^*} & H^{n+1}(G, A) \end{array}$$

Es fácil ver que es conmutativo, y la flecha vertical izquierda es la identidad por hipótesis de inducción, luego también lo es la derecha. Considerando el módulo A^- probamos el teorema para índices negativos. ∎

Hemos definido la conjugación sobre factores S/T de un grupo G porque éste es el caso que aparece en las formaciones. En efecto, si K/k es una extensión cualquiera de una formación y $\sigma \in G$ (el grupo de Galois de la formación) entonces existe un cuerpo $F \subset k$ de manera que $\sigma \in G_F$ (por ejemplo $G_F = \langle G_k, \sigma \rangle$). Sea E una extensión normal de F que contenga a K. Entonces $\sigma G_E \in G_F/G_E = G(E/F)$. Un factor de este grupo viene determinado por los subgrupos $S = G(E/k)$, $T = G(E/K)$. Concretamente $S/T = G(K/k)$. Es fácil ver que su conjugado por σ (en realidad por σG_E) es $G(K/k)^\sigma = G(K^\sigma/k^\sigma)$. Por otra parte, si consideramos el módulo A_E, los submódulos fijados por T y T^σ son A_K y A_{K^σ}, luego tenemos las conjugaciones cohomológicas $\sigma_* : H^n(K/k) \longrightarrow H^n(K^\sigma/k^\sigma)$.

Para relacionar la conjugación con toda la estructura cohomológica de las formaciones conviene introducir un enfoque equivalente.

Definición 15.32 Un *isomorfismo* entre dos formaciones $(G, \{G_K\}_{K \in S}, A)$ y $(T, \{T_K\}_{K \in S}, B)$ (con el mismo conjunto de cuerpos S) es un par (σ, τ) de isomorfismos de grupos $\sigma.G \longrightarrow T$ y $\tau : A \longrightarrow B$ tales que

a) $\tau(ag) = \tau(a)\sigma(g)$, para todo $a \in A$ y todo $g \in G$.

b) $\sigma[G_K] = T_K$ para todo $K \in S$.

Es obvio que dos formaciones isomorfas en este sentido son la misma estructura algebraica, por lo que σ y τ inducen isomorfismos de forma natural entre todos los objetos construidos a partir de ellas.

Dada una formación y un elemento $\sigma \in G$, la conjugación por σ es un automorfismo de G que permuta los subgrupos abiertos ($G_K \mapsto G_{K^\sigma}$) y el

producto por σ es un automorfismo de A (como grupo). Además se cumple obviamente $(ag)\sigma = (a\sigma)g^\sigma$.

Tenemos, pues, un isomorfismo de la formación en sí misma, y es fácil ver que los isomorfismos

$$\sigma_* : H^n(K/k) \longrightarrow H^n(K^\sigma/k^\sigma)$$

inducidos por éste son precisamente las conjugaciones cohomológicas introducidas antes. Desde este punto de vista es evidente que las conjugaciones conservan todas las propiedades definidas sobre una formación arbitraria. En particular conmutan con inflaciones, restricciones y transferencias de manera natural.

El hecho de que conmuten con las inflaciones implica que en las formaciones de cuerpos las conjugaciones se extienden a isomorfismos entre los grupos de Brauer:

$$\sigma^* : H^2(*, k) \longrightarrow H^2(*, k^\sigma).$$

Concretamente, $\sigma_*(f)(x^\sigma, y^\sigma) = f(x, y)$, para x, $y \in G$.

El teorema 15.31 tiene la traducción siguiente:

Teorema 15.33 *Si K/k es una extensión normal en una formación y $\sigma \in G_k$, entonces la conjugación $\sigma_* : H^n(K/k) \longrightarrow H^n(K/k)$ es la identidad.*

Si la formación es de cuerpos y $\sigma \in G_k$ tenemos también que la conjugación $\sigma_* : H^2(*, k) \longrightarrow H^2(*, k)$ es la identidad.

No es evidente que las conjugaciones conserven los índices en las formaciones de clases, pues éstos no se definen algebraicamente a partir de las formaciones, sino que su existencia se postula en un axioma independiente. Pese a ello vamos a ver que es así.

Teorema 15.34 *Sea k un cuerpo de una formación de clases y σ un elemento de su grupo de Galois. Entonces para todo $x \in H^2(*, k)$ se cumple $\mathrm{Inv}_{k^\sigma}(\sigma_*(x)) = \mathrm{Inv}_k(x)$. En particular, si K/k es una extensión normal, se cumple $\sigma_*(\xi_{K/k}) = \xi_{K^\sigma/k^\sigma}$.*

Demostración: Sea F un subcuerpo de k tal que $\sigma \in G_F$. Tenemos que la conjugación σ_* es la identidad en $H^2(*, F)$. Para cada $y \in H^2(*, F)$ se cumple

$$\begin{aligned} \mathrm{Inv}_{k^\sigma}(\sigma_*(\mathrm{Res}_{F,k}(y))) &= \mathrm{Inv}_{k^\sigma}(\mathrm{Res}_{F^\sigma,k^\sigma}(\sigma_*(y))) = |F^\sigma : k^\sigma| \ \mathrm{Inv}_F(\sigma_*(y)) \\ &= |F : k| \ \mathrm{Inv}_F(y) = \mathrm{Inv}_k(\mathrm{Res}_{F,k}(y)). \end{aligned}$$

Como $\mathrm{Res}_{F,k} : H^2(*/F) \longrightarrow H^2(*, k)$ es suprayectiva, tenemos la fórmula buscada. La relación entre las clases fundamentales es obvia. ∎

Capítulo XVI

Teoría general de cuerpos de clases

En este capítulo construiremos el isomorfismo de Artin en una formación de clases arbitraria e introduciremos un último axioma del que se sigue el teorema de existencia. Primero hemos de introducir un nuevo concepto de la cohomología de grupos: el producto exterior.

16.1 Construcción de los productos exteriores

Para definir los productos exteriores necesitamos algunas observaciones previas. La primera concierne a las resoluciones de un grupo. Consideremos, pues una resolución reducida de un grupo G:

$$\cdots \longrightarrow C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

Es claro que también podemos considerarla como una resolución reducida del grupo trivial 1. El argumento del teorema 14.22 prueba que los homomorfismos 0 y 1 del complejo en sí mismo son homotópicos (el hecho de que 0 no sea la identidad en $\mathbb{Z}$, como se supone en 14.22, se suple por el hecho de que $\mathbb{Z}$ es 1-libre). Por lo tanto existen $\mathbb{Z}$-homomorfismos D_n y E tales que

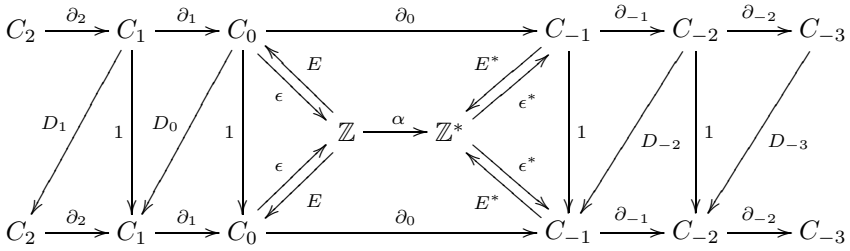
$$\begin{array}{ccccccccccc}
\longrightarrow & C_2 & \xrightarrow{\partial_2} & C_1 & \xrightarrow{\partial_1} & C_0 & \xrightarrow{\epsilon} & \mathbb{Z} & \longrightarrow & 0 \\
 & \downarrow{\scriptstyle 1} & \swarrow{\scriptstyle D_1} & \downarrow{\scriptstyle 1} & \swarrow{\scriptstyle D_0} & \downarrow{\scriptstyle 1} & \swarrow{\scriptstyle E} & \downarrow{\scriptstyle 1} & & \\
\longrightarrow & C_2 & \xrightarrow{\partial_2} & C_1 & \xrightarrow{\partial_1} & C_0 & \xrightarrow{\epsilon} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

$$D_n\partial_{n+1} + \partial_n D_{n-1} = 1 \quad n \geq 1$$
$$D_0\partial_1 + \epsilon E = 1 \qquad\qquad E\epsilon = 1.$$

Considerando las aplicaciones duales y llamando $D_{-1} = E^*\alpha^{-1}E$ (donde α es el isomorfismo canónico entre $\mathbb{Z}$ y $\mathbb{Z}^*$) es fácil ver que la relación

$$D_n\partial_{n+1} + \partial_n D_{n-1} = 1$$

es válida para todo entero n.



De este modo podemos considerar que cada resolución completa de un grupo finito G viene acompañada de estos homomorfismos auxiliares D_n. En el caso de la resolución canónica los homomorfismos D_n (para $n \geq 0$) fueron introducidos explícitamente antes que el operador frontera.

Otro hecho que vamos a necesitar es el siguiente:

Teorema 16.1 *Sea G un grupo finito y C un G-módulo regular. Entonces existe un homomorfismo $\pi \in \mathrm{Hom}(C, C)$ tal que $\mathrm{Tr}(\pi) = 1$.*

Demostración: Por hipótesis $C \cong A \otimes \mathbb{Z}[G]$ para un cierto grupo abeliano A, luego $C = \bigoplus_{\sigma\in G} A\sigma$. Tomamos como $\pi : C \longrightarrow A$ la proyección, o sea, si $c = \sum_{\sigma\in G} a_\sigma\sigma$, entonces $\pi(c) = a_1$ y, por consiguiente, $\pi^\sigma(c) = \pi(c\sigma^{-1})\sigma = a_\sigma\sigma$.

De aquí se desprende que $c = \sum_{\sigma\in G} \pi^\sigma(c) = \mathrm{Tr}(\pi)(c)$, es decir, $\mathrm{Tr}(\pi) = 1$. ∎

Los módulos de cadenas de una resolución completa de un grupo finito G son libres, luego regulares, luego podemos aplicarles el teorema anterior y concluir que existen homomorfismos $\pi_n \in \mathrm{Hom}(C_n, C_n)$ tales que $\mathrm{Tr}(\pi_n) = 1$.

Por último observamos que si A y B son dos G-módulos, entonces el producto tensorial $A \otimes B$ puede dotarse de una única estructura de G-módulo tal que

$$(a \otimes b)\sigma = a\sigma \otimes b\sigma. \tag{16.1}$$

Pasemos ya a la construcción de los productos exteriores. Veremos que éstos tienen una caracterización axiomática sencilla, que es la que tendremos en cuenta en la práctica, pero primero hemos de demostrar su existencia, y esto es un tanto laborioso.

Partimos de un grupo finito G y una resolución completa con todos los complementos que acabamos de asociarle (los homomorfismos D_n, E y π_n). Definimos ahora los siguientes G-homomorfismos:

$$\begin{aligned}
\partial' &= \partial\otimes 1 : C_n\otimes C_m \longrightarrow C_{n-1}\otimes C_m,\\
\partial'' &= 1\otimes\partial : C_n\otimes C_m \longrightarrow C_n\otimes C_{m-1},\\
D' &= \mathrm{Tr}(D\otimes\pi) : C_n\otimes C_m \longrightarrow C_{n+1}\otimes C_m,\\
D'' &= \mathrm{Tr}(\pi\otimes D) : C_n\otimes C_m \longrightarrow C_n\otimes C_{m+1}.
\end{aligned}$$

En todos los productos tensoriales consideramos la estructura de G-módulo determinada por (16.1). Se cumplen las relaciones

$$D'\partial' + \partial' D' = 1, \qquad D''\partial'' + \partial'' D'' = 1.$$

En efecto, para probarlas conviene notar que si f y g son endomorfismos de un G-módulo A entonces $\mathrm{Tr}(fg) = \mathrm{Tr}(f)g$ cuando g es un G-homomorfismo y $\mathrm{Tr}(fg) = f\,\mathrm{Tr}(g)$ cuando f es un G-homomorfismo. La comprobación es sencilla. Entonces

$$\begin{aligned}
D'\partial' + \partial' D' &= \mathrm{Tr}(D\otimes\pi)(\partial\otimes 1) + (\partial\otimes 1)\,\mathrm{Tr}(D\otimes\pi)\\
&= \mathrm{Tr}\big((D\otimes\pi)(\partial\otimes 1) + (\partial\otimes 1)(D\otimes\pi)\big)\\
&= \mathrm{Tr}\big((D\partial+\partial D)\otimes\pi\big)\\
&= \mathrm{Tr}(1\otimes\pi) = 1\otimes\mathrm{Tr}(\pi) = 1.
\end{aligned}$$

Similarmente se prueba la otra relación. Observar también que ∂' y ∂'' conmutan entre sí. El teorema siguiente resuelve toda la parte técnica sobre la existencia de productos exteriores.

Teorema 16.2 *En las condiciones anteriores, existen G-homomorfismos*

$$\phi_{m,n} : C_{m+n} \longrightarrow C_m\otimes C_n$$

tales que para todo par de enteros m, n se cumple la relación

$$[m,n]: \qquad \partial\phi_{m,n} = \phi_{m+1,n}\partial' + (-1)^m\phi_{m,n+1}\partial'',$$

y además $\phi_{0,0}(\epsilon\otimes\epsilon) = \epsilon$ (entendiendo que $\phi_{0,0}(\epsilon\otimes\epsilon) : C_0 \longrightarrow \mathbb{Z}\otimes\mathbb{Z}\cong\mathbb{Z}$).

Demostración: Consideremos la afirmación

$$[m,n]\partial': \qquad \partial\phi_{m,n}\partial' = (-1)^m\phi_{m,n+1}\partial''\partial'.$$

Claramente $[m,n]$ implica $[m,n]\partial'$. Supongamos que $\phi_{m,n}$ está definido para un m y todo n, de modo que se cumpla $[m,n]\partial'$. Entonces

$$\begin{aligned}
\partial\phi_{m,n} &= \partial\phi_{m,n}(D'\partial' + \partial' D') = \partial\phi_{m,n}D'\partial' + \partial\phi_{m,n}\partial' D'\\
&= \partial\phi_{m,n}D'\partial' + (-1)^m\phi_{m,n+1}\partial''\partial' D'\\
&= \partial\phi_{m,n}D'\partial' + (-1)^m\phi_{m,n+1}\partial''(1 - D'\partial')\\
&= \big(\partial\phi_{m,n}D' - (-1)^m\phi_{m,n+1}\partial'' D'\big)\partial' + (-1)^m\phi_{m,n+1}\partial''.
\end{aligned}$$

Definimos $\phi_{m+1,n} = \partial\phi_{m,n}D' - (-1)^m\phi_{m,n+1}\partial''D'$ y entonces la igualdad anterior resulta ser $[m,n]$ (válida para todo n). De aquí se sigue

$$\partial[m,n]: \qquad 0 = \partial\phi_{m+1,n}\partial' + (-1)^m\partial\phi_{m,n+1}\partial'',$$

con lo que $\partial\phi_{m+1,n}\partial' = (-1)^{m+1}\partial\phi_{m,n+1}\partial''$. Aplicamos $[m,n+1]\partial''$ (consecuencia de $[m,n+1]$):

$$\partial\phi_{m+1,n}\partial' = (-1)^{m+1}\phi_{m+1,n+1}\partial'\partial'' = (-1)^{m+1}\phi_{m+1,n+1}\partial''\partial',$$

y esto es $[m+1,n]\partial'$.

Es decir, tenemos las hipótesis de que habíamos partido pero para $m+1$ en lugar de m (además de las igualdades $[m,n]$). Inductivamente podemos construir así las funciones $\phi_{s,n}$ para todo $s \geq m$ y todo n de modo que se cumple $[s,n]$.

Ahora definimos $\phi_{m-1,n} = (-1)^m\phi_{m,n-1}\partial'D''$ y aplicando $[m,n-1]\partial'$ obtenemos

$$\begin{aligned}\partial\phi_{m-1,n} &= (-1)^m\partial\phi_{m,n-1}\partial'D'' = (-1)^{2m}\phi_{m,n}\partial''\partial'D''\\ &= \phi_{m,n}\partial'(1-D''\partial'') = \phi_{m,n}\partial' + (-1)^{m-1}\phi_{m-1,n+1}\partial'',\end{aligned}$$

y esto es $[m-1,n]$, de donde se sigue $[m-1,n]\partial'$, con lo que podemos continuar inductivamente y terminamos con todas las aplicaciones $\phi_{m,n}$ definidas y con todas las igualdades $[m,n]$ probadas.

Después de esto sólo hace falta construir $\phi_{0,n}$ para todo n de modo que se cumplan las igualdades $[0,n]\partial'$ y la última igualdad del enunciado.

Fijemos un $c \in C_0$ tal que $\epsilon(c) = 1$. Sea $\psi_{0,n} : C_n \longrightarrow C_0 \otimes C_n$ el $\mathbb{Z}$-homomorfismo dado por $\psi_{0,n}(x) = c \otimes \pi_n(x)$. Sea $\phi_{0,n} = \mathrm{Tr}(\psi_{0,n})$. Explícitamente,

$$\phi_{0,n}(x) = \sum_{\sigma\in G}\psi_{0,n}(x\sigma^{-1})\sigma = \sum_{\sigma\in G}(c\otimes\pi_n(x\sigma^{-1}))\sigma = \sum_{\sigma\in G}c\sigma\otimes\pi_n^\sigma(x).$$

Entonces

$$\begin{aligned}(\epsilon\otimes\epsilon)(\phi_{0,0}(x)) &= \sum_{\sigma\in G}\epsilon(c)\sigma\otimes\epsilon(\pi_0^\sigma(x)) = 1\otimes\sum_{\sigma\in G}\epsilon(\pi_0^\sigma(x))\\ &= 1\otimes\epsilon(\mathrm{Tr}(\pi_0)(x)) = 1\otimes\epsilon(x) = \epsilon(x).\end{aligned}$$

Sea ahora $x \in C_{n+1}$. Hemos de comprobar que

$$\partial'\big(\phi_{0,n}(\partial(x))\big) = \partial'\big(\partial''(\phi_{0,n+1}(x))\big).$$

El primer miembro es

$$\begin{aligned}\partial'\Big(\sum_{\sigma\in G}c\sigma\otimes\pi_{n+1}^\sigma(\partial x)\Big) &= \sum_{\sigma\in G}\partial_0(c\sigma)\otimes\pi_{n+1}^\sigma(\partial x)\\ &= \sum_{\sigma\in G}\epsilon^*(\alpha(\epsilon(c)\sigma))\otimes\pi_{n+1}^\sigma(\partial x)\\ &= \sum_{\sigma\in G}\epsilon^*(\alpha(1))\otimes\pi_{n+1}^\sigma(\partial x)\\ &= \epsilon^*(\alpha(1))\otimes\mathrm{Tr}(\pi_{n+1})(\partial x) = \epsilon^*(\alpha(1))\otimes\partial x.\end{aligned}$$

El segundo miembro es

$$\begin{aligned}\partial''\Big(\partial'\Big(\sum_{\sigma\in G} c\sigma\otimes\pi^\sigma_{n+1}(x)\Big)\Big) &= \partial''\Big(\sum_{\sigma\in G}\epsilon^*(\alpha(1))\otimes\pi^\sigma_{n+1}(x)\Big)\\ &= \partial''(\epsilon^*(\alpha(1))\otimes x) = \epsilon^*(\alpha(1))\otimes\partial x.\end{aligned}$$

■

Definición 16.3 Sea G un grupo finito y A y B dos G-módulos. Consideremos una resolución completa de G. Para cada par de cocadenas $f\in\mathrm{Hom}_G(C_m,A)$ y $g\in\mathrm{Hom}_G(C_n,B)$ definimos la cocadena $f\cup g : C_{m+n}\longrightarrow A\otimes B$ dada por $f\cup g = \phi_{m,n}\circ(f\otimes g)$, donde $\phi_{m,n}$ es el G-homomorfismo construido en el teorema anterior.

Hemos de probar que este producto no depende de la elección de la resolución, de las aplicaciones D_n, etc., así como que induce aplicaciones entre los grupos de cohomología. Esto último será consecuencia del teorema siguiente.

Teorema 16.4 *En las condiciones de la definición anterior, $f\cup g$ es bilineal y además se tiene la relación*

$$\partial(f\cup g) = \partial f\cup g + (-1)^m f\cup\partial g.$$

Demostración: La bilinealidad es inmediata. Respecto a la igualdad, tenemos que

$$\partial(f\cup g) = \partial\phi_{m,n}(f\otimes g) = \phi_{m+1,n}\partial'(f\otimes g) + (-1)^m\phi_{m,n+1}\partial''(f\otimes g)$$

$$= \phi_{m+1,n}(\partial f\otimes g) + (-1)^m\phi_{m,n+1}(f\otimes\partial g) = \partial f\cup g + (-1)^m f\cup\partial g.$$

■

De aquí se sigue inmediatamente que

$$\begin{aligned}&\text{cociclo}\cup\text{cociclo} = \text{cociclo},\\ &\text{cociclo}\cup\text{cofrontera} = \text{cofrontera},\\ &\text{cofrontera}\cup\text{cociclo} = \text{cofrontera},\\ &\text{cofrontera}\cup\text{cofrontera} = \text{cofrontera}.\end{aligned}$$

A su vez esto justifica la definición siguiente:

Definición 16.5 Sea G un grupo finito y A y B dos G-módulos. Para cada par de números enteros m y n definimos el *producto exterior*

$$H^m(G,A)\times H^n(G,B)\longrightarrow H^{m+n}(G,A\otimes B)$$

dado por $[f]\cup[g] = [f\cup g]$.

Por supuesto sigue pendiente demostrar que los productos exteriores no dependen realmente de las numerosas elecciones que hemos hecho para definirlos. Comenzaremos probándolo para los productos de dimensión 0.

Consideremos una resolución cualquiera de G. La sucesión exacta

$$C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

da lugar a la sucesión exacta

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \xrightarrow{\epsilon^\#} \mathrm{Hom}_G(C_0, A) \xrightarrow{\partial^0} \mathrm{Hom}_G(C_1, A).$$

Esto significa que todo cociclo de dimensión 0 se expresa de forma única como ϵg, para un cierto $g \in \mathrm{Hom}_G(\mathbb{Z}, A)$. A su vez $g \mapsto g(1)$ es un isomorfismo con A^G, luego tenemos un isomorfismo $A^G \cong Z^0(G, A)$, que induce un isomorfismo $A^G/N \cong H^0(G, A)$ (para un cierto subgrupo N, que enseguida probaremos que es AT).

Si tenemos otra resolución $D_0 \xrightarrow{\epsilon'} \mathbb{Z} \longrightarrow 0$, entonces existe un homomorfismo de complejos $u : D_0 \longrightarrow C_0$ que induce un isomorfismo entre los grupos de cohomología, dado por $[f] \mapsto [uf]$. En particular $[eg] \mapsto [u\epsilon g] = [\epsilon' g]$, luego al componer con los isomorfismos $A^G/N \cong H^0(G, A)$ obtenemos la identidad $[a] \mapsto [a]$. En particular esto prueba que N es el mismo subgrupo de A^G independientemente de la resolución y, usando la canónica, concluimos fácilmente que $N = AT$.

En total resulta que la aplicación $A^G/AT \longrightarrow H^0(G, A)$ que a cada $[a]$ le asigna $[\epsilon g_a]$, donde $g_a(n) = an$ es un isomorfismo que conmuta con los isomorfismos canónicos entre los grupos de cohomología calculados con resoluciones distintas.

A través de este isomorfismo el producto exterior para dimensión 0 es

$$[a] \cup [b] = [\epsilon g_a] \cup [\epsilon g_b] = [\epsilon g_a \cup \epsilon g_b] = [\phi_{0,0}(\epsilon g_a \otimes \epsilon g_b)]$$

$$= [\phi_{0,0}(\epsilon \otimes \epsilon)(g_a \otimes g_b)] = [\epsilon(g_a \otimes g_b)] = [\epsilon g_{a\otimes b}] = [a \otimes b].$$

Esto prueba que el producto exterior es (en este caso) independiente de todas las elecciones, en el sentido de que si tomamos dos resoluciones de G, conmuta con los isomorfismos canónicos entre los grupos de cohomología.

Para obtener el mismo resultado en el caso general necesitamos dos propiedades más de los productos exteriores. Las reunimos junto a la anterior en un teorema.

Teorema 16.6 *Sea G un grupo finito. Entonces*

a) Si A y B son G-módulos, entonces el producto exterior en dimensión 0 es la aplicación $A^G/AT \times B^G/BT \longrightarrow (A \otimes B)^G/(A \otimes B)T$ dada por $[a] \cup [b] = [a \otimes b]$.

b) Si $u : A \longrightarrow A'$ y $v : B \longrightarrow B'$ son homomorfismos de G-módulos entonces

$$u_*(x) \cup v_*(y) = (u \otimes v)_*(x \cup y), \qquad \text{para } x \in H^m(G, A), \quad y \in H^n(G, B).$$

c) Si $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *es una sucesión exacta de G-módulos, L es otro G-módulo y la sucesión* $0 \longrightarrow A \otimes L \xrightarrow{\alpha\otimes 1} B \otimes L \xrightarrow{\beta\otimes 1} C \otimes L \longrightarrow 0$ *también es exacta, entonces el diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} H^m(G,C)\times H^n(G,L) & \xrightarrow{\cup} & H^{m+n}(G,C\otimes L) \\ \downarrow{\scriptstyle \delta^*\times 1} & & \downarrow{\scriptstyle \delta^*} \\ H^{m+1}(G,A)\times H^n(G,L) & \xrightarrow{\cup} & H^{m+n+1}(G,A\otimes L) \end{array}$$

Lo mismo es válido si consideramos sucesiones exactas en las segundas componentes, salvo por el hecho de que las dos composiciones del diagrama se diferencian en el factor $(-1)^m$.

DEMOSTRACIÓN: La propiedad a) está probada y la propiedad b) es inmediata a partir de la definición. Veamos c).

Partamos de un par $([f],[g]) \in H^m(G,A)\times H^n(G,B)$. Calculamos $\delta^*\big([f]\big)$ eligiendo f' tal que $f'\beta = f$ y f'' tal que $f''\alpha = \partial f'$. Así $\delta^*\big([f]\big) = [f'']$.

Pero, $(f'\cup g)(\beta\otimes 1) = f\cup g$ y $\partial(f'\cup g) = \partial f'\cup g + (-1)^m(f\cup \partial g) = \partial f'\cup g$ (pues g es un cociclo) y así $\partial(f'\cup g) = (f''\alpha)\cup g = (f''\cup g)(\alpha\otimes 1)$, lo que prueba que

$$\delta^*([f]\cup[g]) = \delta^*([f\cup g]) = [f''\cup g] = \delta^*([f])\cup[g].$$

■

Observar que la propiedad c) se deduce formalmente de la propiedad b) y de la fórmula de derivación dada por el teorema 16.4, luego cualquier aplicación $\cup$ entre pares de cocadenas que cumpla estas dos propiedades cumple también la propiedad c).

Con esto estamos en condiciones de probar la unicidad de los productos exteriores. Emplearemos una variante de la reducción regular.

Teorema 16.7 *Las propiedades a) y c) del teorema anterior caracterizan los productos exteriores, en el sentido de que si tenemos dos familias de aplicaciones* $\cup$ *que satisfagan dichas propiedades entonces conmutan con los isomorfismos naturales entre los grupos de cohomología definidos a partir de resoluciones distintas (y por tanto son iguales sobre los grupos de cohomología definidos con la misma resolución).*

DEMOSTRACIÓN: La propiedad a) justifica la unicidad del producto exterior sobre grupos de dimensión 0. Supongamos que dicha unicidad está probada para pares de grupos de dimensión (m,n). Consideramos la sucesión exacta de G-módulos

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G] \longrightarrow J \longrightarrow 0,$$

donde $\mathbb{Z}$ es trivial como G-módulo y el monomorfismo es el dado por $n \mapsto nT$. La imagen de este monomorfismo está complementada en $\mathbb{Z}[G]$ como $\mathbb{Z}$-módulo. Su complementario es concretamente el subgrupo generado por $G\setminus\{1\}$, pues

$$\sum_{\sigma\in G} n_\sigma\sigma = n_1T + \sum_{\sigma\in G}(n_\sigma - n_1)\sigma.$$

Esto nos permite aplicar el teorema 14.15, según el cual la sucesión

$$0 \longrightarrow \mathbb{Z} \otimes A \longrightarrow \mathbb{Z}[G] \otimes A \longrightarrow J \otimes A \longrightarrow 0$$

es una sucesión exacta de $\mathbb{Z}$-módulos, donde A es cualquier G-módulo. Por otra parte, los homomorfismos que aparecen son en realidad G-homomorfismos si consideramos en los tres grupos la estructura de G-módulo determinada por el producto $(x \otimes y)\sigma = x\sigma \otimes y\sigma$. Por el mismo motivo, si L es cualquier G-módulo también es exacta la sucesión

$$0 \longrightarrow \mathbb{Z} \otimes A \otimes L \longrightarrow \mathbb{Z}[G] \otimes A \otimes L \longrightarrow J \otimes A \otimes L \longrightarrow 0.$$

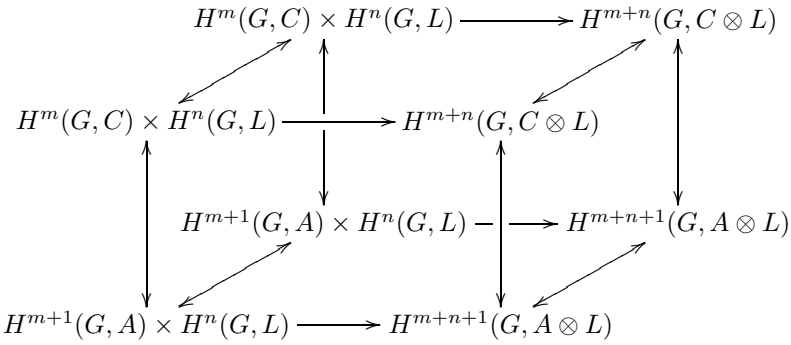
Llamamos $A = \mathbb{Z} \otimes A$, $B = \mathbb{Z}[G] \otimes A$ y $C = J \otimes A$. Entonces tenemos las hipótesis de la propiedad c) del teorema anterior. Más aún, los módulos B y $B \otimes L$ son regulares. Esto no es inmediato por definición, pues no estamos considerando la estructura de G-módulo dada por $\sigma(x \otimes y) = \sigma x \otimes y$. De todos modos

$$B = \Big(\bigoplus_{\sigma\in G} \mathbb{Z}\sigma\Big) \otimes A = \bigoplus_{\sigma\in G} (\sigma \otimes A\sigma) = \bigoplus_{\sigma\in G} (1 \otimes A)\sigma \cong A \otimes \mathbb{Z}[G],$$

y el isomorfismo es de G-módulos si en el último término consideramos el producto $(x \otimes y)\sigma = x \otimes y\sigma$. Similarmente ocurre con $B \otimes L$.

Como consecuencia, los grupos de cohomología correspondientes a B y $B \otimes L$ son nulos, luego la sucesión exacta de cohomología implica que los homomorfismos δ^* son todos isomorfismos.

Ahora supongamos que tenemos dos productos exteriores calculados sobre grupos de cohomología construidos con dos resoluciones cualesquiera de G.



Los grupos de la cara anterior del diagrama son los construidos con una resolución, y los de la cara posterior con la otra. Las caras anterior y posterior conmutan por la propiedad c). Las caras laterales conmutan porque los homomorfismos δ^* conmutan con los isomorfismos canónicos entre los grupos de cohomología. La cara superior conmuta por hipótesis de inducción. Teniendo en cuenta además que todos los homomorfismos verticales son isomorfismos, es fácil ver que la cara inferior también conmuta, lo que nos da la unicidad del producto exterior para dimensiones $(m+1, n)$. Análogamente se prueba la unicidad para dimensiones $(m, n+1)$.

Para disminuir las dimensiones razonamos análogamente pero partiendo de la sucesión exacta (14.9). Partiendo de G-módulos cualesquiera C y L obtenemos una sucesión exacta $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ en las hipótesis de la propiedad c) y donde B es regular (pero ahora es C el módulo arbitrario en vez de A). Tenemos así un cubo de homomorfismos donde ahora es la cara inferior la que conmuta por hipótesis de inducción. ∎

16.2 Propiedades de los productos exteriores

Los productos exteriores tienen un comportamiento bastante sencillo, lo cual compensa la dificultad de calcularlos explícitamente. Vamos a probar las propiedades principales que dan lugar a dicho buen comportamiento. La primera es la propiedad asociativa.

Teorema 16.8 *Sea G un grupo finito y A, B, C tres G-módulos. Entonces podemos definir el producto exterior*

$$H^m(G,A) \times H^n(G,B) \times H^r(G,C) \longrightarrow H^{m+n+r}(G, A \otimes B \otimes C)$$

como $x \cup y \cup z = (x \cup y) \cup z = x \cup (y \cup z)$.

Demostración: Es fácil probar que el doble producto exterior, definido de cualquiera de las dos formas posibles, satisface las propiedades análogas a las del teorema 16.6 (en la propiedad c el diagrama es conmutativo para la primera componente, para la segunda lo es salvo el signo $(-1)^m$ y para la tercera lo es salvo el signo $(-1)^{m+n}$).

Después se comprueba que estas propiedades caracterizan al doble producto, por el mismo argumento empleado en el teorema anterior. ∎

Como consecuencia podemos hablar de productos exteriores con cualquier número de factores. Las propiedades de estos productos generalizados (como la multilinealidad) son consecuencias inmediatas de las propiedades de los productos con dos factores. No daremos más detalles.

Los productos exteriores son conmutativos salvo signo. Para dar sentido a esta afirmación hemos de identificar los grupos $H^n(G, A \otimes B)$ y $H^n(G, B \otimes A)$ a través del isomorfismo inducido por el isomorfismo natural $A \otimes B \cong B \otimes A$. Entonces se tiene:

Teorema 16.9 *Sea G un grupo finito, sean A, B dos G-módulos. Consideremos dos clases de cohomología $x \in H^m(G,A)$, $y \in H^n(G,B)$. Entonces $x \cup y = (-1)^{mn}(y \cup x)$.*

Demostración: Llamemos $f : H^n(G, B \otimes A) \longrightarrow H^n(G, A \otimes B)$ a los isomorfismos naturales y definamos el producto $x \cup' y = (-1)^{mn} f(y \cup x)$. Basta probar que $\cup'$ cumple las propiedades a) y b) del teorema 16.6 y la fórmula de derivación del teorema 16.4 (ver el comentario tras el teorema 16.6).

a) En dimensión 0 tenemos que $[a] \cup' [b] = f([b \cup a]) = f([b \otimes a]) = [a \otimes b]$.

b) Si u y v son homomorfismos de módulos según 16.6 b), entonces

$$u_*(x)\cup' v_*(y) = (-1)^{mn} f(v_*(y)\cup u_*(x)) = (-1)^{mn} f((v\otimes u)_*(y\cup x))$$

$$= (-1)^{mn} f((y\cup x)(v\otimes u)) = (-1)^{mn} f(y\cup x)(u\otimes v) = (x\cup' y)(u\otimes v)$$

$$= (u\otimes v)_*(x\cup' y).$$

La propiedad del teorema 16.4 se refiere a productos de cocadenas y no de clases de homología. Ahora f será el isomorfismo entre $\mathrm{Hom}_G(\mathcal{C}, B\otimes A)$ y $\mathrm{Hom}_G(\mathcal{C}, A\otimes B)$. Por ser un isomorfismo de complejos conmuta con las cofronteras. Así pues

$$\partial(x\cup' y) = \partial((-1)^{mn} f(y\cup x)) = (-1)^{mn} f(\partial(y\cup x))$$

$$= (-1)^{mn} f(\partial y\cup x + (-1)^n y\cup \partial x) = (-1)^{mn} f(\partial y\cup x) + (-1)^{(m+1)n} f(y\cup \partial x)$$

$$= (-1)^m (x\cup' \partial y) + (\partial x\cup' y) = \partial x\cup' y + (-1)^m (x\cup' \partial y).$$

El teorema 16.7 nos da ahora que $x\cup' y = x\cup y$. ∎

Ahora veremos cómo se comportan los productos exteriores con respecto a restricciones, transferencias y conjugaciones.

