GALOIS THEORY MICHAELMAS 2010
(M.W.F. 11AM, MR3)

TERUYOSHI YOSHIDA

Contents

Date: February 11, 2011.

Notation

$\emptyset$ — The empty set (a set without any elements).
$a \in A$ — a is an element of the set A. (Or: an element a of the set A.)
$a \notin A$ — a is not an element of the set A. (Or: an element a not in the set A.)
$|A|$ — The cardinality of the set A.
$\exists x \in A$ — There exists an element x of the set A, (satisfying...).
$\forall x \in A$ — For all elements x of the set A, (the following holds...).
$B \subset A$ — The set B is a subset of the set A. (Or: a subset B of the set A.)
(We decree $\emptyset \subset A$ for any set A.)
$A \cup B$ — The union of the set A and the set B.
$A \cap B$ — The intersection of the set A and the set B.
$\bigcup_{i=1}^{n} A_i = A_1 \cup \cdots \cup A_n$.
$\bigcap_{i=1}^{n} A_i = A_1 \cap \cdots \cap A_n$.
$A \setminus B$ — The set of elements of A not in B.
$f : X \to Y$ — A map f from the set X to Y.
$f : X \ni x \longmapsto y \in Y$ — A map f sending a (general) element x of the set X to the element y of the set Y.
$g \circ f$ — The composite of the maps f and g.
id — The identity map $f : X \ni x \longmapsto x \in X$.
$\mathbb{N}$ — $\{ 0, 1, 2, 3, 4, \dots \}$.
$\mathbb{Z}$ — The set of all integers.
$\mathbb{Q}$ — The set of all rational numbers.
$\mathbb{R}$ — The set of all real numbers.
$\mathbb{C}$ — The set of all complex numbers.
$\deg P$ — The degree of a polynomial P. (We let $\deg 0 = -\infty$.)

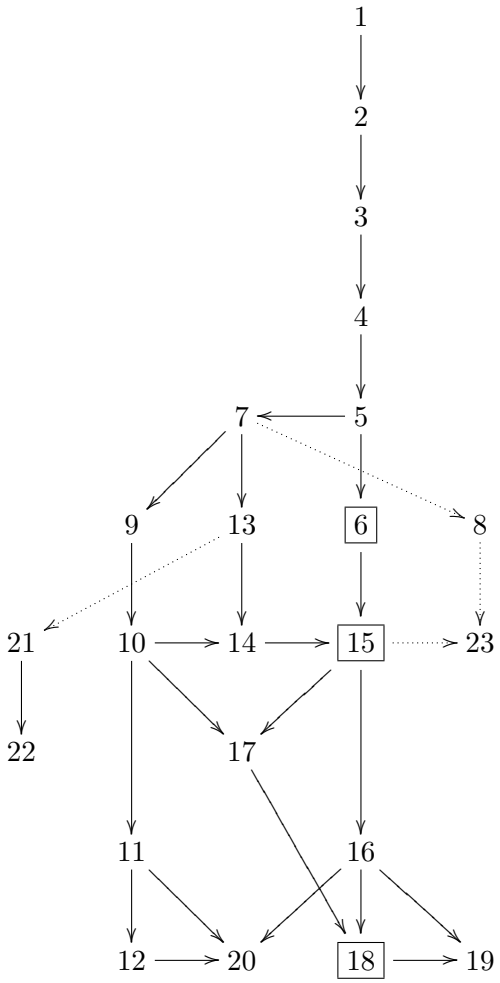
Preface

These are lecture notes I prepared for the Part IID course "Galois Theory" in Michaelmas 2009 and Michaelmas 2010. It is still incomplete and is meant to be completed as lectures proceed. We have two goals in this course-

(i) the fundamental theorem of Galois theory (Lectures 6 and 15), and
(ii) the impossibility of solving general quintic and higher equations by radicals (Lecture 18).

Teruyoshi Yoshida
October 2010

Logical Order



- When two arrows meet at a Lecture, two previous ones are *both* used.
- Dotted lines mean tangential/digression.

Part 1. Galois Theory (1)

Lecture 1. Introduction, adjoining roots (F. 8/10/10)

Motivation

Galois theory is the theory about *solving polynomial equations* in one variable, like:

$$X^7 - 6X^5 + X^4 + 3X^3 + X - 13 = 0.$$

But what does it actually *mean* to solve this equation? Galois theory is, in fact, the theory about explaining what it means to solve an equation (in one variable). When Galois theory showed that it was impossible to find a formula to express roots of general quintic equations in terms of rational functions and radicals of their coefficients — i.e. in the way we know that the roots of $aX^2 + bX + c = 0$ can be expressed as

$$X = (-b \pm \sqrt{b^2 - 4ac})/2a,$$

it wasn't that a mathematical exploration reached a deadend — this negative result brought us to the sight of a whole new mathematical landscape.

Why do we feel that the above formula for the quadratics *solves* the equation? When we say that roots of $X^2 - 6X + 7 = 0$ are $X = 3 \pm \sqrt{2}$, what we are doing is merely to reduce the problem of "solving" this equation to solving a simpler equation:

$$X^2 - 2 = 0.$$

And what do we do with this one? We just name *one* of its roots $\sqrt{2}$. Well, this is just a symbol – we could have used $f(2)$ or s_2 or λ or such like, whatever. Naming a root is logically null; what isn't null is that, once we name one of its roots λ, then we know that the other one is $-\lambda$, or, $(-1) \cdot \lambda$. We could have said a similar thing about the original one: if we denote one of the roots of $X^2 - 6X + 7 = 0$ by α, then the other one has to be $6 - \alpha$, and at the same time $7/\alpha$. Note that this does not depend on whether you set $\alpha = 3 + \sqrt{2}$ or $\alpha = 3 - \sqrt{2}$.

