§17. Группы Галуа

17.1. Соответствие Галуа. Нормальное сепарабельное расширение $\mathbb{K} \supset \Bbbk$ называется *расширением Галуа*, а группа его автоморфизмов над $\Bbbk$ — *группой Галуа* и обозначается

$$\operatorname{Gal} \mathbb{K}/\Bbbk \stackrel{\text{def}}{=} \operatorname{Aut}_{\Bbbk} \mathbb{K}.$$

По теор. 16.3 и сл. 16.8 конечное расширение $\mathbb{K} \supset \Bbbk$ является расширением Галуа тогда и только тогда, когда $|\operatorname{Aut}_{\Bbbk}\mathbb{K}| = \dim_{\Bbbk} \mathbb{K}$ (во многих учебниках это свойство берётся за определение конечного расширения Галуа). Согласно сл. 16.7 нормальное замыкание любого конечного сепарабельного расширения $\mathbb{F} \supset \Bbbk$ является расширением Галуа. По теор. 16.3 любое поле $\mathbb{K}$, на котором эффективно действует автоморфизмами конечная группа G, является расширением Галуа подполя инвариантов $\mathbb{K}^G \subset \mathbb{K}$ с группой Галуа

$$\operatorname{Gal} \mathbb{K}/\mathbb{K}^G = G.$$

В примере из n° 16.6.2 мы видели, что любое конечное поле является расширением Галуа любого своего конечного подполя. Описанное там соответствие между подполями и подгруппами группы Галуа обобщается на произвольные конечные расширения Галуа.

Теорема 17.1 (соответствие Галуа)
Для любого конечного расширения Галуа $\Bbbk \subset \mathbb{K}$ с группой Галуа $G = \operatorname{Gal} \mathbb{K}/\Bbbk = \operatorname{Aut}_{\Bbbk}\mathbb{K}$ отображение, сопоставляющее подгруппе $H \subseteq G$ её поле инвариантов $\mathbb{K}^H \subseteq \mathbb{K}$, и отображение, сопоставляющее содержащему $\Bbbk$ подполю $\mathbb{L} \subseteq \mathbb{K}$ подгруппу $\operatorname{Aut}_{\mathbb{L}}\mathbb{K} \subseteq G$, являются взаимно обратными биекциями между множеством подгрупп $H \subseteq G$ и множеством полей $\mathbb{L}$, таких что $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$. При этом нормальные подгруппы $H \trianglelefteq G$ взаимно однозначно соответствуют содержащимся в $\mathbb{K}$ расширениям Галуа $\mathbb{L} \supset \Bbbk$, и в этом случае $\operatorname{Gal} \mathbb{L}/\Bbbk \simeq G/H$.

Доказательство. Для любого поля $\mathbb{L}$, такого что $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, расширение $\mathbb{L} \subset \mathbb{K}$ нормально по предл. 16.2 и сепарабельно по сл. 16.5. Тем самым, оно является расширением Галуа с группой Галуа $H = \operatorname{Aut}_{\mathbb{L}}\mathbb{K}$, и $|H| = \deg \mathbb{K}/\mathbb{L}$. Очевидно, что H является подгруппой в G, и по сл. 16.8 $K^H = \mathbb{L}$. Отсюда сразу следует первое утверждение о биекции[1].

Для доказательства второго утверждения рассмотрим действие группы $G = \operatorname{Gal}\mathbb{K}/\Bbbk$ на содержащихся в $\mathbb{K}$ подполях $\mathbb{L} \supset \Bbbk$. По уже доказанному, централизатор каждого такого поля $\mathbb{L}$

$$C_{\mathbb{L}} = \{g \in G \mid g|_{\mathbb{L}} = \mathrm{Id}_{\mathbb{L}}\} = \operatorname{Aut}_{\mathbb{L}}\mathbb{K}$$

это в точности подгруппа $H \subseteq G$, отвечающая при соответствии Галуа полю $\mathbb{L}$. Поскольку расширение $\mathbb{K} \supset \Bbbk$ нормально и сепарабельно, любое вложение

$$\varphi : \mathbb{L} \hookrightarrow \mathbb{K} \quad (\text{над } \Bbbk) \tag{17-1}$$

продолжается до автоморфизма $g : \mathbb{K} \xrightarrow{\sim} \mathbb{K}$ над $\Bbbk$, т. е. его образ $\mathbb{L}' = \varphi(\mathbb{L})$ имеет вид $g(\mathbb{L})$ для некоторого $g \in G$. Поэтому централизатор образа $H' = \operatorname{Gal}_{\mathbb{L}'}\mathbb{K} = C_{\mathbb{L}'} = C_{g(\mathbb{L})} = gC_{\mathbb{L}}g^{-1} = gHg^{-1}$ сопряжён подгруппе H. Согласно предл. 16.2 и сл. 16.5 расширение $\mathbb{L} \supset \Bbbk$ всегда сепарабельно, а нормально тогда и только тогда, когда образы всех вложений (17-1) совпадают с $\mathbb{L}$. По предыдущему, это означает, что все подгруппы, сопряжённые с H, совпадают с H, т. е. что $H \trianglelefteq G$ нормальна. В этом случае группа Галуа $\operatorname{Gal}\mathbb{K}/\Bbbk$ переводит $\mathbb{L}$ в себя, и возникает сюръективный гомоморфизм $\operatorname{Gal}\mathbb{K}/\Bbbk \twoheadrightarrow \operatorname{Gal}\mathbb{L}/\Bbbk$, ядром которого является $\operatorname{Gal}\mathbb{K}/\mathbb{L}$. Таким образом, $\operatorname{Gal}\mathbb{L}/\Bbbk = \big(\operatorname{Gal}\mathbb{K}/\Bbbk\big)/\big(\operatorname{Gal}\mathbb{K}/\mathbb{L}\big)$. □

[1] вместо сл. 16.8 для доказательства биективности соответствия Галуа можно было бы воспользоваться теор. 16.3, из которой вытекает, что для любой подгруппы $H \subseteq G$ расширение $\mathbb{K}^H \subseteq \mathbb{K}$ является расширением Галуа с группой Галуа H

Упражнение 17.1. Убедитесь в том, что соответствие Галуа оборачивает включения:

$$H \subset K \subset \operatorname{Gal}\mathbb{K}/\Bbbk \iff \mathbb{K}^H \supset \mathbb{K}^K \supset \Bbbk$$

и что пересечению подгрупп $H_1 \cap H_2$ отвечает композит $\mathbb{K}_1\mathbb{K}_2$ соответствующих им полей $\mathbb{K}_1 = \mathbb{K}^{H_1}$ и $\mathbb{K}_2 = \mathbb{K}^{H_2}$, а пересечению $\mathbb{K}_1 \cap \mathbb{K}_2$ — наименьшая подгруппа в G, содержащая H_1 и H_2.

17.1.1. Пример: построения циркулем и линейкой. Пусть на евклидовой координатной плоскости $\mathbb{R}^2$, которую мы отождествим с полем $\mathbb{C}$, отмечены точки 0 и 1. Легко видеть, что точка $z \in \mathbb{C}$ может быть построена циркулем и линейкой, если и только если она лежит в конечном расширении $\mathbb{L} \supset \mathbb{Q}$, получающемся из $\mathbb{Q}$ цепочкой примитивных квадратичных расширений

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \ \cdots \ \subset \mathbb{L}_{m-1} \subset \mathbb{L}_m = \mathbb{L}, \tag{17-2}$$

в которой $\mathbb{L}_{i+1} = \mathbb{L}_i[\sqrt{a_i}]$ для некоторого $a_i \in \mathbb{F}_i$. В самом деле, все точки из $\mathbb{L}$ строятся при помощи циркуля и линейки.

Упражнение 17.2. Даны точки 0, 1, a, $b \in \mathbb{C}$. Циркулем и линейкой постройте в $\mathbb{C}$ точки $a \pm b$, a/b, ab и $\pm\sqrt{a}$.

Наоборот, если задано подполе $\mathbb{F} \subset \mathbb{C}$, содержащее $\sqrt{-1}$, то точки пересечения окружности произвольного радиуса $\varrho \in \mathbb{F}$ с центром в произвольной точке $c \in \mathbb{F}$ и прямой, проходящей через произвольные две точки $p, q \in \mathbb{F}$, рационально выражаются через элементы поля $\mathbb{F}$ и вещественный корень t квадратного уравнения[1], которое получается из уравнения окружности $(z-c)(\overline{z}-\overline{c}) = \varrho^2$ подстановкой $z = p + (q-p)t$.

Упражнение 17.3. Покажите, что если $\sqrt{-1} \in \mathbb{F}$, то комплексное сопряжение является автоморфизмом поля $\mathbb{F}$ над $\mathbb{Q}$.