Teorema 16.10 *Sea G un grupo finito, $T\trianglelefteq S\le G$, $\sigma\in G$ y A y B dos G-módulos. Entonces*

a) $\mathrm{Res}_{G,S}(x\cup y) = \mathrm{Res}_{G,S}(x)\cup \mathrm{Res}_{G,S}(y)$, $\quad x\in H^m(G,A)$, $y\in H^n(G,B)$.

b) $\mathrm{V}_{S,G}(\mathrm{Res}_{G,S}(x)\cup y) = x\cup \mathrm{V}_{S,G}(y)$, $\quad x\in H^m(G,A)$, $y\in H^n(S,B)$.

c) $\sigma_*(x\cup y) = \sigma_*(x)\cup\sigma_*(y)$, $\quad x\in H^m(S/T,A)$, $y\in H^n(S/T,B)$.

Demostración: La prueba de la propiedad c) es simple rutina, teniendo en cuenta que la conjugación por s induce isomorfismos entre todas las estructuras involucradas.

Las propiedades a) y b) se demuestran para dimensión $(0,0)$ y después se argumenta por inducción como en el teorema 16.7.

En la parte a) el caso de dimensiones nulas es inmediato, pues la restricción está inducida por la inclusión $A^G\longrightarrow A^S$ y el producto exterior está inducido por el producto tensorial.

En la inducción nos aparece un diagrama cúbico como el del teorema 16.7, donde en la cara anterior tenemos los grupos de cohomología de G y en la posterior los de S. El único detalle a tener en cuenta es que ambas caras han de formarse a partir de la misma sucesión exacta

$$0\longrightarrow \mathbb{Z}\otimes A\longrightarrow \mathbb{Z}[G]\otimes A\longrightarrow J\otimes A\longrightarrow 0,$$

lo cual es posible porque el módulo central es regular como G-módulo y por lo tanto también como S-módulo.

Las flechas que conectan ambas caras son las restricciones. Entonces las caras anterior y posterior conmutan por el teorema 16.6, las caras laterales conmutan

porque las restricciones conmutan con los isomorfismos δ^* y la cara superior conmuta por hipótesis de inducción. De aquí obtenemos la conmutatividad de la cara inferior. Igualmente se razona para la inducción decreciente.

La propiedad b) en dimensión 0 se prueba sin dificultad:

$$\mathrm{V}_{S,G}(\mathrm{Res}_{G,S}[a]\cup[b]) = \mathrm{V}_{S,G}([a]\cup[b]) = \mathrm{V}_{S,G}([a\otimes b]) = \mathrm{Tr}_S^G([a\otimes b])$$

$$= [a\otimes \mathrm{Tr}_S^G(b)] = [a]\cup[\mathrm{Tr}_S^G(b)] = [a]\cup \mathrm{V}_{S,G}([b]),$$

(donde en la igualdad del cambio de línea hemos usado que $a\in A^G$).

Para la inducción formamos cubos cuyas caras horizontales son de la forma

$$\begin{array}{ccccc} H^m(G,A)\times H^n(S,L) & \xrightarrow{\mathrm{Res}} & H^m(S,A)\times H^n(S,L) & \xrightarrow{\cup} & H^{m+n}(S,A\otimes L) \\ \downarrow{\scriptstyle 1\times \mathrm{V}} & & & & \downarrow{\scriptstyle \mathrm{V}} \\ H^m(G,A)\times H^n(G,L) & & \xrightarrow{\qquad\qquad\cup\qquad\qquad} & & H^{m+n}(G,A\otimes L) \end{array}$$

La conmutatividad de la cara adyacente a la línea inferior se obtiene por el teorema 16.6, la de la adyacente a la línea superior se obtiene del teorema 16.6 más del hecho de que la restricción conmuta con los homomorfismos de enlace. Los detalles restantes no presentan ninguna dificultad. ∎

También puede probarse la fórmula

$$\mathrm{Inf}_{G/S,G}(x\cup y) = \mathrm{Inf}_{G/S,G}(x)\cup \mathrm{Inf}_{G/S,G}(y),$$

pero la demostración requiere profundizar un poco más en los productos exteriores, y no nos va a ser necesario.

A continuación calcularemos explícitamente algunos casos particulares de productos exteriores. La primera parte del teorema siguiente generaliza la parte a) del teorema 16.6.

Teorema 16.11 *Sea G un grupo finito y A y B dos G-módulos.*

a) El producto exterior

$$A^G/AT\times H^n(G,B)\cong H^0(G,A)\times H^n(G,B)\longrightarrow H^n(G,A\otimes B)$$

viene dado por $[a]\cup[f]=[a\otimes f]$, donde $(a\otimes f)(x)=a\otimes f(x)$.

b) El producto

$$H^1(G,A)\times H^1(G,B)\longrightarrow H^2(G,A\otimes B)$$

(respecto a la resolución canónica) viene dado por $[f]\cup[g]=[f\cup g]$, donde $(f\cup g)(\sigma,\tau)=-f(\sigma)\tau\otimes g(\tau)$.

DEMOSTRACIÓN: Nos basaremos en la propia construcción del producto exterior.

a) Sabemos que la clase $[a]$ se corresponde con la clase de cohomología $[\epsilon g_a]$, donde $g_a(n) = an$. Si $x \in C_n$ tenemos que $\phi_{0,n}(x) = \sum_{\sigma\in G} c\sigma \otimes \pi_n^\sigma(x)$, donde $c \in C_0$ es cualquier cocadena que cumpla $\epsilon(c) = 1$. Así pues,

$$(\epsilon g_a \cup f)(x) = (\epsilon g_a \otimes f)\big(\phi_{0,n}(x)\big) = \sum_{\sigma\in G} g_a\big(\epsilon(c)\sigma\big) \otimes f\big(\pi_n^\sigma(x)\big)$$

$$= \sum_{\sigma\in G} g_a(1) \otimes f\big(\pi_n^\sigma(x)\big) = a \otimes f\Big(\sum_{\sigma\in G} \pi_n^\sigma(x)\Big) = a \otimes f\big(\mathrm{Tr}(\pi_n)(x)\big) = a \otimes f(x).$$

b) Necesitamos calcular $\phi_{1,1} : C_2 \longrightarrow C_1 \otimes C_1$. Según la construcción

$$\phi_{1,1}(\sigma,\tau) = D'(\phi_{0,1}(\partial(\sigma,\tau))) - D'(\partial''(\phi_{0,2}(\sigma,\tau))).$$

Esbozamos los cálculos. Ante todo, podemos tomar $c = 1$. Por otra parte, recordemos que $D(\sigma) = [\sigma]$. Como es fácil comprobar,

$$[\sigma,\tau] \xrightarrow{\partial} [\sigma]\tau - [\sigma\tau] + [\tau] \xrightarrow{\phi_{0,1}} \tau \otimes [\sigma]\tau - 1 \otimes [\sigma\tau] + 1 \otimes [\tau]$$

$$\xrightarrow{D'} [\tau] \otimes [\sigma]\tau - [1] \otimes [\sigma\tau] + [1] \otimes [\tau].$$

$$[\sigma,\tau] \xrightarrow{\phi_{0,2}} 1 \otimes [\sigma,\tau] \xrightarrow{\partial''} 1 \otimes \big([\sigma]\tau - [\sigma\tau] + [\tau]\big)$$

$$\xrightarrow{D'} [1] \otimes [\sigma]\tau - [1] \otimes [\sigma\tau] + [1] \otimes [\tau].$$

Al efectuar la resta queda $\phi_{1,1}(\sigma,\tau) = [\tau]\otimes[\sigma]\tau - [1]\otimes[\sigma]\tau$. De aquí llegamos a que

$$(f \cup g)(\sigma,\tau) = f(\tau) \otimes g(\sigma)\tau - f(1) \otimes g(\sigma)\tau.$$

La ecuación de los cociclos es $f(\sigma\tau) = f(\sigma)\tau + f(\tau)$. Haciendo $\sigma = \tau = 1$ obtenemos $f(1) = 0$ y la expresión se simplifica hasta

$$(f \cup g)(\sigma,\tau) = f(\tau) \otimes g(\sigma)\tau.$$

Para obtener la expresión del enunciado usamos el teorema anterior:

$$(f \cup g)(\sigma,\tau) = -(g \cup f)(\sigma,\tau) = -g(\tau) \otimes f(\sigma)\tau = -f(\sigma)\tau \otimes g(\sigma).$$

∎

Hay otro caso particular de producto exterior que puede calcularse explícitamente y que resulta ser mucho más importante que los que acabamos de estudiar. Para obtenerlo necesitamos el concepto de módulo de escisión de un cociclo de dimensión 2.

Definición 16.12 Sea G un grupo finito y A un G-módulo. Sea $\{a_{\sigma,\tau}\}$ un cociclo de dimensión 2. Sea I el subgrupo de $\mathbb{Z}[G]$ generado por los elementos $d_\sigma = \sigma - 1$, con $\sigma \neq 1$. Sea $\overline{A} = A \oplus I$. Como $\{d_\sigma\}$ es una base de I podemos definir homomorfismos $f_\tau : I \longrightarrow \overline{A}$ mediante $f_\tau(d_\sigma) = d_{\sigma\tau} - d_\tau + a_{\sigma,\tau}$, que a su vez los podemos extender a homomorfismos $f_\tau : \overline{A} \longrightarrow \overline{A}$ mediante $f_\tau(a) = a\tau$ para $a \in A$. Definimos el *módulo de escisión* de $\{a_{\sigma,\tau}\}$ como el grupo $\overline{A}$ con la estructura de G-módulo dada por $x\tau = f_\tau(x)$.

Para comprobar que efectivamente se trata de un G-módulo observamos en primer lugar que la ecuación $d_\sigma\tau = d_{\sigma\tau} - d_\tau + a_{\sigma,\tau}$ es válida también cuando $\sigma = 1$ si convenimos en que $d_1 = a_{1,1}$. En efecto, $d_\tau - d_\tau + a_{1,\tau} = a_{1,\tau} = a_{1,1}\tau$, por la relación de los cociclos. Ahora,

$$\begin{aligned}(d_\sigma\tau)\rho &= d_{\sigma\tau}\rho - d_\tau\rho + a_{\sigma,\tau}\rho = d_{\sigma\tau\rho} - d_\rho + a_{\sigma\tau,\rho}\\ &\quad -d_{\tau\rho} + d_\rho - a_{\tau,\rho} + a_{\sigma,\tau}\rho,\\ d_\sigma(\tau\rho) &= d_{\sigma\tau\rho} - d_{\tau\rho} + a_{\sigma,\tau\rho},\end{aligned}$$

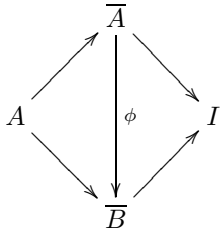
y la relación de los cociclos nos da que ambas expresiones son iguales.

A partir de aquí es fácil probar la misma relación para elementos cualesquiera de $\overline{A}$. También se comprueba que el producto por 1 es trivial.

Es claro que A es un submódulo de $\overline{A}$. El nombre de módulo de escisión se debe a que tenemos que $\{a_{\sigma,\tau}\} = \{d_\sigma\tau + d_\tau - d_{\sigma\tau}\} = \partial\{d_\sigma\}$, es decir, $\{a_{\sigma,\tau}\}$ se escinde en $\overline{A}$.

Observar que tenemos una sucesión exacta $0 \longrightarrow A \longrightarrow \overline{A} \longrightarrow I \longrightarrow 0$, donde la inyección es $a \mapsto (a, 0)$ y la proyección es $(a, b) \mapsto b$.

Es fácil ver que los módulos de escisión de dos cociclos cohomólogos $\{a_{\sigma,\tau}\}$ y $\{b_{\sigma,\tau}\} = \{a_{\sigma,\tau}\}+\{\partial(c_\sigma)\}$ son isomorfos (mediante $\phi(a+d_\sigma) = (a-c_\sigma+d_\sigma)$). Más aún, si A^* es el módulo de escisión de $\{b_{\sigma,\tau}\}$, el isomorfismo ϕ hace conmutativos los diagramas



En particular podemos hablar del *módulo de escisión* de una clase de cohomología de dimensión 2.

El teorema siguiente nos dará la relación entre los módulos de escisión y los productos exteriores.

Teorema 16.13 *Sea G un grupo finito, sea A un G-módulo, sea $\{a_{\sigma,\tau}\}$ un cociclo y sea $\overline{A}$ su módulo de escisión. Consideremos las sucesiones exactas*

$$0 \longrightarrow I \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0, \qquad 0 \longrightarrow A \longrightarrow \overline{A} \longrightarrow I \longrightarrow 0.$$

Entonces $[a_{\sigma,\tau}] = \delta^*\delta^* 1$, *donde* $1 \in H^0(G,\mathbb{Z})$.

DEMOSTRACIÓN: Teniendo en cuenta las observaciones anteriores, podemos sustituir $\{a_{\sigma,\tau}\}$ por cualquier cociclo cohomólogo y, según vimos al estudiar las extensiones de grupos (pág. 362), podemos exigir, por lo tanto, que $a_{1,1} = 0$. De este modo, $\{d_\sigma\}$ es una cocadena de (G, I), y es fácil ver que es un cociclo. Una antiimagen a través de la aplicación $\overline{A} \longrightarrow I$ es la propia $\{d_\sigma\}$, aunque ya no es un cociclo de $(G, \overline{A})$. Según hemos visto, su frontera es $\partial\big(\{d_\sigma\}\big) = \{a_{\sigma,\tau}\}$, que a su vez es un cociclo de (G, A), luego $\delta^*[d_\sigma] = [a_{\sigma,\tau}]$.

Veamos ahora que $[d_\sigma] = \delta^* 1$. Una antiimagen de 1 en $H^0(G,\mathbb{Z}[G])$ es 1. Su frontera es $\partial(1)_\sigma = \sigma - 1 = d_\sigma$ y una antiimagen de $\{d_\sigma\}$ en $H^1(G, I)$ es él mismo, luego ciertamente $[d_\sigma] = \delta^* 1$. ∎

Con ayuda de este teorema vamos a calcular el siguiente producto exterior:

$$\begin{array}{ccc} H^2(G,A) \times H^{-2}(G,\mathbb{Z}) & \longrightarrow & H^0(G, A \oplus \mathbb{Z}) \cong H^0(G,A) \\ \downarrow & & \downarrow \\ H^2(G,A) \times G/G' & \longrightarrow & A^G/AT \end{array}$$

Partimos de un par $(c, \sigma G')$. Digamos que c es la clase del cociclo $\{a_{\sigma,\tau}\}$, de modo que $a_{\tau,1} = a_{1,\tau} = 0$. Según vimos en el capítulo XIV, la clase $\sigma G'$ se corresponde con el cociclo $\{f_\sigma\}$ dado por (14.10), es decir,

$$f_\sigma\big(\langle\tau\rangle\big) = \begin{cases} 1 & \text{si } \tau = \sigma, \\ 0 & \text{si } \tau \neq \sigma. \end{cases}$$

Por otro lado, en las condiciones del teorema anterior, $c = \delta^*\delta^* 1$. Por lo tanto

$$c \cup \sigma G' = c \cup [f_\sigma] = \delta^*\delta^* 1 \cup [f_\sigma] = \delta^*\delta^*(1 \cup [f_\sigma]) = \delta^*\delta^*([f_\sigma]).$$

En la última igualdad hemos empleado el teorema 16.11. Ahora calculemos $\delta^*([f_\sigma])$. Recordemos que se trata del homomorfismo de conexión respecto a la sucesión exacta $0 \longrightarrow I \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$. Una antiimagen de f_σ en $H^{-2}(G,\mathbb{Z}[G])$ es él mismo. Su frontera viene dada por

$$\partial f_\sigma\big(\langle\ \rangle\big) = f_\sigma\big(\partial_{-1}\big(\langle\ \rangle\big)\big) = f_\sigma\Big(\sum_{\tau\in G} \langle\tau\rangle\,(\tau^{-1} - 1)\Big) = \sigma^{-1} - 1 = d_{\sigma^{-1}}.$$

Una antiimagen en $H^{-1}(G, I)$ de este cociclo es él mismo. En total tenemos que $\delta^*([f_\sigma]) = [d_{\sigma^{-1}}]$. Consideramos seguidamente la sucesión exacta

$$0 \longrightarrow A \longrightarrow \overline{A} \longrightarrow I \longrightarrow 0.$$

Una antiimagen del cociclo $d_{\sigma^{-1}}$ en $H^{-1}(G, \overline{A})$ es él mismo. Su frontera es

$$\begin{aligned} \partial(d_{\sigma^{-1}}) &= \sum_{\tau\in G} d_{\sigma^{-1}}\tau = \sum_{\tau\in G}(d_{\sigma^{-1}\tau} - d_\tau + a_{\sigma^{-1},\tau}) = \sum_{\tau\in G} a_{\sigma^{-1},\tau} \\ &= \sum_{\tau\in G} a_{\sigma^{-1},\sigma\tau} = \sum_{\tau\in G}(a_{\sigma^{-1},\sigma}\tau + a_{1,\tau} - a_{\sigma,\tau}) \\ &= \sum_{\tau\in G} a_{\sigma^{-1},\sigma}\tau - \sum_{\tau\in G} a_{\sigma,\tau} = a_{\sigma^{-1},\sigma}T - \sum_{\tau\in G} a_{\sigma,\tau}. \end{aligned}$$

Una antiimagen de este cociclo en $H^0(G,A) = A^G/AT$ es él mismo, y al tomar clases módulo las trazas concluimos que $c \cup \sigma G' = -\big[\sum_{\tau\in G} a_{\sigma,\tau}\big]$. Teniendo en cuenta 14.37 esto se expresa en la forma:

$$c \cup \sigma G' = -E(c)(\sigma).$$

Recogemos este hecho en un teorema:

Teorema 16.14 *Sea G un grupo finito y A un G-módulo. Entonces el producto exterior $H^2(G,A) \times H^{-2}(G,\mathbb{Z}) \longrightarrow H^0(G,A)$, en su versión equivalente $H^2(G,A) \times G/G' \longrightarrow A^G/AT$ viene dado por*

$$[a_{\sigma,\tau}] \cup \sigma G' = -E\big([a_{\sigma,\tau}]\big)(\sigma) = -\sum_{\tau\in G} a_{\sigma,\tau}.$$

Observar que de aquí se deducen las propiedades que demostramos directamente en el capítulo XIV sobre la función E (que está bien definida y es bilineal).

Aplicación a los grupos cíclicos Los productos exteriores, al fijar una componente, inducen homomorfismos entre los grupos de cohomología. Es esta propiedad la que los convierte en una herramienta útil para nuestros fines. Vamos a ver una primera ilustración de este hecho obteniendo una prueba conceptual de la periodicidad de la cohomología de los grupos cíclicos.

Comencemos considerando un grupo finito G y su grupo dual G^*, es decir el grupo de caracteres (lineales) de G, el grupo de homomorfismos de G en $\mathbb{C}^*$. Teniendo en cuenta que los valores que toman los caracteres son sólo raíces de la unidad y que el grupo de raíces de la unidad de $\mathbb{C}$ es isomorfo a $\mathbb{Q}/\mathbb{Z}$, podemos considerar equivalentemente $G^* = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) = H^1(G,\mathbb{Q}/\mathbb{Z})$ (donde en $\mathbb{Q}/\mathbb{Z}$ consideramos la estructura de G-módulo trivial).

Ahora consideramos la sucesión exacta de G-módulos triviales

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Según las observaciones tras el teorema 15.4, los grupos de cohomología de $\mathbb{Q}$ son todos triviales respecto a cualquier grupo. Por lo tanto la sucesión exacta de cohomología nos da un isomorfismo

$$\delta^* : G^* = H^1(G,\mathbb{Q}/\mathbb{Z}) \longrightarrow H^2(G,\mathbb{Z}). \tag{16.2}$$

Vamos a calcularlo explícitamente.

Sea $\chi \in G^*$. Una antiimagen de χ respecto a la aplicación inducida por $\mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z}$ es cualquier función $\overline{\chi} : G \longrightarrow \mathbb{Q}$ que cumpla $\chi(\sigma) = \overline{\chi}(\sigma) + \mathbb{Z}$. Su cofrontera es $\partial\overline{\chi}(\sigma,\tau) = \overline{\chi}(\sigma) + \overline{\chi}(\tau) - \overline{\chi}(\sigma\tau)$. El hecho de que χ sea un homomorfismo implica que $\partial\overline{\chi}(\sigma,\tau) \in \mathbb{Z}$, luego podemos considerarlo como un cociclo de $(G,\mathbb{Z})$, y así

$$\delta^*\chi(\sigma,\tau) = \overline{\chi}(\sigma) + \overline{\chi}(\tau) - \overline{\chi}(\sigma\tau). \tag{16.3}$$

Si sumamos respecto de τ obtenemos

$$\sum_{\tau\in G}\delta^*\chi(\sigma,\tau)=\sum_{\tau\in G}\big(\overline{\chi}(\sigma)+\overline{\chi}(\tau)-\overline{\chi}(\sigma\tau)\big)=\sum_{\tau\in G}\overline{\chi}(\sigma)=|G|\,\overline{\chi}(\sigma).$$

La interpretación de esta igualdad es clara:

Teorema 16.15 *Sea G un grupo de orden n, $\chi\in G^*$ y $\sigma\in G$. Entonces $\chi(\sigma)=m/n+\mathbb{Z}$ para cierto $m\in\mathbb{Z}$. Se cumple*

$$\delta^*\chi\cup\sigma G'=-m+n\mathbb{Z}\in H^0(G,\mathbb{Z})=\mathbb{Z}/n\mathbb{Z}.$$

El interés de este hecho radica en que si $G=\langle\sigma\rangle$ y tomamos el carácter χ de modo que $\chi(\sigma)=-1/n+\mathbb{Z}$, entonces

$$\delta^*\chi\cup\sigma G'=\sigma G'\cup\delta^*\chi=1+n\mathbb{Z}.$$

Esto implica que si A es cualquier G-módulo, las aplicaciones $\cup\,\delta^*\chi$ y $\cup\,\sigma G'$ son homomorfismos inversos entre los grupos $H^r(G,A)$ y $H^{r+2}(G,A)$ para cualquier entero r, pues

$$(x\cup\delta^*\chi)\cup\sigma G'=x\cup(\delta^*\chi\cup\sigma G')=x\cup 1=x,$$

e igualmente al revés.

En particular el isomorfismo $H^2(G,A)\cong H^0(G,A)$ es la multiplicación por $\sigma G'$, o sea, la aplicación $x\mapsto -E(x)(\sigma)$, tal y como obtuvimos en el capítulo XII (el signo $-$ es irrelevante, pues la aplicación $a\mapsto -a$ es un automorfismo de $H^0(G,A)$).

16.3 El isomorfismo de Artin

Vamos a obtener el isomorfismo de Artin como caso particular de un teorema general que, bajo ciertas hipótesis, relaciona los grupos de cohomología de un grupo G respecto a un G-módulo A con sus grupos de cohomología respecto a $\mathbb{Z}$, mucho más fáciles de calcular.

Primero demostramos el criterio de Nakayama-Tate sobre trivialidad cohomológica, que tiene interés por sí mismo. Aunque no vamos a necesitar seriamente este concepto, se dice que un G-módulo A es *cohomológicamente trivial* si $H^n(S,A)=0$ para todo subgrupo $S\le G$ y todo entero n.

Teorema 16.16 (Criterio de Nakayama-Tate) *Sea G un grupo finito y A un G-módulo. Si existe un entero k tal que $H^k(S,A)=0$ y $H^{k+1}(S,A)=0$ para todo $S\le G$, entonces $H^n(S,A)=0$ para todo $S\le G$ y todo entero n.*

Demostración: Por reducción regular podemos suponer que $k=1$. Por el teorema 15.5 podemos suponer también que el orden de G es potencia de primo. Probaremos el teorema por inducción sobre el orden de G. En realidad sólo hay que probar que $H^n(G,A)=0$ para todo entero n.

Si G es cíclico el resultado es evidente, pues cada grupo de cohomología es isomorfo a $H^1(G,A)$ o bien a $H^2(G,A)$. En caso contrario G tiene un subgrupo normal N tal que G/N es cíclico no trivial. Por hipótesis de inducción $H^n(N,A)=0$ para todo entero n, luego el teorema 15.10 nos da que la sucesión

$$0 \longrightarrow H^n(G/N,A^N) \xrightarrow{\text{Inf}} H^n(G,A) \xrightarrow{\text{Res}} H^n(N,A) = 0$$

es exacta para todo $n \geq 1$. En particular $H^k(G/N,A^N)=0$ para $k=1,\,2$, luego por el caso cíclico concluimos que $H^n(G/N,A^N)=0$ para todo entero n y también $H^n(G,A)=0$ para todo $n\geq 1$.

Veamos ahora que $H^0(G,A)=0$. Tomemos un $a\in A^G$. Teniendo en cuenta que $H^0(G/N,A^N)=0$, vemos que existe un $b\in A^N$ tal que $a=N_{G/N}(b)$. Como $H^0(N,A)=0$ existe un $c\in A$ tal que $b=\mathrm{Tr}_N(c)$, luego $a=\mathrm{Tr}_G(c)$ y así $H^0(G,A)=0$.

De aquí se sigue que $H^k(S,A^-)=0$ para $k=1,\,2$, y todo $S\leq G$, luego el razonamiento anterior prueba que $H^0(G,A^-)=0$, es decir, $H^{-1}(G,A)=0$. Repitiendo el proceso se concluye lo mismo para todos los índices negativos. ∎

El resultado que anunciábamos es el siguiente:

Teorema 16.17 (Teorema de Tate) *Sea G un grupo finito y A un G-módulo. Supongamos que existe un entero k tal que para todo $S\leq G$ se cumplen las condiciones:*

a) $H^{k-1}(S,A)=0$,

b) $H^k(S,A)$ *es cíclico del mismo orden que S.*

Entonces para todo entero n y todo $S\leq G$ se tiene el isomorfismo

$$H^{n-k}(S,\mathbb{Z}) \cong H^n(S,A)$$

dado por

$$x \mapsto \mathrm{Res}_{G,S}\, z \cup x,$$

donde z es un generador de $H^k(G,A)$.

Demostración: Veámoslo primero en el caso $k=1$. Sea $z=[a_\sigma]$. Sea $B=A\oplus\mathbb{Z}$ con la estructura de G-módulo dada por $(a,n)\sigma=(a\sigma+na_\sigma,n)$. Es claro que A es un submódulo de B, que $B/A\cong\mathbb{Z}$ y que la acción de G sobre el cociente es trivial. Por lo tanto tenemos una sucesión exacta

$$0\longrightarrow A\longrightarrow B\longrightarrow \mathbb{Z}\longrightarrow 0,$$

que a su vez da lugar a la sucesión exacta

$$0\longrightarrow H^0(S,B)\longrightarrow H^0(S,\mathbb{Z}) \xrightarrow{\delta^*} H^1(S,A)\longrightarrow H^1(S,B)\longrightarrow 0.$$

Tenemos que $H^0(S,\mathbb{Z})\cong\mathbb{Z}/n\mathbb{Z}$, donde $n=|S|$. Vamos a calcular $\delta^*\big([1]\big)$. Es claro que una antiimagen de 1 por la aplicación inducida por $B\longrightarrow\mathbb{Z}$ es la

cocadena de dimensión 0 dada por $(0,1)$. La cofrontera de esta cocadena es la dada por

$$\partial_0(0,1)\big([\sigma]\big) = (0,1)(\sigma-1) = (a_\sigma,1)-(0,1) = (a_\sigma,0), \quad \text{para } \sigma \in S.$$

Una antiimagen de esta cocadena por la aplicación inducida por $A \longrightarrow B$ es el propio $\{a_\sigma\}$ (restringido a S). Así pues, $\delta^*\big([1]\big) = \mathrm{Res}_{G,S}\, z$.

Por otra parte el teorema 15.4 nos da que $\mathrm{V}_{S,G}(\mathrm{Res}_{G,S}\, z) = |G:S|z$, que tiene orden igual a $|S|$, luego el orden de $\mathrm{Res}_{G,S}\, z$ ha de ser como mínimo $|S|$, de donde concluimos que $\mathrm{Res}_{G,S}\, z$ es un generador de $H^1(S,A)$. Por consiguiente δ^* es un isomorfismo.

La exactitud de la sucesión implica que $H^0(S,B) = H^1(S,B) = 0$. Por el teorema anterior $H^n(S,B) = 0$ para todo entero n. Al aplicar este hecho a otro tramo de la sucesión exacta:

$$0 = H^{n-1}(S,B) \longrightarrow H^{n-1}(S,\mathbb{Z}) \xrightarrow{\delta^*} H^n(S,A) \longrightarrow H^n(S,B) = 0$$

obtenemos los isomorfismos buscados $H^{n-1}(S,\mathbb{Z}) \cong H^n(S,A)$. Concretamente, si $x \in H^{n-1}(S,\mathbb{Z})$ tenemos que

$$\delta^* x = \delta^*(1 \cup x) = \delta^* 1 \cup x = \mathrm{Res}_{G,S}\, z \cup x.$$

La reducción regular implica el teorema para un k arbitrario. Por ejemplo, si se cumple para $k-1$ los isomorfismos $H^{n-1}(S,A^+) \cong H^n(S,A)$ nos dan que si A cumple las hipótesis con k entonces A^+ las cumple con $k-1$, luego

$$H^{n-k}(S,\mathbb{Z}) = H^{n-1-(k-1)}(S,\mathbb{Z}) \cong H^{n-1}(S,A^+) \cong H^n(S,A).$$

Con más detalle, tenemos la sucesión exacta $0 \longrightarrow A \longrightarrow B \longrightarrow A^+ \longrightarrow 0$. Si z es un generador de $H^k(G,A)$, existe un generador z^+ de $H^{k-1}(G,A^+)$ de manera que $z = \delta^* z^+$. La composición de los dos isomorfismos es

$$x \mapsto \delta^*(\mathrm{Res}_{G,S}\, z^+ \cup x) = \delta^*(\mathrm{Res}_{G,S}\, z^+) \cup x = \mathrm{Res}_{G,S}(\delta^* z^+) \cup x = \mathrm{Res}_{G,S}\, z \cup x.$$

■

Ahora observamos que el teorema de Tate es aplicable a las formaciones de clases para $k = 2$. En efecto, si K/k es una extensión normal de una formación de clases con grupo de Galois G, cada subgrupo S de G es el grupo de Galois de una extensión K/L, luego $H^1(S,K) = H^1(K/L) = 1$ y $H^2(S,K) = H^2(K/L)$ es cíclico del mismo orden que S. Un generador de $H^2(G,K)$ es la clase fundamental $\xi_{K/k}$ definida en 15.24, luego podemos definir isomorfismos canónicos:

Definición 16.18 Sea K/k una extensión normal en una formación de clases. Sea G su grupo de Galois. Para cada entero r definimos el *isomorfismo canónico*

$$\alpha^r_{K/k} : H^r(G,\mathbb{Z}) \longrightarrow H^{r+2}(K/k)$$

como el dado por $\alpha^r_{K/k}(x) = \xi_{K/k} \cup x$.

En el capítulo XIV hemos visto que

$$H^{-2}(G,\mathbb{Z}) \cong G/G', \quad H^{-1}(G,\mathbb{Z}) = 0, \quad H^0(G,\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}, \quad H^1(G,\mathbb{Z}) = 0.$$

Más aún, al final de la sección anterior construimos el isomorfismo (16.2):

$$H^2(G,\mathbb{Z}) \cong G^* = (G/G')^* \cong G/G'.$$

De aquí se siguen muchos isomorfismos de interés:

$$\begin{aligned} &H^0(K/k) \cong G/G', && H^1(K/k) = 1,\\ &H^2(K/k) \cong \mathbb{Z}/n\mathbb{Z}, && H^3(K/k) = 1,\\ &H^4(K/k) \cong G^* \cong G/G'. \end{aligned}$$

El más importante de todos estos isomorfismos es el primero, que no es sino $A_k/\,\mathrm{N}[A_K] \cong G/G'$, es decir, el isomorfismo de Artin. Antes de estudiarlo con detalle probaremos un par de resultados generales sobre los isomorfismos canónicos.

Teorema 16.19 *Sea K/k una extensión normal en una formación de clases y L un cuerpo intermedio. Entonces las restricciones y transferencias hacen conmutativo el diagrama siguiente:*

$$\begin{array}{ccc} H^r(G(K/k),\mathbb{Z}) & \xrightarrow{\alpha^r} & H^{r+2}(K/k) \\ \mathrm{Res}\downarrow\ \uparrow\mathrm{V} & & \mathrm{Res}\downarrow\ \uparrow\mathrm{V} \\ H^r(G(K/L),\mathbb{Z}) & \xrightarrow[\alpha^r]{} & H^{r+2}(K/L) \end{array}$$

Demostración: Según el teorema 15.25 se cumple $\mathrm{Res}_{k,L}(\xi_{K/k}) = \xi_{K/L}$. Si $x \in H^r(G(K/k),\mathbb{Z})$, el teorema 16.10 nos permite concluir que

$$\begin{aligned} \alpha^r_{K/L}\big(\mathrm{Res}_{G(K/k),G(K/L)}(x)\big) &= \xi_{K/L} \cup \mathrm{Res}_{G(K/k),G(K/L)}(x)\\ &= \mathrm{Res}_{G(K/k),G(K/L)}(\xi_{K/k}) \cup \mathrm{Res}_{G(K/k),G(K/L)}(x)\\ &= \mathrm{Res}_{G(K/k),G(K/L)}(\xi_{K/k} \cup x) = \mathrm{Res}_{k,L}\big(\alpha^r_{K/k}(x)\big). \end{aligned}$$

Del mismo modo, si $x \in H^r(G(K/L),\mathbb{Z})$ se cumple

$$\begin{aligned} \alpha^r_{K/k}\big(\mathrm{V}_{G(K/L),G(K/k)}(x)\big) &= \xi_{K/k} \cup \mathrm{V}_{G(K/L),G(K/k)}(x)\\ &= \mathrm{V}_{G(K/L),G(K/k)}\big(\mathrm{Res}_{k,L}(\xi_{K/k}) \cup x\big)\\ &= \mathrm{V}_{K,k}(\xi_{K/L} \cup x) = \mathrm{V}_{L,k}\big(\alpha^r_{K/L}(x)\big). \end{aligned}$$

■

Similarmente se prueba la conmutatividad con la conjugación:

Teorema 16.20 *Sea K/k una extensión normal en una formación de clases y σ un elemento del grupo de Galois (de la formación). Entonces el diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} H^r(G(K/k),\mathbb{Z}) & \xrightarrow{\alpha^r} & H^{r+2}(K/k) \\ \downarrow{\scriptstyle \sigma_*} & & \downarrow{\scriptstyle \sigma_*} \\ H^r(G(K^\sigma/k^\sigma),\mathbb{Z}) & \xrightarrow[\alpha^r]{} & H^{r+2}(K^\sigma/k^\sigma) \end{array}$$

Definición 16.21 Sea K/k una extensión normal de una formación de clases y G su grupo de Galois. Llamaremos *isomorfismo de Artin* de K/k a la composición de los isomorfismos naturales

$$A_k/\,\mathrm{N}[A_K] \cong H^0(K/k), \qquad H^{-2}(G,\mathbb{Z}) \cong G/G' \tag{16.4}$$

con el isomorfismo canónico $\alpha_{K/k}^{-2}$. Lo representaremos por

$$\omega_{K/k} : A_k/\,\mathrm{N}[A_K] \longrightarrow G/G'.$$

Al componerlo con la proyección canónica $A_k \longrightarrow A_k/\,\mathrm{N}[A_K]$ obtenemos un epimorfismo al que seguiremos llamando $\omega_{K/k}$. Usaremos también la notación tradicional

$$\omega_{K/k}(a) = \left(\frac{K/k}{a}\right) \in G/G'.$$

Así pues,

$$\left(\frac{K/k}{a}\right) = \sigma G' \quad \text{si y sólo si} \quad [a] = \xi_{K/k} \cup \sigma G',$$

donde $\xi_{K/k}$ es la clase fundamental de la extensión.