This seemingly trivial babble contains the seeds of Galois theory — let's tentatively say, a mathematical content of *solving* a polynomial equation is (i) to clarify algebraic relations between the roots, and (ii) to reveal the "symmetry" among the roots. Note that the particular linear "operation" $\alpha \mapsto 6 - \alpha$ is *so* symmetric — to reveal its hidden symmetry, iterate it: then $6 - (6 - \alpha)$ gives you back α!

Actually we did similar things when we extended the set of "numbers" from $\mathbb{N}$ to $\mathbb{Z}$ and $\mathbb{Z}$ to $\mathbb{Q}$: we take an equation $X + 2 = 0$ with coefficients in $\mathbb{N}$ but no root in $\mathbb{N}$, so we name it -2, and then we verify that algebraic operations (addition, multiplication in $\mathbb{N}$) extend to these new numbers, miraculously satisfying the familiar laws (associative, distributive, etc). Moreover, this -2 solves other equations like $2X + 5 = 1$, so we reduce the solution of a whole class of equations to solving some equations of simpler form like $X + 2 = 0$. Then there are still equations like $2X - 1 = 0$; so we name its root $1/2$. We do this with all linear equations with coefficients in $\mathbb{Z}$, verify that addition and multiplication in $\mathbb{Z}$ miraculously extend to these new symbols, satisfying all familiar laws, with some identifications between solutions of different equations as before (say $2X - 1 = 0$ and $6X - 2 = 1$). Thus we have $\mathbb{Q}$. This enables us to solve all

linear equations with coefficients in $\mathbb{Z}$, by definition more or less, but it turns out that it enables us to solve all linear equations with *coefficients in* $\mathbb{Q}$. Now we proceed to polynomial equations with higher degree, and hence our discussion in the beginning.

IDEA

So, mathematically, what we should do first to "solve" an equation like the one we saw in the beginning is to *name* one of its roots. Well, call one of its roots Ψ. But then the real questions are, (i) what are algebraic relations between Ψ and the *other* (presumably six) roots, (ii) and what are the symmetry between the roots?

In this lecture we deal with formulating "naming one of its roots" with logical rigor. We want this new Ψ to be a new "number", i.e. something we can do algebraic operation on. What we do is to first think of this Ψ as a formal variable, i.e. consider the polynomial ring $\mathbb{Q}[\Psi]$. Then we *require* that $\Psi^7 - 6\Psi^5 + \Psi^4 + 3\Psi^3 + \Psi - 13 = 0$. This is done by passing to the *quotient ring*, under the *equivalence relation* defined by the ideal generated by $\Psi^7 - 6\Psi^5 + \Psi^4 + 3\Psi^3 + \Psi - 13$. Now you see the use of ring theory. And here the theorem that *the ring of polynomials in one variable over a field is a PID* is crucial — so that if this equation is *irreducible*, then the resulting quotient ring becomes a *field*. This shows the following: "miraculously, addition, subtraction, multiplication *and division* extend to the new numbers involving Ψ".

Well, the real questions remain. Enjoy the flavour of the real thing by checking the following: if ζ is one of the roots of $X^4 + 52X^3 - 26X^2 - 12X + 1 = 0$, then the other roots are $\dfrac{-4\zeta}{(1-\zeta)^2}$, $\dfrac{1-\zeta}{1+3\zeta}$, $\dfrac{(1-\zeta)(1+3\zeta)}{-4\zeta^2}$. Explore how symmetric these relations are. (This example figures in the entry of 21th March 1797 of C.F. Gauss' diary, when he was nineteen years old. It is related to the theory of elliptic functions.)

MATH

Let K be a field and $P \in K[X] \backslash K$ be a monic irreducible polynomial. By Proposition ix.8(i) and vii.20(i), (P) is a maximal ideal of $K[X]$, hence the quotient ring

$$K_P := K[X]/(P)$$

is a field by Corollary viii.10(ii). As the subring K of $K[X]$ (constant polynomials) are mapped injectively into K_P by the canonical surjection $K[X] \to K_P$ (see Exercise 1.2), we can regard $K \subset K_P$, and the image $\overline{X}$ of X gives a root of P in K_P.

Definition 1.1. The field K_P is called the extension field of K obtained by **adjoining a root** of P.

Exercise 1.2. For a group/ring/A- homomorphism $f : X \to Y$ and a subgroup/subring/A-submodule X' of X, $\operatorname{Ker}(f|_{X'}) = X' \cap \operatorname{Ker} f$. Therefore, by the homomorphism theorem, $f(X') \cong X'/(X' \cap \operatorname{Ker} f)$.

Lecture 2. Field extensions (M. 11/10/10)

Review

I hope the previous discussion reminded you of the mysterious definition of the imaginary number i that you must have heard before — "there is no root of $X^2+1=0$ in $\mathbb{R}$, so let i denote one of its roots, newly considered outside $\mathbb{R}$, then the other root must be $-i$, and $X^2+1=(X-i)(X+i)$." Our construction should logically justify (and ultimately demystify) this. Namely, we define the field of complex numbers $\mathbb{C}$ as the extension field of $\mathbb{R}$ obtained by adjoining a root of X^2+1, i.e. $\mathbb{C}:=\mathbb{R}[X]/(X^2+1)$. The last lecture showed that this is indeed a *field* which contains $\mathbb{R}$, with the newly adjoined root $i:=\overline{X}$ of $X^2+1=0$. Now you learned that complex numbers are the "numbers of the form $a+bi$ with $a,b\in\mathbb{R}$. We are saying that, thinking of complex numbers is equivalent to, or actually defined as, considering all polynomials with real coefficients *modulo* X^2+1, where any polynomial is equivalent to a linear one $a+bX$. Taken modulo X^2+1, check that multiplication of polynomials look just like the multiplication of complex numbers.