Покажем, что конечное расширение Галуа $\mathbb{L} \supset \mathbb{Q}$ тогда и только тогда получается из $\mathbb{Q}$ цепочкой примитивных квадратичных расширений (17-2), когда $\dim_{\mathbb{Q}} \mathbb{L} = |\operatorname{Gal}\mathbb{L}/\mathbb{Q}| = 2^m$ для некоторого $m \in \mathbb{N}$. В одну сторону это очевидно: из мультипликативности степени вытекает, что в башне (17-2) $\deg \mathbb{L}/\mathbb{Q} = 2^m$. Наоборот, если группа Галуа $G = \operatorname{Gal}\mathbb{L}/\mathbb{Q}$ имеет порядок 2^m, то она допускает фильтрацию подгруппами

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ \cdots \ \subset G_{m-1} \subset G_m = G \tag{17-3}$$

в которой каждая подгруппа $G_i \lhd G_{i+1}$ имеет в следующей подгруппе индекс 2, так что $G_{i+1}/G_i \simeq \mathbb{Z}/(2)$. Построить такую фильтрацию можно индукцией по m. Действительно, будучи 2-группой, G имеет нетривиальный центр $C \lhd G$, который является абелевой 2- группой и обладает фильтрацией $\{e\} = C_0 \subset C_1 \subset C_2 \subset \ \cdots \ \subset C_{n-1} \subset C_n = C$ с факторами $C_{i+1}/C_i \simeq \mathbb{Z}/(2)$.

Упражнение 17.4. Выведите из теоремы о строении конечно порождённых абелевых групп, что каждая абелева 2-группа C обладает такой фильтрацией.

По индуктивному предположению, фактор группа $Q = G/C$ также обладает фильтрацией

$$\{e\} = Q_0 \subset Q_1 \subset Q_2 \subset \ \cdots \ \subset Q_{k-1} \subset Q_k = G/C \quad \text{с факторами } Q_{i+1}/Q_i \simeq \mathbb{Z}/(2).$$

Из этих двух фильтраций составляется требуемая фильтрация вида (17-3) на G:

$$\{e\} = C_0 \subset C_1 \subset \ \cdots \ \subset C_{n-1} \subset C \subset CQ_1 \subset CQ_2 \subset \ \cdots \ \subset CQ_{k-1} \subset CQ_k = G$$

в которой $CQ_i \subset G$ суть полные прообразы подгрупп $Q_i \subset G/C$ относительно гомоморфизма факторизации $G \twoheadrightarrow G/C$. Фильтрации (17-3) отвечает в соответствии Галуа башня квадратичных расширений (17-2), что и требовалось. Из сказанного, среди прочего, вытекает

Предложение 17.1
Комплексный корень многочлена $f(x) \in \mathbb{Q}[x]$ может быть построен циркулем и линейкой исходя из точек 0, $1 \in \mathbb{C}$, если и только если степень его поля разложения над $\mathbb{Q}$ является степенью двойки, и в этом случае все корни f строятся циркулем и линейкой.

[1] если у этого уравнения нет вещественных корней, то прямая и окружность не пересекаются

Доказательство. Поле разложения $\mathbb{K}$ многочлена f над $\mathbb{Q}$ является расширением Галуа. Мы только что видели, что если $\deg \mathbb{K}/\mathbb{Q} = 2^m$, то $\mathbb{K}$ можно получить как верхний этаж $\mathbb{L}$ башни (17-2). Наоборот, если $\mathbb{K}$ содержится в некотором расширении $\mathbb{L}$ вида (17-2), то $\deg \mathbb{K}/\mathbb{Q}$ делит $\deg \mathbb{L}/\mathbb{Q}$ и, стало быть, является степенью двойки. □

Например, угол $\pi/3$ нельзя разделить на три равные части циркулем и линейкой. В самом деле, если бы это было возможно, то можно было бы построить и число $\vartheta = \cos(\pi/9)$, удовлетворяющее кубическому уравнению $4\,x^3 - 3\,x = 1/2$ (получающемуся из соотношения $\cos(3\varphi) = 4\cos\varphi - 3\cos^2\varphi$ при $\varphi = \pi/9$). Поскольку многочлен $4\,x^3 - 3\,x - 1/2$ не имеет рациональных корней, он неприводим над $\mathbb{Q}$, и его поле разложения имеет над $\mathbb{Q}$ степень либо 3 либо 6. Поэтому его корни не строятся циркулем и линейкой.

Упражнение 17.5 (задача об удвоении куба). Покажите, что циркулем и линейкой нельзя построить сторону куба, объём которого вдвое больше объёма данного куба.

По тем же причинам нельзя построить циркулем и линейкой правильный 7-угольник: если бы это возможно, то первообразный корень седьмой степени из единицы $\zeta_7 = e^{2\pi i/7} \in \mathbb{C}$ тоже было бы можно построить, но мы увидим ниже в n° 17.3, что группа Галуа поля разложения минимального многочлена числа ζ_7 над $\mathbb{Q}$ изоморфна мультипликативной группе ненулевых вычетов по модулю 7 и, стало быть, имеет порядок 6.

Упражнение 17.6* (построение Гаусса). Постройте циркулем и линейкой правильный 17-угольник.

17.1.2. Влияние побочных иррациональностей. Во всех предыдущих рассуждениях поле $\mathbb{Q}$ можно было бы заменить на произвольное расширение $\mathbb{F} \supset \mathbb{Q}$. Это вытекает из следующего общего результата о том, как влияет на группу Галуа добавление к основному полю «побочных иррациональностей».

Предложение 17.2 (теорема о побочных иррациональностях)
Пусть поля $\mathbb{F}, \mathbb{K} \supset \Bbbk$ содержатся в некотором общем алгебраически замкнутом поле $\mathbb{L}$ и расширение $\mathbb{K} \supset \Bbbk$ является конечным расширением Галуа. Тогда $\mathbb{F}\mathbb{K} \supset \mathbb{F}$ также является конечным расширением Галуа, и его группа Галуа изоморфна подгруппе группы Галуа $\operatorname{Gal}\mathbb{K}/\Bbbk$, отвечающей при соответствии Галуа промежуточному подполю $\Bbbk \subset \mathbb{F} \cap \mathbb{K} \subset \mathbb{K}$.

Доказательство. По предл. 16.3 поле $\mathbb{K}$ является полем разложения некоторого сепарабельного многочлена $f \in \Bbbk[x]$ и порождается как $\Bbbk$-алгебра его корнями $\vartheta_1, \vartheta_2, \ldots, \vartheta_n \in \overline{\Bbbk}$. Поле разложения многочлена f над полем $\mathbb{F}$ представляет собою $\mathbb{F}$-подалгебру $\mathbb{F}[\vartheta_1, \vartheta_2, \ldots, \vartheta_n] \subset \mathbb{L}$, порождённую теми же самыми корнями $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$ и, таким образом, совпадает с композитом $\mathbb{F}\mathbb{K} \subset \mathbb{L}$. Поэтому $\mathbb{F}\mathbb{K}$ является расширением Галуа поля $\mathbb{F}$. Поскольку втоморфизмы $\mathbb{K}$ над $\Bbbk$ и $\mathbb{F}\mathbb{K}$ над $\mathbb{F}$ оставляют многочлен f на месте, они переводят множество его корней в себя. Поэтому каждый автоморфизм однозначно определяется осуществляемой им перестановкой корней. Группа $\operatorname{Gal}\mathbb{K}/\Bbbk$ изоморфна группе таких перестановок корней $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$, которые продолжаются до автоморфизма алгебры $\mathbb{K} = \Bbbk[\vartheta_1, \vartheta_2, \ldots, \vartheta_n]$. Такой автоморфизм продолжается до автоморфизма большей алгебры $\mathbb{F}[\vartheta_1, \vartheta_2, \ldots, \vartheta_n] \supset \Bbbk[\vartheta_1, \vartheta_2, \ldots, \vartheta_n]$ тогда и только тогда, когда он $\mathbb{F}$-линеен, т. е. оставляет на месте подполе $\mathbb{F} \cap \mathbb{K}$. □

17.2. Группы многочленов. Согласно предл. 16.3, поле разложения $\mathbb{K}$ любого сепарабельного многочлена $f \in \Bbbk[x]$ является расширением Галуа поля $\Bbbk$. Его группа Галуа над $\Bbbk$ обозначается через $\operatorname{Gal} f/\Bbbk$ и называется группой Галуа многочлена f над $\Bbbk$. Поскольку поле разложения как алгебра над $\Bbbk$ порождается корнями $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$ многочлена f, каждый автоморфизм из группы Галуа $\operatorname{Gal} f/\Bbbk$ однозначно определяется своим действием на корнях, причём переводит корни в корни. Иначе говоря, группа Галуа любого многочлена канонически вложена в качестве подгруппы в группу перестановок его корней.

Упражнение 17.7. Покажите, что группа Галуа неприводимого сепарабельного кубического многочлена совпадает со всей симметрической группой S_3, если дискриминант этого многочлена не является квадратом, и изоморфна группе $\mathbb{Z}/(3)$ циклических перестановок корней, если дискриминант является квадратом.