Veamos una caracterización que resulta útil en ocasiones. Recordemos el isomorfismo (16.2) $\delta^* : G^* \longrightarrow H^2(G,\mathbb{Z})$.

Teorema 16.22 *Sea K/k una extensión normal de una formación de clases y $a \in A_k$. Entonces $\left(\frac{K/k}{a}\right)$ está caracterizado por la relación*

$$\chi\Big(\left(\frac{K/k}{a}\right)\Big) = -\operatorname{Inv}_k\big([a] \cup \delta^*(\chi)\big), \qquad \textit{para todo } \chi \in G(K/k)^*.$$

Demostración: Sea $G = G(K/k)$ y sea $\left(\frac{K/k}{a}\right) = \sigma G'$. En primer lugar notemos que todo $\chi \in G^*$ tiene a G' en su núcleo, por lo que tiene sentido considerarlo como carácter de G/G', tal y como ocurre en el enunciado. Además, si todos los caracteres (lineales) de G actúan igual sobre dos de sus elementos, entonces ambos determinan la misma clase módulo G', luego efectivamente la propiedad del enunciado caracteriza al símbolo de Artin supuesto que la cumpla.

Sea $n = |G| = |K : k|$ y sea $\chi(\sigma) = m/n$ (mód 1). Entonces tenemos que $[a] = \xi_{K/k} \cup \sigma G'$ y, aplicando los teoremas 16.15 y 16.11 concluimos que

$$[a] \cup \delta^*(\chi) = \xi_{K/k} \cup \sigma G' \cup \delta^*(\chi) = \xi_{K/k} \cup (-m + n\mathbb{Z}) = -m\,\xi_{K/k}.$$

Puesto que por definición $\mathrm{Inv}_k(\xi_{K/k}) = 1/n$ (mód 1), al tomar invariantes queda la relación indicada. ∎

El isomorfismo de Artin relaciona de forma muy simple las aplicaciones entre los grupos $A_k/\,\mathrm{N}[A_K]$ y las aplicaciones entre los grupos G/G'. Veámoslo.

Teorema 16.23 *Sea K/k una extensión normal en una formación de clases y sea L un cuerpo intermedio. Los diagramas siguientes son conmutativos (donde las flechas verticales representan siempre el isomorfismo de Artin).*

$$\begin{array}{ccc} A_k/\,\mathrm{N}[A_K] & \xrightarrow{\text{inclusión}} & A_L/\,\mathrm{N}[A_K] \\ \downarrow & & \downarrow \\ G(K/k)\,/\,G'(K/k) & \xrightarrow[\text{transferencia}]{} & G(K/L)\,/\,G'(K/L) \end{array}$$

$$\begin{array}{ccc} A_L/\,\mathrm{N}[A_K] & \xrightarrow{\mathrm{N}_{L/k}} & A_k/\,\mathrm{N}[A_K] \\ \downarrow & & \downarrow \\ G(K/L)\,/\,G'(K/L) & \xrightarrow[\text{inclusión}]{} & G(K/k)\,/\,G'(K/k) \end{array}$$

Si σ pertenece al grupo de Galois de la formación

$$\begin{array}{ccc} A_k/\,\mathrm{N}[A_K] & \xrightarrow{\text{producto por } \sigma} & A_{k^\sigma}/\,\mathrm{N}[A_{L^\sigma}] \\ \downarrow & & \downarrow \\ G(K/k)\,/\,G'(K/k) & \xrightarrow[\text{conjugación por } \sigma]{} & G(L^\sigma/k^\sigma)\,/\,G'(L^\sigma/k^\sigma) \end{array}$$

Si L/k es normal

$$\begin{array}{ccc} A_k/\,\mathrm{N}[A_K] & \xrightarrow{\text{identidad}} & A_k/\,\mathrm{N}[A_L] \\ \downarrow & & \downarrow \\ G(K/k)\,/\,G'(K/k) & \xrightarrow[\text{proyección}]{} & G(L/k)\,/\,G'(L/k) \end{array}$$

DEMOSTRACIÓN: La conmutatividad del primer diagrama es consecuencia del teorema 16.19. En efecto, el isomorfismo $\alpha_{K/k}^{-2}$ conmuta con las restricciones, luego el isomorfismo de Artin conmuta con los homomorfismos que resultan de componer las restricciones con los isomorfismos naturales (16.22). Éstas son la aplicación $[a] \mapsto [a]$ (claramente) y la transferencia de grupos (teorema 15.3).

Del mismo modo se prueba la conmutatividad de los dos diagramas siguientes, usando, respectivamente, la parte del teorema 16.19 correspondiente a las transferencias y el teorema 16.20.

Para probar la conmutatividad del último diagrama no contamos con ninguna interpretación cohomológica de las aplicaciones involucradas. Usaremos el teorema 16.22.

Tomemos un $a \in A_k$ y sea $\left(\frac{K/k}{a}\right) = \sigma G'(K/k)$. Hemos de probar que

$$\left(\frac{L/k}{a}\right) = \big(\sigma G(K/L)\big)G'(L/k).$$

Para ello tomamos un carácter $\chi \in G(L/k)^*$. Sea $\psi = \mathrm{Inf}\chi \in G(K/k)^*$, es decir, el carácter dado por $\psi(\tau) = \chi\big(\tau G(K/L)\big)$. Una simple comprobación nos da que el diagrama siguiente es conmutativo:

$$\begin{array}{ccc} G(L/k)^* & \xrightarrow{\mathrm{Inf}} & G(K/k)^* \\ {\scriptstyle\delta^*}\downarrow & & \downarrow{\scriptstyle\delta^*} \\ H^2(L/k) & \xrightarrow[\mathrm{Inf}]{} & H^2(K/k) \end{array}$$

Por lo tanto $\delta^*(\psi) = \mathrm{Inf}\delta^*(\chi)$. Aplicamos el teorema 16.22 y luego el teorema 16.11:

$$\chi\big(\sigma G(K/L)\big) = \psi(\sigma) = -\operatorname{Inv}_k\big([a] \cup \delta^*(\psi)\big) = -\operatorname{Inv}_k(a \otimes \mathrm{Inf}\delta^*(\chi)\big).$$

Es fácil comprobar que

$$a \otimes \mathrm{Inf}\delta^*(\chi) = \mathrm{Inf}(a \otimes \delta^*(\chi)).$$

Por lo tanto

$$\begin{aligned} \chi\big(\sigma G(K/L)\big) &= -\operatorname{Inv}_k(\mathrm{Inf}(a \otimes \delta^*(\chi))) = -\operatorname{Inv}_k(a \otimes \delta^*(\chi)) \\ &= -\operatorname{Inv}_k\big([a] \cup \delta^*(\chi)\big). \end{aligned}$$

La penúltima igualdad se debe a que la inflación es la inclusión en el grupo de Brauer. El teorema 16.22 nos da entonces la igualdad buscada. ∎

He aquí un enunciado equivalente al del teorema anterior:

Teorema 16.24 *Sea K/k una extensión normal en una formación de clases y L un cuerpo intermedio.*

a) Si $a \in A_k$, entonces

$$\left(\frac{K/L}{a}\right) = \mathrm{V}_{K/k,K/L}\left(\frac{K/k}{a}\right).$$

b) Si $a \in A_L$, entonces

$$\left(\frac{K/L}{a}\right) G'(K/k) = \left(\frac{K/k}{\mathrm{N}_k^L(a)}\right).$$

c) Si σ pertenece al grupo de Galois de la formación y $a \in A_k$, entonces

$$\left(\frac{K/k}{a}\right)^\sigma = \left(\frac{K^\sigma/k^\sigma}{a\sigma}\right).$$

d) Si L/k es normal y $a \in A_k$, entonces

$$\left(\frac{L/k}{a}\right) = \left(\frac{K/k}{a}\right) G(K/L).$$

Extensiones infinitas Si K/k es una extensión abeliana en una formación de clases y $a \in A_k$, entonces el símbolo de Artin $\left(\frac{K/k}{a}\right)$ es un elemento de G_k/G_K, luego es un subconjunto cerrado de G_k. El apartado d) del teorema anterior nos da que si $k \subset L \subset K$ es una cadena de extensiones abelianas, entonces $\left(\frac{K/k}{a}\right) \subset \left(\frac{L/k}{a}\right)$. Esto implica claramente que la familia $\left\{\left(\frac{K/k}{a}\right)\right\}_K$, para un a fijo y donde K recorre las extensiones abelianas de k, es una familia de cerrados en G_k con la propiedad de la intersección finita. Como G_k es compacto existe un $\sigma \in G_k$ que pertenece a todas las clases,es decir, tal que

$$\left(\frac{K/k}{a}\right) = \sigma G_K, \qquad \text{para toda extensión abeliana } K \text{ de } k.$$

Si llamamos $\overline{G}'_k$ a la intersección de todos los grupos G_K cuando K recorre las extensiones abelianas de k, es claro que se trata de un subgrupo cerrado de G_k, y σ está determinado módulo $\overline{G}'_k$. Por lo tanto podemos definir

$$\left(\frac{k}{a}\right) = \sigma\overline{G}'_k \in G_k/\overline{G}'_k.$$

En el caso en que el grupo de Galois de la formación es un grupo de Galois en el sentido usual es fácil ver que $\overline{G}'_k$ es la clausura del subgrupo derivado de G_k, es decir, el grupo de Galois de la mayor extensión abeliana de k.

Definición 16.25 Sea k un cuerpo en una formación de clases. Con la notación precedente definimos $G(A_k/k) = G_k/\overline{G}'_k$. Llamaremos *homomorfismo de Artin*

de k al homomorfismo $\omega_k : A_k \longrightarrow G(A_k/k)$ que acabamos de construir, y que está determinado por la propiedad:

$$\left(\frac{K/k}{a}\right) = \left(\frac{k}{a}\right) G_K,$$

para todo $a \in A_k$ y toda extensión abeliana K de k.

Claramente el núcleo de (k/a) es la intersección de los núcleos de todos los símbolos de Artin $\left(\frac{K/k}{a}\right)$, es decir, la intersección de todos los grupos de normas $\mathrm{N}_k^K[A_K]$, donde K recorre las extensiones abelianas de k. A dicho grupo lo llamaremos *grupo de normas universales* de k, y lo representaremos por D_k. De este modo tenemos un monomorfismo $\omega_k : A_k/D_k \longrightarrow G(A_k/k)$. En general no es suprayectivo, pero induce isomorfismos $A_k/\,\mathrm{N}_k^K[A_K] \cong G_k/G_K$ para cada extensión abeliana K de k. En particular los grupos de normas se recuperan por la relación $\mathrm{N}_k^K[A_K] = \omega_k^{-1}[G_K/\overline{G}_k']$.

Veamos algunos conceptos más que pueden expresarse en términos de extensiones infinitas. En primer lugar observamos que, a través de los isomorfismos $G^*(K/k) \cong H^1(G(K/k), \mathbb{Q}/\mathbb{Z})$, la inflación $\mathrm{Inf}\, G(K/k)^* \longrightarrow G(L/k)^*$ se corresponde con la aplicación $(\mathrm{Inf}\chi)(\sigma) = \chi\big(\sigma G(L/K)\big)$. Ya hemos usado este hecho alguna vez. En el caso en que los grupos sean auténticos grupos de Galois esto equivale a $(\mathrm{Inf}\chi)(\sigma) = \chi(\sigma|_K)$.

Estas inflaciones son obviamente inyectivas, lo que nos permite considerar a $G(K/k)^*$ como subgrupo de $G(L/k)^*$ exactamente igual a como hacemos con los grupos $H^2(K/k)$. También podemos construir un límite inductivo análogo al grupo de Brauer:

Definición 16.26 Sea k un cuerpo de una formación. Llamaremos G_k^* al grupo de los caracteres (lineales) continuos de G_k, es decir, el grupo de los homomorfismos $\chi : G_k \longrightarrow \mathbb{Q}/\mathbb{Z}$ cuyo núcleo es de la forma $\mathrm{N}_\chi = G_K$, para una cierta extensión K de k, obviamente abeliana.

Si K es una extensión de k, la inflación $\mathrm{Inf} : G(K/k)^* \longrightarrow G_k^*$, definida de forma natural, es inyectiva, y cualquier carácter χ es (por la continuidad) la inflación de un carácter de $G(K/k)$, donde $\mathrm{N}_\chi = G_K$. Esto nos permite considerar a los grupos $G(K/k)^*$ como subgrupos de G_k^*, de modo que éste es la unión de todos ellos. A través de esta identificación las inflaciones se convierten en las inclusiones. En estos términos, un carácter (lineal y continuo) de G_k es simplemente un carácter (lineal) de una extensión de k.

De la propia definición de se desprende que el grupo $\overline{G}_k'$ está contenido en el núcleo de todos los caracteres de G_k, luego $G_k^* = G(A_k/k)^*$, en el sentido de que todo carácter de G_k induce un carácter de $G(A_k/k)$, y esta aplicación es de hecho un isomorfismo. Así pues tiene sentido considerar la imagen por un carácter de un símbolo de Artin. Concretamente

$$\chi(\left(\frac{k}{a}\right)) = \chi(\left(\frac{K/k}{a}\right)),$$

donde K es una extensión de k suficientemente grande para que $\chi \in G(K/k)^*$.

Como las inflaciones conmutan con los isomorfismos (16.2), las inflaciones en los grupos $H^2(G(K/k),\mathbb{Z})$ son inyectivas, y podemos considerar a todos estos grupos como subgrupos de un mismo grupo $H^2(G_k,\mathbb{Z})$, construido igual que el grupo de Brauer, de modo que tenemos un isomorfismo $\delta^* : G_k^* \longrightarrow H^2(G_k,\mathbb{Z})$ dado por $\delta^*\chi(\sigma,\tau) = \bar\chi(\sigma) + \bar\chi(\tau) - \bar\chi(\sigma\tau)$, donde $\bar\chi$ es cualquier función que cumpla $\chi(\sigma) = \bar\chi(\sigma) + \mathbb{Z}$.

Finalmente podemos considerar los productos exteriores

$$\cup : A_k \times H^2\big(G(K/k),\mathbb{Z}\big) \longrightarrow H^2(*/k),$$

que en virtud del teorema 16.11 conmutan con las inflaciones (observar que hemos eliminado el cociente módulo $\mathrm{N}[A_K]$). Estos productos determinan un producto exterior

$$\cup : A_k/D_k \times H^2(G_k,\mathbb{Z}) \longrightarrow H^2(*/k).$$

Con esto resulta inmediato un resultado análogo al teorema 16.22 para extensiones infinitas:

$$\chi\Big(\Big(\frac{k}{a}\Big)\Big) = -\operatorname{Inv}_k\big([a]\cup\delta^*(\chi)\big), \qquad \text{para todo } \chi \in G_k^*. \tag{16.5}$$

Formaciones locales Estudiemos ahora el isomorfismo de Artin en las formaciones locales. En particular veremos que en las formaciones p-ádicas coincide con el que ya teníamos definido.

Sea T/k una extensión no ramificada de cuerpos locales. Sabemos que es cíclica. Sea π un primo en k. Entonces $k^* = U_k \otimes \langle\pi\rangle$, donde U_k es el grupo de unidades de k. Según el teorema 15.17, el índice $|U_k : \mathrm{N}[U_T]|$ es el índice de ramificación, o sea, es 1, de modo que todas las unidades de k son normas, luego están en el núcleo del isomorfismo de Artin. Consecuentemente, el automorfismo $\left(\frac{T/k}{\pi}\right)$ no depende de la elección del primo π y determina completamente el homomorfismo de Artin.

Ahora hemos de notar que si una familia de funciones Inv_k satisfacen el axioma II en una formación, entonces las funciones $-\operatorname{Inv}_k$ también lo satisfacen. En el caso concreto de las formaciones locales hemos definido los invariantes de modo que si $c \in H^2(T/k)$, entonces

$$\operatorname{Inv}_k(c) = (v_k(E(c)(\sigma_{T/k}))/n) \text{ (mód 1)}.$$

En términos de los productos exteriores esta relación se expresa como

$$\operatorname{Inv}_k(c) = -(v_k(c\cup\sigma_{T/k})/n) \text{ (mód 1)}.$$

Si queremos que el isomorfismo de Artin coincida con el usual, hemos de cambiar el signo a los invariantes, de modo que se cumpla

$$\operatorname{Inv}_k(c) = (v_k(c\cup\sigma_{T/k})/n) \text{ (mód 1)}.$$

En particular $[1/n] = \mathrm{Inv}_k(\xi_{T/k}) = [v_k(\xi_{T/k} \cup \sigma_{T/k})/n]$ o, equivalentemente, $v_k(\xi_{T/k} \cup \sigma_{T/k}) = 1$. Esto significa que $\xi_{T/k} \cup \sigma_{T/k} = [\pi]$ y, por la definición del símbolo de Artin,

$$\left(\frac{T/k}{\pi}\right) = \sigma_{T/k}. \tag{16.6}$$

De este modo el isomorfismo de Artin de T/k hace corresponder los primos de k con el automorfismo canónico de la extensión. Con esto ya podemos aplicar el teorema 12.21 para concluir que el símbolo de Artin definido en este capítulo coincide con el que ya teníamos definido para las extensiones abelianas de cuerpos p-ádicos.[1]

Otra alternativa para conseguir (16.6) hubiera sido definir los isomorfismos $\alpha^r_{K/k}$ (y en particular el isomorfismo de Artin) mediante $\alpha^r_{K/k}(x) = -\xi_{K/k} \cup x$. El resultado final es el mismo. La aplicación de Nakayama permite definir los invariantes y el isomorfismo de Artin sin necesidad de productos exteriores, y entonces resulta más natural esta segunda opción. El problema que teníamos y que acabamos de corregir es que habíamos definido los invariantes en términos de la aplicación de Nakayama y el isomorfismo de Artin en términos de productos exteriores.

Volvamos ahora a la igualdad $|U_k : \mathrm{N}[U_K]| = e$, que el teorema 15.17 prueba para extensiones cíclicas. El isomorfismo de Artin nos permite probarla para extensiones abelianas cualesquiera, con lo que generalizamos el teorema de ramificación a formaciones locales arbitrarias.

Teorema 16.27 *Sea K/k una extensión abeliana de cuerpos locales. Sea L su cuerpo de inercia. Sean U_K y U_k los grupos de unidades de K y k respectivamente. Entonces*

$$\left(\frac{K/k}{U_k}\right) = G(K/L)$$

y además el isomorfismo de Artin induce un isomorfismo

$$U_k/\,\mathrm{N}_{K/k}[U_K] \cong G(K/L).$$

En particular $|U_k : \mathrm{N}_{K/k}[U_K]| = e$ (el índice de ramificación de K/k).

Demostración: Del teorema 16.24 se sigue que la imagen por el isomorfismo de Artin del grupo de normas $\mathrm{N}_{L/k}[L^*]$ es $G(K/L)$. Ahora bien, si U_L es el grupo de unidades de L y π es cualquier primo en L, entonces $L^* = U_L \times \langle\pi\rangle$, luego

$$\mathrm{N}_{L/k}[L^*] = \mathrm{N}_{L/k}[U_L] \times \left\langle \mathrm{N}_{L/k}(\pi)\right\rangle = U_k \times \left\langle \mathrm{N}_{L/k}(\pi)\right\rangle,$$

pues la extensión L/k es no ramificada y ya hemos observado antes que entonces $\mathrm{N}_{L/k}[U_L] = U_k$.

Por otra parte la extensión K/L tiene grado e índice de ramificación iguales a e, por lo que, si ρ es un primo en K, entonces $\mathrm{N}_{K/L}(\rho)$ es primo en L y,

[1] Observemos que, según ya sabemos, el grupo de normas universales D_k para un cuerpo p-ádico k es trivial, por lo que el símbolo de Artin ω_k es inyectivo, tal y como se exige en 12.21.

como π es arbitrario, podemos tomar $\pi = \mathrm{N}_{K/L}(\rho)$. De este modo tenemos que $\mathrm{N}_{L/k}(\pi) = \mathrm{N}_{K/k}(\rho) \in \mathrm{N}_{K/k}[K^*]$, y éste es el núcleo del símbolo de Artin. De aquí se sigue la primera igualdad del enunciado, que junto con la obvia relación $U_k \cap \mathrm{N}_{K/k}[K^*] = \mathrm{N}_{K/k}[U_K]$ nos lleva al isomorfismo indicado. ∎

16.4 Cuerpos de clases

Veamos ahora el tratamiento general del concepto de cuerpo de clases en formaciones de clases arbitrarias.

Definición 16.28 Sea k un cuerpo de una formación de clases. A cada extensión K de k le podemos asociar el grupo $\mathrm{N}_{K/k}[A_K] \leq A_k$, que recibe el nombre de *grupo de normas* de K en k.

En primer lugar es obvio que la correspondencia $K \mapsto \mathrm{N}_{K/k}[A_K]$ invierte las inclusiones. Si la extensión K/k es normal entonces el grupo de normas de K es precisamente el núcleo del símbolo de Artin. Vamos a ver que el símbolo de Artin también determina los grupos de normas de las extensiones que no son normales.

Teorema 16.29 *Sea $k \subset L \subset K$ una cadena de cuerpos en una formación de clases. Supongamos que la extensión K/k es normal. Sea $a \in A_k$. Entonces*

$$a \in \mathrm{N}_{L/k}[A_L] \quad \textit{si y sólo si} \quad \left(\frac{K/k}{a}\right) \in G(K/L)G'(K/k) \,/\, G'(K/k).$$

Demostración: Si $a \in \mathrm{N}_{L/k}[A_L]$, digamos $a = \mathrm{N}_{L/k}(b)$, con $b \in A_L$, entonces el teorema 16.24 nos da que

$$\left(\frac{K/k}{a}\right) = \left(\frac{K/L}{b}\right) G'(K/k) \in G(K/L)G'(K/k) \,/\, G'(K/k).$$

Así mismo, si $\left(\frac{K/k}{a}\right) \in G(K/L)G'(K/k) \,/\, G'(K/k)$, digamos $\left(\frac{K/k}{a}\right) = \sigma G'(K/k)$, con $\sigma \in G(K/L)$, la suprayectividad del homomorfismo de Artin $A_L \longrightarrow G(K/L) \,/\, G'(K/L)$ implica que existe un $b \in A_L$ tal que $\left(\frac{K/L}{b}\right) = \sigma G'(K/L)$, luego

$$\begin{aligned} \left(\frac{K/k}{a}\right) &= \sigma G'(K/k) = \sigma G'(K/L)G'(K/k) \\ &= \left(\frac{K/L}{b}\right) G'(K/k) = \left(\frac{K/k}{\mathrm{N}_{L/k}(b)}\right). \end{aligned}$$

Como el núcleo del homomorfismo de Artin de K/k es $\mathrm{N}_{K/k}[A_K]$, existe un $c \in A_K$ tal que

$$\begin{aligned} a &= \mathrm{N}_{K/k}(c)\,\mathrm{N}_{L/k}(b) = \mathrm{N}_{L/k}\big(\mathrm{N}_{K/L}(c)\big)\,\mathrm{N}_{L/k}(b) \\ &= \mathrm{N}_{L/k}\big(\mathrm{N}_{K/L}(c)b\big) \in \mathrm{N}_{L/k}[A_L]. \end{aligned}$$

∎

Observamos ahora que si K/k es una extensión en una formación, entonces existe una máxima extensión abeliana L de k contenida en K. En efecto, el producto de extensiones abelianas es claramente abeliano, luego basta tomar el producto de todas las extensiones abelianas de k contenidas en K.

Teorema 16.30 *Sea K/k una extensión en una formación de clases y sea L la mayor extensión abeliana de k contenida en K. Entonces el grupo de normas de K/k es el mismo que el de L/k. La extensión K/k es abeliana si y sólo si $|A_k : \mathrm{N}_{K/k}[A_K]| = |K : k|$.*

Demostración: Sea E una extensión normal de k que contenga a K. El teorema anterior implica que

$$a \in \mathrm{N}_{K/k}[A_K] \quad \text{si y sólo si} \quad \left(\frac{E/k}{a}\right) \in G(E/K)G'(E/k) \,/\, G'(E/k).$$

El grupo $G(E/K)G'(E/k)$ se corresponde con un cuerpo $k \subset L' \subset K$ y, como el cociente $G(E/k) \,/\, G(E/K)G'(E/k)$ es abeliano, de hecho $L' \subset L$.

Por otro lado $G'(E/k) \subset G(E/L)$ (porque L/k es abeliana) y ciertamente $G(E/K) \subset G(E/L)$, luego $G(E/K)G'(E/k) \subset G(E/L)$ y así $L = L'$. Aplicando de nuevo el teorema anterior llegamos a que

$$a \in \mathrm{N}_{K/k}[A_K] \quad \text{si y sólo si} \quad \left(\frac{E/k}{a}\right) \in G(E/L) \,/\, G'(E/k)$$

$$\text{si y sólo si} \quad a \in N_{L/k}[A_L].$$

Si K/k es abeliana entonces el isomorfismo de Artin hace corresponder el grupo $A_k/\,\mathrm{N}_{K/k}[A_K]$ con el grupo de Galois $G(K/k)$, luego se tiene la igualdad de índices del enunciado. Si se da dicha igualdad, por la parte anterior tenemos que $|L : k| = |K : k|$, luego ciertamente $K = L$ y K/k es abeliana. ∎

Definición 16.31 Si k es un cuerpo de una formación de clases, usaremos la notación $S \leftrightarrow K$ para indicar que K es una extensión abeliana de k y $S = \mathrm{N}_{K/k}[A_k]$. En tal caso diremos que K es el *cuerpo de clases* de S o que S es el *grupo de clases* de K.

Las propiedades básicas de los cuerpos de clases se prueban sin dificultad en el contexto general:

Teorema 16.32 *Sea k un cuerpo en una formación de clases (con grupo de Galois G). Entonces la relación $S \leftrightarrow K$ biyecta los grupos de normas de k con las extensiones abelianas de k. Además se cumplen las propiedades siguientes:*

a) Si $S_1 \leftrightarrow K_1$ y $S_2 \leftrightarrow K_2$, entonces $S_1 \le S_2$ si y sólo si $K_2 \subset K_1$.

b) Si $S_1 \leftrightarrow K_1$ y $S_2 \leftrightarrow K_2$, entonces $S_1 \cap S_2 \leftrightarrow K_1K_2$.

c) Si $S \leftrightarrow K$ y $\sigma \in G$ entonces $S^\sigma \leftrightarrow K^\sigma$ (sobre k^σ).

d) Si $k \subset E$ y $S \leftrightarrow K$ (sobre E) entonces $\mathrm{N}_{E/k}^{-1}(S) \leftrightarrow EK$ (sobre E).

e) Todo subgrupo de A_k que contiene un grupo de normas es un grupo de normas.

DEMOSTRACIÓN: Supongamos que K_1 y K_2 son cuerpos de clases de un mismo grupo S. Entonces $K = K_1K_2$ es una extensión abeliana de k, y el teorema 16.29, tomando como L bien K_1 o bien K_2 afirma que

$$a \in \mathrm{N}_{L/k}[A_L] \quad \text{si y sólo si} \quad \left(\frac{K/k}{a}\right) \in G(K/L).$$

Puesto que $\mathrm{N}_{L/k}[A_L] = S$ en ambos casos, la suprayectividad del símbolo de Artin implica que $G(K/K_1) = G(K/K_2)$, luego $K_1 = K_2$.

Si $K_2 \subset K_1$ es claro que $S_1 \leq S_2$. Esto es la mitad de a). De aquí se sigue la mitad de b): Si S es el grupo de normas del producto K_1K_2 entonces $S \leq S_1 \cap S_2$. Recíprocamente si $a \in S_1 \cap S_2$ entonces $\left(\frac{K_1/k}{a}\right) = 1$ y $\left(\frac{K_2/k}{a}\right) = 1$. El teorema 16.24 implica que

$$\left(\frac{K_1K_2/k}{a}\right) \in G(K_1K_2/K_1) \cap G(K_1K_2/K_2) = 1.$$

Esto significa que $a \in S$. Ahora tenemos probado b) y de aquí se sigue inmediatamente a).

Comprobar la propiedad c) es una simple rutina.

Veamos la propiedad e): Si $S_1 \leq S$ y $S_1 \leftrightarrow K$, el isomorfismo de Artin $A_k/S_1 \cong G(K/k)$ hace corresponder S con un subgrupo de $G(K/k)$, que será de la forma $G(K/L)$ para una cierta extensión (abeliana) L de k. Concretamente tenemos que $a \in S$ si y sólo si $\left(\frac{K/k}{a}\right) \in G(K/L)$. El teorema 16.30 prueba que $S = \mathrm{N}_{L/k}[A_L]$.

Sólo falta la propiedad d). Tenemos que EK es la menor extensión L de E tal que $K \subset L$. Por otra parte, una extensión L de E cumple $K \subset L$ si y sólo si $\mathrm{N}_{L/k}[A_L] \subset S$ (si se cumple esta segunda inclusión entonces K está contenido en el cuerpo de clases de $\mathrm{N}_{L/k}[A_L]$, que está contenido en L).

A su vez esto equivale a que $\mathrm{N}_{L/E}[A_L] \subset \mathrm{N}_{E/k}^{-1}(S)$. Por lo tanto EK es la menor extensión L de E tal que $\mathrm{N}_{L/E}[A_L] \subset \mathrm{N}_{E/k}^{-1}(S)$.

La propiedad e), ya probada, implica que $\mathrm{N}_{E/k}^{-1}(S)$ es un grupo de normas, luego tiene un cuerpo de clases $C \subset EK$. Pero la minimalidad de EK respecto a la propiedad anterior implica que de hecho $C = EK$. ∎

El teorema de existencia caracteriza los grupos de normas en términos topológicos. Para formularlo en términos de formaciones debemos introducir una topología en los módulos A_k. Esto nos lleva a la noción de formación topológica:

Definición 16.33 Una *formación topológica* es una formación en la que para cada cuerpo K, el módulo A_K tiene asociada una topología de modo que se cumpla:

a) Para todo cuerpo K, el módulo A_K es un grupo topológico, es decir, el producto y la aplicación $a \mapsto a^{-1}$ son continuas.

b) Si K/k es una extensión entonces la topología de A_k es la inducida por la topología de A_K.

c) Si σ es un elemento del grupo de Galois de la formación y K es un cuerpo entonces el producto $\sigma : A_K \longrightarrow A_{K^\sigma}$ es una aplicación continua.

Es obvio que toda formación local es una formación topológica. También es claro que las aplicaciones consideradas en el apartado c) son de hecho homeomorfismos, ya que sus inversas son también continuas por el mismo apartado. Las normas $\mathrm{N}_{K/k} : A_K \longrightarrow A_k$ son continuas, pues son producto de un número finito de aplicaciones continuas. Finalmente notamos que si K/k es una extensión entonces A_k es cerrado en A_K, pues es el conjunto de elementos de A_K invariantes por un número finito de aplicaciones continuas.

En este contexto el teorema de existencia se puede enunciar como que todo subgrupo abierto de índice finito en A_k tiene un cuerpo de clases. Vamos a dar axiomas suficientes para que una formación topológica satisfaga el teorema de existencia. El primero es el siguiente:

Axioma III a): *Para cada extensión K/k, la norma $\mathrm{N}_{K/k} : A_K \longrightarrow A_k$ tiene imagen cerrada y núcleo compacto.*

Es fácil probar que las formaciones locales satisfacen este axioma. En efecto, si K/k es una extensión finita separable de cuerpos locales y $a \in K$, tomando valores absolutos en una extensión de Galois de k que contenga a K vemos que $|\mathrm{N}_{K/k}(a)| = |a|^n$, con $n = |K : k|$. Por lo tanto, si C es un subconjunto compacto de k se cumple que $\mathrm{N}_{K/k}^{-1}[C]$ es cerrado y acotado en K, luego es compacto. Si hacemos $C = 1$ tenemos la compacidad del núcleo de la norma.

Para probar que la imagen es cerrada tomamos una sucesión en dicha imagen convergente a un elemento no nulo de k. La sucesión estará contenida en un compacto C, luego será la imagen de una sucesión en el compacto $\mathrm{N}_{K/k}^{-1}[C]$, la cual tendrá una subsucesión convergente a un elemento de $\mathrm{N}_{K/k}^{-1}[C]$, luego la sucesión de partida tendrá una subsucesión convergente a la norma de dicho elemento, luego su límite será una norma.

Si una formación de clases satisface este axioma III a) entonces los grupos de normas, al tener índice finito, son abiertos. Esto es el recíproco del teorema de existencia. Veremos que este teorema está muy relacionado con la divisibilidad infinita de los grupos de normas universales D_k. De momento podemos probar lo siguiente:

Teorema 16.34 *Si K/k es una extensión en una formación topológica que satisfaga el axioma III a) entonces $\mathrm{N}_{K/k}[D_K] = D_k$.*

Demostración: La transitividad de normas implica que los elementos de $\mathrm{N}_{K/k}[D_K]$ son normas para cualquier extensión de k (pues toda extensión de k está contenida en una extensión de K). Por lo tanto $\mathrm{N}_{K/k}[D_K] \subset D_k$. Para

probar la inclusión inversa tomamos $a \in D_k$. Para cada extensión L/K definimos $T_L = \mathrm{N}_{L/K}[A_L] \cap \mathrm{N}_{K/k}^{-1}[\{a\}]$. Basta probar que la intersección de todos los conjuntos T_L es no vacía, pues dicha intersección es $D_K \cap \mathrm{N}_{K/k}^{-1}[\{a\}]$.