Idea

So this is how $\mathbb{C}$ was *constructed* from $\mathbb{R}$. In general, we are interested in a situation where one field is contained in another, like $\mathbb{R}\subset\mathbb{C}$, in which case we call $\mathbb{C}$ is an *extension field* of $\mathbb{R}$ and $\mathbb{R}$ is the *base field*. Another example is $\mathbb{Q}\subset\mathbb{R}$. Now note that $\mathbb{C}$ turned out to be a vector space over $\mathbb{R}$ of dimension 2, with bases $\{1,i\}$. This is a typical situation, as we will see in Proposition 2.7. Here we emphasize the fact that $\mathbb{C}$ was a field *as well as* being a vector space over $\mathbb{R}$. Rings which are at the same time a vector space over a field K are called *K-algebras* (see subsection ix), which constitute a natural category in which to build the theory of equations, or more generally *algebraic geometry*, over the field K. Naturally, ring theory and linear algebra both come into play and can be used according to your purpose. In this lecture, we see the extension fields primarily as vector spaces over the base field. Now the most fundamental fact about vector spaces is that, as long as they are finitely generated, they are completely classified up to isomorphism by its *dimension*, an invariant which is a natural number. Therefore, an extension field which is finite dimensional as a vector space over the base field (*finite extension*) has its dimension, which we call its *degree*. So $\mathbb{R}$ is not a finite extension of $\mathbb{Q}$. We will almost entirely restrict ourselves to the study of *finite* extensions.

Math

The letters F,K,L denote fields.

Definition 2.1. When a subring K of a field F is a field, we call K a **subfield** of F, and F an **extension field** of K. The pair of K and its extension field F is called an **extension** F/K. A field L satsifying $F\supset L\supset K$ is called an **intermediate field** of the extension F/K, and L/K is called a **subextension** of F/K.

In the following, let F be an extension field of K. The field F can naturally be regarded as a vector space over K (Exercise iii.3(v)).

Definition 2.2. The dimension of F as a K-vector space is called the **extension degree** of F/K, and is denoted by $[F : K]$. When $[F : K] = n \in \mathbb{N}$, F/K is called a **finite extension [of degree n]**, and when $[F : K] = \infty$, an **infinite extension**.

Example 2.3. $[F : K] = 1 \iff F = K$.

Proposition 2.4. (The tower law) $F \supset L \supset K \Longrightarrow [F : K] = [F : L][L : K]$.

Proof. If one of $F/L, L/K$ is an infinite extension, this is a formal equality $\infty = \infty$. If both are finite extensions, let $\{a_i\}$ be a basis of F over L and $\{b_j\}$ a basis of L over K. Then $\{a_i b_j\}$ gives a basis of F over K. □

Exercise 2.5. Elaborate the above proof using the definition of bases.

Example 2.6. The main object of algebraic number theory is the finite extensions of $\mathbb{Q}$. A finite extension field of $\mathbb{Q}$ is called an (**algebraic**) **number field**.

Proposition 2.7. $[K_P : K] = \deg P$.

Proof. Putting $\deg P = n$, the set $\{1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{n-1}\}$ generates K_P as a K-module, and as the ideal (P) of $K[X]$ does not contain polynomials with degree less than n, they are linearly independent over K. □

THOUGHTS

But extension fields of K (or K-algebras in general) are not just K-vector spaces. Two K-algebras can be isomorphic as K-vector spaces but *not* isomorphic as rings. Therefore, finite extensions of K are *not* classified just by the degrees. Can you show that $\mathbb{Q}[X]/(X^2 + 3)$ and $\mathbb{Q}[X]/(X^2 + 1)$ are both *quadratic fields* (extension fields of degree 2) over $\mathbb{Q}$ but not isomorphic to each other as fields? But then $\mathbb{R}[X]/(X^2+3)$ is isomorphic to $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ as fields — can you construct an isomorphism? Why didn't this work over $\mathbb{Q}$? Then how about $\mathbb{Q}[X]/(X^2 - 2)$ and $\mathbb{Q}[X]/(X^2 - 6X + 7)$?

You might have seen the notation like $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[X]/(X^2 - 2)$, where $\sqrt{2}$ denotes the specified root $\overline{X}$ of $X^2 - 2$ in $\mathbb{Q}[X]/(X^2 - 2)$. Now consider $\mathbb{Q}[X]/(X^3 - 2)$. We tend to think of roots of polynomials in a fixed ambient field $\mathbb{C}$ of complex numbers. There are three roots $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ of $X^3 - 2$ in $\mathbb{C}$, where $\sqrt[3]{2}$ denotes the one in $\mathbb{R}$ and $\omega = (-1 + \sqrt{-3})/2$ is a cubic root of unity. If we define extension fields of $\mathbb{Q}$ as subfields of $\mathbb{C}$ like

$$\mathbb{Q}(\sqrt[3]{2}) := \left\{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \;\middle|\; a, b, c \in \mathbb{Q}\right\} \subset \mathbb{C},$$

then three fields $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2)$ are all different subfields of $\mathbb{C}$ (different as subsets, their intersection being $\mathbb{Q}$, prove it), but they are all isomorphic to the extension field $\mathbb{Q}[X]/(X^3 - 2)$. Is this confusing?