Перестановка корней лежит в группе Галуа тогда и только тогда, когда она продолжается до автоморфизма всего поля разложения, т. е. *сохраняет все алгебраические соотношения* между корнями. Точнее, будем называть многочлен $\psi(t_1, t_2, \dots, t_n) \in \Bbbk[t_1, t_2, \dots, t_n]$ от $n = \deg f$ алгебраически независимых переменных $t_1, t_2, \dots, t_n$ *соотношением* между корнями $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ многочлена

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \Bbbk[x] \tag{17-4}$$

если $\psi(\vartheta_1, \vartheta_2, \dots, \vartheta_n) = 0$ в поле $\mathbb{K}$. Соотношения составляют в $\Bbbk[t_1, t_2, \dots, t_n]$ идеал $I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$ — ядро гомоморфизма вычисления

$$\mathrm{ev}_{\vartheta_1,\vartheta_2,\dots,\vartheta_n} : \Bbbk[t_1, t_2, \dots, t_n] \xrightarrow{\psi\mapsto\psi(\vartheta_1,\vartheta_2,\dots,\vartheta_n)} \overline{\Bbbk}, \tag{17-5}$$

образом которого является поле разложения $\mathbb{K}$ многочлена (17-4). Сам Галуа определял группу $\mathrm{Gal}\, f/\Bbbk$ как подгруппу в S_n, состоящую из всех перестановок переменных $t_1, t_2, \dots, t_n$, переводящих идеал $I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$ в себя. Подчеркнём, что это определение, равно как и сам гомоморфизм (17-5), а также идеал $I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$, *зависят от выбора нумерации* корней ϑ_i.

Упражнение 17.8. Убедитесь, что определение Галуа эквивалентно данному нами в n° 17.1 выше, т. е. покажите, что $\mathrm{Aut}_{\Bbbk}\mathbb{K} \simeq \{g \in S_n \mid g(I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}) \subset I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}\}$.

Предложение 17.3
Множество нулей $V(I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}) \subset \mathbb{A}^n(\overline{\Bbbk})$ идеала $I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$ представляет собою набор из

$$m = \deg \mathbb{K}/\Bbbk = |\mathrm{Gal}\, f/\Bbbk|$$

различных точек, образующих одну орбиту свободного действия группы Галуа $\mathrm{Gal}\, f/\Bbbk$ на $\mathbb{A}^n$ перестановками координат, и координаты всех точек этой орбиты являются перестановками корней $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ многочлена (17-4).

Доказательство. Для любой перестановки $\sigma \in S_n$ и любого многочлена $\psi \in \Bbbk[t_1, t_2, \dots, t_n]$ положим $\psi^\sigma(t_1, t_2, \dots, t_n) = \psi\left(t_{\sigma(1)}, t_{\sigma(2)}, \dots, t_{\sigma(n)}\right)$. Если $\sigma \in \mathrm{Gal}\, f/\Bbbk$, то для каждого $\psi \in I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$ многочлен ψ^σ также лежит в $I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$, а значит

$$\psi\left(\vartheta_{\sigma(1)}, \vartheta_{\sigma(2)}, \dots, \vartheta_{\sigma(n)}\right) = \psi^\sigma(\vartheta_1, \vartheta_2, \dots, \vartheta_n) = 0\,,$$

т. е. все точки, получающиеся из $(\vartheta_1, \vartheta_2, \dots, \vartheta_n) \in \mathbb{A}^n$ перестановками координат из группы Галуа, лежат на многообразии $V(I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n})$. Наоборот, если $(\alpha_1, \alpha_2, \dots, \alpha_n) \in V(I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n})$, то значения элементарных симметрических многочленов $e_i(t_1, t_2, \dots, t_n)$ на этой точке суть

$$e_i(\alpha_1, \alpha_2, \dots, \alpha_n) = a_i\,,$$

так как все разности $e_i(t_1, t_2, \dots, t_n) - (-1)^i a_i$ лежит в идеале $I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$. Поэтому

$$(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = f(x)\,,$$

т. е. $(\alpha_1, \alpha_2, \dots, \alpha_n) = \left(\vartheta_{\sigma(1)}, \vartheta_{\sigma(2)}, \dots, \vartheta_{\sigma(n)}\right)$ для некоторой перестановки $\sigma \in S_n$, которая лежит в группе Галуа, поскольку иначе нашлась бы функция $\psi \in I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$, образ которой $\psi^\sigma \notin I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n}$, т. е. $\psi^\sigma(\vartheta_1, \vartheta_2, \dots, \vartheta_n) = \psi\left(\vartheta_{\sigma(1)}, \vartheta_{\sigma(2)}, \dots, \vartheta_{\sigma(n)}\right) = \psi(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$, вопреки предположению о том, что $(\alpha_1, \alpha_2, \dots, \alpha_n) \in V(I_{\vartheta_1,\vartheta_2,\dots,\vartheta_n})$. □

Упражнение 17.9. Покажите, что сепарабельный многочлен $f \in \Bbbk[x]$ неприводим тогда и только тогда, когда группа Галуа $\mathrm{Gal}\, f/\Bbbk$ транзитивно действует на его корнях.

17.2.1. Поведение группы Галуа при редукции коэффициентов. Обозначим через $\mathbb{K} \supset \Bbbk$ поле разложения многочлена $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \Bbbk[x]$ и рассмотрим в кольце $\mathbb{K}[t_1, t_2, \ldots, t_n]$ линейную форму $\psi = \vartheta_1 t_1 + \vartheta_2 t_2 + \cdots + \vartheta_n t_n$, коэффициенты которой $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$ суть корни f в $\mathbb{K}$. Образуем из неё следующий многочлен степени $n!$:

$$F(t_1, t_2, \ldots, t_n) = \prod_{\sigma \in S_n} \psi^\sigma(t_1, t_2, \ldots, t_n) = \prod_{\sigma \in S_n} \left(\vartheta_1 t_{\sigma(1)} + \vartheta_2 t_{\sigma(2)} + \cdots + \vartheta_n t_{\sigma(n)}\right). \tag{17-6}$$

Объединим сомножители этого произведения в группы, отвечающие левым смежным классам группы Галуа $G = \operatorname{Gal}\mathbb{K}/\Bbbk$, рассматриваемой как подгруппа в S_n. Все перестановки из смежного класса $[\sigma] = \sigma G \subset S_n$ имеют вид σg, где g пробегает группу Галуа G, и произведение соответствующих сомножителей из (17-6) равно

$$\begin{aligned} F_{[\sigma]} &= \prod_{g \in G} \left(\vartheta_1 t_{\sigma(g(1))} + \vartheta_2 t_{\sigma(g(2))} + \cdots + \vartheta_n t_{\sigma(g(n))}\right) = \\ &= \prod_{g \in G} \left(\vartheta_{g^{-1}(1)} t_{\sigma(1)} + \vartheta_{g^{-1}(2)} t_{\sigma(2)} + \cdots + \vartheta_{g^{-1}(n)} t_{\sigma(n)}\right) = \prod_{h \in G} h\left(\psi^\sigma\right) \end{aligned} \tag{17-7}$$

где через $h : \mathbb{K}[t_1, t_2, \ldots, t_n] \xrightarrow{\sim} \mathbb{K}[t_1, t_2, \ldots, t_n]$ обозначен автоморфизм кольца многочленов, получающийся применением к коэффициентам каждого многочлена автоморфизма

$$h = g^{-1} \in \operatorname{Gal}\mathbb{K}/\Bbbk = \operatorname{Aut}_{\Bbbk}\mathbb{K}$$

из группы Галуа поля $\mathbb{K}$. Так как все линейные формы в произведении (17-7) различны и составляют одну орбиту действия группы Галуа G на $\mathbb{K}[t_1, t_2, \ldots, t_n]$, каждый из многочленов $F_{[s]}$ лежит в $\Bbbk[t_1, t_2, \ldots, t_n]$ и неприводим над $\Bbbk$. Поэтому, многочлен (17-6) тоже лежит в $\Bbbk[t_1, t_2, \ldots, t_n]$ и его разложение на неприводимые множители в кольце $\Bbbk[t_1, t_2, \ldots, t_n]$ имеет вид

$$F(t_1, t_2, \ldots, t_n) = \prod_{[\sigma] \in S_n/G} F_{[s]}(t_1, t_2, \ldots, t_n) \tag{17-8}$$

где произведение берётся по всем левым смежным классам подгруппы Галуа $G \subset S_n$. Формулы (17-6) и (17-7) показывают, что неприводимые множители $F_{[s]}$ образуют одну орбиту действия симметрической группы S_n на кольце $\Bbbk[t_1, t_2, \ldots, t_n]$ перестановками координат, а группа Галуа G изоморфна стабилизатору множителя $F_{[e]}$ этой орбиты и сопряжена стабилизаторам всех остальных множителей. Мы получили