Cada T_L es no vacío, pues a es una norma universal, luego existe un $b \in A_L$ tal que $\mathrm{N}_{L/k}(b) = a$, y entonces $\mathrm{N}_{L/K}(b) \in T_L$. Además los conjuntos T_L tienen la propiedad de la intersección finita, pues si L'/L es una extensión entonces $T_{L'} \subset T_L$.

Por último, el axioma III a) implica que cada T_L es la intersección de un cerrado y un compacto, luego es un compacto. Así pues, la intersección total es no vacía. ∎

El axioma siguiente reduce la divisibilidad infinita del grupo de normas universales a una propiedad más técnica pero más fácil de probar en la práctica.

Axioma III b): *Para cada primo p existe un cuerpo L_p tal que, para todo cuerpo k que contenga a L_p, la aplicación $A_k \longrightarrow A_k$ dada por $a \mapsto a^p$ tiene núcleo compacto y su imagen contiene a D_k.*

En el caso de las formaciones locales el núcleo de la aplicación $a \mapsto a^p$ es finito, luego compacto. La segunda propiedad que se exige es que para todo cuerpo k suficientemente grande toda norma universal de k tenga raíz p-ésima en A_k. En todos los casos particulares de interés, la condición "suficientemente grande" significa que k contenga a las raíces p-ésimas de la unidad. Sin embargo esta condición no tiene sentido en el contexto general de formaciones, por lo que no puede aparecer en el axioma.

De este modo, en el caso local tenemos pendiente demostrar la segunda parte del axioma III b). Ahora veamos que éste implica la divisibilidad infinita del grupo de normas universales:

Teorema 16.35 *Si k es un cuerpo de una formación topológica que satisface los axiomas III a), b), entonces $D_k^m = D_k$ para todo natural m no nulo. Además*

$$D_k = \bigcap_{m=1}^{\infty} A_k^m.$$

Demostración: Para la primera afirmación basta probar que $D_k^p = D_k$ para todo primo p. Sea K una extensión de k suficientemente grande según el axioma III b). Entonces, usando también el teorema anterior, vemos que

$$D_k = \mathrm{N}_{K/k}[D_K] \subset \mathrm{N}_{K/k}[A_K^p] = \mathrm{N}_{K/k}[A_K]^p.$$

Para cada $a \in D_k$, sea $a^{1/p}$ el conjunto de las raíces p-ésimas de a en A_k. Acabamos de probar que el conjunto $T_K = \mathrm{N}_{K/k}[A_K] \cap a^{1/p}$ es no vacío. Claramente los conjuntos T_K tienen la propiedad de la intersección finita (cuando K varía en las extensiones de k) y son compactos porque el grupo de normas es cerrado por el axioma a) y $a^{1/p}$ es compacto por el axioma b). Concluimos que la intersección de todos ellos es no vacía, pero dicha intersección es $D_k \cap a^{1/p}$, luego $a \in D_k^p$.

De la parte ya probada se sigue inmediatamente la inclusión $D_k \subset \bigcap_{m=1}^{\infty} A_k^m$. Para probar la inclusión opuesta tomamos un elemento a de la intersección y consideramos una extensión K/k. Sea $m = |K : k|$. Entonces $a = b^m = \mathrm{N}_{K/k}(b)$, para un cierto $b \in A_k$, luego $a \in D_k$. ∎

El último axioma nos dará la conexión entre todo esto y el teorema de existencia:

Axioma III c): *Para cada cuerpo k existe un subgrupo compacto U_k de A_k tal que todo subgrupo abierto de índice finito en A_k que contiene a U_k es un grupo de normas.*

Llamaremos Axioma III a la conjunción de los tres axiomas III a), b), c).

En una formación local el axioma III c) se satisface tomando como grupo U_k el grupo de las unidades de k. En efecto, tenemos la sucesión exacta

$$1 \longrightarrow U_k \longrightarrow k^* \longrightarrow \mathbb{Z} \longrightarrow 0,$$

determinada por la factorización $k^* = U_k \times \langle\pi\rangle$, donde π es un primo en k. De ella se desprende que los subgrupos de índice finito en k^* que contienen a U_k se corresponden con los subgrupos no triviales de $\mathbb{Z}$, luego son los subgrupos $H_n = U_k \times \langle\pi^n\rangle$, para cada natural n no nulo. Es inmediato comprobar que H_n es el grupo de normas de la extensión no ramificada de grado n.

El teorema principal es el siguiente:

Teorema 16.36 (Teorema de existencia abstracto) *Si k es un cuerpo de una formación topológica que satisface los axiomas I, II y III entonces los grupos de normas de k son exactamente los subgrupos abiertos de índice finito en A_k.*

Demostración: Ya sabemos que los grupos de normas son abiertos y de índice finito. Sea ahora H un grupo en estas condiciones. Si $|A_k : H| = m$ entonces es claro que $D_k \subset A_k^m \subset H$. Si N recorre los grupos de normas de k, tenemos que

$$\bigcap_N (N \cap U_k) = D_k \cap U_k \subset H,$$

donde U_k es el grupo compacto dado por el axioma III c).

Los grupos $N \cap U_k$ son compactos y H es abierto, luego[2] existe un N tal que $N \cap U_k \subset H$.

El grupo $N \cap H$ es abierto y de índice finito (pues tanto N como H lo son), y el grupo $U_k(N \cap H)$ es abierto, de índice finito y contiene a U_k, luego por el axioma III c) es un grupo de normas. Entonces $N \cap (U_k(N \cap H))$ es también un grupo de normas y está contenido en H. En efecto: todo elemento de la intersección es de la forma $ab \in N$, con $a \in U_k$ y $b \in N \cap H$, luego

[2]Esto es un resultado topológico general, pero vamos a probarlo: Tomando complementarios, los abiertos $A_k \setminus (N \cap U_k)$ cubren el compacto $(A_k \setminus H) \cap U_k$, luego podemos extraer un subcubrimiento finito. Como la intersección de grupos de normas es un grupo de normas existe un N tal que $(A_k \setminus H) \cap U_k \subset A_k \setminus (N \cap U_k)$, luego $N \cap U_k \subset H$.

$a \in N \cap U_k \subset H$ y también $ab \in H$. Así pues H es un grupo de normas, ya que contiene un grupo de normas. ∎

En definitiva, con este planteamiento hemos reducido el teorema de existencia para formaciones locales a probar el resultado siguiente:

> (∗) *Si k es un cuerpo local que contiene a las raíces p-ésimas de la unidad, entonces todas las normas universales de k tienen raíz p-ésima en k.*

Estudiaremos este problema en la sección siguiente.

16.5 El teorema de existencia local

Para probar el teorema de existencia en las formaciones locales generalizaremos la teoría de Kummer que estudiamos en el capítulo VII, a la vez que aprovechamos para presentarla en términos de cohomología.

Cuerpos de Kummer En general, un *cuerpo de Kummer* de grado n es un cuerpo k cuya característica no divide a n y que contiene a las raíces n-simas de la unidad. Éstas forman un grupo cíclico de orden n al que llamaremos R_n.

En lo sucesivo fijaremos una raíz n-sima primitiva ω e identificaremos R_n con $\mathbb{Z}/n\mathbb{Z}$ mediante el isomorfismo $\omega^m \leftrightarrow [m]$. Así $\mathbb{Z}/n\mathbb{Z} \le k^*$.

Sea S la clausura separable de k y consideremos la sucesión exacta

$$1 \longrightarrow R_n \longrightarrow S^* \longrightarrow S^* \longrightarrow 1,$$

donde la tercera flecha representa al homomorfismo $x \mapsto x^n$. Ahora nos apoyaremos en que todos los resultados de cohomología de grupos finitos que hemos visto valen también para grupos infinitos si nos restringimos a índices positivos y cambiamos la definición de H^0 de modo que $H^0(G, A) = A^G$ (ver los comentarios finales de la sección 14.2). Si $G = G(S/k)$ tenemos la sucesión exacta $H^0(G, S^*) \longrightarrow H^1(G, R_n) \longrightarrow H^1(G, S^*)$.

El primer homomorfismo puede verse como $\delta^* : k^* \longrightarrow \mathrm{Hom}(G, R_n)$. Recordando la construcción de los homomorfismos de conexión, la imagen de un $b \in k^*$ es el homomorfismo χ_b calculado como sigue: Consideramos el cociclo asociado a b, que es $1 \mapsto b$; le calculamos una antiimagen por la aplicación inducida por $x \mapsto x^n$, que es la cocadena $1 \mapsto \sqrt[n]{b}$; calculamos la cofrontera de esta cocadena, que es la cofrontera $\sigma \mapsto \sigma\big(\sqrt[n]{b}\big)/\sqrt[n]{b} \in R_n$; calculamos una antiimagen de esta cofrontera por la aplicación inducida por la inclusión $R_n \longrightarrow S^*$, que es ella misma. Así pues

$$\chi_b(\sigma) = \frac{\sigma\big(\sqrt[n]{b}\big)}{\sqrt[n]{b}},$$

donde $\sqrt[n]{b}$ es cualquier raíz n-sima de b. Es fácil comprobar que $\chi_b(\sigma)$ no depende de la elección de la raíz (aunque esto ya lo garantiza el hecho de que δ^* está bien definido).

En particular observamos que $\chi_b(\sigma) = 1$ si y sólo si $\sigma\big(\sqrt[n]{b}\big) = \sqrt[n]{b}$, luego el núcleo de χ_b es $G\big(S/k\big(\sqrt[n]{b}\big)\big)$. Por lo tanto χ_b es un homomorfismo continuo.

La aplicación $H^1(G, R_n) \longrightarrow H^1(G, S^*)$ es simplemente la inclusión inducida por la inclusión $R_n \longrightarrow S^*$. Si $\chi \in \mathrm{Hom}(G, R_n)$ es un homomorfismo continuo, es decir, si su núcleo es de la forma $G(S/K)$ para una cierta extensión (claramente finita) de k, entonces, visto como cociclo en $H^1(G, S^*)$, induce un cociclo en $H^1(K/k) = 1$ dado por $\chi\big(\sigma G(S/K)\big) = \chi(\sigma)$. Por lo tanto existe un $x \in S^*$ tal que $\chi(\sigma) = \sigma(x)/x$ para todo σ,. Esto mismo muestra que χ es también una cofrontera en $H^1(G, S^*)$, luego está en la imagen de δ^*.

En otras palabras, la imagen de $\delta^* : k^* \longrightarrow \mathrm{Hom}(G, R_n)$ está formada exactamente por los homomorfismos continuos. Si identificamos

$$R_n = \mathbb{Z}/n\mathbb{Z} \cong \langle 1/n\rangle \leq \mathbb{Q}/\mathbb{Z},$$

entonces la imagen de δ^* se identifica con un subgrupo de $G(S/k)^*$, el formado por todos los caracteres cuya imagen está contenida en $\langle 1/n\rangle$. Tenemos así un homomorfismo $\delta^* : k^* \longrightarrow G(S/k)^*$ cuya imagen es la unión de todos los grupos $G(K/k)^*$ con $|K : k| \,\big|\, n$.

Por otra parte, $\chi_b = 1$ si y sólo si $\sigma\big(\sqrt[n]{b}\big) = \sqrt[n]{b}$ para todo $\sigma \in G(S/k)$, o sea, si y sólo si $\sqrt[n]{b} \in k$ o, equivalentemente, si $b \in k^{*n}$. Por consiguiente tenemos un monomorfismo

$$k^*/k^{*n} \longrightarrow G(S/k)^*.$$

El símbolo de Hilbert Ahora introducimos el símbolo de Hilbert en el contexto general de los cuerpos locales. Conviene considerar primero otro concepto más general:

Definición 16.37 Sea k un cuerpo local. Sea S una clausura separable de k. Para cada $a \in k^*$ y cada $\chi \in G(S/k)^*$ definimos

$$(a, \chi) = -\operatorname{Inv}_k\big([a] \cup \delta^*(\chi)\big) \in \mathbb{Q}/\mathbb{Z}.$$

La fórmula (16.5) nos da la interpretación de este símbolo y nos muestra, de hecho, que determina al símbolo de Artin de k. En efecto, se cumple

$$(a, \chi) = \chi\Big(\Big(\frac{k}{a}\Big)\Big).$$

También es claro que (a, χ) es bilineal. Si k es un cuerpo de Kummer podemos considerar el *símbolo de Hilbert,* dado por

$$(a, b) = (a, \chi_b) = \chi_b\Big(\Big(\frac{k}{a}\Big)\Big) = \frac{1}{\sqrt[n]{b}}\left(\frac{k\big(\sqrt[n]{b}\big)/k}{a}\right) \in R_n.$$

Este símbolo determina el símbolo de Artin de todas las extensiones de k de grado divisor de n. Observamos que el papel de a y b en (a, b) es asimétrico pues, mientras a representa realmente a un elemento de k^*, en realidad b determina un

carácter de $G(S/k)$. Por ello resulta especialmente notable el teorema siguiente, que nos da una caracterización simétrica en términos de un producto exterior.

Dados $a,\ b \in k^*$, podemos considerar $\chi_a,\ \chi_b \in H^1\big(G(k(\sqrt[n]{a},\ \sqrt[n]{b})/k), R_n\big)$, con lo que podemos formar el producto

$$\chi_a \cup \chi_b \in H^2((G(k(\sqrt[n]{a},\ \sqrt[n]{b})/k), R_n \otimes R_n).$$

A través de la identificación $R_n = \mathbb{Z}/n\mathbb{Z}$ podemos identificar $R_n \otimes R_n = R_n$ y la inclusión $R_n \subset k^*$ nos permite considerar que $\chi_a \cup \chi_b \in H^2\big(k(\sqrt[n]{a},\ \sqrt[n]{b})/k\big)$.

Teorema 16.38 *En las condiciones anteriores, si $a,\ b \in K^*$ se cumple*

$$(a, b) = \mathrm{Inv}_k(\chi_a \cup \chi_b).$$

Demostración: Según las definiciones que hemos adoptado,

$$(a, b) = (a, \chi_b) = -\mathrm{Inv}_k\big([a] \cup \delta^*(\chi_b)\big),$$

luego basta probar que $-[a] \cup \delta^*(\chi_b) = \chi_a \cup \chi_b$. Para ello calcularemos explícitamente ambos productos exteriores. Para simplificar la notación representaremos todos los módulos aditivamente, incluidos los grupos multiplicativos de los cuerpos.

Llamemos $K = k(\sqrt[n]{a},\ \sqrt[n]{b})$. En principio $\chi_b : G(K/k) \longrightarrow R_n$, pero podemos considerar que $\chi_b : G(K/k) \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

Sea $\bar\chi_b : G(K/k) \longrightarrow \mathbb{Z}$ tal que $\chi_b(\sigma) = \bar\chi_b(\sigma) + n\mathbb{Z}$. Para considerar a χ_b con imágenes en $\mathbb{Q}/\mathbb{Z}$ hemos de pasar a la aplicación $(1/n)\chi_b$. Ahora estamos en condiciones de aplicar la fórmula (16.3), según la cual

$$\delta^*(\chi_b)(\sigma, \tau) = \frac{1}{n}\big(\bar\chi_b(\sigma) + \bar\chi_b(\tau) - \bar\chi_b(\sigma\tau)\big).$$

Con notación aditiva, $a = n\sqrt[n]{a}$ y, según el teorema 16.11,

$$\big([a] \cup \delta^*(\chi_b)\big)(\sigma, \tau) = a\delta^*(\chi_b)(\sigma, \tau) = \sqrt[n]{a}\big(\bar\chi_b(\sigma) + \bar\chi_b(\tau) - \bar\chi_b(\sigma\tau)\big) \in K^*.$$

Por otro lado, también según 16.11 (y teniendo en cuenta que la acción de G sobre R_n es trivial) tenemos

$$\begin{aligned}(\chi_a \cup \chi_b)(\sigma, \tau) &= -(\chi_b \cup \chi_a)(\sigma, \tau) = \chi_b(\sigma) \otimes \chi_a(\tau) = \bar\chi_b(\sigma) \otimes \bar\chi_a(\tau)\\ &= \bar\chi_b(\sigma)\bar\chi_a(\tau) = \bar\chi_b(\sigma)\sqrt[n]{a}\,(\tau - 1)\\ &= \sqrt[n]{a}\,\bar\chi_b(\sigma)\tau - \sqrt[n]{a}\,\bar\chi_b(\sigma) \in R_n \subset K^*.\end{aligned}$$

Por lo tanto

$$\big([a] \cup \delta^*(\chi_b)\big) + (\chi_a \cup \chi_b)(\sigma, \tau) = \sqrt[n]{a}\,\bar\chi_b(\sigma)\tau - \sqrt[n]{a}\,\bar\chi_b(\sigma) - \sqrt[n]{a}\,\bar\chi_b(\sigma\tau),$$

y esto es la cofrontera de la cocadena $\sqrt[n]{a}\,\bar\chi_b(\sigma)$, luego al tomar clases de cohomología concluimos que $-[a] \cup \delta^*(\chi_b) = \chi_a \cup \chi_b$. ∎

A partir de aquí es muy fácil derivar las propiedades del símbolo de Hilbert:

Teorema 16.39 *Sea k un cuerpo local que además sea un cuerpo de Kummer de grado n. Entonces*

a) $(aa', b) = (a, b)(a', b)$, $(a, bb') = (a, b)(a, b')$.

b) $(a, b) = (b, a)^{-1}$.

c) $(a, b) = 1$ *si y sólo si* $a \in \mathrm{N}\big[k[\sqrt[n]{b}]\big]$.

d) $(a, b) = 1$ *para todo* $a \in k^*$ *si y sólo si* $b \in k^{*n}$.

Demostración: La propiedad a) es evidente. La propiedad b) es consecuencia del teorema anterior y de la anticonmutatividad del producto exterior. Para probar c) observamos que $(a, b) = 1$ si y sólo si

$$\frac{1}{\sqrt[n]{b}}\left(\frac{k(\sqrt[n]{b})/k}{a}\right)(\sqrt[n]{b}) = 1,$$

lo cual equivale a que

$$\left(\frac{k(\sqrt[n]{b})/k}{a}\right) = 1,$$

y, por consiguiente, a que $a \in \mathrm{N}\big[k[\sqrt[n]{b}]\big]$.

Para la propiedad d) notamos que $(a, b) = 1$ si y sólo si

$$\chi_b\Big(\left(\frac{k(\sqrt[n]{b})/k}{a}\right)\Big) = 1.$$

Si esto ocurre para todo a, entonces $\chi_b = 1$, luego $b \in k^{*n}$. El recíproco es obvio. ∎

Con esto podemos probar:

Teorema 16.40 *Sea k un cuerpo local que contenga a las raíces n-simas de la unidad, donde n no es divisible entre la característica de k. Si $a \in k^*$ es una norma para todas las extensiones cíclicas de k de orden divisor de n (en particular si a es una norma universal) entonces $a \in k^{*n}$.*

Demostración: Aplicamos varias veces el teorema anterior: por c) tenemos que $(a, b) = 1$ para todo $b \in k^*$, luego por b) también $(b, a) = 1$ y por d) concluimos que $a \in k^{*n}$. ∎

Esto prueba la afirmación $(*)$ de la pág. 429 para primos distintos de la característica de k. En particular tenemos $(*)$, y por consiguiente el teorema de existencia, para cuerpos locales de característica 0. Para cuerpos de característica prima p sólo falta probar lo siguiente

> $(**)$*Si k es un cuerpo local de característica prima p, entonces las normas universales de k tienen raíz p-ésima en k.*

La prueba de $(**)$ requiere ideas bastante diferentes de las que estamos utilizando. En el apéndice B damos una demostración que supone conocidas las propiedades básicas de las formas diferenciales y los residuos en cuerpos de series formales de potencias.

La topología de clases Observemos ahora que el teorema de existencia permite probar de hecho que los grupos de normas universales en las formaciones locales son triviales. En efecto, si k es un cuerpo local y $\mathfrak{p}$ es su ideal primo, los grupos $U_n = 1 + \mathfrak{p}^n$ forman una base de entornos abiertos y cerrados de 1. Obviamente un subgrupo de k^* que contenga a un grupo U_n es abierto (es unión de clases módulo U_n, que son abiertas) y el recíproco es obvio. Por lo tanto un subgrupo de índice finito de k^* es un grupo de normas si y sólo si contiene un U_n. No obstante hay que tener presente que los propios grupos U_n no son de índice finito, luego no son grupos de normas. En efecto, si llamamos U_0 al grupo de las unidades de k, entonces $U_n \leq U_0$ y U_0 tiene índice infinito en k^*, pues $k^* = U_0 \times \langle\pi\rangle$, donde π es un primo en k.

Los ejemplos más simples de grupos de normas son los grupos de la forma $V_{n,m} = U_n \times \langle\pi^m\rangle$. En efecto, la compacidad de U_0 obliga a que los índices $|U_0 : U_n|$ sean finitos (en otro caso las clases módulo U_n serían un cubrimiento abierto sin subcubrimientos finitos), luego

$$k^*/V_{n,m} \cong (U_0/U_n) \times \big(\langle\pi\rangle \,/\, \langle\pi^m\rangle\big)$$

tiene orden $m|U_0 : U_n|$.

Obviamente la intersección de todos los grupos $V_{n,m}$ es trivial, luego lo mismo ocurre con la intersección de todos los grupos de normas. Esto equivale a la inyectividad del símbolo de Artin de un cuerpo local. Más aún:

Teorema 16.41 *Si k es un cuerpo local, entonces el grupo de normas universales D_k es trivial, luego el homomorfismo de Artin es un monomorfismo $\omega_k : k^* \longrightarrow G(A_k/k)$. Además es continuo y su imagen es densa.*

Demostración: Acabamos de probar que el núcleo de ω_k es trivial. La continuidad se debe a que un entorno básico de 1 en $G(A_k/k)$ es un grupo $G(A_k/K)$, donde K es una extensión abeliana finita de k, y su antiimagen por ω_k es el núcleo del homomorfismo $\omega_k : k^* \longrightarrow G(K/k)$, es decir, el grupo de normas $\mathrm{N}[K]$, que es abierto.

Si $\beta \in A_k$, $\beta \notin k$, sea L/k una extensión finita tal que $\beta \in L$. Por la suprayectividad del homomorfismo de Artin para extensiones finitas existe un $\alpha \in k^*$ tal que

$$\left(\frac{L/k}{\alpha}\right)(\beta) \neq \beta.$$

Por lo tanto $\left(\frac{k}{\alpha}\right)(\beta) \neq \beta$, con lo que hemos probado que el cuerpo fijado por $\omega_k[k^*]$ es igual a k. Esto significa que $\omega_k[k^*]$ es denso en $G(A_k/k)$. ∎

Si k es un cuerpo local, ahora podemos definir la *topología de clases* en k^* como la topología que convierte en homeomorfismo al isomorfismo de Artin, es decir, la que tiene como abiertos a las antiimágenes de los abiertos de $G(A_k/k)$.

Así mismo es fácil probar para cuerpos locales arbitrarios los hechos que en el capítulo XII demostramos para cuerpos p-ádicos. En particular, la topología de clases coincide con la métrica en el grupo de unidades U de k y es el producto de las topologías inducidas en U y $\langle\pi\rangle$ (donde π es un primo en k). En particular el teorema 12.21 es válido para cuerpos locales arbitrarios.

Capítulo XVII

La teoría global

Aquí aplicaremos la teoría general que hemos estudiado en los capítulos precedentes al caso de los cuerpos numéricos, es decir, a la formación $\mathbb{A}$ de los cuerpos numéricos, a la formación J de los grupos de elementos ideales y a la formación C de los grupos de clases de elementos ideales. En el capítulo XV vimos que las tres son formaciones de cuerpos. Si el interés del enfoque cohomológico de la teoría local de cuerpos de clases consistía en que nos permite construir explícitamente el isomorfismo de Artin, sin referencias a la teoría global, el interés en el caso global reside en que la cohomología muestra claramente la conexión entre el símbolo de Artin global y los símbolos locales.

La conexión entre las tres formaciones que nos ocupan viene dada por las sucesiones exactas

$$0 \longrightarrow K^* \longrightarrow J_K \longrightarrow C_K \longrightarrow 0,$$

para cada cuerpo numérico K, que se reúnen en una sola:

$$0 \longrightarrow \mathbb{A} \longrightarrow J \longrightarrow C \longrightarrow 0.$$

Estudiaremos en primer lugar la cohomología de J. Veremos que J no es una formación de clases, pero los resultados que obtendremos se trasladarán a C a través de la sucesión exacta anterior, y ésta sí resultará ser una formación de clases.

17.1 La cohomología de los elementos ideales

Si K/k es una extensión normal de cuerpos numéricos y G su grupo de Galois, usaremos la notación $H^n_J(K/k) = H^n(G, J_K)$. Vamos a expresar estos grupos en función de los grupos de cohomología de las extensiones locales asociadas. Sea E un conjunto finito de primos de k que contenga a los primos arquimedianos. Identificaremos a E con el conjunto de los primos de K que dividen a los primos de E. El grupo J_K es la unión de todos los subgrupos $J_E = \prod_{\mathfrak{p}\in E} K^*_\mathfrak{p} \times \prod_{\mathfrak{p}\notin E} U_\mathfrak{p}$. Investigaremos primero la cohomología de estos subgrupos. En primer lugar tenemos el teorema siguiente:

Teorema 17.1 *Sea G un grupo finito y $\{M_i\}$ una familia de G-módulos. Entonces para todo entero n se cumple*

$$H^n(G, \prod_i M_i) \cong \prod_i H^n(G, M_i).$$

DEMOSTRACIÓN: Sea $\mathcal{C}$ una resolución completa de G. Es claro que

$$\pi_\# = \prod_i \pi_{i\#} : \mathrm{Hom}_G(\mathcal{C}, \prod_i M_i) \longrightarrow \prod_i \mathrm{Hom}_G(\mathcal{C}, M_i)$$

es un isomorfismo de complejos, donde el operador cofrontera del complejo de la derecha es $\prod_i \partial_i$. La conclusión es evidente. ∎

Para aplicar el teorema a nuestro caso definimos

$$M_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} K^*_\mathfrak{P} \quad \text{si } \mathfrak{p} \in E \quad \text{y} \quad M_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} U_\mathfrak{P} \quad \text{si } \mathfrak{p} \notin E.$$

Es claro que $M_\mathfrak{p}$ es un G-submódulo de J_E y que J_E es el producto de todos ellos. Por lo tanto podemos concluir que

$$\bar{\pi}_\# : H^n(G, J_E) \longrightarrow \prod_\mathfrak{p} H^n(G, M_\mathfrak{p})$$

es un isomorfismo de grupos. Ahora reduciremos los grupos de cohomología de los módulos $M_\mathfrak{p}$ a los de sus factores. También lo haremos a partir de un resultado general.

Sea G un grupo abeliano y S un subgrupo de G. Sea N un S-módulo y $M = N \otimes_S \mathbb{Z}[G]$. Sea $\sigma_1, \ldots, \sigma_r$ una transversal derecha de G/S (tal que $\sigma_1 = 1$). Es claro que $\{\sigma_i\}$ es una base de $\mathbb{Z}[G]$ como S-módulo izquierdo, luego el teorema 14.10 nos da que

$$M = \bigoplus_{i=1}^r N \otimes \sigma_i.$$

Cada sumando es un subgrupo abeliano y si $\sigma \in G$, entonces $u_i\sigma = su_j$ para un $\sigma \in S$ y algún índice j, luego $N \otimes u_i\sigma = N \otimes u_j$. Es claro que G permuta transitivamente los sumandos, así como que $N \otimes 1$ es un S-submódulo de M isomorfo a N.

Recíprocamente, supongamos que M es un G-módulo que como grupo abeliano se descompone en suma directa $M = \bigoplus_{i=1}^r N_i$ y cada $\sigma \in G$ permuta transitivamente los subgrupos N_i, es decir, $N_i\sigma = N_j$ para algún j y siempre existe un σ que hace corresponder un i y un j dados. Sea $S = \{\sigma \in G \mid N_1\sigma = N_1\} \leq G$. Entonces $N = N_1$ es un S-módulo y $M \cong N \otimes_S \mathbb{Z}[G]$ (se toma una transversal $\{\sigma_i\}$ y se identifica $n\sigma_i$ con $n \otimes \sigma_i$).

En cualquiera de estas dos situaciones equivalentes diremos que el G-módulo M está inducido por N. En estos términos, un G-módulo es regular según la definición 14.28 si es inducido por un 1-módulo. El teorema siguiente generaliza a 14.29 (comparar con 7.7):

Teorema 17.2 *Si M es un G-módulo inducido por un S-módulo N, entonces para todo entero n se cumple $H^n(G,M) \cong H^n(S,N)$.*

DEMOSTRACIÓN: Para una prueba rápida podemos usar los grupos de homología (lo cual es equivalente). Basta tener en cuenta los siguientes isomorfismos de complejos:

$$M \otimes_G \mathcal{C} \cong (N \otimes_S \mathbb{Z}[G]) \otimes_G \mathcal{C} \cong N \otimes_S (\mathbb{Z}[G] \otimes_G \mathcal{C}) \cong N \otimes_S \mathcal{C}.$$

Si $\mathcal{C}$ es una resolución completa de G también lo es de S, luego los grupos de homología son isomorfos. ∎

Ahora daremos una prueba alternativa del teorema anterior que muestre explícitamente el isomorfismo entre los grupos de cohomología. En primer lugar tenemos el isomorfismo de G-módulos

$$M = N \otimes_S \mathbb{Z}[G] \longrightarrow \mathrm{Hom}_S(\mathbb{Z}[G], N)$$

que a cada $m \in M$ le asigna el homomorfismo dado por $f_m(\sigma) = \pi(m\sigma)$, donde $\pi : M \longrightarrow N$ es la proyección (homomorfismo de S-módulos). Recordemos que la operación de G-módulo en $\mathrm{Hom}_S(\mathbb{Z}[G], N)$ es la dada por $(f\sigma)(x) = f(\sigma x)$.

Ahora usaremos el isomorfismo

$$\mathrm{Hom}_A\big(M, \mathrm{Hom}_B(N,R)\big) \cong \mathrm{Hom}_B(M \otimes_A N, R),$$

donde M es un A-módulo derecho, N un A-B-módulo y R un B-módulo derecho. Explícitamente es el dado por

$$f \mapsto f^*(m \otimes n) = f(m)(n).$$

En nuestro caso concreto, si $\mathcal{C}$ es una resolución completa de G, tenemos

$$\begin{aligned} \mathrm{Hom}_G(\mathcal{C}, M) &\cong \mathrm{Hom}_G\big(\mathcal{C}, \mathrm{Hom}_S(\mathbb{Z}[G], N)\big) \cong \mathrm{Hom}_S(\mathcal{C} \otimes_G \mathbb{Z}[G], N) \\ &\cong \mathrm{Hom}_S(\mathcal{C}, N). \end{aligned}$$

Es simple rutina comprobar que estos isomorfismos son realmente isomorfismos de complejos, es decir, respetan las cofronteras. Si f es una cocadena de (G,M), el primer isomorfismo la convierte en $f'(c)(\sigma) = \pi(f(c)\sigma)$, el segundo en $f''(c \otimes \sigma) = \pi(f(c)\sigma)$ y el tercero en $f'''(c) = \pi\big(f(c)\big)$. En definitiva el isomorfismo es $\pi_\#$, que induce isomorfismos entre los grupos de cohomología.

Si queremos el isomorfismo en términos de una resolución distinta $\mathcal{C}'$ para S (que no sea necesariamente una resolución de G) no tenemos más que considerar un homomorfismo $i : \mathcal{C}' \longrightarrow \mathcal{C}$ y pasar al cociclo $f^{iv}(c) = \pi(f(i^\#(c)))$, con lo que el isomorfismo es en definitiva $x \mapsto \bar{\pi}_\#\big(\mathrm{Res}_{G,S}(x)\big)$.

Calculemos el isomorfismo inverso. Si f es una cocadena de (S,N) sus antiimágenes por la cadena de isomorfismos anteriores son: $f'(c \otimes \sigma) = f(c\sigma)$, $f''(c)(\sigma) = f(c\sigma)$,

$$f'''(c) = \sum_{i=1}^{r} f(c\sigma_i^{-1}) \otimes \sigma_i = \sum_{i=1}^{r} f(c\sigma_i^{-1})\sigma_i.$$

(La última igualdad corresponde a la identificación $M = N \otimes_S \mathbb{Z}[G] = \bigoplus_{i=1}^{r} N_i$.)

Observar que si $M = \bigoplus_{i=1}^{r} N_i$ y llamamos $S_i = \{\sigma \in G \mid N_i\sigma = N_i\}$, los grupos $H^n(S_i, N_i)$ son isomorfos entre sí, pues todos ellos son isomorfos a $H^n(G, M)$. Los cálculos que hemos hecho muestran que al componer el isomorfismo $H^n(S_1, N_1) \cong H^n(G, M)$ con el isomorfismo $H^n(G, M) \cong H^n(S_i, N_i)$ obtenemos el isomorfismo $[f] \mapsto [f^\sigma]$, donde $\sigma \in G$ es cualquier elemento que cumpla $N_i = N_1\sigma$ y $f^\sigma(c) = f(c\sigma^{-1})\sigma$.

Ahora particularizamos a los G-módulos $M_\mathfrak{p}$. Si $\mathfrak{p} \notin E$ nos queda que

$$H^n(G, M_\mathfrak{p}) \cong H^n(G_\mathfrak{P}, U_\mathfrak{P}),$$

donde $\mathfrak{P}$ es un divisor cualquiera de $\mathfrak{p}$ en K y $G_\mathfrak{P} = G(K_\mathfrak{P}/k_\mathfrak{p})$. Similarmente, si $\mathfrak{p} \in E$ llegamos a que $H^n(G, M_\mathfrak{p}) \cong H^n(G_\mathfrak{P}, K_\mathfrak{P}^*) = H^n(K_\mathfrak{P}, k_\mathfrak{p})$.

Ahora bien, si el primo $\mathfrak{p}$ es no arquimediano y no ramificado, el teorema 15.17 implica que $H^n(G_\mathfrak{P}, U_\mathfrak{P}) = 1$, luego si suponemos que E contiene al menos a todos los primos arquimedianos y a todos los ramificados (que son ciertamente un número finito) hemos probado que

$$H^n(G, J_E) \cong \bigoplus_{\mathfrak{p}\in E} H^n(K_\mathfrak{P}, k_\mathfrak{p}),$$

donde se entiende que $\mathfrak{P}$ es un divisor cualquiera de $\mathfrak{p}$ en K (elegido arbitrariamente).