Lecture 3. K-homomorphisms (W. 13/10/10)

Idea

When we constructed K_P, we saw the extensions from the point of view of K, from the bottom up. Another point of view would be to see the extensions, including the adjoined roots, from the top, or inside a big ambient field, say the field $\mathbb{C}$ of complex numbers. As we saw in the previous discussion, the extension field $\mathbb{Q}[X]/(X^3-2)$ has three different embeddings, or realizations, in $\mathbb{C}$, all different as subfields of $\mathbb{C}$. More than that. Even though the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(-\sqrt{2})$ are the *same* subfields of $\mathbb{C}$, they are different realizations of $\mathbb{Q}[X]/(X^2-2)$, realizing $\overline{X}$ as $\sqrt{2}$ or $-\sqrt{2}$. It's this difference that Galois theory exploits — it's this seemingly subtle difference that knows the hidden symmetry of the equations. To keep track of this carefully, we need to formulate the notion of isomorphisms, or morphisms, between extension fields.

Math

Definition 3.1. For two extension fields F, F' of a field K, if a ring homomorphism $f : F \to F'$ satisfies $f|_K = \mathrm{id}$, f is called a **K-homomorphism**. The set of all K-homomorphisms from F to F' is denoted by $\mathrm{Hom}_K(F, F')$. A bijective K-homomorphism is called a **K-isomorphism**. When there exists a K-isomorphism $F \to F'$, we say F and F' are **(K-)isomorphic**, and we write $F \cong F'$. In particular, a K-isomorphism $F \to F$ is called a **K-automorphism** of F, and the group consisting of all K-automorphisms of F is denoted by $\mathrm{Aut}_K(F)$.

Exercise 3.2. (i) If $f : F \to F'$ is a ring homomorphism between extension fields of K, then f is a K-homomorphism if and only if it is K-linear as a map between K-vector spaces.
(ii) If $F \cong F'$, then $[F : K] = [F' : K]$.

Lemma 3.3. *Every K-homomorphism $f : F \to F'$ of extension fields is injective, and its image is a subextension of F'/K. In particular, if F'/K is finite then so is F/K.*

Proof. As $\mathrm{Ker}\, f$ is an ideal of F, it must be equal to F or 0 by Exercise iii.8(ii). If $\mathrm{Ker}\, f = F$ then $1 = f(1) = 0$ in F', which is impossible as F' is not the zero ring. □

Lemma 3.4. *If $[F : K] = [F' : K]$ for two finite extensions F/K and F'/K, every K-homomorphism $f : F \to F'$ is a K-isomorphism. In particular, $\mathrm{Hom}_K(F, F) = \mathrm{Aut}_K(F)$ for a finite extension F/K.*

Proof. Lemma 3.3, Corollary vi.6. □

Exercise 3.5. Let $F/K, F'/K$ be extensions with F/K finite. If $\mathrm{Hom}_K(F, F')$ and $\mathrm{Hom}_K(F', F)$ are both non-empty, then $F \cong F'$ as extensions of K. (Lemmas 3.3, 3.4.)

Background

We will always consider an extension field of K as a K-algebra. As we do not assume that you have seen K-algebras or category theory before, we defined the notion of K-homomorphisms only for the extension fields, but these are really the morphisms of

K-algebras. Let me give the first reason why it is important to think "categorically": it clarifies what are the most natural ways to think about mathematical objects, and what are the natural ("canonical") methods to treat them. For example, if you think of $\mathbb{Q}(\sqrt{2})$ as a *field*, well, fields are a special kind of *rings*, so the natural methods to apply will be from ring theory. The morphisms between them are ring homomorphisms. On the other hand, if you think of $\mathbb{Q}(\sqrt{2})$ as a $\mathbb{Q}$-*vector space*, then the methods are those of linear algebra. The morphisms between these objects are $\mathbb{Q}$-linear maps. Same for topological spaces and continuous maps, smooth manifolds and differentiable maps, etc. Interesting mathematical objects tend to be many things at the same time (a number field is a $\mathbb{Q}$-vector space *and* a field, a Lie group is a group *and* a manifold, etc.), but when we do mathematical operations on them it helps to know what we are treating them as. Natural categories like those of *vector spaces*, *rings* or *topological spaces* have their own rich general theory. So when we think about extension fields, we think of them as vector spaces and rings, and employ linear algebra and ring theory. Try to dissect the proofs and arguments we are making, and tease apart where we use what, and how each of the arguments can or cannot be generalized[1].

Now what are we doing by thinking of extension fields of K as K-algebras? We are not thinking of them as subsets of anything. As subfields of $\mathbb{C}$, the fields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(-\sqrt{2})$, and $\mathbb{Q}(1+\sqrt{2})$ are all identical. But the extension field $\mathbb{Q}[X]/(X^2-2)$ is an extension constructed from bottom up, with a specified root $\overline{X}$ of the equation X^2-2. So the fact that you can map $\overline{X}$ to two different elements in $\mathbb{C}$ *means* something. And the fact that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1+\sqrt{2})$ shows that the two extensions $\mathbb{Q}[X]/(X^2-2)$ and $\mathbb{Q}[X]/(X^2-2X-1)$ are $\mathbb{Q}$-isomorphic. So we have translated the question of

expressing a root of one equation P as a K-rational function
(or equivalently, a K-polynomial) of a root of another equation Q

into that of *finding a K-homomorphism from K_P into K_Q*.

We will elaborate this translation further in Lecture 5. Note that this gives more precision and clarity, as a different K-homomorphism correspond to a different expression, depending on a choice of roots: you can send $\overline{X} \in \mathbb{Q}[X]/(X^2-2X-1)$ into $1+\overline{X}$ or $1-\overline{X}$ in $\mathbb{Q}[X]/(X^2-2)$. This can get more tricky for equations of higher degree!

[1]Categorically speaking, it is incorrect to define K-isomorphisms as bijective K-homomorphisms. In general, isomorphisms are the morphisms which have an inverse. In our case it is equivalent to our definition — if a K-homomorphism is bijective, i.e. has an inverse as a map between sets, then the inverse map is automatically a K-homomorphism. Was this true for continuous maps between topological spaces?