Предложение 17.4
Перестановки переменных $t_1, t_2, \ldots, t_n$, оставляющие неизменным какой-либо множитель $F_{[s]}$ из разложения (17-8) многочлена (17-6) на неприводимые множители в кольце $\Bbbk[t_1, t_2, \ldots, t_n]$, образуют в S_n подгруппу $\sigma G \sigma^{-1}$, сопряжённую группе Галуа $G = \operatorname{Gal} f/\mathbb{Q} \subset S_n$. □

Предложение 17.5
Для неприводимого многочлена $f = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$ обозначим через

$$\overline{f} = x^n + \overline{a}_1 x^{n-1} + \cdots + \overline{a}_{n-1}x + \overline{a}_n \in \mathbb{F}_p[x], \quad \text{где } \overline{a}_i = a_i \pmod p \in \mathbb{Z}/(p),$$

его редукцию по простому модулю p. Если многочлен $\overline{f} \in \mathbb{F}_p[x]$ сепарабелен, то

$$\operatorname{Gal}\overline{f}/\mathbb{F}_p \subset \operatorname{Gal} f/\mathbb{Q}.$$

Доказательство. Обозначим через $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$ корни многочлена f в его поле разложения $\mathbb{K} \supset \mathbb{Q}$. Поскольку все они целы над $\mathbb{Z}$, коэффициенты формы $\psi = \vartheta_1 t_1 + \vartheta_2 t_2 + \cdots + \vartheta_n t_n$ лежат в кольце целых $O \subset \mathbb{K}$, построенный из формы ψ по формуле (17-6) многочлен

$$F(t_1, t_2, \ldots, t_n) = \prod_{\sigma \in S_n} \psi^\sigma(t_1, t_2, \ldots, t_n) \in \mathbb{Q}[x_1, x_2, \ldots, x_n]$$

имеет целые коэффициенты, и все сомножители в его разложении (17-8) на неприводимые множители лежат в $\mathbb{Z}[t_1, t_2, \dots, t_n]$. Приводя (17-8) по модулю p, получаем в кольце $\mathbb{F}_p[t_1, t_2, \dots, t_n]$ равенство:

$$\overline{F}(t_1, t_2, \dots, t_n) = \prod_{[\sigma]\in G/S_n} \overline{F}_{[s]}(t_1, t_2, \dots, t_n) \tag{17-9}$$

Классы $\overline{\vartheta}_i = \vartheta_i \pmod p \in O/(p)$ являются элементами коммутативной $\mathbb{F}_p$-алгебры $A = O/(p)$, и многочлен $\overline{f}(x) = \prod(x - \overline{\vartheta}_i)$ полностью раскладывается в $A[x]$ в произведение различных линейных множителей.

Упражнение 17.10. Покажите, что $\mathbb{F}_p$-подалгебра $\mathbb{F} = \mathbb{F}_p[\vartheta_1, \vartheta_2, \dots, \vartheta_n] \subset A$, порождённая классами $\overline{\vartheta}_i = \vartheta_i \pmod p$, изоморфна полю разложения многочлена $\overline{f}$ над $\mathbb{F}_p$.

Таким образом, $\overline{F} \in \mathbb{F}_p[t_1, t_2, \dots, t_n]$ представляет собою многочлен (17-6), построенный по $\overline{f} \in \mathbb{F}_p[x]$ над $\mathbb{F}_p$, и группа Галуа $\operatorname{Gal}\overline{f}/\mathbb{F}_p$ изоморфна группе перестановок переменных $t_1, t_2, \dots, t_n$, сохраняющих один из сомножителей, назовём его P, разложения многочлена $\overline{F}$ на неприводимые множители в кольце $\mathbb{F}_p[t_1, t_2, \dots, t_n]$. Множитель P приходит из разложения на неприводимые одного из сомножителей $\overline{F}_{[s]}$ произведения (17-9). Поэтому стабилизатор P в S_n содержится в стабилизаторе $F_{[s]}$, что и даёт включение $\operatorname{Gal}\overline{f}/\mathbb{F}_p \subset \operatorname{Gal} f/\mathbb{Q}$. □

Следствие 17.1
Пусть при редукции по простому модулю p неприводимый приведённый многочлен $f \in \mathbb{Z}[x]$ распадается в $\mathbb{F}_p[x]$ в произведение $\overline{f} = q_1 q_2 \dots q_m$ неприводимых многочленов $q_1, q_2, \dots, q_m$ степеней $\lambda_1 \geqslant \lambda_2 \geqslant \dots \geqslant \lambda_m$. Тогда группа Галуа $\operatorname{Gal} f/\mathbb{Q}$ многочлена f над $\mathbb{Q}$ содержит перестановку корней f циклового типа λ.

Доказательство. Поле разложения многочлена $\overline{f}$ над $\mathbb{F}_p$ конечно. Согласно n° 16.6.2 его группа Галуа над $\mathbb{F}_p$ циклическая. Так как эта циклическая группа транзитивно действует на корнях каждого из неприводимых многочленов q_i, её образующий элемент является перестановкой циклового типа λ. По предл. 17.5 эта перестановка содержится и в $\operatorname{Gal} f/\mathbb{Q}$. □

17.2.2. Пример многочлена с группой S_5. Покажем что группа Галуа над $\mathbb{Q}$ многочлена

$$f(x) = x^5 - x - 1$$

изоморфна S_5. Для этого разложим его на неприводимые множители над $\mathbb{F}_2$ и над $\mathbb{F}_3$. Если $\overline{f}$ оказывается приводимым, один из его неприводимых приведённых делителей имеет степень $\leqslant 2$. Согласно упр. 16.15, произведение всех неприводимых приведённых многочленов степени $\leqslant 2$ в $\mathbb{F}_p[x]$ равно $x^{p^2} - x$. При помощи алгоритма Евклида убеждаемся, что над полем $\mathbb{F}_2$

$$\text{нод}\left(x^5 - x - 1\,,\ x^4 - x\right) = \text{нод}\left(x^5 + x + 1\,,\ x^4 + x\right) = x^2 + x + 1$$

и разложение $\overline{f}$ на неприводимые в кольце $\mathbb{F}_2[x]$ имеет вид $(x^2 + x + 1) \cdot (x^3 + x^2 + 1)$, а над $\mathbb{F}_3$

$$\text{нод}\left(x^5 - x - 1\,,\ x^9 - x\right) = \text{нод}\left(x^5 - x - 1\,,\ x^4 - 1\right) = 1\,,$$

откуда мы заключаем, что f неприводим в $\mathbb{F}_3[x]$. По сл. 17.1 группа Галуа $\operatorname{Gal} f/\mathbb{Q}$ содержит цикл длины 5 и перестановку циклового типа $(3, 2)$, куб которой — транспозиция. Так как цикл максимальной длины и транспозиция порождают всю симметрическую группу, $\operatorname{Gal} f/\mathbb{Q} \simeq S_5$. Ниже, в n° 17.5 мы увидим, что из этого вытекает, что корни многочлена $x^5 - x - 1$ не выражаются в радикалах через рациональные числа.

17.3. Группы круговых полей. Расширение $\mathbb{Q}[\zeta_n] \supset \mathbb{Q}$, порождённое как алгебра над $\mathbb{Q}$ примитивным корнем n-той степени из единицы

$$\zeta_n = e^{2\pi i/n} \in \mathbb{C}\,,$$

называется n-тым *круговым* (или *циклотомическим*) полем. Это поле является полем разложения сепарабельного многочлена $x^n - 1$ и, стало быть, является расширением Галуа поля $\mathbb{Q}$.

Каждый автоморфизм σ из группы Галуа $\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q}$ переводит ζ_n в некоторую образующую циклической мультипликативной группы $\boldsymbol{\mu}_n \subset \mathbb{Q}[\zeta_n]$ корней n-той степени из единицы, т. е. $\sigma(\zeta_n) = \zeta_n^{m(\sigma)}$, где $m(\sigma) \in (\mathbb{Z}/(n))^*$ лежит в мультипликативной группе обратимых элементов кольца вычетов $\mathbb{Z}/(n)$. Таким образом мы получаем вложение (мультипликативных) групп

$$\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q} \xrightarrow{\sigma\mapsto m(\sigma)} (\mathbb{Z}/(n))^* \tag{17-10}$$

и заключаем, что множество всех первообразных корней степени n из единицы

$$R_n = \{\zeta_n^m \mid \text{нод}(n, m) = 1\} \subset \boldsymbol{\mu}_n$$

является объединением орбит группы Галуа $\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q}$. Следовательно, коэффициенты n-того *кругового многочлена*

$$\Phi_n(x) = \prod_{\xi\in R_n} (x - \xi)$$

инвариантны относительно действия группы Галуа, а значит, лежат в $\mathbb{Q}$. А так как все его корни ξ целы над $\mathbb{Z}$, круговой многочлен $\Phi_n(x) \in \mathbb{Z}[x]$. Например, $\Phi_2(x) = x + 1$,

$$\begin{aligned}
&\Phi_3(x) = (x - \omega)(x - \omega^2) = x^2 + x + 1\,,\\
&\Phi_4(x) = (x - i)(x + i) = x^2 + 1\,,\\
&\Phi_5(x) = (x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1\,,\\
&\Phi_6(x) = (z - \zeta_6)(x - \zeta_6^{-1}) = x^2 - x + 1\,, \quad \ldots
\end{aligned}$$

Теорема 17.2
Многочлен Φ_n является является минимальным многочленом элемента ζ_n и, в частности, неприводим над $\mathbb{Q}$.