Además el isomorfismo es el inducido por las proyecciones $\pi_\mathfrak{P} : J_E \longrightarrow K_\mathfrak{P}^*$, para cada $\mathfrak{P} \mid \mathfrak{p} \in E$, es decir, dada una clase $x \in H^n(G, J_E)$ le asociamos las clases de cohomología $x_\mathfrak{P} = \bar{\pi}_{\mathfrak{P}\#}\big(\mathrm{Res}_{G,G_\mathfrak{P}}(x)\big) \in H^n(K_\mathfrak{P}, k_\mathfrak{p})$. Más concretamente, si $x = [f]$ y queremos calcular su imagen con la misma resolución de G (o si consideramos las resoluciones canónicas para G y $G_\mathfrak{P}$) entonces $x_\mathfrak{P}$ es la clase inducida por el cociclo $f_\mathfrak{P}(c) = f(c)_\mathfrak{P}$.

A la hora de relacionar los grupos de cohomología en extensiones distintas convendrá considerar a $H^n(G, J_E)$ como subgrupo de $\bigoplus_{\mathfrak{P}\in E} H^n(K_\mathfrak{P}, k_\mathfrak{p})$, es decir, cada $x \in H^n(G, J_E)$ está determinado por sus proyecciones $x_\mathfrak{P}$, pero teniendo en cuenta que éstas no son independientes, sino que si $\mathfrak{P}$ y $\mathfrak{Q}$ dividen a un mismo primo de k entonces $x_\mathfrak{Q} = x_\mathfrak{P}^\sigma$, donde σ es cualquier k-automorfismo que cumpla $\sigma(\mathfrak{P}) = \mathfrak{Q}$. Cada elemento de la suma directa que cumpla esta restricción determina un único elemento de $H^n(G, J_E)$.

Pasemos ahora a los grupos de cohomología de J_K. En primer lugar observemos que si $E \subset F$ entonces la inclusión $H^n(G, J_E) \longrightarrow H^n(G, J_F)$ se corresponde con la inclusión natural entre las sumas directas, pero ésta es inyectiva, luego aquélla también. De aquí que las inclusiones $H^n(G, J_E) \longrightarrow H^n(G, J_K)$ también son inyectivas, pues si un $[f]$ tiene imagen trivial, esto significa que $f = \partial g$ para una cocadena g de (G, J_K), que de hecho será una cocadena de (G, J_F) para un F suficientemente grande que contenga a E, pero entonces $[f] = 1$ en $H^n(G, J_F)$ y, como esta inclusión sí es inyectiva, concluimos que $[f]$ es trivial en $H^n(G, J_E)$. Identificando a cada $H^n(G, J_E)$ con su imagen en $H^n(G, J_K)$ es fácil ver que $H^n(G, J_K) = \bigcup_E H^n(G, J_E)$, donde E recorre los

conjuntos finitos de primos en k que contienen a los primos arquimedianos y ramificados. Ahora el teorema siguiente es inmediato:

Teorema 17.3 *Sea K/k una extensión normal de cuerpos numéricos y sea G su grupo de Galois. Entonces*

$$H^n_J(K/k) \cong \bigoplus_{\mathfrak{p}} H^n(K_{\mathfrak{P}}, k_{\mathfrak{p}}),$$

donde $\mathfrak{p}$ recorre los primos de k y $\mathfrak{P}$ es un divisor arbitrario de $\mathfrak{p}$ en K.

Si $x = [f] \in H^n_J(K/k)$ definimos $x_{\mathfrak{P}} = \bar{\pi}_{\mathfrak{P}\#}\big(\mathrm{Res}_{G,G_{\mathfrak{P}}}(x)\big) \in H^n(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ que, al igual que antes, respecto a la misma resolución de G o respecto a las resoluciones canónicas de G y $G_{\mathfrak{P}}$, está determinado por el cociclo $f_{\mathfrak{P}}(c) = f(c)_{\mathfrak{P}}$. Tenemos que $x_{\mathfrak{P}} = 1$ para casi todo primo $\mathfrak{P}$. Además, si $\mathfrak{P}$ y $\mathfrak{Q}$ dividen a un mismo primo de k y $\sigma(\mathfrak{P}) = \mathfrak{Q}$, entonces $x_{\mathfrak{Q}} = x^{\sigma}_{\mathfrak{P}}$. El grupo $H^n_J(K/k)$ es isomorfo al subgrupo de $\bigoplus_{\mathfrak{P}} H^n(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ formado por los elementos $(x_{\mathfrak{P}})$ que cumplen esta restricción.

Veamos ahora la expresión de las aplicaciones entre grupos de cohomología en términos de esta representación.

Teorema 17.4 *Sea $k \subset K \subset L$ una cadena de cuerpos numéricos con L/k normal.*

a) Si K/k es normal la inflación $\mathrm{Inf}^n_{K/k,L/k} : H^n_J(K/k) \longrightarrow H^n_J(L/k)$ está determinada por la relación $\mathrm{Inf}(x)_{\mathfrak{P}'} = \mathrm{Inf}(x_{\mathfrak{P}})$, donde $\mathfrak{P}$ es el primo de K que divide a $\mathfrak{P}'$, es decir, la inflación global es la suma directa de las inflaciones locales.

b) La restricción $\mathrm{Res}^n_{L/k,L/K} : H^n_J(L/k) \longrightarrow H^n_J(L/K)$ está determinada por la relación $\mathrm{Res}(x)_{\mathfrak{P}'} = \mathrm{Res}(x_{\mathfrak{P}'})$. es decir, la restricción global es la suma directa de las restricciones locales.

c) La transferencia $\mathrm{V}^n_{L/K,L/k} : H^n_J(L/K) \longrightarrow H^n_J(L/k)$ está determinada por la relación

$$\mathrm{V}(x)_{\mathfrak{P}'} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{V}(x_{\mathfrak{P}''}),$$

donde $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}'$ y $\mathfrak{P}''$ es cualquier divisor de $\mathfrak{P}$ en L. Más explícitamente, si $\sigma(\mathfrak{P}'') = \mathfrak{P}'$ la expresión $\mathrm{V}(x_{\mathfrak{P}''})$ es en realidad $V(x_{\mathfrak{P}''})^{\sigma} \in H^n(K_{\mathfrak{P}'}/k_{\mathfrak{p}})$.

Demostración: a) Sean $\mathcal{C}(L/k)$ y $\mathcal{C}(K/k)$ resoluciones reducidas de los grupos de Galois. Consideremos un homomorfismo $u : \mathcal{C}(L/k) \longrightarrow \mathcal{C}(K/k)$. Si $x = [f]$, por definición tenemos que $\mathrm{Inf}(x) = u^*(f) = u \circ f$, luego se cumple $\mathrm{Inf}(x)_{\mathfrak{P}'} = u \circ f \circ \pi_{\mathfrak{P}'}$. Ahora bien, como $f \in \mathrm{Hom}_{G(K/k)}(\mathcal{C}(K/k), J_K)$, de hecho $u \circ f \circ \pi_{\mathfrak{P}'}$ toma valores en $K_{\mathfrak{P}}$, luego

$$\mathrm{Inf}(x)_{\mathfrak{P}'} = u \circ f \circ \pi_{\mathfrak{P}} = u \circ f_{\mathfrak{P}} = \mathrm{Inf}\big([f_{\mathfrak{P}}]\big) = \mathrm{Inf}(x_{\mathfrak{P}}).$$

La prueba de b) es muy similar a la anterior. Veamos c).

Sean $G = G(L/k)$ y $S = G(L/K)$. Consideremos resoluciones completas $\mathcal{C}(G)$ y $\mathcal{C}(S)$ y sea $v : \mathcal{C}(G) \longrightarrow \mathcal{C}(S)$ un homomorfismo entre ellas. Para calcular la transferencia necesitamos una transversal derecha de G/S. Vamos a construir una adecuada.

Sea $G = \bigcup_{i=1}^{r} G_{\mathfrak{P}'}\sigma_i S$ una descomposición de G en clases dobles. Sea $\mathfrak{P}'_i = \sigma_i(\mathfrak{P}')$, sea $\mathfrak{P}_i$ el primo de K divisible entre $\mathfrak{P}'_i$. Podemos suponer que $\sigma_1 = 1$ y así $\mathfrak{P}'_1 = \mathfrak{P}'$.

Dado $\sigma \in G$, podemos expresarlo como $\sigma = g\sigma_i s$, donde $g \in G_{\mathfrak{P}'}$ y $s \in S$. Entonces $\sigma(\mathfrak{P}') = s\big(\sigma_i(\mathfrak{P}')\big)$, luego $\sigma(\mathfrak{P}') \mid \mathfrak{P}_i$. Esto implica que los primos $\mathfrak{P}_i$ son todos los divisores de $\mathfrak{p}$ en K.

Por otro lado, si $\mathfrak{P}_i = \mathfrak{P}_j$ entonces existe $s \in S$ tal que $\sigma_i(\mathfrak{P}') = s\big(\sigma_j(\mathfrak{P}')\big)$, luego existe $g \in G_{\mathfrak{P}'}$ tal que $\sigma_i = g\sigma_j s$ y por lo tanto $i = j$. Así pues, los primos $\mathfrak{P}_i$ son distintos dos a dos.

Sea $G_{\mathfrak{P}'} = \bigcup_{j=1}^{s} (G_{\mathfrak{P}'} \cap S^{\sigma_i^{-1}})\tau_{i,j}$ una descomposición en clases de congruencia. Veamos que los elementos $\sigma_i^{-1}\tau_{i,j}$ constituyen una transversal derecha de G/S.

En efecto, todo $\sigma \in G$ se expresa en la forma $\sigma = s\sigma_i^{-1}g$, con $s \in S$ y $g \in G_{\mathfrak{P}'}$. A su vez $g = s_1^{\sigma_i^{-1}}\tau_{i,j}$, luego $\sigma = s\sigma_i^{-1}s_1^{\sigma_i^{-1}}\tau_{i,j} = s_2\sigma_i^{-1}\tau_{i,j}$. Con igual facilidad se comprueba que los elementos $\sigma_i^{-1}\tau_{i,j}$ son no congruentes dos a dos módulo S (por la derecha).

Sea ahora $x = [f]$, donde $f \in \mathrm{Hom}_S(\mathcal{C}(S), J_L)$ es un cociclo. Entonces $\mathrm{V}(x)_{\mathfrak{P}'}$ es la clase del cociclo dado por

$$\mathrm{V}(f)_{\mathfrak{P}'}(c) = \prod_{i,j} v^*(f)^{\sigma_i^{-1}\tau_{i,j}}(c)_{\mathfrak{P}'} = \prod_{i,j} v^*(f)^{\tau_{i,j}^{\sigma_i}\sigma_i^{-1}}(c)_{\mathfrak{P}'}$$

$$= \prod_{i,j}\big(v^*(f)\big(c\sigma_i(\tau_{i,j}^{\sigma_i})^{-1}\big)\tau_{i,j}^{\sigma_i}\sigma_i^{-1}\big)_{\mathfrak{P}'} = \prod_i \sigma_i^{-1}\Big(\prod_j \tau_{i,j}^{\sigma_i}\big(v^*(f)(c\sigma_i(\tau_{i,j}^{\sigma_i})^{-1})_{\mathfrak{P}'_i}\big)\Big).$$

En total nos queda

$$\mathrm{V}(f)_{\mathfrak{P}'}(c) = \prod_i \sigma_i^{-1}\Big(\prod_j v^*(f_{\mathfrak{P}'_i})^{\tau_{i,j}^{\sigma_i}}(c\sigma_i)\Big).$$

Ahora bien, como los elementos $\tau_{i,j}$ constituyen una transversal derecha de $G_{\mathfrak{P}'}$ sobre $G_{\mathfrak{P}'} \cap S^{\sigma_i^{-1}}$ es claro que los elementos $\tau_{i,j}^{\sigma_i}$ son una transversal de $G_{\mathfrak{P}'_i}$ sobre $G_{\mathfrak{P}'_i} \cap S$, es decir, de $G(L_{\mathfrak{P}'_i}/k_{\mathfrak{p}})$ sobre $G(L_{\mathfrak{P}'_i}/K_{\mathfrak{P}_i})$. Por lo tanto

$$\mathrm{V}(f)_{\mathfrak{P}'}(c) = \prod_i \sigma_i^{-1}\big(\mathrm{V}(f_{\mathfrak{P}'_i})(c\sigma_i)\big) = \prod_i \mathrm{V}(f_{\mathfrak{P}'_i})^{\sigma_i^{-1}}(c),$$

y al tomar clases llegamos a la fórmula del enunciado. ∎

Ahora definiremos invariantes sobre los grupos de Brauer $H_J^2(*, k)$. Notemos que si K/k es una extensión normal de cuerpos numéricos, $\mathfrak{P}$ es un primo arquimediano de K y $\mathfrak{p}$ es el primo de k divisible entre $\mathfrak{P}$, entonces la extensión

$K_{\mathfrak{P}}/k_{\mathfrak{p}}$ es $\mathbb{C}/\mathbb{C}$, $\mathbb{R}/\mathbb{R}$ o $\mathbb{C}/\mathbb{R}$, con lo que $H^2(*, k_{\mathfrak{p}})$ es trivial o de orden 2, y podemos definir un único monomorfismo $\mathrm{Inv}_{k_{\mathfrak{p}}} : H^2(*, k_{\mathfrak{p}}) \longrightarrow \mathbb{Q}/\mathbb{Z}$ de forma obvia. Los resultados sobre invariantes que usaremos en virtud de la teoría local son obvios en el caso arquimediano.

Teorema 17.5 *Sea K/k una extensión normal de cuerpos numéricos. Consideremos $x \in H^2_j(K/k)$ y $\mathfrak{p}$ un primo de k. Entonces $\mathrm{Inv}_{k_{\mathfrak{p}}}(x_{\mathfrak{P}})$ es independiente de $\mathfrak{P}$ (donde $\mathfrak{P}$ es cualquiera de los divisores de $\mathfrak{p}$ en K).*

Demostración: Podemos suponer que los primos son no arquimedianos. La prueba es una comprobación rutinaria que se puede simplificar a partir de las consideraciones generales siguientes: Si C y C' son dos clausuras algebraicas de $\mathbb{Q}_p$, entonces existe un k-isomorfismo $\tau : C \longrightarrow C'$, que a su vez induce un isomorfismo $\sigma : H \longrightarrow H'$ entre los grupos de Galois. El par (σ, τ) constituye un isomorfismo de formaciones en el sentido de 15.32 y es evidente que induce isomorfismos entre todas las estructuras derivadas (grupos de cohomología, grupos de Brauer, etc.). Los invariantes locales han sido definidos algebraicamente en términos de productos exteriores, automorfismos canónicos de extensiones no ramificadas, etc., sin ningún margen de arbitrariedad, por lo que son conservados por el par (σ, τ), es decir, por el isomorfismo que éste induce entre los grupos de Brauer.

Más concretamente, si K/k es una extensión normal de cuerpos locales contenidos en C y K^τ/k^τ es su correspondiente en C' entonces σ induce un isomorfismo entre los grupos de Galois $G = G(K/k)$ y $G' = G(K^\tau/k^\tau)$ (que seguiremos llamando σ). Las resoluciones completas de estos grupos están en correspondencia biunívoca. Una resolución de G se convierte en una resolución de G' sin más que dotar a sus módulos C_n de estructura de G' módulo mediante la operación $cg' = c\sigma^{-1}(g')$ y a su vez τ induce de forma natural un isomorfismo entre los grupos $\mathrm{Hom}_G(C_n, K^*)$ y $\mathrm{Hom}_{G'}(C_n, K^{\tau *})$, que a su vez induce un isomorfismo entre los grupos $H^2(K/k)$ y $H^2(K^\tau/k^\tau)$. Según lo dicho anteriormente, este isomorfismo conserva los invariantes.

Ahora particularicemos al caso que nos ocupa. Sean K/k, $\mathfrak{p}$ y $\mathfrak{P}$ según el enunciado. Cualquier otro divisor de $\mathfrak{p}$ en K es de la forma $\mathfrak{P}' = \tau(\mathfrak{P})$, para un cierto $\tau \in G(K/k)$. Tenemos que τ se extiende a un $k_{\mathfrak{p}}$-isomorfismo entre $K_{\mathfrak{P}}$ y $K_{\mathfrak{P}'}$ que a su vez se extiende a un $k_{\mathfrak{p}}$-isomorfismo entre dos clausuras algebraicas. El isomorfismo σ que induce τ entre los grupos de Galois de dichas clausuras viene dado por $\sigma(g) = \tau^{-1} g \tau$, luego el isomorfismo que induce σ sobre los grupos $G(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ y $G(K_{\mathfrak{P}'}/k_{\mathfrak{p}})$, cuando los consideramos como subgrupos de $G(K/k)$, es simplemente la conjugación por τ.

Si tomamos una resolución completa de $G(K/k)$ y la consideramos como resolución de $G_{\mathfrak{P}}$, la estructura de $G_{\mathfrak{P}'}$-módulo que adquieren sus módulos C_n según las consideraciones anteriores es la dada por $c\sigma = c\tau^{-1}\sigma\tau$, pero C_n con esta estructura de $G_{\mathfrak{P}'}$-módulo es isomorfo a C_n con su estructura de $G_{\mathfrak{P}'}$-módulo natural (por restricción de su estructura de G-módulo) a través del isomorfismo dado por $c \mapsto c\tau$, luego podemos usar esta estructura en lugar de aquélla para calcular el grupo $H^2(K_{\mathfrak{P}'}/k_{\mathfrak{p}})$ (pues los invariantes no dependen de la resolución que se utilice para calcular los grupos de cohomología).

Ahora es fácil comprobar que el isomorfismo entre los grupos $H^2(K_\mathfrak{P}/k_\mathfrak{p})$ y $H^2(K_{\mathfrak{P}'}/k_\mathfrak{p})$ inducido por τ cuando calculamos ambos grupos con una misma resolución completa de G(K/k) es precisamente la conjugación inducida por $f^\tau(c) = f(c\tau^{-1})\tau$. Según venimos diciendo, este isomorfismo conserva invariantes, luego

$$\mathrm{Inv}_{k_\mathfrak{p}}(x_\mathfrak{P}) = \mathrm{Inv}_{k_\mathfrak{p}}(x_\mathfrak{P}^\tau) = \mathrm{Inv}_{k_\mathfrak{p}}(x_{\tau(\mathfrak{P})}) = \mathrm{Inv}_{k_\mathfrak{p}}(x_{\mathfrak{P}'}).$$

■

Definición 17.6 Sea K/k una extensión normal de cuerpos numéricos, sea $\mathfrak{p}$ un divisor primo de k y $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en K. Si $x \in H^2_J(K/k)$ definimos

$$\mathrm{Inv}_\mathfrak{p}(x) = \mathrm{Inv}_{k_\mathfrak{p}}\, 2(x_\mathfrak{P}) \in \mathbb{Q}/\mathbb{Z}.$$

El teorema anterior implica que $\mathrm{Inv}_\mathfrak{p}(x)$ no depende de la elección de $\mathfrak{P}$. El teorema 17.4 implica que $\mathrm{Inv}_\mathfrak{p}$ es consistente con las inflaciones, por lo que en realidad tampoco depende de K, es decir, que tenemos definido un homomorfismo de grupos $\mathrm{Inv}_\mathfrak{p} : H^2_H(*, k) \longrightarrow \mathbb{Q}/\mathbb{Z}$ (suprayectivo si $\mathfrak{p}$ no es arquimediano).

Ahora definimos el homomorfismo $\mathrm{Inv}_k : H^2_J(*, k) \longrightarrow \mathbb{Q}/\mathbb{Z}$ dado por

$$\mathrm{Inv}_k(x) = \sum_\mathfrak{p} \mathrm{Inv}_\mathfrak{p}(x),$$

donde $\mathfrak{p}$ recorre los divisores primos de k. Notar que la suma contiene sólo un número finito de sumandos no nulos pues todas las componentes locales de x son triviales salvo un número finito de ellas. Es obvio que las inflaciones respetan estos invariantes globales. Veamos su relación con la restricción y la transferencia.

Teorema 17.7 *Sea K/k una extensión de cuerpos numéricos.*

a) Si $x \in H^2_J(*, k)$, entonces $\mathrm{Inv}_K\big(\mathrm{Res}_{k,K}(x)\big) = |K : k|\ \mathrm{Inv}_k(x)$.

b) Si $x \in H^2_J(*, K)$, entonces $\mathrm{Inv}_k\big(\mathrm{V}_{k,K}(x)\big) = \mathrm{Inv}_K(x)$.

Demostración: Usamos el teorema 17.4 y la propiedad análoga de los invariantes locales. En las fórmulas siguientes $\mathfrak{p}$ recorre los primos de k y $\mathfrak{P}$ los de K.

$$\mathrm{Inv}_K\big(\mathrm{Res}_{k,K}(x)\big) = \sum_\mathfrak{P} \mathrm{Inv}_\mathfrak{P}\big(\mathrm{Res}_{k,K}(x)\big) = \sum_\mathfrak{P} |K_\mathfrak{P} : k_\mathfrak{p}|\ \mathrm{Inv}_\mathfrak{p}(x)$$

$$= \sum_\mathfrak{p} \sum_{\mathfrak{P}|\mathfrak{p}} |K_\mathfrak{P} : k_\mathfrak{p}|\ \mathrm{Inv}_\mathfrak{p}(x) = \sum_\mathfrak{p} |K : k|\ \mathrm{Inv}_\mathfrak{p}(x) = |K : k|\ \mathrm{Inv}_k(x).$$

b) El argumento es similar al del apartado anterior:

$$\mathrm{Inv}_k\big(\mathrm{V}_{k,K}(x)\big) = \sum_\mathfrak{P} \mathrm{Inv}_\mathfrak{p}\big(\mathrm{V}_{k,K}(x)\big) = \sum_\mathfrak{P} \mathrm{Inv}_{k_\mathfrak{p}}\Big(\prod_{\mathfrak{P}|\mathfrak{p}} V(x_{\mathfrak{P}'})\Big) =$$

$$= \sum_{\mathfrak{P}} \mathrm{Inv}_{k_\mathfrak{p}}\big(\mathrm{V}(x_{\mathfrak{P}'})\big) = \sum_{\mathfrak{P}} \mathrm{Inv}_{\mathfrak{P}}(x) = \mathrm{Inv}_K(x).$$

■

Los invariantes que acabamos de definir no son el equivalente global de los invariantes locales pues, a diferencia de éstos, no son isomorfismos y por consiguiente no convierten a la formación de grupos de elementos ideales en una formación de clases. Lo que haremos con ellos será probar que inducen invariantes en la formación de grupos de clases de elementos ideales que sí cumplen la definición de formación de clases. De ello nos ocuparemos en la sección siguiente. Acabamos esta sección estudiando más detalladamente los invariantes de las extensiones cíclicas.

Sea K/k una extensión cíclica de cuerpos numéricos, sea $G = G(K/k)$ y sea χ un generador del grupo dual G^*. Según vimos tras el teorema 16.15, el carácter χ determina un isomorfismo $J_k/\,\mathrm{N}_{K/k}[J_K] \cong H^2_J(K/k)$ dado por $[\alpha] \mapsto [\alpha] \cup \delta^*\chi$.

Si $x = [\alpha] \cup \delta^*\chi$, vamos a obtener una expresión para el invariante de x en términos de χ y de α. Si $\mathfrak{P}$ es un primo de K, llamamos $\chi_\mathfrak{P}$ a la restricción de χ a $G_\mathfrak{P}$. Sea $\mathfrak{p}$ el primo de k divisible entre $\mathfrak{P}$. En primer lugar,

$$x_\mathfrak{P} = \bar{\pi}_{\mathfrak{P}\#}\big(\mathrm{Res}_{G,G_\mathfrak{P}}([\alpha] \cup \delta^*\chi)\big) = \bar{\pi}_{\mathfrak{P}\#}([\alpha] \cup \delta^*\chi_\mathfrak{P}) = [\alpha_\mathfrak{p}] \cup \delta^*\chi_\mathfrak{P}.$$

(La última igualdad se deduce fácilmente de la definición del producto exterior.)

Ahora aplicamos el teorema 16.22, según el cual

$$\mathrm{Inv}_\mathfrak{p}(x) = \mathrm{Inv}_{k_\mathfrak{p}}([\alpha_\mathfrak{p}] \cup \delta^*\chi_\mathfrak{P}) = -\chi_\mathfrak{P}\Big(\left(\frac{K_\mathfrak{P}/k_\mathfrak{p}}{\alpha_\mathfrak{p}}\right)\Big) = -\chi\Big(\left(\frac{K_\mathfrak{P}/k_\mathfrak{p}}{\alpha_\mathfrak{p}}\right)\Big). \quad (17.1)$$

Definimos

$$\left(\frac{K/k}{\alpha}\right) = \prod_{\mathfrak{p}} \left(\frac{K_\mathfrak{P}/k_\mathfrak{p}}{\alpha_\mathfrak{p}}\right) \in G. \quad (17.2)$$

La igualdad (17.1) muestra que casi todos los factores son triviales, luego el producto está bien definido. Como G es abeliano tampoco importa el orden de los factores.

Sumando los invariantes locales obtenemos que

$$\mathrm{Inv}_k([\alpha] \cup \delta^*\chi) = -\chi\Big(\left(\frac{K/k}{\alpha}\right)\Big).$$

El lector reconocerá el símbolo que acabamos de introducir como el símbolo de Artin global para la extensión K/k. La última fórmula es la particularización del teorema 16.22 para la teoría global. Sin embargo no estamos en condiciones de probar directamente las propiedades del símbolo local ni siquiera en el caso cíclico que acabamos de considerar.

17.2 La cohomología de los grupos de clases de elementos ideales

El estudio de la cohomología de los grupos de elementos ideales no puede ir mucho más lejos porque, como ya hemos comentado, la formación que determinan no es una formación de clases, entre otras cosas porque los invariantes no determinan los elementos del grupo de Brauer. Para obtener una formación de clases hemos de pasar a los grupos de clases de elementos ideales C_K.

La sucesión exacta

$$1 \longrightarrow K^* \longrightarrow J_K \longrightarrow C_K \longrightarrow 1$$

nos da la sucesión exacta de cohomología

$$1 = H^1_C(K/k) \longrightarrow H^2(K/k) \longrightarrow H^2_J(K/k) \longrightarrow H^2_C(K/k).$$

Estas aplicaciones conmutan con las inflaciones, por lo que determinan una sucesión exacta entre los grupos de Brauer

$$1 \longrightarrow H^2(*/k) \longrightarrow H^2_J(*/k) \longrightarrow H^2_C(*/k).$$

En particular podemos identificar a $H^2(*/k)$ con un subgrupo de $H^2_J(*/k)$. Probaremos que la última aplicación de la sucesión anterior es de hecho suprayectiva, con lo que también tendremos una descripción de $H^2_C(*/k)$ en términos de $H^2_J(*/k)$.

Nuestro objetivo a medio plazo es definir invariantes sobre $H^2_C(*/k)$, para lo cual demostraremos que todos los elementos de $H^2(*/k)$ tienen invariante nulo, lo que nos permitirá pasar los invariantes al cociente. Primero probamos un resultado técnico que nos va a hacer falta. Recordemos que un cuerpo ciclotómico es un cuerpo numérico contenido en una extensión ciclotómica de $\mathbb{Q}$.

Teorema 17.8 *Dado un número natural m y un conjunto finito de primos, existe un cuerpo ciclotómico K tal que la extensión $K/\mathbb{Q}$ es cíclica de grado múltiplo de m, para cada primo p del conjunto prefijado, el grado local en p es múltiplo de m y el grado local en ∞ es 2.*

Demostración: Podemos suponer que m es potencia de primo, $m = r^k$ y construir K de modo que su grado sea también potencia de r, pues el producto de cuerpos construidos de este modo para las diferentes potencias de primo que dividen al m dado es también una extensión cíclica (porque los grados son primos entre sí), desde luego ciclotómica, y claramente cumple lo pedido.

Supongamos que r es impar. Sea C_{r^n} la extensión ciclotómica de $\mathbb{Q}$ de orden r^n. Es conocido que C_{r^n} contiene un subcuerpo cíclico K_n de grado r^{n-1}. Sea p un primo, $\mathfrak{p}$ un divisor de p en K_n y $\mathfrak{P}$ un divisor de $\mathfrak{p}$ en C_{r^n}.

Como $|C_{r^n} : K_n| = r-1$ se cumple también $|(C_{r^n})_{\mathfrak{P}} : (K_n)_{\mathfrak{p}}| \leq r-1$. Basta probar que $|(C_{r^n})_{\mathfrak{P}} : \mathbb{Q}_{\mathfrak{p}}|$ tiende a infinito con n, pues entonces $|(K_n)_{\mathfrak{p}} : \mathbb{Q}_p|$ también tenderá a infinito y bastará tomar n grande. (Es claro que K_n es

imaginario, con lo que el grado local en infinito es 2.) Ahora bien, por [3.20] el grado local en p de la extensión $C_{r^n}/\mathbb{Q}$ es el orden de p módulo r^n si $p \neq r$ y es $(r-1)r^{n-1}$ si $p = r$. En cualquier caso tiende a infinito con n.

Si $r = 2$ podemos suponer que $n \geq 3$. En tal caso C_{2^n} contiene un subcuerpo cíclico K_n de grado 2^{n-2} (y es imaginario, porque su grupo de Galois tiene por complemento al subgrupo generado por la conjugación compleja). El resto del argumento es prácticamente igual al caso anterior. ∎

Notemos una consecuencia de este teorema que necesitaremos después: todo cuerpo numérico k tiene extensiones cíclicas de cualquier orden. En efecto, sea A la adjunción a $\mathbb{Q}$ de todas las raíces de la unidad, sea $F = k \cap A$ y sea $m = |F : \mathbb{Q}|$. Dado un entero n, sea $K \subset A$ tal que $K/\mathbb{Q}$ sea cíclica y de grado divisible entre mn. Entonces kK/k es también cíclica y, como $k \cap K \subset F$, tenemos que

$$|kK : k| = |K : k \cap K| = \frac{|K : \mathbb{Q}|}{|k \cap K : \mathbb{Q}|} \mid \frac{m}{|k \cap K : \mathbb{Q}|}\, n.$$

Como la extensión es cíclica podemos tomar un cuerpo intermedio cuyo grado sobre k sea exactamente n.

Teorema 17.9 *Si k es un cuerpo numérico y $x \in H^2(*/k)$, entonces se cumple* $\mathrm{Inv}_k(x) = 0$.

Demostración: Vamos a reducir el caso general al caso $k = \mathbb{Q}$. Sea K una extensión normal de k tal que $x \in H^2(K/k)$. Podemos suponer que es normal sobre $\mathbb{Q}$. Entonces $\mathrm{V}_{k,\mathbb{Q}}(x) \in H^2(K/\mathbb{Q})$ y por el teorema 17.7 tenemos que $\mathrm{Inv}_k(x) = \mathrm{Inv}_{\mathbb{Q}}\big(\mathrm{V}_{k,\mathbb{Q}}(x)\big)$, luego si el teorema es cierto en el caso $k = \mathbb{Q}$, también $\mathrm{Inv}_k(x) = 0$.

A continuación reducimos el teorema al caso en que K es un cuerpo ciclotómico y cíclico. Sabemos que $\mathrm{Inv}_p(x)$ sólo puede ser no nulo en un número finito de primos p. Para estos primos, sea m_p el denominador de un representante de $\mathrm{Inv}_p(x) \in \mathbb{Q}/\mathbb{Z}$. Sea m el mínimo común múltiplo de los números m_p y sea K' según el teorema anterior.

Para cada primo p, sea n_p el grado local en p de la extensión $K'/\mathbb{Q}$. Sea $L = KK'$. Sea $\mathfrak{p}$ un divisor de p en K'. Por la teoría local tenemos que

$$\mathrm{Inv}_p\big(\mathrm{Res}_{K'}\big(\mathrm{Inf}_L(x)\big)\big) = n_p\,\mathrm{Inv}_p\big(\mathrm{Inf}_L(x)\big) = n_p\,\mathrm{Inv}_p(x).$$

Si p es uno de los primos para los que $\mathrm{Inv}_p(x) \neq 0$ (incluyendo $p = \infty$) entonces el último término es 0, puesto que $m_p \mid n_p$, luego el último término es nulo en cualquier caso. Como los invariantes locales sí son biyectivos tenemos que $\mathrm{Res}_{K'}(\mathrm{Inf}_L(x))_p = 1$ para todo primo p de K', luego $\mathrm{Res}_{K'}\big(\mathrm{Inf}_L(x)\big) = 1$.

En una formación de cuerpos la sucesión

$$1 \longrightarrow H^2_J(K'/\mathbb{Q}) \xrightarrow{\mathrm{Inf}} H^2_J(L/\mathbb{Q}) \xrightarrow{\mathrm{Res}} H^2_J(L/K')$$

es exacta, luego existe un $y \in H^2_J(K'/\mathbb{Q})$ tal que $\mathrm{Inf}_L(x) = \mathrm{Inf}_L(y)$. Al tomar invariantes queda $\mathrm{Inv}(x) = \mathrm{Inv}(y) = 0$ (supuesto el teorema para cuerpos ciclotómicos cíclicos).

Sea, pues, $x \in H^2(K/\mathbb{Q})$, donde K es un cuerpo ciclotómico y cíclico. Aplicamos las observaciones finales de la sección anterior. Sabemos que x es de la forma $[r] \cup \delta^* \chi$ para un cierto $r \in \mathbb{Q}^*$ y que

$$\mathrm{Inv}_{\mathbb{Q}}(x) = -\chi\Big(\Big(\frac{K/\mathbb{Q}}{r}\Big)\Big).$$

Una de las propiedades del símbolo de Artin es que $\mathbb{Q}^*$ está en su núcleo. En la sección siguiente daremos una prueba directa de ello para el caso de $\mathbb{Q}$. Si lo aceptamos de momento concluimos ciertamente que $\mathrm{Inv}_{\mathbb{Q}}(x) = 0$. ∎

Definición 17.10 Sea k un cuerpo numérico. Llamaremos $\overline{H}^2_C(*/k)$ a la imagen de $H^2_J(*/k)$ en $H^2_C(*/k)$ a través de la aplicación canónica de la sucesión exacta

$$1 \longrightarrow H^2(*/k) \longrightarrow H^2_J(*/k) \longrightarrow H^2_C(*/k).$$

El teorema anterior justifica que la aplicación Inv_k induce una asignación de invariantes en $\overline{H}^2_C(*/k)$ a la que seguiremos llamando $\mathrm{Inv}_k : \overline{H}^2_C(*/k) \longrightarrow \mathbb{Q}/\mathbb{Z}$, que por supuesto es un homomorfismo de grupos.