Lecture 4. Finite extensions (F. 15/10/10)

Musings

Let me try to continue babbling on the difference betweeen *equations* and *extension fields*. The starting point is that (infinitely) many equations P define the same (or K-isomorphic) extension fields K_P, hence extension fields are, clumping up or groupings of equations such that solving one member of the group will solve all the other equations (i.e. the roots of other equations can be expressed as a rational function, or even a K-polynomial, of the root of one equation). If we feel comfortable with the thought that once we have "solved" X^2-2 we have "solved" X^2-2X-1 as well, after figuring out that the roots of the latter are 1 plus the roots of the former, then it seems natural that the groups of simultaneously solved equations, or extension fields, are natural objects to study. But this shift of focus, shift of emphasis has a *huge* bonus, which is the fact that extension fields exist in a *finite, discrete* manner. What do I mean by this? Between the field $\mathbb{Q}$, which is a 1-dimensional $\mathbb{Q}$-vector space, and $\mathbb{Q}(\sqrt[3]{2})$, which is a 3-dimensional $\mathbb{Q}$-vector space, there are infinitely many 2-dimensional $\mathbb{Q}$-vector spaces V, *none of which are fields* because of the tower law. For a vector space, it's such a difficult thing to become a field — extension fields are such rare occurences. Consequently, in most cases (which will be called *separable extensions* later), a finite extension has only *finitely many* intermediate extensions. This is a very good news — instead of trying to solve infinitely many different equations and chasing after expressions and relations among infinitely many roots, now we have a class of objects which we can count up, classify and compare as finite sets. More precise way of saying this is that, for any pair of finite extensions F, F', the set of K-homomorphisms $\mathrm{Hom}_K(F, F')$ is a finite set, and those finite sets know everything about the possible algebraic relations between *all* roots of *all* equations. So the shift from equations to fields extracts a finite, tractable, structure which we can manipulate, from the chaos of infinite number of elements — this was the genius in the insight of Galois.

In this lecture and the next we complete the dictionary between the roots and K-homomorphisms. In Lecture 1 we constructed a finite extension from an irreducible polynomial, but now we go other way around. If we have a finite extension F/K, every element x of F is a root of *some* K-polynomial (because the set $\{1, x, x^2, x^3, \dots\} \subset F$ has to be linearly dependent!), and as the set of all such polynomials make up an ideal in $K[X]$, it is the set of multiples of a unique monic called the *minimal polynomial* P_x of x. If we can find an $x \in F$ such that $\deg P_x = [F : K]$, then $K_{P_x} \cong F$, or every element of F is expressed as a K-polynomial in x (we say x *generates* F, which means that the minimal subfield of F containing x is going to be the whole of F). Such F is called a *simple extension*, and it turns out later that most finite extensions (all separable extensions) are simple. Note that, for a simple extension F/K, there can be many choices of x such that $F = K(x)$: for instance, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(1+\sqrt{2})$. We occasionally consider infinite extensions which has elements that are not roots of any K-polynomial (*transcendental*), and as far as the algebra goes we can treat these elements as if they are formal variables, i.e. generating a field of *rational functions*.

MATH

Let F/K be an extension and $x \in F$. The "substitution" map

$$f_x : K[X] \ni P \longmapsto P(x) \in F$$

is a ring homomorphism. We consider this homomorphism, using the homomorphism theorem and the theory of PID. First, $\operatorname{Im} f_x$ is a subring of F, therefore a domain (Exercise vii.3(i)), hence by Corollary viii.10(i), $\operatorname{Ker} f_x \in \operatorname{Spec}(K[X])$.

Definition 4.1. If $\operatorname{Ker} f_x \neq 0$ (resp. $\operatorname{Ker} f_x = 0$), then we say x is **algebraic** (resp. **transcendental**) over K. If every $x \in F$ is algebraic, then we say F/K is **algebraic**.

Lemma 4.2. *Finite extensions are algebraic.*

Proof. As f_x is K-linear, $\operatorname{Im} f_x$ is a K-subspace of F, therefore finite-dimensional over K by Lemma iv.8, and as $K[X]$ has infinite dimension over K, we have $\operatorname{Ker} f_x \neq 0$. □

Exercise 4.3. F/K : algebraic $\iff$ F : a union of finite extensions of K.

Exercise 4.4. If $x \in F$ is transcendental, then $K[X] \cong \operatorname{Im} f_x \subset F$, and by Exercise ix.12, the extension F/K has an intermediate extension $\operatorname{Frac}(\operatorname{Im} f_x)/K$, isomorphic to the fraction field $K(X)$ of $K[X]$ (called the **rational function field** over K). We write $K(x) := \operatorname{Frac}(\operatorname{Im} f_x)$, which is the minimal subextension of F/K containing x.

Now let $x \in F$ be algebraic over K. By Proposition ix.8(i) and Exercise vii.14(i), $\operatorname{Ker} f_x$ is a principal ideal (P_x) generated by an irreducible polynomial, and the quotient ring $K[X]/(P_x)$ is the extension field K_{P_x} of K obtained by adjoining a root of P_x. Consequently, by the homomorphism theorem, we have a K-homomorphism between extension fields as follows:

$$f_x : \ K_{P_x} \xrightarrow{\cong} \operatorname{Im} f_x \subset F \ .$$

Definition 4.5. We call the monic gererator P_x of $\operatorname{Ker} f_x$ the **minimal polynomial** of x over K. It is irreducible. The subextension $\operatorname{Im} f_x$ of F/K is denoted by $K(x)$, and called the field **generated by** x over K. A finite extension F/K is called a **simple extension** if $F = K(x)$ for some $x \in F$. In this case $F \cong K_P$ for $P = P_x$.

Exercise 4.6. (i) If $x \in F$ is a root of an irreducible $P \in K[X]$, then P is a constant multiple of P_x. (ii) The minimal polynomial P_x has the minimal degree among the polynomials in $K[X]$ which has x as a root. If $F = K(x)$, then $[F : K] = \deg P_x$.