Доказательство. Временно обозначим минимальный многочлен ζ_n над $\mathbb{Q}$ через $f_n \in \mathbb{Q}[x]$. Тогда

$$\Phi_n(x) = f_n(x) \cdot q(x)$$

где оба многочлена $f_n, q \in \mathbb{Q}[x]$ приведены. Поскольку все корни Φ_n целы над $\mathbb{Z}$, коэффициенты обоих многочленов f_n и q целы над $\mathbb{Z}$, а значит, лежат в $\mathbb{Z}$. При этом каждый примитивный корень $\xi \in R_n$ является корнем ровно одного из них: либо f_n, либо q.

Для каждого простого $p \nmid n$, автоморфизм возведения в p-тую степень

$$F_p : \boldsymbol{\mu}_n \xrightarrow{\xi\mapsto\xi^p} \boldsymbol{\mu}_n \tag{17-11}$$

переводит множество первообразных корней $R_n \subset \boldsymbol{\mu}_n$ в себя. Применяя к корню $\zeta_n \in R_n$ автоморфизмы F_p, отвечающие всевозможным простым $p \nmid n$, а также их итерации, можно получить все первообразные корни. В самом деле, любой первообразный корень $\xi \in R_n$ равен ζ_n^m для некоторого $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, взаимно простого с n, откуда $\xi = F_{p_1}^{m_1} F_{p_2}^{m_2} \cdots F_{p_k}^{m_k} \zeta_n$.

Для доказательства теоремы достаточно проверить, что при любом простом $p \nmid n$ автоморфизм (17-11) переводит корни f_n в корни f_n: тогда все корни кругового многочлена будут одновременно корнями f_n, и мы получим требуемое равенство $f_n = \Phi_n$.

Допустим, что существует корень $\xi \in R_n$ многочлена f_n, такой что ξ^p является корнем не f_n, а q. Тогда многочлен $q(x^p)$ аннулирует ξ и, стало быть, делится на f_n в $\mathbb{Q}[x]$. Так как $q(x^p)$ приведён и имеет целые коэффициенты, $q(x^p) = f_n(x)h(x)$ для некоторого $h \in \mathbb{Z}[x]$ (по лемме Гаусса). Применим к этому равенству гомоморфизм редукции по модулю p:

$$\mathbb{Z}[x] \xrightarrow{g\mapsto\overline{g}=g\,(\mathrm{mod}\ p)} \mathbb{F}_p[x]\,.$$

Поскольку $\forall\ \overline{g} \in \mathbb{F}_p[x]$ выполняется тождество $\overline{g}(x^p) = \overline{g}(x)^p$, в кольце $\mathbb{F}_p[x]$ будет выполнено равенство $\overline{q}^p = \overline{f}_n \cdot \overline{h}$, из которого следует, что всякий корень многочлена $\overline{f}_n$ в поле разложения многочлена $x^n - 1$ над $\mathbb{F}_p$ является одновременно корнем многочлена $\overline{q}$. Но многочлен $x^n - 1$ сепарабелен над $\mathbb{F}_p$ при $p \nmid n$, а значит и его делитель $\overline{\Phi}_n = \overline{f}_n \cdot \overline{q}$ тоже сепарабелен, так что множества корней многочленов $\overline{f}_n$ и $\overline{q}$ не могут пересекаться. Противоречие. □

Следствие 17.2
Группа Галуа $\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q} \simeq (\mathbb{Z}/(n))^*$, и степень $\deg \mathbb{Q}[\zeta_n]/\mathbb{Q} = \varphi(n)$, где φ — функция Эйлера.

Доказательство. Поскольку многочлен Φ_n неприводим, действие группы Галуа на его корнях транзитивно, и тем самым её порядок равен $|R_n| = \varphi(n)$. □

Упражнение 17.11. Покажите, что а) при нечётном n $\quad \Phi_{2n}(x) = \Phi_n(-x)$ $\quad$ б) $x^n - 1 = \prod\limits_{d|n} \Phi_d(x)$

в) $\Phi_n(x) = \prod\limits_{d|n} (x^{n/d} - 1)^{\mu(d)}$ (используйте подходящую модификацию обращения Мёбиуса)

г) при простом p $\quad \Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + x + 1$, $\quad$ а $\quad \Phi_{p^k}(x) = \Phi_p\left(x^{p^{k-1}}\right)$

д) при простом $p \nmid m$ $\quad \Phi_{pm}(x) = \Phi_m\left(x^p\right)/\Phi_m(x)$

е) $\Phi_{p_1^{k_1} \cdots p_n^{k_n}}(x) = \Phi_{p_1 p_2 \cdots p_n}\left(x^{p_1^{k_1-1} \cdots p_n^{k_n-1}}\right)$, где p_i — различные простые

Следствие 17.3 (элементы Фробениуса)
Для любого простого $p \nmid n$ автоморфизм F_p из формулы (17-11) однозначно продолжается до автоморфизма кругового поля $\mathbb{Q}[\zeta_n]$ над $\mathbb{Q}$ (это продолжение называется *элементом p-Фробениуса* в группе Галуа $\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q}$).

17.3.1. Пример: гауссова сумма. Пусть $p > 2$ простое и $\zeta = \zeta_p \in R_p$. Поскольку любая мультипликативная подгруппа индекса 2 в мультипликативной группе $\mathbb{F}_p^*$ содержит все ненулевые квадраты поля $\mathbb{F}_p$, в группе Галуа кругового поля $\operatorname{Gal}\mathbb{Q}[\zeta]/\mathbb{Q} \simeq \mathbb{F}_p^*$ есть ровно одна подгуппа индекса 2, и это — подгруппа ненулевых квадратов $\mathbb{F}_p^{*2} \subset \mathbb{F}_p^*$. Согласно соответствию Галуа, это означает, что в круговом поле $\mathbb{Q}[\zeta]$ содержится ровно одно квадратичное расширение $\mathbb{K} \supset \mathbb{Q}$ поля $\mathbb{Q}$. Оно порождается над $\mathbb{Q}$ элементом

$$\vartheta = \sum_{\sigma \in \mathbb{F}_p^{*2}} \sigma(\zeta) - \sum_{\sigma \notin \mathbb{F}_p^{*2}} \sigma(\zeta) = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \cdot \zeta^m, \tag{17-12}$$

где *символ Лежандра – Якоби* определяется правилом

$$\left(\frac{m}{p}\right) = m^{(p-1)/2} \pmod p = \begin{cases} 1 & , \quad \text{если } m \pmod p \text{ квадрат в } \mathbb{F}_p^* \\ -1 & , \quad \text{если } m \pmod p \text{ не квадрат в } \mathbb{F}_p^*. \end{cases}$$

В самом деле, число (17-12) инвариантно относительно подгруппы $\mathbb{F}_p^{*2} \subset \operatorname{Gal}\mathbb{Q}[\zeta]/\mathbb{Q}$, а под действием всех остальных автоморфизмов кругового поля оно меняет знак.

Упражнение 17.12. Покажите, что поле $\mathbb{Q}[\vartheta]$ содержит $\sqrt{p \cdot (-1)^{\frac{p-1}{2}}}$ и явно выразите этот квадратный корень через корни p-той степени из единицы.

17.4. Циклические расширения. Элемент ζ произвольного поля $\Bbbk$ называется *первообразным* (или *примитивным*) корнем степени m из единицы, если $\zeta^m = 1$ и $\zeta^i \neq 1$ при всех $0 < i < m$. Если поле $\Bbbk$ содержит примитивный корень степени m из единицы, то циклическая мультипликативная группа корней уравнения $x^m = 1$ имеет порядок m, порождается элементом ζ, и множество образующих этой группы есть множество примитивных корней из единицы степени m. Отметим, что сепарабельность многочлена $x^m - 1$ автоматически влечёт за собой, что m не делится на $\operatorname{char}(\Bbbk)$, и что все многочлены $x^d - a \in \Bbbk[x]$ степени $d|m$ тоже сепарабельны.

Как и в n° 17.3, мы будем обозначать группу корней m-той степени из единицы через $\boldsymbol{\mu}_m \subset \Bbbk^*$. Через $\Bbbk^*/\Bbbk^{*m}$ мы обозначаем мультипликативную группу классов ненулевых элементов поля $\Bbbk$ по модулю их умножения на m-тые степени ненулевых элементов поля $\Bbbk$. Это абелева группа *показателя*[1] m.