Vamos a probar que la formación C satisface el axioma II′. El apartado a) afirma que $\mathrm{Res}_{k,K}\big[\overline{H}^2_C(*/k)\big] \subset \overline{H}^2_C(*/K)$ y que

$$\mathrm{Inv}_K\big(\mathrm{Res}_{k,K}(c)\big) = |K:k|\ \mathrm{Inv}_k(c).$$

Esto es evidente: si llamamos $j : H^2_J(*/k) \longrightarrow H^2_C(*/k)$ es inmediato comprobar que j conmuta con la restricción:

$$\mathrm{Res}_{k,K}\big(j(x)\big) = j\big(\mathrm{Res}_{k,K}(x)\big),$$

lo que nos da la inclusión $\mathrm{Res}_{k,K}\big[\overline{H}^2_C(*/k)\big] \subset \overline{H}^2_C(*/K)$, y así mismo

$$\mathrm{Inv}_K\big(\mathrm{Res}_{k,K}(j(x))\big) = \mathrm{Inv}_K\big(j(\mathrm{Res}_{k,K}(x))\big)$$

$$= \mathrm{Inv}_K\big(\mathrm{Res}_{k,K}(x)\big) = |K:k|\ \mathrm{Inv}_k(x) = |K:k|\ \mathrm{Inv}_k\big(j(x)\big).$$

Para probar la parte b) del axioma II′ necesitamos el teorema 7.17, que es una consecuencia de la primera desigualdad fundamental. Hemos de probar que $\overline{H}^2_C(*/k)$ contiene subgrupos cíclicos de cualquier orden finito. Basta probarlo para órdenes potencia de primo p^n. Según la observación tras el teorema 17.8, existe un cuerpo numérico K tal que K/k es una extensión cíclica de grado p^n. Por el teorema 7.17 existe un primo $\mathfrak{p}$ en k que se conserva primo en K.

El grado local en $\mathfrak{p}$ de K/k es precisamente p^n y, por la teoría local, tenemos que $H^2(K_{\mathfrak{p}}/k_{\mathfrak{p}})$ es cíclico de orden p^n. Sea $x_{\mathfrak{p}}$ un generador, digamos el que cumple $\mathrm{Inv}_{k_{\mathfrak{p}}}(x_{\mathfrak{p}}) = [1/p^n]$. Completando con unos obtenemos un $x \in H^2_J(K/k)$ de modo que $\mathrm{Inv}_k(x) = [1/p^n]$ y, en consecuencia, $c = j(x) \in \overline{H}^2_C(K/k)$ cumple $\mathrm{Inv}_k(c) = [1/p^n]$. Esto implica que el orden del subgrupo generado por c es al

menos p^n y, tomando un subgrupo, llegamos a un subgrupo cíclico de $\overline{H}^2_C(*/k)$ de orden exactamente p^n.

El axioma II′ implica el axioma II, y en particular tenemos que $\overline{H}^2_C(*/k) = H^2_C(*/k)$, así como que la asignación de invariantes es inyectiva. Por lo tanto tenemos probado lo siguiente:

Teorema 17.11 *Sea k un cuerpo numérico.*

a) La formación de clases de elementos ideales es una formación de clases.

b) La sucesión $1 \longrightarrow H^2(*/k) \longrightarrow H^2_J(*/k) \longrightarrow H^2_C(*/k) \longrightarrow 1$ es exacta.

c) $\mathrm{Inv}_k : H^2_C(*/k) \longrightarrow \mathbb{Q}/\mathbb{Z}$ es un isomorfismo de grupos.

Si K/k es una extensión normal de cuerpos numéricos ya conocemos la estructura de los grupos $H^2_J(K/k)$ (suma directa de grupos cíclicos de ordenes iguales a los grados locales) y $H^2_C(K/k)$ (cíclico de orden igual al grado global).

La propiedad c) nos da ahora la estructura del grupo $H^2(K/k)$: Es isomorfo al grupo de todas las aplicaciones $\mathfrak{p} \mapsto x_\mathfrak{p}$ del conjunto de los primos de k en $\mathbb{Q}/\mathbb{Z}$ tales que

a) Casi todo $x_\mathfrak{p}$ es 0,

b) $n_\mathfrak{p} x_\mathfrak{p} = 0$ (donde $n_\mathfrak{p}$ el grado local),

c) $\sum_\mathfrak{p} x_\mathfrak{p} = 0$.

En efecto, las propiedades a) y b) determinan un elemento de $H^2_J(K/k)$ y la propiedad c) implica que de hecho está en $H^2(K/k)$.

17.3 El símbolo de Artin sobre $\mathbb{Q}$

En la sección anterior ha quedado pendiente demostrar que el símbolo definido por (17.2) para $k = \mathbb{Q}$ tiene en su núcleo a $\mathbb{Q}^*$. Esto es inmediato si tenemos en cuenta que se trata del símbolo de Artin global, pero, por supuesto, si queremos una introducción autocontenida a la teoría de cuerpos de clases no podemos usar este argumento.

Sea A la extensión ciclotómica maximal de $\mathbb{Q}$, es decir, la adjunción a $\mathbb{Q}$ de las raíces de la unidad (sabemos que es la máxima extensión abeliana de $\mathbb{Q}$, pero no podemos usar este hecho). Para cada primo p, sea A_p la extensión ciclotómica maximal de $\mathbb{Q}_p$ (incluyendo $A_\infty = \mathbb{C}$). Fijando arbitrariamente un monomorfismo $t : A \longrightarrow A_p$ podemos identificar a A con un subcuerpo de A_p, y entonces $A_p = A\mathbb{Q}_p$.

En particular identificamos $G = G(A/\mathbb{Q})$ con $G(t[A]/\mathbb{Q})$ a través del isomorfismo dado por $\sigma \mapsto t^{-1}\sigma t$. Es importante observar que cualquier otro isomorfismo entre A y $t[A]$ ha de ser de la forma $s = \tau t$, para un cierto $\tau \in G$ y, como G es abeliano, el isomorfismo $\sigma \mapsto s^{-1}\sigma s$ es el mismo que el inducido por

t, de modo que la identificación entre los grupos de Galois es independiente de la elección del isomorfismo de cuerpos t. Claramente se trata de un isomorfismo topológico.

Sea $G_p = G(A_p/\mathbb{Q}_p) \cong G\big(A/(A\cap\mathbb{Q}_p)\big) \leq G$. El monomorfismo de G_p en G es canónico, en el sentido de que no depende tampoco de la elección de t (consiste en la restricción a $t[A]$ seguido del isomorfismo inducido por t). Obviamente es continuo, y así la topología de G_p (como grupo de Galois) es la inducida desde G.

Por el teorema [3.20], las extensiones ciclotómicas de $\mathbb{Q}_p$ no ramificadas son las de la forma $\mathbb{Q}_p(\zeta)$, donde ζ es una raíz de la unidad de orden primo con p. Sea T_p la adjunción a $\mathbb{Q}_p$ de todas estas raíces. Entonces T_p es la extensión no ramificada maximal de $\mathbb{Q}_p$ (pues toda extensión del cuerpo de restos de $\mathbb{Q}_p$ se obtiene adjuntando una raíz de la unidad de orden primo con p). El automorfismo que induce el automorfismo de Frobenius en la extensión de los cuerpos de restos es precisamente el caracterizado por $\zeta \mapsto \zeta^p$. Llamemos ϕ_p a una extensión arbitraria de este automorfismo a G_p.

Llamemos U al grupo de los $\alpha \in J_\mathbb{Q}$ tales que $\alpha_\infty = 1$ y, para cada primo p, la componente α_p es una unidad de $\mathbb{Q}_p$. Así $J_\infty = \mathbb{R}^* \times U$. También es fácil ver que $J_\mathbb{Q} = \mathbb{Q}^* \times \mathbb{R}^+ \times U$, y además la topología de $J_\mathbb{Q}$ es el producto de las topologías de los factores.[1]

Vamos a construir un isomorfismo $U \cong G$. Dado $m \in \mathbb{Z}$, llamaremos m_p a la mayor potencia de p que divide a m. Dados $m \in \mathbb{Z}$ y $u \in U$, existe un $n \in \mathbb{Z}$ único (mód m) tal que $n \equiv u_p$ (mód m_p) para todo primo (finito) p. En efecto, la condición es trivial si $p \nmid m$ y para los primos restantes se trata del teorema chino del resto. Obviamente $(m, n) = 1$. Para abreviar expresaremos este hecho como $n \equiv u$ (mód m). Podemos exigir que n sea impar.

Si ζ es una raíz m-sima primitiva de la unidad definimos $\zeta^u = \zeta^n$. Es obvio que la condición $\zeta \mapsto \zeta^u$ determina un automorfismo de $\mathbb{Q}(\zeta)$. Si $\zeta' \in \mathbb{Q}(\zeta)$ es otra raíz de la unidad entonces $\zeta' = \pm\zeta^k$, luego la imagen de ζ' por el automorfismo es $\pm\zeta^{nk} = \zeta'^n$ (pues n es impar). El orden de ζ' es un $m' \mid 2m$, luego también $n \equiv u$ (mód m') y por lo tanto la imagen de ζ' es ζ'^u.

Esto prueba que el automorfismo que u induce en $\mathbb{Q}(\zeta)$ no depende de la elección de ζ, así como que el automorfismo que u induce en $\mathbb{Q}(\zeta')$ es la restricción del que induce en $\mathbb{Q}(\zeta)$. Como consecuencia u induce un automorfismo $\sigma_u \in G$ determinado por la condición $\sigma_u(\zeta) = \zeta^u$ para toda raíz de la unidad ζ.

Es inmediato comprobar que $\zeta^{uv} = (\zeta^u)^v$, de donde la aplicación $\sigma : U \longrightarrow G$ dada por $u \mapsto \sigma_u$ es un homomorfismo de grupos.

Su núcleo lo forman las unidades que cumplen $u \equiv 1$ (mód m) para todo entero m, pero es claro que esto implica $u = 1$. Así pues, se trata de un monomorfismo.

Por otra parte σ es continuo: un entorno básico de 1 en G es un grupo $G\big(A/\mathbb{Q}(\zeta)\big)$ y su antiimagen por σ es el conjunto $\{u \in U \mid u \equiv 1 \text{ (mód } m)\}$, donde m es el orden de ζ. Claramente se trata de un abierto básico en U.

[1] Notar que el grupo $\mathbb{R}^+ \times U$ es abierto y cerrado en $\mathbb{R}^* \times U$, que por definición es abierto y cerrado en $J_\mathbb{Q}$. Por consiguiente la topología producto y la de $J_\mathbb{Q}$ tienen una misma base de entornos de 1.

Dado $\sigma \in G\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big)$, existe un $u \in U$ tal que $\sigma = \sigma_u|_{\mathbb{Q}(\zeta)}$. En efecto, si el orden de ζ es m entonces $\sigma(\zeta) = \zeta^n$ para un cierto n primo con m. Definimos u mediante

$$u_p = \begin{cases} n & \text{si } p \mid m, \\ 1 & \text{en caso contrario.} \end{cases}$$

Entonces $\zeta^u = \zeta^n$, luego u cumple lo pedido.

Esto implica que $\sigma[U]$ es denso en G. Como también es compacto, de hecho $\sigma[U] = G$ y, en definitiva, $\sigma : U \longrightarrow G$ es un isomorfismo topológico.

Seguidamente extendemos σ a todo el grupo de elementos ideales. En realidad, para obtener el isomorfismo de Artin clásico hemos de hacer una leve modificación (tomar inversos):

Dado $\alpha = rsu \in J_{\mathbb{Q}} = \mathbb{Q}^* \times \mathbb{R}^+ \times U$, definimos $\sigma(\alpha) = \sigma_{u^{-1}}$. De este modo tenemos un epimorfismo topológico $\sigma : J_{\mathbb{Q}} \longrightarrow G$ cuyo núcleo es $\mathbb{Q}^* \times \mathbb{R}^+$ (la continuidad se debe a que σ es la composición de la proyección sobre U, la inversión en U y el isomorfismo que acabamos de construir).

Equivalentemente, podemos considerar a σ definido sobre $C_{\mathbb{Q}} = \mathbb{R}^+ \times U$ con núcleo $\mathbb{R}^+$.

Ahora evaluaremos la restricción de σ a cada grupo $\mathbb{Q}_p^*$ y demostraremos que se trata del isomorfismo de Artin local.

En primer lugar, si $p = \infty$, sea $\alpha_\infty = \epsilon r$, con $\epsilon = \pm 1$ y $r \in \mathbb{R}^+$. Representaremos los elementos ideales como sucesiones cuyo primer término es la coordenada en $p = \infty$. Entonces

$$\alpha_\infty = (\epsilon r, 1, 1, \ldots) = (\epsilon, \epsilon, \epsilon, \ldots)(r, 1, 1, \ldots)(1, \epsilon, \epsilon, \ldots) \in \mathbb{Q}^* \times \mathbb{R}^+ \times U,$$

y además $\epsilon \equiv u^{-1} \pmod m$ para cualquier m, luego $\sigma(\alpha_\infty)(\zeta) = \zeta^\epsilon$. En otros términos:

$$\sigma(\alpha_\infty)(\zeta) = \zeta^{\mathrm{sig}(\alpha_\infty)}.$$

Sea ahora p finito. Representaremos los elementos de $\mathbb{Q}_p^*$ escribiendo primero la componente ∞, luego la componente p y luego las componentes restantes. De este modo, si tenemos $\alpha_p = p^k u_p$, con $u_p \in U_p$, la descomposición de α_p como elemento de $\mathbb{Q}^* \times \mathbb{R}^+ \times U$ es

$$\alpha_p = (1, p^k u_p, 1, 1, \ldots) = (p^k, p^k, p^k, p^k, \ldots)(p^{-k}, 1, 1, 1, \ldots)(1, u_p, p^{-k}, p^{-k}, \ldots)$$

Toda raíz de la unidad factoriza como $\zeta = \zeta_0\zeta'$, donde ζ_0 tiene orden m_0 primo con p y ζ' tiene orden potencia de p. Por lo tanto basta describir la acción de $\sigma(\alpha_p)$ sobre ambos tipos de raíces.

Si $k \geq 0$ entonces $p^k \equiv u^{-1} \pmod{m_0}$, luego $\sigma(\alpha_p)(\zeta_0) = \zeta_0^{p^k} = \phi_p^k(\zeta_0)$. Como σ es un isomorfismo de grupos, lo mismo vale si $k < 0$. En otros términos:

$$\sigma(\alpha_p)(\zeta_0) = \phi_p^{v_p(\alpha_p)}(\zeta_0),$$

donde v_p denota la valoración p-ádica.

Respecto de la acción de $\sigma(\alpha_p)$ sobre ζ' no podemos decir más que lo que indica la definición: si el orden de ζ' es p^r y $u_p^{-1} \equiv n \pmod{p^r}$, entonces

$$\sigma(\alpha_p)(\zeta') = \zeta'^n.$$

Definición 17.12 Definimos las aplicaciones $\sigma_p : \mathbb{Q}_p^+ \longrightarrow G$ del modo siguiente:

a) Si $p = \infty$ entonces $\sigma_p(\alpha_p)(\zeta) = \zeta^{\mathrm{sig}(\alpha_p)}$.

b) Si p es finito $\sigma_p(\alpha_p)$ es el automorfismo determinado por:

$$\sigma_p(\alpha_p)(\zeta_0) = \phi_p^{v_p(\alpha_p)}(\zeta_0), \qquad \sigma(\alpha_p)(\zeta') = \zeta'^{u^{-1}},$$

donde $\alpha_p = p^{v_p(\alpha_p)}u$, ζ_0 es cualquier raíz de la unidad de orden primo con p y ζ' es cualquier raíz de la unidad de orden potencia de p.

Estas aplicaciones están bien definidas porque, según acabamos de ver, son las restricciones de σ a los grupos $\mathbb{Q}_p^*$. Por este mismo motivo son homomorfismos continuos. Es claro por la definición que el núcleo de σ_∞ es $\mathbb{R}^+$, mientras que los homomorfismos restantes son inyectivos (un $\alpha_p = p^{v_p(\alpha_p)}u$ en el núcleo de σ_p ha de cumplir que $\phi_p^{v_p(\alpha)}(\zeta_0) = \zeta_0$ para todo ζ_0, luego $v_p(\alpha_p) = 0$, y también $u \equiv 1 \pmod{p^r}$ para todo r, luego $u = 1$).

Los homomorfismos σ_p determinan a σ del modo siguiente: Todo $\alpha \in J_\mathbb{Q}$ se puede expresar como producto infinito

$$\alpha = \prod_p \alpha_p$$

en sentido topológico, es decir, la sucesión de los productos parciales ordenados de cualquier manera converge a α. Como σ es continuo tenemos que

$$\sigma(\alpha) = \prod_p \sigma_p(\alpha_p).$$

Teniendo en cuenta la topología de G, esto significa que en cada cuerpo ciclotómico K todos los factores salvo un número finito de ellos son la identidad, y $\sigma(\alpha)|_K$ es la composición de los restantes. Para demostrar que σ es el isomorfismo de Artin empezamos probando lo siguiente:

Teorema 17.13 *Sea ζ una raíz de la unidad, $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta)$ y $H = G(A/K)$. Si $\alpha \in \mathbb{Q}^* \,\mathrm{N}_\mathbb{Q}^K[J_K]$ entonces $\sigma(\alpha) \in H$.*

Demostración: Sea m el orden de ζ y E el conjunto de los primos arquimedianos de K y los que dividen a m. Sea $\alpha = a\,\mathrm{N}_\mathbb{Q}^K(\beta)$. Dado un número real $\epsilon > 0$, por el teorema de aproximación existe un $b \in K^*$ tal que $|b^{-1} - \beta_\mathfrak{p}^{-1}|_\mathfrak{p} < |\beta_\mathfrak{p}^{-1}|_\mathfrak{p}\epsilon$, para todo $\mathfrak{p} \in E$.

De aquí se sigue que $|\beta_\mathfrak{p} b^{-1} - 1|_\mathfrak{p} < \epsilon$. Llamemos $\gamma = \beta b^{-1}$. Entonces $\beta = b\gamma$ y tenemos que $|\gamma_\mathfrak{p} - 1|_\mathfrak{p} < \epsilon$. Con esto podemos expresar $\alpha = a\,\mathrm{N}_\mathbb{Q}^K(b)\,\mathrm{N}_\mathbb{Q}^K(\gamma) = c\,\mathrm{N}_\mathbb{Q}^K(\gamma)$. Por definición de σ tenemos que $\sigma(c) = 1$, luego $\sigma(\alpha) = \sigma\big(\mathrm{N}_\mathbb{Q}^K(\gamma)\big)$. Como H es cerrado, basta probar que cada $\sigma_p\big(\mathrm{N}_\mathbb{Q}^K(\gamma)_p\big) \in H$.

Sea $p \mid m$ o $p = \infty$. La función σ_p es continua y H es abierto, luego para garantizar que $\sigma_p\big(\mathrm{N}_\mathbb{Q}^K(\gamma)_p\big) \in H$ es suficiente garantizar que $\mathrm{N}_\mathbb{Q}^K(\gamma)_p$ está en un cierto entorno de 1 y, por la continuidad de las normas locales, para ello basta

con que $\gamma_\mathfrak{p}$ esté suficientemente cerca de 1 para cada $\mathfrak{p} \in E$. Así pues, en este caso basta elegir ϵ adecuadamente.

Supongamos ahora que p es finito y $p \nmid m$. Entonces la extensión $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ es no ramificada luego, si $\mathfrak{p}$ es cualquier divisor de p en K, la extensión $K_\mathfrak{p}/\mathbb{Q}_p$ también lo es. Por lo tanto es cíclica y, de hecho, el grupo de Galois está generado por la restricción del automorfismo de Frobenius ϕ_p. Así, si llamamos n_p al grado local, concluimos que $\phi_p^{n_p}$ fija a $K_\mathfrak{p}$, luego a K.

Ahora observamos que $\mathrm{N}_\mathbb{Q}^K(\gamma)_p$ es la norma de un elemento de $K_\mathfrak{p}$, luego se ha de cumplir $v_p\big(\mathrm{N}_\mathbb{Q}^K(\gamma)_p\big) = kn_p$. Como $p \nmid m$, la definición de σ_p nos da que

$$\sigma_p\big(\mathrm{N}_\mathbb{Q}^K(\gamma)_p\big)(\zeta) = \phi_p^{n_p k}(\zeta).$$

En particular $\sigma_p\big(\mathrm{N}_\mathbb{Q}^K(\gamma)_p\big)|_K = \phi_p^{n_p k}|_K = 1$, es decir, $\sigma_p\big(\mathrm{N}_\mathbb{Q}^K(\gamma)_p\big) \in H$. ∎

De aquí deducimos el resultado análogo local:

Teorema 17.14 *Para cada primo (finito) p, la aplicación $\sigma_p : \mathbb{Q}_p^* \longrightarrow G_p$ es un monomorfismo continuo con imagen densa. Si $K_\mathfrak{p}$ es una extensión finita ciclotómica de $\mathbb{Q}_p$, $H = G(A_p/K_\mathfrak{p})$ y $\alpha_p \in \mathrm{N}_{\mathbb{Q}_p}^{K_\mathfrak{p}}[K_\mathfrak{p}^*]$, entonces $\sigma_p(\alpha_p) \in H$.*

Demostración: Veamos primero la segunda parte. Sea S un subgrupo abierto de G. Entonces SH también es abierto y $SH = G(A/E)$, para cierto cuerpo E. Sea $\mathfrak{P}$ un primo de E que divida a p. Entonces $G(A_p/E_\mathfrak{P}) = SH \cap G_p$. Como $H \leq G_p$ resulta que $H \leq SH \cap G_p$, luego $E_\mathfrak{P} \subset K_\mathfrak{p}$. Esto implica que α_p es una norma de $E_\mathfrak{P}$ luego, visto en $J_\mathbb{Q}$, es una norma de J_E. Por el teorema anterior $\sigma_p(\alpha_p) \in SH$ o, equivalentemente, $\sigma_p(\alpha_p)S \cap H \neq \varnothing$. Como H es cerrado y S es arbitrario, tenemos que $\sigma_p(\alpha_p) \in H$.

Para probar la primera parte, tomando $K_\mathfrak{p} = \mathbb{Q}_p$ y $H = G_p$ en la parte ya probada, concluimos que si $\alpha_p \in \mathbb{Q}_p^*$ entonces $\sigma_p(\alpha_p) \in G_p$.

La imagen será densa si todo automorfismo de cada extensión $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ es la restricción de algún $\sigma_p(\alpha_p)$. Si descomponemos $\zeta = \zeta_0\zeta'$, donde el orden de ζ_0 es primo con p y el de ζ' es potencia de p, entonces la extensión $\mathbb{Q}_p(\zeta_0)/\mathbb{Q}_p$ es no ramificada, luego la imagen de ζ_0 ha de ser $\phi_p^k(\zeta_0)$ para cierto k. Por otra parte la imagen de ζ' ha de ser ζ'^n, para un cierto n primo con p. Claramente $\alpha_p = n^{-1}p^k$ induce el automorfismo considerado. ∎

La segunda desigualdad nos da los recíprocos de los dos últimos teoremas:

Teorema 17.15 *a) Si $K/\mathbb{Q}$ es una extensión finita ciclotómica entonces*

$$\sigma(\alpha) \in G(A/K) \quad \textit{si y sólo si} \quad \alpha \in \mathbb{Q}^*\,\mathrm{N}_\mathbb{Q}^K[J_K].$$

b) Si $K_\mathfrak{p}/\mathbb{Q}_p$ es una extensión finita ciclotómica entonces

$$\sigma_p(\alpha_p) \in G(A_p/K_\mathfrak{p}) \quad \textit{si y sólo si} \quad \alpha_p \in \mathrm{N}_{\mathbb{Q}_p}^{K_\mathfrak{p}}[K_\mathfrak{p}^*].$$

DEMOSTRACIÓN: La prueba es formalmente idéntica en los dos casos. Llamemos $H = G(A/K)$ (resp. $H = G(A_p/K_\mathfrak{p})$), sea M el conjunto de los $\alpha \in J_\mathbb{Q}$ (resp. $\alpha_p \in \mathbb{Q}_p^*$) cuya imagen por σ (resp. σ_p) está en H. Si componemos σ (resp. σ_p) con la proyección módulo H obtenemos un epimorfismo en $G(K/\mathbb{Q})$ (resp. $G(K_\mathfrak{p}/\mathbb{Q}_p)$) (porque σ es suprayectiva y σ_p es densa). El núcleo de este epimorfismo es M por definición, luego por el teorema de isomorfía resulta que

$$|J_\mathbb{Q} : M| = |K : \mathbb{Q}|, \quad (\text{resp. } |\mathbb{Q}_p^* : M| = |K_\mathfrak{p} : \mathbb{Q}_p|).$$

Por otra parte la segunda desigualdad es

$$|J_\mathbb{Q} : \mathbb{Q}^* \,\mathrm{N}_\mathbb{Q}^K[J_K]| \le |K : \mathbb{Q}|, \quad (\text{resp. } |\mathbb{Q}_p^* : \mathrm{N}_{\mathbb{Q}_p}^{K_\mathfrak{p}}[K_\mathfrak{p}^*]| \le |K_\mathfrak{p} : \mathbb{Q}_p|),$$

y los dos teoremas anteriores nos dan las inclusiones

$$\mathbb{Q}^* \,\mathrm{N}_\mathbb{Q}^K[J_K] \le M \quad (\text{resp. } \mathrm{N}_{\mathbb{Q}_p}^{K_\mathfrak{p}}[K_\mathfrak{p}^*] \le M).$$

Obviamente entonces las inclusiones han de ser igualdades. ∎

Ahora podemos aplicar el teorema 12.21 y concluir que A_p es de hecho la mayor extensión abeliana de $\mathbb{Q}_p$, así como que σ_p es el homomorfismo de Artin local. Hemos probado el siguiente teorema (puramente local):

Teorema 17.16 *Sea p un número primo. Entonces las extensiones abelianas de $\mathbb{Q}_p$ son exactamente las ciclotómicas. Además el símbolo de Artin de $\mathbb{Q}_p$ está determinado explícitamente como sigue:*

a) Si ζ_0 es una raíz de la unidad de orden primo con p, entonces

$$\left(\frac{\mathbb{Q}_p}{\alpha}\right)(\zeta_0) = \phi_p^{v_p(\alpha_p)}(\zeta_0),$$

b) Si ζ' es una raíz de la unidad de orden p^r, entonces

$$\left(\frac{\mathbb{Q}_p}{\alpha}\right)(\zeta') = \zeta'^n,$$

donde $\alpha = p^{v_p(\alpha)}u$ y $nu \equiv 1 \pmod{p^r}$.

Además sabemos que la aplicación σ se expresa como

$$\sigma(\alpha) = \prod_p \left(\frac{\mathbb{Q}_p}{\alpha_p}\right). \tag{17.3}$$

Si K es una extensión finita ciclotómica de $\mathbb{Q}$ y restringimos los automorfismos a K obtenemos el símbolo (17.2) para $k = \mathbb{Q}$:

$$\sigma(\alpha)|_K = \prod_p \left(\frac{K_\mathfrak{p}/\mathbb{Q}_p}{\alpha_p}\right) = \left(\frac{K/k}{\alpha}\right)$$

El resultado que quedó pendiente en la sección anterior es que el núcleo de este automorfismo contiene a $\mathbb{Q}^*$, y de hecho hemos probado que es $\mathbb{Q}^* \,\mathrm{N}_\mathbb{Q}^K[J_K]$.

Con los resultados que veremos en la sección siguiente, la expresión (17.3) probará que σ es el símbolo de Artin de $\mathbb{Q}$ y, por consiguiente, que A es la mayor extensión abeliana de $\mathbb{Q}$ (el teorema de Kronecker).

17.4 La teoría global de cuerpos de clases

En este punto tenemos probado que la formación C de los grupos de clases de elementos ideales es una formación de clases. Por consiguiente, para cada extensión abeliana K/k de cuerpos numéricos, tenemos definido el isomorfismo de Artin $\omega_{K/k} : C_k/\operatorname{N}_k^K[C_K] \longrightarrow G(K/k)$, aunque también lo podemos considerar como $\omega_{K/k} : J_k/k^* \operatorname{N}_k^K[J_K] \longrightarrow G(K/k)$.

Si llamamos A_k a la mayor extensión abeliana de k, estos homomorfismos inducen un homomorfismo $\omega_k : C_k \longrightarrow G(A_k/k)$ cuyo núcleo es el grupo D_k de las normas universales de C_k (alternativamente, $\omega_k : J_k \longrightarrow G(A_k/k)$). Ahora podemos relacionar el símbolo de Artin global con los símbolos locales.

Teorema 17.17 *Sea k un cuerpo numérico.*

a) Si $\alpha \in J_k$, entonces

$$\left(\frac{k}{\alpha}\right) = \prod_{\mathfrak{p}} \left(\frac{k_p}{\alpha_{\mathfrak{p}}}\right).$$

b) Si K es una extensión abeliana finita de k entonces

$$\left(\frac{K/k}{\alpha}\right) = \prod_{p} \left(\frac{K_{\mathfrak{P}}/k_{\mathfrak{p}}}{\alpha_{\mathfrak{p}}}\right).$$

Demostración: Veamos primero b). Notemos que el producto es finito, pues si $\mathfrak{p}$ es no ramificado y $\alpha_{\mathfrak{p}}$ es una unidad, entonces $\left(\frac{K_{\mathfrak{P}}/k_{\mathfrak{p}}}{\alpha}\,\mathfrak{p}\right) = 1$. Basta probar que para todo carácter χ del grupo de Galois $G(K/k)$ se cumple

$$\chi(\left(\frac{K/k}{\alpha}\right)) = \chi\left(\prod_{\mathfrak{p}} \left(\frac{K_{\mathfrak{P}}/k_{\mathfrak{p}}}{\alpha_{\mathfrak{p}}}\right)\right).$$

Ahora bien, por el teorema 16.22, seguido del mismo razonamiento que al final de la sección 17.1,

$$\begin{aligned}
\chi(\left(\frac{K/k}{\alpha}\right)) &= -\operatorname{Inv}_k([\alpha] \cup \delta^*\chi) = -\sum_{\mathfrak{p}} \operatorname{Inv}_{k_{\mathfrak{p}}}\left([\alpha_{\mathfrak{p}}] \cup \delta^*\chi_{\mathfrak{P}}\right) \\
&= \sum_{\mathfrak{p}} \chi_{\mathfrak{P}}(\left(\frac{K_{\mathfrak{P}}/k_{\mathfrak{p}}}{\alpha_{\mathfrak{p}}}\right)) = \sum_{\mathfrak{p}} \chi(\left(\frac{K_{\mathfrak{P}}/k_{\mathfrak{p}}}{\alpha_{\mathfrak{p}}}\right)) \\
&= \chi\left(\prod_{\mathfrak{p}} \left(\frac{K_{\mathfrak{P}}/k_{\mathfrak{p}}}{\alpha_{\mathfrak{p}}}\right)\right).
\end{aligned}$$

El apartado a) se sigue fácilmente de b) (hay que probar que el producto converge). ∎

Notemos que en este punto podríamos repetir la prueba del teorema 12.9, que nos da, entre otras cosas, la suprayectividad del homomorfismo de Artin ω_k.

Veamos ahora que se cumple el teorema de existencia global. Es evidente que la formación de grupos de clases de elementos ideales es una formación topológica. Hemos de comprobar que cumple el axioma III (ver el capítulo anterior).

El axioma III a) tiene consta de dos afirmaciones: en primer lugar el grupo de normas $\mathrm{N}_k^K[C_K]$ es cerrado porque es la antiimagen de $G(A_k/K)$ por el homomorfismo de Artin (equivalentemente, por el teorema 6.19). En segundo lugar hemos de ver que el conjunto de los $\alpha \in C_K$ tales que $\mathrm{N}_k^K(\alpha) = 1$ es compacto, para lo cual basta ver que está contenido en C^0.

Teniendo en cuenta la definición de la norma de un elemento ideal, es claro que $\alpha_\mathfrak{P}$ es una unidad para todo $\mathfrak{P}$ no arquimediano, luego $\|\alpha_\mathfrak{P}\|_\mathfrak{P} = 1$. Respecto a las componentes arquimedianas, tenemos que el producto de todas las normas $\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P})$ correspondientes a un mismo primo $\mathfrak{p}$ de k es igual a 1.

Si $\mathfrak{p}$ es complejo, la extensión $K_\mathfrak{P}/k_\mathfrak{p}$ es trivial y $\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P}) = \alpha_\mathfrak{P}$. Tomando módulos y elevando al cuadrado queda que el producto de todos los $\|\alpha_\mathfrak{P}\|_\mathfrak{P}$ (con $\mathfrak{P} \mid \mathfrak{p}$) es 1.

Si $\mathfrak{p}$ es real, entonces $|\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P})| = |\alpha_\mathfrak{P}| = \|\alpha_\mathfrak{P}\|_\mathfrak{P}$ cuando el primo $\mathfrak{P}$ es real y $|\mathrm{N}_\mathfrak{P}(\alpha_\mathfrak{P})| = |\alpha_\mathfrak{P}|^2 = \|\alpha_\mathfrak{P}\|_\mathfrak{P}$ cuando $\mathfrak{P}$ es complejo, luego llegamos a la misma conclusión.

La conclusión final es que $\|\alpha\| = 1$, es decir, $\alpha \in C^0$.

Así pues se verifica el axioma III a). Esto implica que los grupos de normas universales se comportan adecuadamente, en el sentido de que $\mathrm{N}_k^K[D_K] = D_k$.

La primera parte del axioma III b) es evidente: el conjunto de los $\alpha \in C_K$ tales que $\alpha^p = 1$ es compacto, pues obviamente $\|\alpha\|^p = 1$, luego $\|\alpha\| = 1$ y así $\alpha \in C^0$.

El único resultado no trivial es la segunda parte de III b): que todo elemento de D_k tiene raíz p-ésima en C_k. Esto es la afirmación $(*)$ en la prueba del teorema 12.13. Vemos que descansa fuertemente en la aritmética de los cuerpos numéricos.

Con esto tenemos que D_k es el conjunto de los elementos infinitamente divisibles de C_k, de donde a su vez se sigue que está contenido en todo subgrupo abierto de C_k de índice finito: Si $r \in D_k$ y H es un subgrupo de C_k de índice n, entonces podemos expresar $r = s^n$, y así $[r] = [s]^n = [1]$ en C_k/H, luego $r \in H$.

El axioma III c) se cumple tomando $U = D_k \cap C^0$ (observar que $D^k = \mathbb{R}^+ \times U$), pero cuesta lo mismo probar esto que probar directamente el teorema de existencia.

Teorema 17.18 (Teorema de existencia global) *Si k es un cuerpo numérico y H es un subgrupo abierto de índice finito en C_k, entonces existe una extensión abeliana K de k tal que $H = \mathrm{N}_k^K[C_K]$.*

Demostración: Tenemos que $\mathbb{R}^+ \le D_k \le H$, luego $HC^0 = C_k$. Sea $H^0 = H \cap C^0$. Entonces H^0 es compacto y

$$|G(A_k/k) : \omega_k[H^0]| = |C^0/(D_k \cap C^0) : H^0/(D_k \cap C^0)| = |C^0 : H^0| = |C_k : H|.$$

Así pues, $\omega_k[H^0]$ es un subgrupo cerrado de índice finito en $G(A_k/k)$ (y por tanto abierto). Sea K su cuerpo fijado, de modo que $\omega_k[H^0] = G(A_k/K)$. Como $D_k \leq H$, se cumple que la antiimagen por ω_k de $\omega_k[H^0]$ es H, pero por otra parte es $\mathrm{N}_k^K[C_K]$. ∎

A partir de aquí ya es fácil obtener todos los resultados de la teoría global de cuerpos de clases. Veamos por ejemplo una prueba alternativa del teorema 8.17. Se basa en la siguiente observación elemental: si Si K/k es una extensión finita abeliana de cuerpos numéricos y $a \in k^*$ es una norma local para todos los primos de k salvo quizá para uno de ellos, entonces también es una norma local para dicho primo. En efecto, a está en el núcleo del homomorfismo de Artin global y en el de todos los homomorfismos locales salvo quizá en el de uno de ellos, pero por la fórmula del teorema 17.17 también ha de estar en el núcleo de éste.