Definition 4.7. If $x_1, \dots, x_n \in F$ are algebraic, we inductively define the subextensions $K(x_1, \dots, x_n)$ of F/K **generated by** $x_1, \dots, x_n$ as follows:

$$K_0 = K, \ K_{i+1} := K_i(x_{i+1}) \ (0 \leq i \leq n-1), \quad K(x_1, \dots, x_n) := K_n.$$

The field $K(x_1, \dots, x_n)$ is the intersection of all subextensions of F/K that contains $x_1, \dots, x_n$, thus is independent of the ordering of $x_1, \dots, x_n$.

Proposition 4.8. *For a finite extension F/K, $\exists x_1, \dots, x_n \in F$, $F = K(x_1, \dots, x_n)$.*

Proof. Use the tower law, or take a basis $\{e_i\}$ of F over K and let $x_i = e_i$. □

Lecture 5. Galois groups (M. 18/10/10)

Think Categorically

Back to the extension $K_P := K[X]/(P)$ for an irreducible $P \in K[X]$. We think of this object as an object incarnating the spirit of "a root of P" — it is an object which has a specified, *universal*, root $\overline{X}$ of P, which has no qualification, no property, no distinction, other than that it is a root of P. Thus whenever there is a field extension F/K which contains some roots of P, we can map this universal root $\overline{X} \in K_P$ to your favourite root of P in F, and that gives you a K-homomorphism from K_P to F.

Another funny way of looking at this situation — think of P as a machine, a black box, whose inputs are extension fields F of K, and the output is a finite set $\mathrm{Root}_P(F)$ of all roots of P in F (this is a set with cardinality bounded by $\deg P$). Even if we don't know much about the internal structures of each fields F, we try to understand them via this machine (a *functor*) which spits out a finite set every time you throw in a field. Then this machine has an avatar K_P in the following sense — we can consider these outputs (finite sets) as the finite sets $\mathrm{Hom}_K(K_P, F)$, i.e. we find out that this black box was simply detecting the relation between F and the fixed object K_P (the functor Root_P is *represented* by K_P).

Think Symmetrically

Symmetry is the key. The key to understand Galois theory, to understand all of modern mathematics, to understand just about everything. Whenever you see a mathematical object defined, be critical, be suspicious — *Is this definition canonical? Isn't there a hidden choice we made, a breaking of symmetry, in the way we define it?* After all, we can't define any concrete example without labeling the elements (a fundamental limitation of human brains?). But don't worry — as long as you keep track of the *automorphism group* of the object in question, you can recover the symmetry. When we first see an n-dimensional $\mathbb{R}$-vector space, it comes as $\mathbb{R}^n$, with a standard basis. Later we learn that vector spaces exist even if we don't specify a basis. The freedom we have for the choice of bases is measured by its automorphism group $GL_n(\mathbb{R})$. Same for the roots of an irreducible polynomial; we know that we cannot distinguish 4 different roots of $X^4 + X^3 + X^2 + X + 1 = 0$ (the *primitive 5-th roots of unity*), but to fix our idea we need to choose one and call it ζ. Then we argue that all the other roots are expressed as ζ^2, ζ^3 and ζ^4. But keeping the symmetry (that we tentatively broke) in mind, check that we could change our mind any time and re-declare ζ^2 to be ζ. then now ζ^4 is ζ^2, now ζ is ζ^3 and ζ^3 is ζ^4. Keeping track of the *automorphism group* $\mathrm{Aut}_K(F)$, i.e. the group of K-isomorphisms from F to F, is to keep track of the possible permutation we can have on the set of roots of a fixed P. Then we find that between the roots like ζ and the symmetric polynomials like $\zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1 \in \mathbb{Q}$, there are *partially* symmetric expressions like $\zeta + \zeta^4$ and $\zeta^2 + \zeta^3$, which are symmetric under the subgroup of order 2, and which turn out to be $(-1 \pm \sqrt{5})/2$. This is how this quartic is solved via iterated square roots.

MATH

Let F/K be an extension. We fix an irreducible $P \in K[X]$, and consider the set $\mathrm{Root}_P(F)$ of all roots of P in F. The next proposition is proven simply by checking that the following two maps are inverse to each other, and recalling Proposition ix.8(ii).

Proposition 5.1. *The following maps are bijections that are inverse to each other:*

$$\mathrm{Root}_P(F) \ni x \longmapsto f_x \in \mathrm{Hom}_K(K_P, F),$$
$$\mathrm{Hom}_K(K_P, F) \ni f \longmapsto f(\overline{X}) \in \mathrm{Root}_P(F).$$

In particular, $|\mathrm{Hom}_K(K_P, F)| = |\mathrm{Root}_P(F)| \leq \deg P = [K_P : K]$.

If F is a simple extension $K(x)$, or equivalently if there exists a K-isomorphism in $\mathrm{Hom}_K(K_{P_x}, F)$, then all elements of $\mathrm{Hom}_K(K_{P_x}, F)$ are K-isomorphisms. Thus we can interprete the permutations of roots as K-automorphisms of a simple extension. In general, the group of K-automorphisms $\mathrm{Aut}_K(F)$ of F acts on the set $\mathrm{Hom}_K(K_P, F)$ as follows:

$$\mathrm{Aut}_K(F) \times \mathrm{Hom}_K(K_P, F) \ni (\sigma, f) \longmapsto \sigma \circ f \in \mathrm{Hom}_K(K_P, F),$$

which can be interpreted as an action on $\mathrm{Root}_P(F)$: as the bijection $f \mapsto f(\overline{X})$ of Proposition 5.1 sends $\sigma \circ f_x$ to $\sigma(x)$ (i.e. $\sigma \circ f_x = f_{\sigma(x)}$), we have:

$$\mathrm{Aut}_K(F) \times \mathrm{Root}_P(F) \ni (\sigma, x) \longmapsto \sigma(x) \in \mathrm{Root}_P(F).$$

Proposition 5.2. *Assume $F \cong K_P$. For any $x \in \mathrm{Root}_F(P)$, the map*

$$\mathrm{Aut}_K(F) \ni \sigma \longmapsto \sigma(x) \in \mathrm{Root}_P(F)$$

is bijective. In particular, $|\mathrm{Aut}_K(F)| \leq [F : K]$.