Упражнение 17.13. Покажите, что порядок любого элемента группы $\Bbbk^*/\Bbbk^{*m}$ нацело делит m и что в $\Bbbk^*/\Bbbk^{*m}$ имеются элементы порядка m (ср. с упр. 16.6).

Теорема 17.3
Пусть поле $\Bbbk$ содержит первообразный корень m-той степени из единицы, и класс элемента $a \in \Bbbk^*$ в мультипликативной фактор-группе $\Bbbk^*/(\Bbbk^*)^m$ имеет порядок n. Тогда двучлен

$$f(x) = x^m - a \in \Bbbk[x] \tag{17-13}$$

является произведением m/n неприводимых двучленов вида $x^n - b$, и группа Галуа его поля разложения над $\Bbbk$ является циклической группой порядка n. При $n = m$ двучлен (17-13) неприводим, и его поле разложения представляет собою примитивное расширение $\Bbbk[\sqrt[m]{a}] = \Bbbk[x]/(x^m - a)$.

Доказательство. Все корни двучлена $f(x) = x^m - a \in \Bbbk[x]$ имеют вид $\xi\alpha$, где α — какой-то один фиксированный корень, а ξ пробегает циклическую мультипликативную группу $\boldsymbol{\mu}_m \subset \Bbbk$. Поле разложения $\mathbb{K} \subset \overline{\Bbbk}$ двучлена f порождается ими как $\Bbbk$-алгебра, и действие любого автоморфизма $\sigma \in \operatorname{Gal}\mathbb{K}/\Bbbk$ полностью определяется его действием на корни $\xi\alpha$, которые он както переставляет. Эта перестановка однозначно восстанавливается по элементу $\zeta_\sigma \in \boldsymbol{\mu}_m$, такому что $\sigma(\alpha) = \zeta_\sigma \cdot \alpha$, поскольку $\sigma(\xi\alpha) = \xi\sigma(\alpha) = \xi\zeta_\sigma\alpha$ для любого другого корня $\xi\alpha$. Сопоставление $\sigma \mapsto \zeta_\sigma$ задаёт вложение группы $G = \operatorname{Gal}\mathbb{K}/\Bbbk$ в группу $\boldsymbol{\mu}_m$. Образ этого вложения является циклической подгруппой порядка $d|m$, и порождается некоторым примитивным корнем ζ степени d. Смежные классы $G\cdot\xi \subset \mu_m$ подгруппы G биективно соответствуют орбитам действия группы Галуа на корнях двучлена f, и каждой такой орбите отвечает его неприводимый множитель

$$f_\xi(x) = \prod_{\sigma\in G}(x - \zeta_\sigma\xi\alpha) = \prod_{\nu=0}^{d-1}(x - \zeta^\nu\xi\alpha) = x^d + (-\xi)^d\alpha^d \in \Bbbk[x]$$

(в последнем равенстве мы воспользовались тем, что $x^d - 1 = \prod\limits_{\nu=0}^{d-1}(x - \zeta^\nu)$, так что все элементарные симметрические полиномы e_i с $1 \leqslant i \leqslant d-1$ зануляются на корнях многочлена f_ξ:

$$e_i(\zeta^0\xi\alpha, \zeta^1\xi\alpha, \ldots, \zeta^{d-1}\xi\alpha) = \xi^i\alpha^i e_i(\zeta^0, \zeta^1, \ldots, \zeta^{d-1}) = 0\,).$$

Мы видим, что из свободного члена $a = \alpha^n$ двучлена $f(x) = x^m - a$ извлекается в поле $\Bbbk$ корень $b = \sqrt[m/d]{a} = \alpha^d \in \Bbbk$ и что f раскладывается над $\Bbbk$ в произведение m/d неприводимых двучленов вида $x^d - b$, причём степень d всех этих двучленов равна порядку n класса элемента α в $\Bbbk^*/\Bbbk^{*m}$. В частности, f неприводим тогда и только тогда, когда $n = d = m$. В этом случае вложение $\operatorname{Gal}\mathbb{K}/\Bbbk \hookrightarrow \boldsymbol{\mu}_m$ является изоморфизмом, и $\mathbb{K} = \Bbbk[\sqrt[m]{a}] = \Bbbk[x]/(f)$, поскольку вместе с корнем $\alpha = x \pmod f$ в поле $\Bbbk[x]/(f)$ лежат и все остальные корни $\{\xi\alpha\}$ двучлена f. □

Упражнение 17.14. Покажите, что в фиксированном алгебраическом замыкании $\overline{\Bbbk} \supset \Bbbk$ равенство подполей $\Bbbk[\sqrt[m]{a}] = \Bbbk[\sqrt[n]{b}]$ равносильно равенству $a = b^r c^m$ для некоторого $c \in \Bbbk$ и целого r, взаимно простого с m.

Определение 17.1
Расширение Галуа $\mathbb{K} \supset \Bbbk$ называется *циклическим степени* m, если $\operatorname{Gal}\mathbb{K}/\Bbbk$ является циклической группой m-того порядка.

[1] напомним, что это означает, что $a^m = 1$ для любого элемента этой группы, и существует элемент, порядок которого в точности равен m

Теорема 17.4
Всякое циклическое расширение степени m любого поля $\Bbbk$, содержащего первообразный корень m-той степени из единицы, является полем разложения неприводимого двучлена $x^m - a$ с $a \in \Bbbk$.

Доказательство. Пусть группа Галуа $G = \operatorname{Gal}\mathbb{K}/\Bbbk$ циклического расширения $\mathbb{K} \supset \Bbbk$ порождена автоморфизмом $\sigma \in \operatorname{Aut}_{\Bbbk}\mathbb{K}$ порядка m. Фиксируем какой-нибудь первообразный корень m-той степени из единицы $\zeta \in \Bbbk$ и рассмотрим $\Bbbk$-линейное преобразование поля $\mathbb{K}$

$$L_\zeta = \sum_{i=0}^{p-1} \zeta^i \sigma^i : \mathbb{K} \longrightarrow \mathbb{K}$$

Оператор L_ζ коммутирует с σ по правилу $\sigma L_\zeta = \zeta^{-1} L_\zeta$. Поэтому его образ состоит из собственных векторов оператора σ с собственным значением ζ^{-1}. Этот образ отличен от нуля, поскольку $L_\zeta \neq 0$. В самом деле, отображения $\sigma^0 = \mathrm{Id}$, σ, σ^2, $\ldots$, σ^{m-1} можно воспринимать как характеры различных одномерных представлений абелевой мультипликативной группы $\mathbb{K}^*$ над полем $\mathbb{K}$, из чего вытекает из линейная независимость над $\mathbb{K}$.

Упражнение 17.15. Покажите, что любой набор попарно различных гомоморфизмов $\{\psi_\nu\}$ из произвольной (в том числе неабелевой) группы G в мультипликативную группу ненулевых элементов произвольного поля $\mathbb{F}$ линейно независим в векторном пространстве всех функций на G со значениями в поле $\mathbb{F}$.

Итак, существует $\beta \in \mathbb{K}$, такой что $\alpha = L_\zeta(\beta) \neq 0$. Тогда $\sigma(\alpha) = \zeta^{-1}\alpha$, и значит, $\varphi(\alpha^i) = \zeta^{-i}\alpha^i$ при $1 \leqslant i \leqslant m$. Следовательно, из всех степеней α^i с $1 \leqslant i \leqslant m$ только степень α^m инвариантна относительно действия группы Галуа. Поэтому число $a = \alpha^m$ лежит в $\Bbbk$, и его порядок в группе $\Bbbk^{(m)} = \Bbbk^*/\Bbbk^{*m}$ равен m. Как мы уже видели, двучлен $f(x) = x^m - a$ в этом случае неприводим над $\Bbbk$. Поле $\mathbb{K}$ совпадает с его полем разложения, так как содержит все его корни $\boldsymbol{\mu}_m \cdot \alpha$ и имеет над $\Bbbk$ ту же группу Галуа $\boldsymbol{\mu}_m$, что и поле разложения f. □

Упражнение 17.16* (изоморфизм Куммера). Для каждого элемента $a \in \Bbbk^*/\Bbbk^{*m}$ зафиксируем некоторый корень $\alpha = \sqrt[m]{a} \in \overline{\Bbbk}$ и сопоставим каждому автоморфизму $\sigma \in \operatorname{Gal}\overline{\Bbbk}/\Bbbk$ корень из единицы $\zeta_\sigma = \sigma(\alpha)/\alpha \in \boldsymbol{\mu}_m$. Покажите, что таким образом корректно задаётся изоморфизм групп

$$\Bbbk^*/\Bbbk^{*m} \xrightarrow{\sim} \operatorname{Hom}\left(\operatorname{Gal}\overline{\Bbbk}/\Bbbk, \boldsymbol{\mu}_m\right).$$

17.5. Разрешимые расширения. Конечная группа G называется *разрешимой*, если можно построить цепочку подгрупп

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_{m-1} \subset G_m = G \tag{17-14}$$

в которой каждая подгруппа $G_i \lhd G_{i+1}$ нормальна в следующей подгруппе, и фактор группа G_{i+1}/G_i абелева для каждого i.