Teorema 17.19 *Sea K/k una extensión finita abeliana de cuerpos numéricos. Si $\mathfrak{p}$ es un primo de k y $\mathfrak{P}$ uno de sus divisores en K, entonces se cumple* $\mathrm{N}[C_K] \cap k_{\mathfrak{p}}^* = \mathrm{N}[K_{\mathfrak{P}}^*]$.

Demostración: En términos de elementos ideales hemos de probar que $\mathrm{N}[J_K]k^* \cap k_{\mathfrak{p}}^* k^* = \mathrm{N}[K_{\mathfrak{P}}^*]k^*$. Una inclusión es obvia. Para la contraria notamos que si $\mathrm{N}(\alpha)a = \beta_{\mathfrak{p}} b$, entonces b/a es una norma local respecto a todos los primos de k salvo quizá respecto a $\mathfrak{p}$, luego por la observación anterior también lo es respecto a $\mathfrak{p}$. Por lo tanto $\beta_{\mathfrak{p}} = \mathrm{N}(\alpha)(a/b) \in \mathrm{N}[K_{\mathfrak{p}}^*]$. ∎

De aquí se deducen inmediatamente los teoremas de ramificación y de escisión completa.

Terminamos la sección con algunos hechos aislados sobre la cohomología global que tienen interés en sí mismos aunque no nos han hecho falta para desarrollar el grueso de la teoría.

Hemos probado que la proyección $j : H_J^2(*/k) \longrightarrow H_C^2(*/k)$ es suprayectiva, pero esto no implica que las proyecciones $j : H_J^2(K/k) \longrightarrow H_C^2(K/k)$ también lo sean: un elemento de $H_C^2(K/k)$ puede tener sus antiimágenes por j en un grupo $H_J^2(L/k)$ para una cierta extensión L de K, no necesariamente igual a K.

En efecto, sea $n = |K : k|$ y m el mínimo común múltiplo de los grados locales de la extensión (claramente $m \mid n$). Primeramente observamos que todo $x \in H_J^2(K/k)$ cumple $\mathrm{Inv}_k(x) = [r/m]$, para cierto entero r, pues el invariante se calcula sumando fracciones con denominadores divisibles entre m. Esto prueba que $\mathrm{Inv}_k[H_J^2(K/k)] \leq \langle [1/m] \rangle$, que es un grupo de orden m.

Para probar la igualdad construimos un $x \in H_J^2(K/k)$ que cumpla $\mathrm{Inv}_k(x) = [1/m]$. Basta tener en cuenta que m será el mínimo común múltiplo de un número finito de grados locales $n_1, \ldots, n_k$; claramente existen números $r_i \mid n_i$ primos entre sí dos a dos y cuyo producto es m; de aquí se obtienen fácilmente fracciones con denominador r_i y cuya suma es $1/m$; eligiendo componentes locales con invariantes dichas fracciones se obtiene un x que cumple lo pedido.

Así pues, $\mathrm{Inv}_k[H^2_J(K/k)] = \langle[1/m]\rangle$, e igualmente $\mathrm{Inv}_k\big[j[H^2_J(K/k)]\big] = \langle[1/m]\rangle$, con la diferencia de que los invariantes en C son inyectivos, luego concluimos que $j[H^2_J(K/k)]$ es un grupo cíclico de orden m, no necesariamente igual a n, que es el orden de $H^2_C(K/k)$.

Esto está relacionado con el grupo $H^3(K/k)$. En efecto, tenemos la sucesión exacta de cohomología

$$H^2_J(K/k) \longrightarrow H^2_C(K/k) \longrightarrow H^3(K/k) \longrightarrow H^3_J(K/k).$$

La teoría local y el teorema 17.3 implican que $H^3_J(K/k) = 1$, por lo que la aplicación $\delta^* : H^2_C(K/k) \longrightarrow H^3(K/k)$ es suprayectiva. Su núcleo es la imagen de j, que, según acabamos de ver, tiene m elementos, luego el grupo $H^3(K/k)$ es cíclico de orden n/m.

Más concretamente, si llamamos $\xi_{K/k} \in H^2_C(K/k)$ a la clase fundamental de la extensión, entonces $H^3(K/k)$ está generado por su imagen $t_{K/k}$ (conocida como *cociclo de Teichmuller).*

Con esto conocemos la estructura de los grupos de cohomología de dimensión 3 de las tres formaciones globales.

Finalmente citaremos el *teorema de las normas,* que es una consecuencia inmediata de que $H^1_C(K/k) = 1$. Si la extensión es cíclica, la periodicidad de los grupos de cohomología implica que $H^{-1}(K/k) = 1$, con lo que la inclusión $H^0(K/k) \longrightarrow H^0_J(K/k)$ es inyectiva. Esta inclusión se interpreta como la inclusión natural $k^*/\,\mathrm{N}[K^*] \longrightarrow J_k/\,\mathrm{N}[J_K]$, y la inyectividad se traduce en que un elemento de k^* es una norma desde K^* si y sólo si es una norma desde todas las extensiones locales. Esto es falso en general para extensiones no cíclicas.

17.5 El teorema de los ideales principales

Terminamos el capítulo con uno de los teoremas más celebrados de la teoría de cuerpos de clases. En 1899 Hilbert conjeturó la existencia de lo que hoy conocemos como el cuerpo de clases de Hilbert de un cuerpo numérico, y conjeturó sus propiedades fundamentales, es decir: si K es el cuerpo de clases de Hilbert de k, entonces la extensión K/k es abeliana, su grupo de Galois es isomorfo al grupo de clases de k, la extensión es no ramificada y los ideales primos que se escinden completamente en K son los principales. Él mismo demostró la existencia de un cuerpo con estas características cuando k es un cuerpo cuadrático, y en 1907 un alumno suyo, Furtwängler, demostró la existencia en el caso general. Sin embargo Hilbert había conjeturado una propiedad adicional que no fue demostrada hasta 1930 por el propio Furtwängler, a saber, que todos los ideales de k son principales cuando son considerados como ideales de K.

Este resultado se conoce como teorema de los ideales principales y puede considerarse como el colofón de la teoría que inició Kummer, según la cual en los anillos de enteros algebraicos tiene sentido hablar de divisores "ideales" que se comportan "como si fueran reales", es decir, como si fueran realmente enteros algebraicos a pesar de que no existen como tales. En términos algebraicos, el trabajo de Kummer mostraba que los ideales de un anillo de enteros algebraicos

pueden ser tratados en muchos aspectos como si fueran principales. El teorema de los ideales principales nos da una representación de los ideales de un cuerpo como ciertos enteros de su cuerpo de clases de Hilbert y explica en cierto modo este buen comportamiento que descubrió Kummer.

La prueba original de Furtwängler era bastante compleja. Poco más tarde, Iyanaga obtuvo una mucho más simple siguiendo una sugerencia de Artin.

Antes de adentrarnos más en el problema, conviene notar que en realidad es fácil convertir en principales los ideales de un cuerpo numérico dado. Por ejemplo, si $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ son representantes del grupo de clases de un cuerpo numérico k y h_i es el orden de $[\mathfrak{p}_i]$ en el grupo de clases, entonces $\mathfrak{p}_i^{h_i} = (\alpha_i)$ es principal, y basta considerar el cuerpo $K = k\big(\sqrt[h_i]{\alpha_i}, i = 1, \ldots, h\big)$.

Entonces, como ideales de K, se cumple claramente que $\mathfrak{p}_i = \big(\sqrt[h_i]{\alpha_i}\big)$. Todo ideal de k se diferencia de un $\mathfrak{p}_i$ en un ideal principal en k, que sigue siendo principal en K, luego todo ideal de k es principal en K.

Se puede mejorar las características de la extensión si adjuntamos además una raíz h-ésima primitiva de la unidad y las raíces h-ésimas de todas las unidades de k. Como el grupo de unidades es finitamente generado, la extensión resultante es finita, pero además es abeliana. El inconveniente es que el proceso se basa en ramificar ideales y adjuntar muchos elementos, por lo que obtenemos extensiones de grado elevado y discriminante elevado. El cuerpo de Hilbert es mucho más interesante en la práctica, si bien la prueba de que efectivamente principaliza a los ideales es mucho más compleja.

Está de más advertir que el teorema de los ideales principales no afirma que todos los ideales del cuerpo de clases de Hilbert de un cuerpo dado sean principales, sino sólo que los ideales de k se vuelven principales en el cuerpo de clases. Esto no impide que en general haya ideales no principales en la extensión.

La sugerencia de Artin a la que hacíamos referencia concernía a la propiedad del símbolo de Artin expresada por el primer diagrama conmutativo del teorema 16.23. Aquí la necesitamos en términos de ideales y no de clases de elementos ideales. Para ello, dada una cadena de cuerpos numéricos $k \subset K \subset L$, tomamos un divisor $\mathfrak{m}$ admisible para todas las extensiones y consideramos los diagramas siguientes

$$\begin{array}{ccccc}
I_k(\mathfrak{m})/P_{\mathfrak{m}}\,\mathrm{N}_k^L(\mathfrak{m}) & \longrightarrow & J_k/k^*\,\mathrm{N}[J_L] & \longrightarrow & G(L/k)\ /\ G'(L/k) \\
\downarrow & & \downarrow & & \downarrow \\
I_K(\mathfrak{m})/P_{\mathfrak{m}}\,\mathrm{N}_k^K(\mathfrak{m}) & \longrightarrow & J_K/K^*\,\mathrm{N}[J_L] & \longrightarrow & G(L/K)\ /\ G'(L/K)
\end{array}$$

Las dos primeras flechas verticales son los homomorfismos inducidos por las inclusiones, y la tercera la transferencia V dada por (15.5). Las flechas horizontales son los isomorfismos del teorema 6.21 y los isomorfismos de Artin. Es fácil comprobar que el primer diagrama es conmutativo, y el segundo lo es por el teorema 16.23. De aquí deducimos que, para todo ideal $\mathfrak{a} \in I_k(\mathfrak{m})$, se cumple

$$\left(\frac{L/K}{\mathfrak{a}}\right) = V\Big(\left(\frac{L/k}{\mathfrak{a}}\right)\Big).$$

Ésta es la relación que necesitamos. Consideremos ahora el caso particular en que k es un cuerpo numérico, K es su cuerpo de clases de Hilbert y L es el cuerpo de clases de Hilbert de K (con lo que podemos tomar $\mathfrak{m} = 1$). Por el teorema 11.1, sabemos que K es la mayor extensión abeliana de k contenida en L, es decir, que $G(L/K) \,/\, G'(L/K) = G(K/k)$ y, a través de esta identificación,

$$\left(\frac{L/k}{\mathfrak{a}}\right) = \left(\frac{K/k}{\mathfrak{a}}\right).$$

Esto es la versión para ideales de la propiedad d) del teorema 16.24. En definitiva, la relación anterior se convierte en

$$\left(\frac{L/K}{\mathfrak{a}}\right) = V\Big(\left(\frac{K/k}{\mathfrak{a}}\right)\Big),$$

para todo ideal $\mathfrak{a}$ de k.

El teorema de los ideales principales afirma que todo ideal de k es principal en K, pero el isomorfismo de Artin de L/K es un isomorfismo $I_K/P_K \cong G(K/k)$, luego, lo que hemos de probar es que, para todo ideal $\mathfrak{a}$ de k se cumple

$$\left(\frac{K/k}{\mathfrak{a}}\right) = 1.$$

Equivalentemente, hemos de probar que la transferencia

$$V : G(L/K) \longrightarrow G(K/k)$$

es trivial. Esto es un caso particular de un resultado mucho más general:

Teorema 17.20 (Teorema de los ideales principales) *Sea U un grupo tal que U' es abeliano y finitamente generado y U/U' es finito. Entonces la transferencia $V : U/U' \longrightarrow U'$ es trivial.*

Este teorema no es trivial, pero hemos reducido el problema a un resultado de la teoría de grupos pura. Necesitaremos algunos hechos generales sobre extensiones de grupos y módulos de escisión.

Sea G un grupo finito, A un G-módulo y U una extensión de A por G, es decir, U es un grupo que contiene a A como subgrupo normal y $U/A \cong G$. Sea $\{u_\sigma\}_{\sigma\in G}$ una transversal de U sobre A. Podemos tomarla de modo que el isomorfismo haga corresponder cada $\sigma \in G$ con la clase $[u_\sigma] \in U/A$. Además podemos exigir que $u_1 = 1$. Sea $\{a_{\sigma,\tau}\}$ el cociclo que determina la extensión respecto a esta transversal, es decir, el que cumple (14.11). En particular $a_{1,1} = 1$.

Sea B el módulo de escisión del cociclo $\{a_{\sigma,\tau}\}$, es decir, $B = A \oplus I$, donde I es el ideal de $\mathbb{Z}[G]$ generado por los elementos $d_\sigma = \sigma - 1$ y la acción de G es la determinada por $d_\sigma\tau = d_{\sigma\tau} - d_\tau + a_{\sigma,\tau}$.

Teorema 17.21 *Con la notación anterior, el grupo U/U' es isomorfo a B/BI. El isomorfismo hace corresponder cada clase $u_\sigma a U'$ con la clase $d_\sigma + a + BI$.*

DEMOSTRACIÓN: Sea $\log : U \longrightarrow B/BI$ la aplicación dada por

$$\log(u_\sigma a) = d_\sigma + a + BI.$$

Veamos que es un homomorfismo. En efecto:

$$\begin{aligned} \log(u_\sigma a\, u_\tau b) &= \log(u_{\sigma\tau} a_{\sigma,\tau} a^\tau b) = d_{\sigma\tau} + a_{\sigma,\tau} + a\tau + b + BI, \\ \log(u_\sigma a) + \log(u_\tau b) &= d_\sigma + a + d_\tau + b + BI. \end{aligned}$$

Notar que usamos notación multiplicativa a^τ cuando consideramos a A como subgrupo de U y notación aditiva $a\tau$ cuando lo consideramos como G-módulo. Ahora probamos que ambas clases son la misma:

$$d_{\sigma\tau} + a_{\sigma,\tau} + a\tau + b - (d_\sigma + a + d_\tau + b) = d_{\sigma\tau} + (d_\sigma\tau - d_{\sigma\tau} + d_\tau) + a\tau - d_\sigma - a - d_\tau$$

$$= d_\sigma\tau + a\tau - d_\sigma - a = d_\sigma(\tau - 1) + a(\tau - 1) \in BI.$$

Como B/BI es un grupo abeliano, el homomorfismo log induce un homomorfismo en el cociente $\log : U/U' \longrightarrow B/BI$.

Recíprocamente definimos $\exp : B \longrightarrow U/U'$ como el homomorfismo determinado por $\exp a = aU'$, para cada $a \in A$ y $\exp d_\sigma = u_\sigma U'$, para cada $\sigma \in G$ (tener presente la estructura de $B = A \oplus I$). En principio la igualdad $\exp d_\sigma = u_\sigma U'$ la podemos exigir sólo para $\sigma \neq 1$, pero, teniendo en cuenta que $u_1 = 1$, se cumple trivialmente en este caso. De este modo vemos que $\exp(d_\sigma + a) = u_\sigma a U'$. Si probamos que BI está contenido en el núcleo de exp tendremos que exp inducirá un homomorfismo $\exp : B/BI \longrightarrow U/U'$, que obviamente será el inverso de log, luego el teorema quedará probado. En efecto:

$$\begin{aligned} \exp\big(a(\tau - 1)\big) &= a^\tau a^{-1} U' = a a^{-1} U' = 1, \\ \exp\big(d_\sigma(\tau - 1)\big) &= \exp(d_{\sigma\tau} - d_\tau + a_{\sigma,\tau} - d_\sigma) = u_{\sigma\tau} u_\tau^{-1} a_{\sigma,\tau} u_\sigma^{-1} U' \\ &= u_\sigma u_\tau u_\sigma^{-1} u_\tau^{-1} U' = 1. \end{aligned}$$

■

Teorema 17.22 *En las condiciones anteriores, si $\alpha \in \mathbb{Z}[G]$, se cumple $B\alpha \subset A$ si y sólo si $\alpha = mT$, para un cierto $m \in \mathbb{Z}$, donde $T = \sum_{\sigma \in G} \sigma$ es la traza de G.*

DEMOSTRACIÓN: Puesto que $B\alpha = A \oplus I\alpha$, la condición $B\alpha \subset A$ equivale a que $I\alpha \subset A \cap I = 0$, es decir, a que $I\alpha = 0$ o, equivalentemente, a que $(\tau - 1)\alpha = 0$ para todo $\tau \in G$.

Sea $\alpha = \sum_{\sigma \in G} m_\sigma \sigma$, con $m_\sigma \in \mathbb{Z}$. Entonces $\tau\alpha = \sum_{\sigma \in G} m_{\tau^{-1}\sigma} \sigma$, y la condición $\tau\alpha = \alpha$ equivale a que $m_{\tau^{-1}\sigma} = m_\sigma$, para todo $\sigma \in G$. En particular, $m_1 = m_\tau$ para todo $\tau \in G$. La conclusión es ahora evidente. ■

Teorema 17.23 *A través del isomorfismo del teorema* 17.21, *la transferencia $V : U/U' \longrightarrow A$ se corresponde con el homomorfismo $T : B/IB \longrightarrow A$ determinado por la multiplicación por la traza.*

DEMOSTRACIÓN: Ante todo, las trazas están en A por el teorema anterior. Para calcular $V(u_\sigma U')$ mediante (15.5) podemos usar como transversal derecha la propia $\{u_\tau\}$. Así, puesto que, según (14.11), $u_\sigma u_\tau = u_{\sigma\tau} a_{\sigma,\tau}$, tenemos que $\widetilde{u_\sigma u_\tau} = a_{\sigma,\tau}$, de donde

$$V(u_\sigma U') = \sum_{\tau\in G} a_{\sigma,\tau} = \sum_{\tau\in G}(d_{\sigma\tau} + d_\tau - d_{\sigma\tau}) = \sum_{\tau\in G} d_{\sigma\tau} = d_\sigma T = \log(u_\sigma U')T.$$

Sobre los elementos aU' tenemos que $au_\tau = u_\tau a^\tau$, luego $\widetilde{au_\tau} = a^\tau = a\tau$. Por consiguiente

$$V(aU') = \sum_{\tau\in G} a\tau = aT = \log(aU')T.$$

Claramente esto implica que $V(\alpha) = (\log\alpha)T$ para todo $\alpha \in U/U'$. ∎

Con esto estamos es condiciones de probar el teorema de los ideales principales:

DEMOSTRACIÓN: Tenemos un grupo U tal que el derivado $A = U'$ es abeliano y finitamente generado y el cociente $G = U/U'$ es finito. Hemos de probar que la transferencia $V : U/U' \longrightarrow A$ es trivial.

Esta situación es un caso particular de la que estábamos considerando en los teoremas anteriores. Continuamos con la misma notación: la transversal $\{u_\sigma\}$, el cociclo $a_{\sigma,\tau}$, el módulo de escisión B, etc. Según el teorema anterior, basta probar que $bT = 0$, para todo $b \in T$.

Puesto que $B/A \cong I$, se trata de un grupo abeliano finitamente generado (libre, de hecho). Por hipótesis A también lo es, de donde concluimos que B es finitamente generado. El grupo B/BI es abeliano y finito (es isomorfo a G). Digamos que tiene n elementos. Podemos descomponerlo en producto directo de grupos cíclicos. Sean $b_1, \ldots, b_m$ elementos de B cuyas clases módulo BI generen los factores. Sea e_i el orden de $b_i + BI$.

Por otro lado, BI es un subgrupo de B, que es finitamente generado, luego BI también lo es. Sea $b_{m+1}, \ldots, b_s$ un generador de BI. Definimos $e_i = 1$ para $i = m+1, \ldots, s$. Entonces tenemos:

a) $b_1, \ldots, b_s$ son un sistema generador de B.

b) $e_i b_i \in BI$ para $i = 1, \ldots, s$.

c) $e_1 \cdots e_s = n$.

Por a) tenemos que $B = \sum_{j=1}^{s} \mathbb{Z} b_j$, luego $IB = \sum_{j=1}^{s} I b_j$, luego por b) existen elementos $\alpha_{ij} \in I$ tales que

$$e_i b_i = \sum_{j=1}^{s} \alpha_{ij} b_j.$$

Llamando $\gamma_{ij} = e_i\delta_{ij} - a_{ij}$ (donde (δ_{ij}) es la matriz identidad de orden s), tenemos

$$\sum_{j=1}^{s} \gamma_{ij} b_j = 0. \tag{17.4}$$

La matriz (γ_{ij}) tiene sus coeficientes en el anillo $\mathbb{Z}[G]$, y lo mismo le sucede a su matriz adjunta, es decir, a la matriz (β_{ij}) que cumple

$$(\beta_{ij})(\gamma_{ij}) = \det(\gamma_{ij})(\delta_{ij}).$$

Llamemos $\Delta = \det(\gamma_{ij}) \in \mathbb{Z}[G]$. Multiplicando (17.4) por β_{ki} y sumando sobre i queda: $\Delta b_k = 0$, para $k = 1, \ldots, s$.

Como los elementos b_k generan B, vemos que $\Delta B = 0$ y, en particular, $\Delta B \subset A$. Por el teorema 17.22 tenemos que $\Delta = rT$, para un $r \in \mathbb{Z}$. Basta probar que $r = 1$, pues entonces tendremos que $Tb = 0$ para todo $b \in B$, como queríamos probar.

Consideremos el homomorfismo de anillos $f : \mathbb{Z}[G] \longrightarrow \mathbb{Z}$ dado por

$$f\Big(\sum_{\tau\in G} n_\tau \tau\Big) = \sum_{\tau\in G} n_\tau.$$

Su núcleo es I. Claramente $f(\Delta) = f(rT) = rn$, pero, por otro lado,

$$\begin{aligned} f(\Delta) &= f(\det \gamma_{ij}) = \det\big(f(\gamma_{ij})\big) = \det\big(f(e_i\delta_{ij} - a_{ij})\big) = \det\big(f(e_i\delta_{ij})\big) \\ &= e_1 \cdots e_s = n. \end{aligned}$$

Así pues, $r = 1$. ∎

Apéndice A

El lema de Hensel

En este apéndice probaremos un resultado importante sobre cuerpos completos no arquimedianos, del cual deduciremos entre otras cosas que la hipótesis de separabilidad del teorema 2.13 (y de sus consecuencias) puede eliminarse.

En primer lugar observamos que si K es un cuerpo métrico no arquimediano (no necesariamente discreto), podemos definir su *anillo de enteros* como

$$E = \{\alpha \in K \mid |\alpha| \leq 1\}.$$

Claramente se trata de un anillo y K es su cuerpo de cocientes. Las unidades de E son los elementos de K con valor absoluto 1. También es claro que E tiene un único ideal maximal, a saber,

$$\mathfrak{p} = \{\alpha \in K \mid |\alpha| < 1\}.$$

(Notar que $\mathfrak{p}$ está formado por los elementos no unitarios de E.)

También tenemos definido el *cuerpo de restos* $\overline{K} = E/\mathfrak{p}$.

Teorema A.1 *Sea K un cuerpo métrico no arquimediano. Entonces cualquier valor absoluto de K se extiende a un valor absoluto no arquimediano sobre el cuerpo de fracciones algebraicas $K(x)$ de manera que para cada polinomio $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ se cumple $|f(x)| = \max\limits_{0\leq i\leq n} \{|a_i|\}$.*

Demostración: Consideremos la aplicación definida sobre el anillo de polinomios $K[x]$ como indica el enunciado y vamos a probar que verifica los axiomas de un valor absoluto no arquimediano.

El único que no es inmediato es que esta aplicación conserva los productos. Si tenemos dos polinomios f y g con coeficientes $\{a_i\}$ y $\{b_j\}$ entonces un coeficiente de su producto es de la forma $\sum\limits_{i=0}^{k} a_i b_{k-i}$, y ciertamente

$$\Big|\sum_{i=0}^{k} a_i b_{k-i}\Big| \leq \max_i |a_i b_{k-i}| \leq \max_i |a_i| \max_j |b_j|,$$

de donde $|f(x)g(x)| \leq |f(x)|\,|g(x)|$. Hemos de probar la igualdad.

Llamemos $f_1(x)$ a la suma de los monomios $a_i x^i$ tales que $|a_i| = |f(x)|$ y $f_2(x)$ a la suma de los monomios restantes. Así $f(x) = f_1(x) + f_2(x)$. Descomponemos igualmente $g(x) = g_1(x) + g_2(x)$. Notar que $|f_2(x)| < |f_1(x)|$ y $|g_2(x)| < |g_1(x)|$. Así

$$f(x)g(x) = f_1(x)g_1(x) + f_1(x)g_2(x) + f_2(x)g_1(x) + f_2(x)g_2(x).$$

Es fácil ver que el valor absoluto de los tres últimos factores es estrictamente menor que el del primero, luego por la desigualdad triangular no arquimediana (que ya hemos dicho que se cumple) concluimos que $|f(x)g(x)| = |f_1(x)g_1(x)|$.

Por la desigualdad ya probada $|f_1(x)g_1(x)| \leq |f_1(x)|\,|g_1(x)|$ y, considerando el coeficiente director, vemos que de hecho se tiene la igualdad. Así pues $|f(x)g(x)| = |f_1(x)|\,|g_1(x)| = |f(x)||g(x)|$.

Esta propiedad justifica que $|f(x)/g(x)| = |f(x)|/|g(x)|$ no depende del representante elegido para la fracción algebraica y claramente es un valor absoluto en $K(x)$ (conviene probar la desigualdad triangular usual, y el hecho de que la restricción a K sea el valor absoluto no arquimediano de partida implica que la extensión es no arquimediana). ∎

Observar que los distintos valores absolutos de K inducen valores absolutos equivalentes en $K(x)$, por lo que, en definitiva, cada cuerpo métrico no arquimediano K induce una única estructura de cuerpo métrico no arquimediano en $K(x)$. Veamos ahora un resultado técnico previo al lema de Hensel.

Teorema A.2 *Sea K un cuerpo métrico no arquimediano, sean dos polinomios $g(x)$, $g_0(x) \in K[x]$ de modo que $g_0(x)$ es mónico y $|g_0(x)| \leq 1$. Consideremos la división euclídea*

$$g(x) = g_0(x)c(x) + r(x), \qquad \operatorname{grad} r(x) < \operatorname{grad} g_0(x), \qquad c(x), r(x) \in K[x].$$

Entonces $|r(x)| \leq |g(x)|$.

Demostración: Sean

$$g(x) = a_n x^n + \cdots + a_1 x + a_0, \qquad g_0(x) = x^m + \cdots + b_1 x + b_0.$$

Entonces

$$|g_0(x)a_n x^{n-m}| = |g_0(x)|\,|a_n| \leq |a_n| \leq |g(x)|,$$

luego $|g(x) - g_0(x)a_n x^{n-m}| \leq |g(x)|$. Continuando el proceso de la división llegamos a que $|r(x)| \leq |g(x)|$. ∎

Si K es un cuerpo métrico no arquimediano, E es su anillo de enteros y

$$\mathfrak{p} = \{f(x) \in E[x] \mid |f(x)| < 1\},$$

es claro que $\mathfrak{p}$ es un ideal primo de $E[x]$ y que el cociente $E[x]/\mathfrak{p}$ es isomorfo de forma natural al anillo de polinomios $\overline{K}[x]$. Representaremos por $\bar{f}(x)$ la clase de $f(x)$ en el cociente.

Teorema A.3 (Lema de Hensel) *Sea K un cuerpo métrico completo no arquimediano y sea E su anillo de enteros. Supongamos que un polinomio de $E[x]$ factoriza módulo $\mathfrak{p}$ como $\bar{f}(x) = \bar{g}_0(x)\bar{h}_0(x)$, donde $g_0(x)$ es mónico y $\bar{g}_0(x)$ y $\bar{h}_0(x)$ son primos entre sí. Entonces existen polinomios $g(x)$, $h(x) \in E[x]$ tales que $f(x) = g(x)h(x)$, $g(x)$ es mónico, tiene el mismo grado que $g_0(x)$ y $\bar{g}(x) = \bar{g}_0(x)$, $\bar{h}(x) = \bar{h}_0(x)$.*

DEMOSTRACIÓN: Por hipótesis existe un polinomio $p(x) \in E[x]$ tal que

$$f(x) = g_0(x)h_0(x) + p(x) \qquad \text{y} \qquad |p(x)| < 1. \tag{A.1}$$

El hecho de que $\bar{g}_0(x)$ y $\bar{h}_0(x)$ sean primos entre sí se traduce en que existen polinomios $a(x)$, $b(x)$, $c(x) \in E[x]$ de modo que

$$a(x)g_0(x) + b(x)h_0(x) = 1 + c(x) \qquad \text{y} \qquad |c(x)| < 1. \tag{A.2}$$

Multiplicamos por $p(x)$:

$$a(x)p(x)g_0(x) + b(x)p(x)h_0(x) = p(x) + c(x)p(x). \tag{A.3}$$

Dividimos $b(x)p(x)$ y $c(x)p(x)$ entre $g_0(x)$:

$$\begin{aligned} b(x)p(x) &= g_0(x)q(x) + u_1(x), \qquad \operatorname{grad} u_1(x) < \operatorname{grad} g_0(x), & \text{(A.4)}\\ c(x)p(x) &= g_0(x)q_1(x) + r(x), \qquad \operatorname{grad} r(x) < \operatorname{grad} g_0(x). & \text{(A.5)} \end{aligned}$$

El teorema anterior nos da

$$\begin{aligned} |u_1(x)| &\leq |b(x)p(x)| = |b(x)|\,|p(x)| \leq |p(x)| < 1, & \text{(A.6)}\\ |r(x)| &\leq |c(x)p(x)| = |c(x)||p(x)| \leq |p(x)| < 1. & \text{(A.7)} \end{aligned}$$

Sustituyendo (A.4) y (A.5) en (A.3) obtenemos:

$$\big(a(x)p(x) + q(x)h_0(x) - q_1(x)\big)g_0(x) + u_1(x)h_0(x) = p(x) + r(x).$$

Llamamos $v_1(x)$ a la expresión entre paréntesis, y así queda

$$v_1(x)g_0(x) + u_1(x)h_0(x) = p(x) + r(x). \tag{A.8}$$

La desigualdad triangular junto con (A.6), (A.7) y (A.8) nos da que

$$|v_1(x)g_0(x)| \leq \text{máx}\{|u_1(x)h_0(x)|, |p(x)|, |r(x)|\} = |p(x)|$$

y, como $|g_0(x)| = 1$, concluimos que

$$|v_1(x)| \leq |p(x)| < 1. \tag{A.9}$$

Definimos

$$\begin{aligned} g_1(x) &= g_0(x) + u_1(x), & \text{(A.10)}\\ h_1(x) &= h_0(x) + v_1(x). & \text{(A.11)} \end{aligned}$$

Así $g_1(x)$ es mónico y del mismo grado que $g_0(x)$. Por (A.6) y (A.9) resulta

$$|g_1(x)| = |g_0(x)| = 1, \quad |h_1(x)| \leq 1, \quad \bar{g}_1(x) = \bar{g}_0(x), \quad \bar{h}_1(x) = \bar{h}_0(x).$$

Sea

$$p_1(x) = f(x) - g_1(x)h_1(x). \tag{A.12}$$

Usando (A.1) y (A.8) tenemos

$$\begin{aligned} p_1(x) &= f(x) - g_0(x)h_0(x) - g_0(x)v_1(x) - u_1(x)h_0(x) - u_1(x)v_1(x) \\ &= p(x) - p(x) - r(x) - u_1(x)v_1(x) = -r(x) - u_1(x)v_1(x), \end{aligned}$$

luego por (A.6), (A.7) y (A.9)

$$\begin{aligned} |p_1(x)| &\leq \text{máx}\big\{|r(x)|, |u_1(x)v_1(x)|\big\} \leq \text{máx}\big\{|c(x)|\,|p(x)|, |p(x)|\,|p(x)|\big\} \\ &\leq \text{máx}\big\{|c(x)|, |p(x)|\big\}|p(x)| = k|p(x)|, \end{aligned} \tag{A.13}$$

donde $k = \text{máx}\big\{|c(x)|, |p(x)|\big\} < 1$. Más aún, (A.2), (A.10) y (A.11) implican

$$\begin{aligned} a(x)g_1(x) + b(x)h_1(x) &= a(x)g_0(x) + a(x)u_1(x) + b(x)h_0(x) + b(x)v_1(x) \\ &= 1 + c(x) + a(x)u_1(x) + b(x)v_1(x) = 1 + c_1(x), \end{aligned}$$

con $c_1(x) = c(x) + a(x)u_1(x) + b(x)v_1(x)$ y, en virtud de (A.6), (A.9) y (A.13),

$$|c_1(x)| < 1, \quad \text{máx}\big\{|c_1(x)|, |p_1(x)|\big\} \leq \text{máx}\big\{|c(x)|, |p(x)|\big\} = k.$$

Por otro lado,

$$\begin{aligned} &\text{grad}(g_1(x)h_1(x)) = \text{grad}(g_0(x)h_1(x)) \\ &\quad\leq [(A.11)]\,\text{máx}\big\{\text{grad}(g_0(x)h_0(x)), \text{grad}(g_0(x)v_1(x))\big\} \\ &\quad\leq [(A.1), (A.8)]\,\text{máx}\big\{\text{grad}\, f(x), \text{grad}\, p(x), \text{grad}(u_1(x)h_0(x)), \text{grad}\, r(x)\big\} \\ &\quad\leq [(A.1), (A.4), (A.5)]\,\text{máx}\big\{\text{grad}\, f(x), \text{grad}\, p(x)\big\} = m. \end{aligned}$$

En resumen tenemos dos polinomios $g_1(x)$, $h_1(x)$ que cumplen las hipótesis del teorema en lugar de $g_0(x)$ y $h_0(x)$ y además

$$|p_1(x)| \leq k|p(x)|, \qquad \text{grad}(g_1(x)h_1(x)) \leq m.$$

Podemos repetir el proceso indefinidamente, y así obtenemos polinomios $g_n(x)$, $h_n(x)$, $p_n(x)$, $u_n(x)$, $v_n(x)$ tales que

$$\begin{aligned} g_n(x) &= g_0(x) + \sum_{i=1}^{n} u_i(x), \quad |u_i(x)| \leq |p_{i-1}(x)| \leq k^i, \\ h_n(x) &= h_0(x) + \sum_{i=1}^{n} v_i(x), \quad |v_i(x)| \leq |p_{i-1}(x)| \leq k^i, \\ f(x) &= g_n(x)h_n(x) + p_n(x), \quad |p_n(x)| \leq k^{n+1}. \end{aligned}$$

Además los polinomios $g_n(x)$ son mónicos, todos del mismo grado y

$$\operatorname{grad} h_n(x) \leq m - \operatorname{grad} g_0(x).$$

Definimos

$$g(x) = g_0(x) + \sum_{i=1}^{\infty} u_i(x), \qquad h(x) = h_0(x) + \sum_{i=1}^{\infty} v_i(x).$$

Notar que la convergencia de las series no se sigue simplemente de que las sucesiones $|u_i(x)|$ y $|v_i(x)|$ tiendan a 0, pues $K(x)$ no es completo, pero el grado de los sumandos está acotado y, al intercambiar formalmente las series con las sumas de cada polinomio, obtenemos un polinomio cuyos coeficientes son series convergentes (pues K sí que es completo) y es fácil ver que tales polinomios son realmente las sumas de las series.