Proof. As $[F : K] = [K_P : K]$, the map $f_x \in \mathrm{Hom}_K(K_P, F)$ is a K-isomorphism by Lemma 3.4, therefore induces a bijection:

$$\mathrm{Aut}_K(F) = \mathrm{Hom}_K(F, F) \ni \sigma \longmapsto \sigma \circ f_x \in \mathrm{Hom}_K(K_P, F)$$

(use Lemma 3.4 for the first equality), which, composed with the bijection $f \mapsto f(\overline{X})$ of Proposition 5.1, gives the desired bijection. The latter part follows from Proposition ix.8(ii), as $|\mathrm{Root}_F(P)| \leq \deg P = [F : K]$. □

Definition 5.3. A simple extension F/K is called a **Galois extension** if it satisfies $|\mathrm{Aut}_K(F)| = [F : K]$. In this case we call $\mathrm{Aut}_K(F)$ the **Galois group** of F/K, and denote it by $\mathrm{Gal}(F/K)$. By definition, $|\mathrm{Gal}(F/K)| = [F : K]$.

Let $F = K(x) \cong K_P$ with $P = P_x$. Then F/K is Galois if and only if $|\mathrm{Root}_P(F)| = [F : K] = \deg P$, i.e. P *has* $\deg P$ *distinct roots in* $F = K(x)$ by Proposition 5.2. This means that P has no multiple roots, and all the roots of P (called **conjugates** of x over K) are written as some polynomial of x with coefficients in K.

Exercise 5.4. (i) Quadratic extensions (extensions of degree 2) of $\mathbb{Q}$ are Galois.
(ii) $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[X]/(X^3 - 2)$ is not a Galois extension of $\mathbb{Q}$.

Lecture 6. Galois theory I: simple extensions (W. 20/10/10)

Idea

Recall what we proved in Lecture 5 for the *Galois* extensions, i.e. simple extensions $F = K(x)$ such that F contains all the $[F : K]$ distinct roots of the minimal polynomial $P = P_x$ of x over K. That is to say, all the roots of P are distinct, and they are all K-polynomials of the chosen root x (think of the examples we saw in Lecture 1 or Lecture 4). But then, they are all K-polynomials of *any* chosen root of P by symmetry, because we cannot distinguish the roots of an irreducible polynomial from the point of view of the base field K. We expressed this symmetry in the following language. For such extension F/K, its *Galois group* $\mathrm{Gal}(F/K)$ is the group of automorphism of F over K as an extension field, that is the set of all K-homomorphisms $\sigma : F \to F$, being a group under composition. But such a K-homomorphism σ are determined if we specify the image $\sigma(x)$ of the generator x, which has to be *another* root of P. All the other roots of P, being K-polynomials in x, are sent to K-polynomials in $\sigma(x)$, but these also have to be roots of P, and we see that σ *permutes* the set of all roots of P. Therefore we can see $\mathrm{Gal}(F/K)$ as a subgroup of the group of all permutations of the set $\mathrm{Root}_P(F)$, or the symmetric group S_n of n letters, if $n := [F : K]$. But it is a rather small subgroup of S_n, since it has only n elements out of $n!$.

Now we present, at this early stage, the main theorem of the Galois theory, namely the one-to-one correspondence between the subfields and the subgroups of the Galois group. As we briefly saw in Lecture 5, the way $X^4 + X^3 + X^2 + X + 1 = 0$ was "solved" (in terms of square roots) was to observe that between $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$ (where ζ is a root of this quartic, a primitive 5th root of unity), there are *partially symmetric* polynomials $\zeta + \zeta^4,\ \zeta^2 + \zeta^3$, that turn out to be roots of a quadratic equation $X^2 + X - 1 = 0$ over $\mathbb{Q}$, hence belong to $\mathbb{Q}(\sqrt{5})$. This is due to the fact that in the Galois group $\{\mathrm{id},\ \zeta \mapsto \zeta^2,\ \zeta \mapsto \zeta^3,\ \zeta \mapsto \zeta^4\} \cong \mathbb{Z}/4\mathbb{Z}$, there is a proper subgroup $\{\mathrm{id},\ \zeta \mapsto \zeta^4\} \cong \mathbb{Z}/2\mathbb{Z}$, by which the quotient of $\mathbb{Z}/4\mathbb{Z}$ is again $\mathbb{Z}/2\mathbb{Z}$. Thus, if we think of "solving" equations as climbing from K to F, then it is important to find out these partially symmetric polynomials of the roots, corresponding to the subgroups of $\mathrm{Gal}(F/K)$. This is why this correspondence is called the *fundamental theorem* of Galois theory. The theorem implies that $F = \mathbb{Q}(\sqrt{5})$ is the only quadratic subfield of $\mathbb{Q}(\zeta)$, whereas $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, also being a field of degree 4, has 3 quadratic subfields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$ — the different Galois groups $\mathrm{Gal}(F/K)$ account for different subfield structures.