Расширение Галуа $\mathbb{K} \supset \Bbbk$ поля $\Bbbk$ характеристики нуль называется *разрешимым*, если разрешима его группа Галуа $\operatorname{Gal}\mathbb{K}/\Bbbk$.

Эта терминология возникла в связи с классической задачей о выражении корней многочлена через его коэффициенты[1] посредством четырёх арифметических действий и извлечения корней. Препятствием к решению этой задачи является неразрешимость группы Галуа поля разложения многочлена над полем, порождённым его коэффициентами.

Лемма 17.1
Если группа G разрешима, то цепочку (17-14) можно выбрать так, чтобы все факторы G_{i+1}/G_i были циклическими группами простых порядков.

Доказательство. Из теоремы о строении конечно порождённых абелевых групп вытекает, что любая конечная абелева группа A допускает цепочку подгрупп

$$0 = A_0 \subset A_1 \subset A_2 \subset \cdots \subset A_k \subset A_{k+1} = A \tag{17-15}$$

[1] в своей классической постановке эта задача относилась к полям характеристики нуль

в которой все факторы A_{i+1}/A_i являются циклическими группами простых порядков.

Упражнение 17.17. Докажите это.

Беря такую цепочку для каждой абелевой группы $A = G_{i+1}/G_i$ из (17-14), мы можем вставить между группами G_i и G_{i+1} в башне $\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_{m-1} \subset G_m = G$ фрагмент

$$G_i = A_0G_i \subset A_1G_i \subset A_2G_i \subset \cdots \subset A_{k-1}G_i \subset A_kG_i \subset A_{k+1}G_i = G_{i+1}\,,$$

в котором $A_jG_i \subset G_{i+1}$ это полный прообраз подгруппы $A_j \subset A = G_{i+1}/G_i$ при гомоморфизме факторизации $G_{i+1} \twoheadrightarrow G_{i+1}/G_i$. Легко видеть, что $(A_{j+1}G_i)/(A_jG_i) \simeq A_{j+1}/A_j$. □

Упражнение 17.18. Убедитесь в этом, а также в том, что если $N \lhd G$ — нормальная, а $H \subset G$ — любая подгруппа произвольной группы G, то $HN = \{hf \mid h \in H,\, f \in N\}$ является подгруппой в G, подгруппа $N \subset HN$ нормальна в HN, подгруппа $H \cap N$ нормальна в H, и $H/(H\cap N) \simeq HN/N \subset G/N$.

Лемма 17.2
Если группа G разрешима, то любая её подгруппа $H \subset G$ и любая её фактор группа $Q = G/N$ тоже разрешимы. Наоборот, если нормальная подгруппа $H \lhd G$ и фактор G/H разрешимы, то и G разрешима.

Доказательство. Пересекая цепочку (17-14) с подгруппой $H \subset G$, получим цепочку подгрупп

$$\{e\} = G_0 \cap H \subset G_1 \cap H \subset G_2 \cap H \subset \cdots \subset G_{m-1} \cap H \subset G_m \cap H = H$$

с последовательными факторами

$$\frac{G_{i+1} \cap H}{G_i \cap H} \simeq \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \simeq \frac{(G_{i+1} \cap H)\cdot G_i}{G_i} \subset \frac{G_{i+1}}{G_i}\,.$$

Будучи подгруппами абелевых факторов G_{i+1}/G_i из цепочки (17-14), они тоже абелевы.

Умножая элементы цепочки (17-14) на нормальную подгруппу $N \subset G$ получаем цепочку

$$N \subset G_1N \subset G_2N \subset \cdots \subset G_{m-1}N \subset G_mN = G$$

Факторы которой по нормальной подгруппе N дают цепочку подгрупп, ведущую от $e = N/N$ к G/N с последовательными факторами

$$\frac{G_{i+1}N/N}{G_iN/N} \simeq \frac{G_{i+1}N}{G_iN} \simeq \frac{G_{i+1}(G_iN)}{G_iN} \simeq \frac{G_{i+1}}{(G_iN)\cap G_{i+1}} \simeq \frac{G_{i+1}}{G_i(N\cap G_{i+1})} \simeq \frac{G_{i+1}/G_i}{(G_{i+1}\cap N)/G_i}\,.$$

Будучи факторами абелевых групп G_{i+1}/G_i из цепочки (17-14), они тоже абелевы.

Наконец, из двух цепочек (17-14) для H и G/H

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_{m-1} \subset H_m = H$$
$$\{e\} = Q_0 \subset Q_1 \subset Q_2 \subset \cdots \subset Q_{k-1} \subset Q_k = G/H$$

собирается одна цепочка $H_0 \subset H_1 \subset \cdots \subset H \subset Q_1H \subset Q_2H \subset \cdots \subset Q_kH = G$ для группы G (через Q_iH, как и выше, обозначены полные прообразы подгрупп $Q_i \subset G/H$ относительно гомоморфизма факторизации $G \twoheadrightarrow G/H$). □

Упражнение 17.19 (теорема Жордана-Гёльдера). Цепь подгрупп

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_{m-1} \subset G_m = G$$

называется *композиционным рядом* группы G, если каждая подгруппа $G_i \lhd G_{i+1}$ нормальна в следующей подгруппе, и каждая фактор группа $Q_i = G_i/G_{i-1}$ проста. Покажите, что набор *композиционных факторов* $Q_1, Q_2, \ldots, Q_m$ с точностью до перенумерации не зависит от выбора композиционного ряда, а зависит только от группы G, и приведите пример конечной группы G и двух её композиционных рядов, факторы которых нетривиально переставлены друг по отношению к другу.

Теорема 17.5
Пусть[1] $\mathrm{char}(\Bbbk) = 0$ и один из корней неприводимого многочлена $f \in \Bbbk[x]$ выражается через элементы поля $\Bbbk$ посредством четырёх арифметических действий и извлечений корней произвольных степеней. Тогда группа $\mathrm{Gal}\, f/\Bbbk$ разрешима.

Доказательство. Зафиксируем алгебраическое замыкание $\overline{\Bbbk} \supset \Bbbk$. Пусть корень $\alpha \in \overline{\Bbbk}$ многочлена f выражается в радикалах. Это означает, что α лежит в подполе $\mathbb{L} \subset \overline{\Bbbk}$, которое можно получить из $\Bbbk$ несколькими последовательными примитивными расширениями

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \ \cdots \ \subset \mathbb{L}_m = \mathbb{L} \tag{17-16}$$

вида $\mathbb{L}_{i+1} = \mathbb{L}_i[\sqrt[k_i]{a_i}] = \mathbb{L}_i[x]/(x^{k_i} - a_i)$, где $a_i \in \mathbb{L}_i$. Для доказательства теоремы достаточно вложить поле $\mathbb{L}$ в поле $\mathbb{L}' \supset \Bbbk$, являющееся расширением Галуа с разрешимой группой $\mathrm{Gal}\, \mathbb{L}'/\Bbbk$. Тогда поле разложения $\mathbb{K}$ многочлена f будет нормальным подполем в $\mathbb{L}'$, и его группа Галуа

$$\mathrm{Gal}\, \mathbb{K}/\Bbbk = (\mathrm{Gal}\, \mathbb{L}'/\Bbbk)/(\mathrm{Gal}\, \mathbb{L}'/\mathbb{K})$$

будет фактор группой разрешимой группы $\mathrm{Gal}\, \mathbb{L}'/\Bbbk$, а значит, будет разрешима по лем. 17.2.

Для построения поля $\mathbb{L}'$ по индукции расширим башню полей (17-16) до башни

$$\Bbbk \subset \mathbb{L}'_0 \subset \mathbb{L}'_1 \subset \mathbb{L}'_2 \subset \ \cdots \ \subset \mathbb{L}'_m = \mathbb{L}', \tag{17-17}$$

в которой $\mathbb{L}_i \subset \mathbb{L}'_i$, и каждое $\mathbb{L}'_i$ является расширением Галуа поля $\Bbbk$. В качестве $\mathbb{L}'_0$ возьмём поле разложения многочлена $x^N - 1$ с таким N, чтобы в $\mathbb{L}'_0$ содержались первообразные корни из единицы всех тех же степеней, что и радикалы, необходимые для вычисления α. Если $\mathbb{L}'_i$ уже построено, то в качестве $\mathbb{L}'_{i+1}$ берём поле разложения над полем $\mathbb{L}'_i$ многочлена

$$\prod_{\sigma \in \mathrm{Gal}\, \mathbb{L}'_i/\Bbbk} \Big(x^{k_i} - \sigma(a_i)\Big) \in \Bbbk[x] \subset \mathbb{L}'_i[x]$$

Коэффициенты этого многочлена инвариантны относительно действия группы Галуа $\mathrm{Gal}\, \mathbb{L}'_i/\Bbbk$, т. е. лежат в $\Bbbk$. По предл. 16.3 и сл. 16.6 расширение $\mathbb{L}'_{i+1} \supset \Bbbk$ является расширением Галуа и очевидно содержит $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/(x^{k_i} - a_i)$. Отметим, что поле $\mathbb{L}'_{i+1}$ можно получить из поля $\mathbb{L}'_i$ цепочкой последовательных переходов к полям разложения двучленов вида $x^n - a$ с $a \in \mathbb{L}'_i$. По теор. 17.3 все такие переходы являются расширениями Галуа с циклическими группами Галуа. Согласно сл. 17.2 и сл. 16.6 первый шаг нашего построения — переход от $\Bbbk$ к $\mathbb{L}'_0$ — также является расширением Галуа с абелевой группой Галуа. Таким образом, поле $\mathbb{L}'$ можно получить из $\Bbbk$ последовательными абелевым расширением Галуа, и его группа $\mathrm{Gal}\, \mathbb{L}'/\Bbbk$ разрешима. □

Следствие 17.4
В условиях теор. 17.5 все корни f выражаются в радикалах через элементы поля $\Bbbk$.