Por otro lado es claro que la sucesión $p_n(x)$ tiende a 0, luego $f(x) = g(x)h(x)$. Claramente

$$|g(x) - g_0(x)| \leq \max_i \{|u_i(x)|\} < 1, \qquad |h(x) - h_0(x)| \leq \max_i \{|v_i(x)|\} < 1$$

y además $g(x)$ es mónico y tiene el mismo grado que $g_0(x)$. ∎

Veamos dos casos particulares:

Teorema A.4 *Sea K un cuerpo completo no arquimediano y*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

un polinomio con coeficientes enteros (en K), $a_n \neq 0$. Si $|a_n| < 1$ y $|a_i| = 1$ para un $i \neq 0$ entonces f es reducible.

Demostración: Sea $0 < i < n$ el mayor índice tal que $|a_i| = 1$. Definimos

$$g_0(x) = \frac{1}{a_i}(a_i x^i + \cdots + a_1 x + a_0), \qquad h_0(x) = a_i.$$

Claramente ambos polinomios tienen coeficientes enteros, son primos entre sí, $g_0(x)$ es mónico y

$$|f(x) - g_0(x)h_0(x)| = |a_n x_n + \cdots + a_{i+1} x^{i+1}| < 1.$$

También es obvio que $\bar{g}_0(x)$ y $\bar{h}_0(x)$ son primos entre sí. El lema de Hensel implica que f se descompone en producto de dos polinomios, uno de grado i y otro de grado $n - i$, luego es reducible. ∎

Teorema A.5 *Sea K un cuerpo completo no arquimediano y $f(x)$ un polinomio mónico irreducible en $K[x]$. Si el término independiente de $f(x)$ es entero, entonces los coeficientes restantes también lo son.*

DEMOSTRACIÓN: Sea c el coeficiente de $f(x)$ con mayor valor absoluto. Hemos de probar que $|c| \leq 1$. En caso contrario $f(x)/c$ tiene todos sus coeficientes enteros y uno de ellos igual a 1. Su coeficiente director es $1/c$, y se cumple $|1/c| < 1$, luego por el teorema anterior $f(x)$ sería reducible, en contra de lo supuesto. ∎

Nos ocupamos ahora del problema de extender el valor absoluto de un cuerpo completo a una extensión finita. En primer lugar probamos la unicidad de la extensión. El teorema siguiente es más preciso que 2.12.

Teorema A.6 *Sea k un cuerpo métrico completo y K/k una extensión finita de grado n. Si un valor absoluto de k se extiende a K, entonces la extensión viene dada necesariamente por $|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}$, para todo $\alpha \in K$, donde $\mathrm{N} : K \longrightarrow k$ es la norma de K/k.*

DEMOSTRACIÓN: Sea $\{\alpha_1, \ldots, \alpha_n\}$ una k-base de K. Si $\alpha \in K$ se expresa como

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n, \qquad \text{con } x_1, \ldots, x_n \in k,$$

teniendo en cuenta el teorema 2.10, es claro que la aplicación

$$\|\alpha\| = \max_{1\leq i\leq n} |x_i|$$

es una norma en K, que por 2.11 será equivalente al valor absoluto de K.

Tomemos un $\alpha \in K$ tal que $|\alpha| < 1$. Entonces la sucesión $\{\alpha^m\}$ tiende a 0 (para el valor absoluto y, por lo tanto, para la norma). Sea

$$\alpha^m = x_{m1}\alpha_1 + \cdots + x_{mn}\alpha_n, \qquad \text{con } x_{mj} \in k.$$

La convergencia en norma implica que las sucesiones $\{x_{mj}\}_m$ tienden a 0 (respecto al valor absoluto de k).

Notemos que $N(x_{m1}\alpha_1 + \cdots + x_{mn}\alpha_n)$ se calcula como producto de n polinomios homogéneos lineales en las variables $x_1, \ldots, x_n$. No es difícil ver que sus coeficientes están en k, luego concluimos[1] que $\{N(\alpha^m)\}$ converge a 0 en k.

Como $\mathrm{N}(\alpha^m) = \mathrm{N}(\alpha)^m$, concluimos que $|\,\mathrm{N}(\alpha)| < 1$. Tomando inversos deducimos que si $|\alpha| > 1$ entonces $|\,\mathrm{N}(\alpha)| > 1$. Por lo tanto $|\alpha| = 1$ si y sólo si $|\,\mathrm{N}(\alpha)| = 1$.

Ahora, si $\alpha \in K$ es no nulo, tenemos $\mathrm{N}(\alpha^n/\,\mathrm{N}(\alpha)) = 1$, luego $|\alpha^n/\,\mathrm{N}(\alpha)| = 1$ y así $|\alpha|^n = \mathrm{N}(\alpha)$. Como $|\alpha| > 0$ podemos tomar raíces n-simas. ∎

Para completar este teorema sólo falta probar que $|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}$ es realmente un valor absoluto en K.

Teorema A.7 *Sea k un cuerpo métrico completo. Sea K/k una extensión finita de grado n. Entonces cada valor absoluto de k se extiende de forma única a un valor absoluto de K que viene dado por $|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}$.*

[1] Alternativamente, los coeficientes están en una extensión finita de k, las sucesiones $\{x_{mj}\}_m$ tienden a 0 respecto a la norma en dicha extensión, luego la sucesión $\{N(\alpha^m)\}$ converge a 0 en dicha extensión y, al estar en k, converge a 0 en k.

DEMOSTRACIÓN: La única extensión no trivial de un cuerpo arquimediano completo es $\mathbb{C}/\mathbb{R}$ con la topología usual, y en tal caso el resultado es evidente (ver la sección 2.6). Podemos suponer, pues, que k es no arquimediano.

Es obvio que la aplicación $|\alpha| = \sqrt[n]{|\,\mathrm{N}(\alpha)|}$ extiende al valor absoluto de k, así como que satisface los axiomas de valor absoluto salvo quizá la desigualdad triangular.

Hemos de probar que si $|\alpha| \le |\beta|$ entonces $|\alpha+\beta| \le |\beta|$ o, equivalentemente, que $|\alpha/\beta+1| \le 1$, para todo α, $\beta \in K$, $\beta \neq 0$. Alternativamente, basta ver que si $|\alpha| \le 1$ entonces $|\alpha+1| \le 1$. En nuestro caso concreto esto equivale a que si $|\,\mathrm{N}(\alpha)| \le 1$ entonces $|\,\mathrm{N}(\alpha+1)| \le 1$. Como $\mathrm{N}_{K/k}(\alpha) = (\mathrm{N}_{k(\alpha)/k}(\alpha))^{|K:k(\alpha)|}$, podemos suponer que $K = k(\alpha)$.

Sea $f(x)$ el polinomio mínimo de α en $k[x]$. Su término independiente es, salvo el signo, $\mathrm{N}_{K/k}(\alpha)$, luego es entero en k. El teorema A.5 implica que todos sus coeficientes son enteros. El polinomio mínimo de $\alpha+1$ es $f(x-1)$, que también tiene sus coeficientes enteros, en particular su término independiente, luego $|\,\mathrm{N}(\alpha+1)| \le 1$. ∎

Notemos que dos valores absolutos de k se diferencian en un exponente, luego lo mismo les sucede a sus extensiones. Así pues, la estructura métrica que obtenemos en K no depende del valor absoluto de k del que partamos, y así K se convierte en un cuerpo métrico completo de modo que sus valores absolutos están en biyección con los de k (la completitud la garantiza 2.12).

Ahora probaremos los resultados sobre el grado de inercia y el índice de ramificación que en el capítulo II se prueban para extensiones separables. En primer lugar observamos que si, en las condiciones del teorema anterior, el valor absoluto de k está inducido por una valoración v, entonces su extensión a K está inducida por una valoración v^* que cumple $v^*(\alpha) = ev(\alpha)$, para todo $\alpha \in k^*$, donde e es un cierto número natural no nulo.

En efecto, si el valor absoluto de k es $|\alpha| = r^{v(\alpha)}$, con $0 < r < 1$, entonces la imagen de k^* por el valor absoluto es el subgrupo cíclico de $\mathbb{R}^*$ generado por r. La imagen de K^* por la norma es un subgrupo de k^*, y la imagen de éste por el valor absoluto de k es un subgrupo de $\langle r\rangle$, luego será de la forma $\langle r^f\rangle$, para un cierto natural no nulo f. Las raíces n-simas de los elementos de este grupo forman el grupo $\langle r^{f/n}\rangle$. Así pues, para cada $\alpha \in K^*$ existe un único entero $v^*(\alpha)$ tal que $|\alpha| = r^{(f/n)v^*(\alpha)}$. Equivalentemente,

$$v^*(\alpha) = \frac{n \log|\alpha|}{f \log r}.$$

Es fácil ver que v^* es una valoración en K que induce su valor absoluto. También es claro que si $\alpha \in k^*$ entonces $v^*(\alpha) = ev(\alpha)$, donde $e = n/f$. Tomando un $\alpha \in k^*$ tal que $v(\alpha) = 1$ concluimos que e es un número natural.

En estas condiciones es claro que el anillo de enteros de k está contenido en el anillo de enteros de K. Más aún, si π es un primo en K y ρ es un primo en k (es decir, $v^*(\pi) = 1$ y $v(\rho) = 1$), tenemos que $|\rho| = |\pi|^e$.

Con esto tenemos definido el índice de ramificación de la extensión, y claramente es multiplicativo (es decir, el índice de una cadena de extensiones es el producto de los índices). Para definir el grado de inercia hemos de justificar que la extensión de los cuerpos de restos $\overline{K}/\overline{k}$ es finita.

Sea π un primo en K y sea $\{[\omega_1],\dots,[\omega_f]\}$ un conjunto $\overline{k}$-linealmente independiente en $\overline{K}$. Veamos que $\omega_i\pi^j$, para $i=1,\dots,f$, $j=0,\dots,e-1$ son k-linealmente independientes en K. Consideremos una combinación lineal

$$\sum_{i,j} c_{ij}\,\omega_i\,\pi^j, \qquad \text{con } c_{ij}\in k.$$

Fijado j, supongamos que algún coeficiente c_{ij} es no nulo. Reordenándolos podemos suponer que $c_{1j}\neq 0$ es el coeficiente con mayor valor absoluto. Entonces

$$\Big|\sum_i c_{ij}\,\omega_i\Big| = |c_{1j}|\,\left|\omega_1+\frac{c_{2j}}{c_{1j}}\,\omega_2+\cdots+\frac{c_{fj}}{c_{1j}}\,\omega_f\right|.$$

Todos los coeficientes de la última combinación lineal son enteros, luego podemos tomar clases módulo el primo de K. Como el coeficiente de $[\omega_1]$ es 1, concluimos que toda la combinación lineal es no nula, es decir, que no está en el ideal primo de K (pero es entera), luego es una unidad y tiene valor absoluto 1. En definitiva (y teniendo en cuenta la reordenación que hemos hecho)

$$\Big|\sum_i c_{ij}\,\omega_i\Big| = \max_i |c_{ij}|.$$

Obviamente, si todos los coeficientes fueran nulos esta igualdad se sigue cumpliendo. Por lo tanto

$$\Big|\sum_i c_{ij}\,\omega_i\,\pi^j\Big| = |\pi|^j\ \max_i |c_{ij}|.$$

La imagen de K^* por el valor absoluto es el subgrupo $G_K=\langle|\pi|\rangle$ de $\mathbb{R}^*$, mientras que la imagen de k^* es el subgrupo $G_k=\langle|\pi|^e\rangle$. Claramente, las potencias $|\pi|^j$, para $j=0,\dots,e-1$, son representantes de las e clases del cociente G_K/G_k, luego los miembros derechos de la igualdad anterior son representantes de esas mismas clases. En particular son distintos dos a dos, luego la desigualdad triangular no arquimediana para su suma es de hecho una igualdad:

$$\Big|\sum_{i,j} c_{ij}\,\omega_i\,\pi^j\Big| = \max_j\Big|\sum_i c_{ij}\,\omega_i\,\pi^j\Big| = \max_{i,j}|c_{ij}|\,|\pi|^j. \tag{A.14}$$

Ahora es claro que los elementos $\omega_i\,\pi^j$ son linealmente independientes (en particular distintos dos a dos), pues si el miembro izquierdo es nulo el miembro derecho muestra que todos los c_{ij} son nulos.

En particular esto prueba que la extensión de cuerpos de restos $\overline{K}/\overline{k}$ es finita, con lo que tenemos definido el grado de inercia f y es inmediato que es multiplicativo.

Supongamos ahora que $[\omega_1], \ldots, [\omega_f]$ son una $\overline{k}$-base de $\overline{K}$ y veamos que los elementos $\omega_i\,\pi^j$ son una k-base de K. Con esto habremos probado también la relación $n = ef$, donde n es el grado de la extensión.

Aplicaremos el teorema [7.16]. Para cada entero n sea $n = ke + r$, con $0 \le r < e$. Definimos $\pi_n = \rho^k \pi^r$. De este modo $v^*(\pi_n) = n$. Sea A un conjunto de representantes de las clases de $\overline{K}$ formado por combinaciones lineales de $\omega_1, \ldots, \omega_f$ con coeficientes en k (enteros). Según el teorema [7.16] todo $\alpha \in K$ se expresa en la forma

$$\alpha = \sum_{n=s}^{+\infty} x_n \pi_n, \qquad \text{con } x_n \in A, \quad s \in \mathbb{Z}.$$

Equivalentemente

$$\alpha = \sum_{n=s}^{+\infty} \sum_{r=0}^{e-1} \left(\sum_{i=1}^{f} a_{kri}\,\omega_i \right) \rho^k \pi^r = \sum_{r=0}^{e-1} \sum_{i=1}^{f} \left(\sum_{k=s}^{+\infty} a_{kri}\,\rho^k \right) \omega_i\,\pi^r.$$

(Todas las series en cuerpos no arquimedianos pueden ser reordenadas.)

Esto prueba que los elementos $\omega_i\,\pi^j$ son ciertamente una k-base de K, luego en efecto $n = ef$. Más aún, vamos a ver que los enteros de K son exactamente los elementos con coordenadas enteras en esta base. Obviamente los elementos con coordenadas enteras son enteros. Supongamos ahora que

$$\alpha = \sum_{i,j} c_{ij}\,\omega_i\,\pi^j, \qquad |\alpha| \le 1.$$

La igualdad (A.14) prueba que $|c_{ij}\pi^j| \le 1$, luego $|c_{ij}| \le |\pi|^{-j} < |\pi|^{-e} = |\rho|^{-1}$.

Equivalentemente, $v(c_{ij}) > -v(\rho) = -1$, luego $v(c_{ij}) \ge 0$ y así cada c_{ij} es entero.

Para acabar sólo queda probar que el anillo de enteros de K es la clausura entera en K del anillo de enteros de k. De este modo tales anillos formarán una extensión de dominios de Dedekind.

Dado un entero $\alpha \in K$, el valor absoluto de K se puede prolongar hasta una extensión que contenga todos los conjugados de α. La unicidad de la extensión hace que los k-isomorfismos sean isometrías, por lo que todos los conjugados de α tienen valor absoluto menor o igual que 1, es decir, son enteros. Por consiguiente lo mismo vale para los coeficientes del polinomio mínimo de α, que son, por tanto, enteros de k. Así pues, α es entero sobre el anillo de los enteros de k.

Recíprocamente, si $\alpha \in K$ es entero sobre el anillo de enteros de k, en particular es entero sobre el anillo de enteros de K, que es íntegramente cerrado, por ser un dominio de ideales principales, luego α es un entero de k. ∎

Terminamos este apéndice con una aplicación interesante del lema de Hensel. Vamos a demostrar que los únicos cuerpos métricos localmente compactos de

característica prima son los cuerpos de series formales de potencias sobre cuerpos finitos. Recordemos que si K es un cuerpo, $K[[x]]$ es el anillo de series formales de potencias con coeficientes en K (definido en [7.23]) y $K((x))$ es el cuerpo de series formales de potencias con coeficientes en K (ver los ejercicios siguientes).

Teorema A.8 *Sea K un cuerpo métrico localmente compacto de característica prima p. Sea π un primo en K. Entonces K contiene un cuerpo k isomorfo a su cuerpo de restos de modo que la aplicación $k((x)) \longrightarrow K$ dada por $f(x) \mapsto f(\pi)$ es un isomorfismo topológico.*

Demostración: Por el teorema [7.15] el cuerpo de restos $\overline{K}$ de K es finito. Digamos que tiene p^n elementos. El polinomio $q(x) = x^{p^n} - x$ se escinde en factores lineales distintos en $\overline{K}$ luego aplicando varias veces el lema de Hensel vemos que lo mismo le ocurre en K. Más aún, las raíces de $q(x)$ en K recorren todas las clases de $\overline{K}$. La adjunción al cuerpo primo de K de estas raíces es un cuerpo finito k de p^n elementos.

El teorema [7.16] implica que la aplicación descrita es biyectiva. Es fácil ver que es un homomorfismo y por lo tanto un isomorfismo. También es claro $v\big(f(x)\big) = v\big(f(\pi)\big)$ para todo $f(x) \in k((x))$, por lo que el isomorfismo es topológico. ∎

Apéndice B

El teorema de existencia local

En este apéndice demostraremos la afirmación (∗∗) de la página 432 para cuerpos de característica p, que es lo único que quedaba pendiente para probar el teorema de existencia para cuerpos locales de característica prima. Supondremos al lector familizarizado con las propiedades básicas de las formas diferenciales y los residuos en cuerpos de series de potencias.

La dificultad que plantea la prueba de (∗∗) es que no podemos usar la teoría de Kummer. En esta sección veremos que podemos reemplazarla por una teoría análoga. Consideramos un cuerpo k de caracteróstica prima p. La idea es reemplazar el grupo de las raíces p-ésimas de la unidad de la teoría de Kummer por el cuerpo primo $\mathbb{Z}/p\mathbb{Z}$ de k. En lugar del polinomio x^n consideraremos el polinomio

$$\wp(x) = x^p - x.$$

Observemos que si S es la clausura separable de k, entonces $\wp : S \longrightarrow S$ es un homomorfismo entre los grupos aditivos. De hecho es un epimorfismo, pues si $\beta \in S$ entonces el polinomio $x^p - x - \beta$ es separable (tiene derivada -1), luego tiene sus raíces en S. Si α es una de dichas raíces, las demás son $\alpha + n$, donde n recorre el cuerpo primo de k. Esto no sólo prueba que $\wp$ es suprayectiva, sino además vemos que su núcleo es el cuerpo primo. En otros términos, tenemos una sucesión exacta

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow S \xrightarrow{\wp} S \longrightarrow 0.$$

Para cada $\beta \in S$ llamamos $(\beta/\wp)$ a una raíz del polinomio $x^p - x - \beta$, que está unívocamente determinada salvo un elemento del cuerpo primo. (Es el análogo a una raíz n-sima en la teoría de Kummer.) Si $G = G(S/k)$, ahora tenemos una sucesión exacta

$$H^0(G, S) \longrightarrow H^1(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(G, S).$$

Para calcular el primer homomorfismo $\delta^* : k \longrightarrow \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$ partimos de un $\beta \in k$, tomamos una antiimagen por $\wp$, o sea, $(\beta/\wp)$, pasamos a la cofrontera de la cocadena que representa, es decir, a $\sigma \mapsto (\beta/\wp)^\sigma - (\beta/\wp) \in \mathbb{Z}/p\mathbb{Z}$ y esta cocadena (de (G, S)) nos sirve como cociclo de $H^1(G, \mathbb{Z}/p\mathbb{Z})$. Visto como homomorfismo es

$$\phi_\beta(\sigma) = (\beta/\wp)^\sigma - (\beta/\wp).$$

Vemos que $\phi_\beta(\sigma) = 0$ si y sólo si $(\beta/\wp)^\sigma = (\beta/\wp)$, luego el núcleo de ϕ_β es $G(S/k(\beta/\wp))$ y así ϕ_β es un homomorfismo continuo.

El mismo razonamiento empleado en la teoría de Kummer prueba ahora que ϕ_β recorre todos los homomorfismos continuos de G en $\mathbb{Z}/p\mathbb{Z}$ (ahora usamos que el primer grupo de cohomología del grupo aditivo de una extensión abeliana es trivial).

Si identificamos $\mathbb{Z}/p\mathbb{Z} \cong \langle 1/p\rangle \leq \mathbb{Q}/\mathbb{Z}$ entonces la imagen de δ^* se identifica con el subgrupo de $G(S/k)^*$ formado por todos los caracteres con imagen en $\langle 1/p\rangle$. Tenemos así un homomorfismo $\delta^* : k \longrightarrow G(S/k)^*$, cuya imagen es el grupo $G(K/k)^*$, para cualquier extensión K de k de grado p.

Así mismo, $\phi_\beta = 1$ si y sólo si $(\beta/\wp)^\sigma = (\beta/\wp)$ para todo $\sigma \in G(S/k)$, es decir, si y sólo si $(\beta/\wp) \in k$ o, equivalentemente, si $\beta \in \wp[k]$.

Por consiguiente tenemos un monomorfismo

$$k/\wp[k] \longrightarrow G(S/k)^*.$$

Definimos ahora el análogo al símbolo de Hilbert:

Definición B.1 Si k es un cuerpo local de característica prima p, para cada $\alpha \in k^*$ y cada $\beta \in k$ definimos

$$(\alpha, \beta] = (\alpha, \phi_\beta) = \phi_\beta\left(\frac{k}{\alpha}\right) = \left(\frac{k(\beta/\wp)/k}{\alpha}\right)(\beta/\wp) - (\beta/\wp) \in \mathbb{Z}/p\mathbb{Z}.$$

En esta ocasión el símbolo es asimétrico (como refleja la notación), pues es multiplicativo en la primera componente y aditivo en la segunda. Recogemos este hecho y otros más en un teorema:

Teorema B.2 *Sea k un cuerpo local de característica p. Se cumple:*

a) $(\alpha\alpha', \beta] = (\alpha, \beta] + (\alpha', \beta], \quad (\alpha, \beta + \beta'] = (\alpha, \beta] + (\alpha, \beta']$.

b) $(\alpha, \beta] = 0$ *si y sólo si* $\alpha \in \mathrm{N}[k(\beta/\wp)]$.

c) $(\alpha, \alpha] = 0$ *para todo* $\alpha \in k^*$.

d) $(\alpha, \beta] = 0$ *para todo* $\alpha \in k^*$ *si y sólo si* $\beta \in \wp[k]$.

DEMOSTRACIÓN: a) es evidente.

b) Se cumple $(\alpha,\beta]=0$ si y sólo si

$$\left(\frac{k(\beta/\wp)/k}{\alpha}\right)(\beta/\wp)=(\beta/\wp),$$

si y sólo si

$$\left(\frac{k(\beta/\wp)/k}{\alpha}\right)=1,$$

si y sólo si $\alpha\in \mathrm{N}[k(\beta/\wp)]$.

c) Observemos que la extensión $k(\beta/\wp)/k$ tiene grado 1 o p. En efecto, si no tiene grado 1 entonces $(\beta/\wp)$ tiene un conjugado de la forma $(\beta/\wp)+n$, para un $n\neq 0$, luego todos los elementos de la forma $(\beta/\wp)+mn$ con $m\in\mathbb{Z}$ son conjugados, pero mn recorre todo $\mathbb{Z}/p\mathbb{Z}$, luego $(\beta/\wp)$ tiene al menos p conjugados, y al ser raíz de $x^p-x-\beta$, tiene exactamente p conjugados.

Si $|k(\alpha/\wp):k|=1$ entonces $\alpha=\mathrm{N}(\alpha)$ y si el grado es p entonces el polinomio mínimo de $(\alpha/\wp)$ es $x^p-x-\alpha$, luego $\alpha=\mathrm{N}(\alpha/\wp)$. Ahora basta aplicar b)

d) Se cumple $(\alpha,\beta]=0$ para todo $\alpha\in k^*$ si y sólo si

$$\phi_\beta\left(\frac{k(\beta/\wp)/k}{\alpha}\right)(\beta/\wp)=0$$

para todo $\alpha\in k^*$, si y sólo si $\phi_\beta=0$ si y sólo si $\beta\in\wp[k]$, pues tenemos que $\phi_\beta\in G(k(\beta/\wp)/k)^*$ y el símbolo de Artin es biyectivo. ∎

Para calcular explícitamente el símbolo $(\alpha,\beta]$ consideramos el teorema A.8, según el cual todo cuerpo local k de característica prima contiene un subcuerpo k_0 isomorfo a su cuerpo de restos, de modo que $k=k_0((\pi))$, para cualquier primo π de k. Esto nos permite hablar de formas diferenciales en k.

Teorema B.3 *Si k es un cuerpo local de característica p y ξ es un primo en k, entonces, para todo $\alpha,\beta\in k$, $\alpha\neq 0$, se cumple*

$$(\alpha,\beta]=(\xi,\mathrm{Res}\left(\frac{\beta}{\alpha}\,d\alpha\right)]$$

DEMOSTRACIÓN: Ambos miembros son bilineales (respecto al producto por la izquierda y la suma por la derecha). Podemos expresar $\alpha=\pi\xi^n$, con $n\in\mathbb{Z}$ y $\pi\in K$ primo, con lo que la igualdad que hemos de probar se reduce a dos igualdades similares con α primo. Así pues, podemos suponer que $\alpha=\pi$ es un primo no necesariamente igual a ξ.

Igualmente, descomponemos

$$\beta=\sum_{n<0}b_n\pi^n+b_0+\sum_{n>0}b_n\pi^n$$

y podemos considerar los tres sumandos por separado.

a) Si $\beta = u\pi^{-n}$, con $u \in k_0$, $n > 0$, entonces

$$\mathrm{Res}\left(\frac{\beta}{\alpha}\,d\alpha\right) = \mathrm{Res}(u\pi^{-n-1}\,d\pi) = \mathrm{Res}_\pi(u\pi^{-n-1}) = 0.$$

En correspondencia hemos de probar que $(\pi, u\pi^{-n}] = 0$. Lo haremos por inducción sobre n. Supongamos primero que $p \nmid n$ (en particular si $n = 1$). Entonces

$$-n(\pi, u\pi^{-n}] = (\pi^{-n}, u\pi^{-n}] = (u\pi^{-n}, u\pi^{-n}] - (u, u\pi^{-n}] = 0,$$

donde hemos usado el apartado c) del teorema anterior y el hecho de que u es una potencia de p (porque k_0 es finito). Por lo tanto $(\pi, u\pi^{-n}] = 0$.

Supongamos ahora que $n = mp$ y sea $u = v^p$. Entonces

$$u\pi^{-n} = \wp(v\pi^{-m}) + v\pi^{-m},$$

luego $(\pi, u\pi^{-n}] = (\pi, v\pi^{-m}] = 0$, por el apartado d) del teorema anterior y la hipótesis de inducción.

b) Si $\beta = \sum_{n>0} b_n\pi^n$ entonces

$$\mathrm{Res}\left(\frac{\beta}{\alpha}\,d\alpha\right) = \mathrm{Res}_\pi\left(\sum_{n>0} b_n\pi^{n-1}\right) = 0,$$

y también tenemos que $(\pi, \beta] = 0$, pues $\beta = \wp(\gamma)$, donde

$$\gamma = \sum_{n\geq 0} \beta^{p^n}.$$

(La serie converge porque $|\beta| < 1$.)

c) Si $\beta \in k_0$ entonces

$$\mathrm{Res}\left(\frac{\beta}{\alpha}\,d\alpha\right) == \beta\mathrm{Res}_\pi(1/\pi) = \beta.$$

Hemos de probar que $(\pi, \beta] = (\xi, \beta]$ para cualquier par de primos de k y cualquier $\beta \in k_0$. Esto equivale a que $(\epsilon, \beta] = 0$ para toda unidad ϵ de k. Por el teorema anterior basta con que $\epsilon \in \mathrm{N}[k(\beta/\wp)]$ y a su vez para esto es suficiente que la extensión $k(\beta/\wp)/k$ sea no ramificada.

Sea $K = k(\beta/\wp)$ y sea $F = k_0(\beta/\wp)$. Claramente F es un cuerpo finito, pues $(\beta/\wp)$ es algebraico sobre k_0. Además

$$K = k_0((\xi))(\beta/\wp) = k_0(\beta/\wp)((\xi)) = F((\xi)).$$

Es obvio que el valor absoluto de K inducido por esta representación extiende al valor absoluto de k, luego se trata de la única extensión de dicho valor absoluto. Así es evidente que ξ sigue siendo primo en K, luego la extensión K/k es no ramificada. ∎

Una versión equivalente de la fórmula que acabamos de probar es

$$(\alpha, \alpha\beta] = (\xi, \mathrm{Res}(\beta\, d\alpha)],$$

para cualquier primo ξ de k. El miembro derecho sólo depende de la forma diferencial $\beta\, d\alpha$, luego podemos introducir la notación siguiente:

Definición B.4 Sea k un cuerpo local de característica prima p. Para cada par de elementos α, $\beta \in k$ definimos

$$\int \beta\, d\alpha = (\alpha, \alpha\beta] = \left(\frac{k}{\alpha}\right)\left(\frac{\alpha\beta}{\wp}\right) - \left(\frac{\alpha\beta}{\wp}\right) \in \mathbb{Z}/p\mathbb{Z}.$$

Las propiedades siguientes son inmediatas:

$$\int (\beta\, d\alpha + \beta'\, d\alpha') = \int \beta\, d\alpha + \int \beta'\, d\alpha',$$

$$\int d\alpha = (\alpha, \alpha] = 0, \qquad \int \beta\, d\alpha = -\int \alpha\, d\beta.$$

El teorema siguiente nos da una expresión explícita para el símbolo $(\alpha, \beta]$:

Teorema B.5 *Sea k un cuerpo local de característica p, sea k_0 su cuerpo de restos y $\mathrm{Tr} : k_0 \longrightarrow \mathbb{Z}/p\mathbb{Z}$ la traza. Entonces, para todo α,$\beta \in k$, se cumple que*

$$\int \beta\, d\alpha = \mathrm{Tr}(\mathrm{Res}(\beta\, d\alpha)).$$

Demostración: Hemos de probar que $(\alpha, \alpha\beta] = \mathrm{Tr}(\mathrm{Res}(\beta\, d\alpha))$ o, equivalentemente, que

$$(\xi, \mathrm{Res}(\beta\, d\alpha)] = \mathrm{Tr}(\mathrm{Res}(\beta\, d\alpha)).$$

Más en general, vamos a ver que $(\xi, u] = \mathrm{Tr}(u)$, para todo primo ξ de k y todo $u \in k_0$.

Sea $K = k(u/\wp)$. Entonces

$$(\xi, u] = \left(\frac{K/k}{\xi}\right)\left(\frac{u}{\wp}\right) - \left(\frac{u}{\wp}\right).$$

En la prueba del teorema B.3 hemos visto que la extensión K/k es no ramificada, luego el símbolo de Artin de ξ es el automorfismo canónico de K/k, es decir, el que induce en el cuerpo de restos el automorfismo de Frobenius. Por la unicidad de dicho automorfismo, se trata del dado por

$$\left(\frac{K/k}{\xi}\right)(\alpha) = \alpha^{p^n},$$

donde $|k_0| = p^n$. Si llamamos $v = (u/\wp)$ entonces $u = v^p - v$ y

$$(\xi, u] = v^{p^n} - v = (v^{p^n} - v^{p^{n-1}}) + \cdots + (v^p - v) = u^{p^{n-1}} + \cdots + u = \mathrm{Tr}(u).$$

■

Como consecuencia tenemos la siguiente propiedad de las integrales:

Teorema B.6 *Sea k un cuerpo local de característica prima p. Si $\alpha \in k$ cumple que $\int \beta\, d\alpha = 0$ para todo $\beta \in k$, entonces $d\alpha = 0$.*

DEMOSTRACIÓN: Supongamos que $d\alpha \neq 0$. Digamos que

$$\alpha = \sum_n a_n \xi^n, \qquad \frac{d\alpha}{d\xi} = \sum_n n a_n \xi^{n-1} \neq 0.$$

Sea r el menor índice tal que $ra_r \neq 0$. Entonces, para todo $b \in k_0$,

$$0 = \int b\xi^{-r}\, d\alpha = \mathrm{Tr}(\mathrm{Res}(b\xi^{-r}\, d\alpha)) = \mathrm{Tr}\left(\mathrm{Res}_\xi\left(b\xi^{-r}\frac{d\alpha}{d\xi}\right)\right) = \mathrm{Tr}(rba_r).$$

Cuando b recorre k_0 también rga_r recorre k_0, luego hemos llegado a que $\mathrm{Tr}[k_0] = 0$, lo cual es imposible. ∎

Finalmente podemos probar el resultado que perseguíamos:

Teorema B.7 *Sea k un cuerpo local de característica prima p y sea $\alpha \in k$ tal que α es una norma para toda extensión cíclica de k de grado p. Entonces $\alpha \in k^p$.*

DEMOSTRACIÓN: Tenemos que α es una norma para cada extensión de la forma $k(\beta/\wp)/k$, luego según B.2 ha de ser $(\alpha, \beta] = 0$ para todo $\beta \in k$, o también $(\alpha, \alpha\beta] = 0$, es decir,

$$\int \beta\, d\alpha = 0,$$

para todo $\beta \in k$. Según el teorema anterior $d\alpha = 0$, por las propiedades de las formas diferenciales esto equivale a que $\alpha \in k^p$. ∎

Bibliografía

[1] Artin, E. *Algebraic Numbers and Algebraic Functions.* Nelson, 1967.

[2] Artin, E. y Tate, J. *Class Field Theory.* Benjamin, New York, 1967.

[3] Bastida, J.R. *Field extensions and Galois theory.* Addison-Wesley P.C., California, 1984.

[4] Babakhanian, A. *Cohomological methods in group theory.* M. Dekker, New York, 1972.

[5] Cohn, H. *A Classical Invitation to Algebraic Numbers and Class Fields.* Springer, New York, 1978.

[6] Ireland, K. y Rosen, M. *A Classical Introduction to Modern Number Theory.* Springer, New York 1982.

[7] Iyanaga, S. (Ed.) *The Theory of Numbers.* North Holland, Amsterdam, 1969.

[8] Lang, S. *Algebraic Number Theory.* Addison Wesley, Massachusetts, 1970.

[9] Ribenboim, P. *13 Lectures on Fermat's Last Theorem.* Springer, New York, 1979.

[10] Serre, J.P. *Corps locaux.* Hermann, Paris, 1968.

[11] Weil, A. *Basic Number Theory.* Springer, New York, 1968.

Índice de Materias