Доказательство. В доказательстве теор. 17.5 мы видели, что поле разложения f содержится в поле $\mathbb{L}'$, все элементы которого выражаются в радикалах через элементы поля $\Bbbk$. □

17.5.1. Пример: «общее» уравнение степени $n \geqslant 5$ неразрешимо в радикалах. Зафиксируем произвольное поле $\mathbb{F}$. Многочлен

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}(a_1, a_2, \ldots, a_n)[x]\,, \tag{17-18}$$

рассматриваемый над полем $\Bbbk = \mathbb{F}(a_1, a_2, \ldots, a_n)$ рациональных функций от n алгебраически независимых переменных $a_1, a_2, \ldots, a_n$ с коэффициентами в $\mathbb{F}$, называется *общим*, поскольку придавая его коэффициентам конкретные значения из поля $\mathbb{F}$, можно получить любой «конкретный»

[1] требование $\mathrm{char}(\Bbbk) = 0$ можно ослабить до требования, чтобы $\mathrm{char}(\Bbbk)$ не делила ни один из показателей радикалов, участвующих в формуле для вычисления корня; заинтересованный читатель может убедиться, что приводимое здесь доказательство проходит и для этого случая

многочлен $f \in \mathbb{F}[x]$. В частности, если имеется формула, выражающая корни общего многочлена (17-18) через элементы поля $\Bbbk = \mathbb{F}(a_1, a_2, \ldots, a_n)$ в радикалах[1], то эта формула позволяет единообразно выразить в радикалах через элементы поля $\mathbb{F}$ корни сразу всех «конкретных» многочленов из $\mathbb{F}[x]$. Пример n° 17.2.2 показывает, что нал полем $\mathbb{F} = \mathbb{Q}$ для общего многочлена степени 5 такой формулы нет. Поучительно, однако, проанализировать этот вопрос независимо над произвольным полем $\mathbb{F}$.

Для этого вычислим группу Галуа поля разложения $\mathbb{K} \supset \Bbbk$ многочлена (17-18) над $\mathbb{F}$. Обозначим через $x_1, x_2, \ldots, x_n$ корни f в $\mathbb{K}$. Поскольку $\mathbb{K}$ алгебраично над $\Bbbk$, базис трансцендентности $\mathbb{K}$ над $\mathbb{F}$ состоит из n элементов. Элементы $a_1, a_2, \ldots, a_n$, образующие базис трансцендентности $\Bbbk$ над $\mathbb{F}$, являются многочленами от $x_1, x_2, \ldots, x_n$ с коэффициентами из $\mathbb{F}$. Поэтому поле $\mathbb{K}$ алгебраично над полем частных алгебры $\mathbb{F}[x_1, x_2, \ldots, x_n]$, и по лем. 14.3 базис трансцендентности $\mathbb{K}$ над $\mathbb{F}$ можно выбрать из элементов $x_1, x_2, \ldots, x_n$. Так как этот базис должен состоять из n элементов, уже сами $x_1, x_2, \ldots, x_n$ образуют базис трансцендентности $\mathbb{K}$ над $\mathbb{F}$.

Тем самым, $x_1, x_2, \ldots, x_n$ алгебраически независимы над $\mathbb{F}$ (в частности, различны), многочлен f сепарабелен, а поле $\mathbb{K} = \mathbb{F}(x_1, x_2, \ldots, x_n)$ есть поле рациональных функций от $x_1, x_2, \ldots, x_n$ и является расширением Галуа поля $\Bbbk = \mathbb{F}(a_1, a_2, \ldots, a_n)$. Поскольку любая перестановка независимых переменных продолжается до автоморфизма поля рациональных функций, $\operatorname{Gal}\mathbb{K}/\Bbbk = S_n$, $\deg \mathbb{K}/\Bbbk = n!$ и $\mathbb{F}(x_1, x_2, \ldots, x_n)^{S_n} = \mathbb{F}(a_1, a_2, \ldots, a_n)$.

Упражнение 17.20. Покажите, что поле инвариантов $\mathbb{K}^{A_n}$ нормальной знакопеременной подгруппы $A_n \lhd S_n$ является квадратичным расширением поля $\Bbbk$ при помощи квадратного корня

$$\Delta(f) = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j) = \sqrt{D(f)}$$

из дискриминанта $D(f) = \Delta(f)^2 \in \Bbbk$ многочлена (17-18).

Следствие 17.5 (теорема Абеля)
Ни для какого поля $\mathbb{F}$ характеристики нуль[2] не существует формулы, выражающей корни многочлена $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}(a_1, a_2, \ldots, a_n)[x]$ степени $n \geqslant 5$ через элементы поля $\mathbb{F}(a_1, a_2, \ldots, a_n)$ посредством сложения, вычитания, умножения, деления и извлечения корней произвольных степеней.

Доказательство. При $n \geqslant 5$ группа Галуа $\operatorname{Gal} f/\Bbbk \simeq S_n$ неразрешима, поскольку неразрешима её знакопеременная подгруппа $A_n \lhd S_n$. □

Замечание 17.1. Отсутствие «общей формулы» для решения в радикалах полиномиального уравнения $f(x) = 0$ степени n не означает, что не существует формул, выражающих корни «конкетных» многочленов $f \in \mathbb{F}$ через элементы $\mathbb{F}$ в радикалах, и для многих многочленов таковые формулы действительно имеются.

Теорема 17.6
Пусть[3] $\operatorname{char}(\Bbbk) = 0$ и $f \in \Bbbk[x]$ приведён и неприводим. Если его группа Галуа $\operatorname{Gal} f/\Bbbk$ разрешима, то все корни f выражаются через элементы поля $\Bbbk$ посредством четырёх арифметических действий и извлечения корней.

Доказательство. Обозначим через $\mathbb{K} \supset \Bbbk$ поле разложения многочлена f, а через $\mathbb{L} \supset \Bbbk$ результат присоединения к $\Bbbk$ первообразного корня из единицы степени $|\operatorname{Gal}\mathbb{K}/\Bbbk|$. Все элементы поля $\mathbb{L}$

[1] как это делает, например, школьная формула $x_{1,2} = \left(p \pm \sqrt{p^2 - 4q}\right)/2$ для решения «общего квадратного уравнения» $x^2 + px + q = 0$

[2] оригинально теорема Абеля была им сформулирована и доказана для поля $\mathbb{F} = \mathbb{C}$

[3] требование $\operatorname{char}(\Bbbk) = 0$ можно ослабить до требования, чтобы $\operatorname{char}(\Bbbk)$ не совпадала ни с одним из порядков простых композиционных факторов Жордана – Гёльдера группы Галуа многочлена f; заинтересованный читатель может убедиться, что приводимое здесь доказательство проходит и для этого случая

выражаются в радикалах через элементы поля $\Bbbk$. По условию, группа Галуа $\mathbb{K}$ над $\Bbbk$ разрешима. По сл. 16.6 расширение $\mathbb{LK} \supset \mathbb{L}$ является расширением Галуа, и его группа Галуа G по сл. 16.7 является подгруппой в $\operatorname{Gal}\mathbb{K}/\Bbbk$, а значит, тоже разрешима и допускает фильтрацию (17-14)

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ \cdots \ \subset G_{m-1} \subset G_m = G$$

в которой каждая подгруппа $G_i \lhd G_{i+1}$ нормальна в следующей подгруппе, и фактор группа G_{i+1}/G_i при всех i циклическая. Поэтому поле $\mathbb{LK}$ получается из поля $\mathbb{L}$ последовательностью циклических расширений Галуа. По теор. 17.4 каждое такое расширение есть присоединение радикала. Следовательно, все элементы поля $\mathbb{LK} \supset \mathbb{K}$ выражаются в радикалах через элементы поля $\Bbbk$. □