Math

Proposition 6.1. *Let L be an intermediate field of a Galois extension F/K. Then F/L is also a Galois extension, and $\mathrm{Gal}(F/L)$ is a subgroup of $\mathrm{Gal}(F/K)$.*

Proof. If $F = K(x)$, then $F = L(x)$. Let the minimal polynomials of x over K, L be respectively P, Q. Then $Q \mid P$, and as F/K is Galois P has $\deg P$ distinct roots in F, therefore Q has $\deg Q$ distinct roots in F and F/L is Galois. The latter part is clear because every L-homomorphism of F is also a K-automorphism. □

Theorem 6.2. (The fundamental theorem of Galois theory) *For a Galois extension F/K, let A be the set of all intermediate fields of F/K, and B be the set of all subgroups of $G = \mathrm{Gal}(F/K)$. Then the map $A \ni L \longmapsto \mathrm{Aut}_L(F) \in B$ is bijective. More precisely, the following are inverse to each other (note $\Phi(L) = \mathrm{Gal}(F/L)$):*

$$\Phi : A \ni L \longmapsto \Phi(L) = \{\sigma \in G \mid \forall x \in L \ \ \sigma(x) = x\} \in B,$$
$$\Psi : B \ni H \longmapsto \Psi(H) = \{x \in F \mid \forall \sigma \in H \ \ \sigma(x) = x\} \in A.$$

(We also denote $\Psi(H)$ by F^H, the **fixed field** *of H.)*

Proof. We immediately have $L \subset \Psi(\Phi(L))$, $H \subset \Phi(\Psi(H))$, so in order to show $L = \Psi(\Phi(L))$, $H = \Phi(\Psi(H))$, it is enough to compare the degrees and cardinalities:

$$[F : \Psi(\Phi(L))] = [F : L], \quad |\Phi(\Psi(H))| = |H|.$$

(the first equality and Proposition 2.4 gives $[\Psi(\Phi(L)) : L] = 1$, and use Example 2.3.) These two equalities follow from the following lemma. □

Lemma 6.3. $|\Phi(L)| = [F : L]$, $|H| = [F : \Psi(H)]$.

Proof. The first equality $|\Phi(L)| = |\mathrm{Gal}(F/L)| = [F : L]$ is Proposition 6.1. To show the second, by $H \subset \Phi(\Psi(H))$ we have $|H| \leq |\Phi(\Psi(H))| = [F : \Psi(H)]$, therefore it is enough to show the inverse inequality. Let $F = K(x)$, and consider a polynomial:

$$P(X) = \prod_{\sigma \in H} (X - \sigma(x)) \in F[X].$$

Then all the coefficients of P are symmetric polynomials of the set $\{\sigma(x) \mid \sigma \in H\}$, therefore invariant under the action of elements of H, i.e. belong to $\Psi(H)$. Therefore $P \in \Psi(H)[X]$, hence the minimal polynomial Q_x of x over $\Psi(H)$ divides P, which shows that $[F : \Psi(H)] = \deg Q_x \leq \deg P = |H|$. □

Idea of Proof

Note that for a subfield L of F/K, it is the extension F/L that corresponds to a subgroup of $\mathrm{Gal}(F/K)$, and the extension L/K is not even Galois in general. Therefore, the Galois correspondence between the fields and the groups is *inclusion-reversing*. Now there aren't many ways of proving a bijective correspondence. Usually you define the maps in both ways and show that they are inverse to each other. In our case we have a very nice symmetrical definitions of maps Φ and Ψ: we take the Galois group $\mathrm{Gal}(F/L)$ for a subfield L, and we take the *fixed field* (sometimes denoted by F^H) of a subgroup H. We need to show $L = \Psi(\Phi(L))$ and $H = \Phi(\Psi(H))$ and one inclusion is clear in both equalities; so it suffices to prove the other inclusion. For this we appeal to the counting argument, as we know that what we are dealing with is essentially *finite* objects. To show the equalities it suffices to show the equalities of finite invariants, *degree* and *cardinality*. To show that Φ and Ψ converts these natural numbers into each other, the only non-trivial inequality is $|H| \geq [F : \Psi(H)]$, i.e. showing that the fixed field $\Psi(H)$ is *large*. So we produce enough elements of $\Psi(H)$ by taking the primitive symmetric polynomials of the set $\{\sigma(x) \mid \sigma \in H\} \subset \mathrm{Root}_P(F)$, where x is the generator of F. This was exactly what we did for $X^4 + X^3 + X^2 + X + 1$.

Part 2. Examples (1)

Lecture 7. Splitting fields (F. 22/10/10)

Idea

Before building up the general theory we will digress into a more concrete construction of extension fields. This is not only to provide enough examples for illustrating the theory (and examining) but is essential for understanding most of the applications.

The construction we have in mind is called the *splitting field* of a polynomial $P \in K[X]$. In Lecture 1 we introduced the field obtained by adjoining a root of P when P is irreducible, but now (for general P) we will adjoin *all* roots of P so that it *splits* completely into linear factors, and we show that there is a unique minimal extension which realizes this splitting. The construction is easy: we adjoin each of the roots of P, one by one, i.e. when we have a root α of P, factorize $P = (X - \alpha)Q$, then adjoin a root of Q, and iterate this procedure. This is a tower of finite simple extensions, so we arrive at a finite extension.

More generally, by iterating simple extensions we arrive at arbitrary finite extensions, because once we adjoin all of the basis elements we get the whole extension. If we have a large ambient extension like $\mathbb{C}/\mathbb{Q}$, then we can adjoin any set of algebraic elements to specify a finite subextension, like $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}), \mathbb{Q}(\sqrt[4]{2}, i)$, etc. But when iterating a simple extension like $K_P := K[X]/(P)$ and then considering K-homomorphism between each other, it is essential to generalize the notion of extension fields a little bit; actually making it more natural, i.e. the notion of "K-algebras that are fields". When we have two *isomorphic* extensions K', K'' of K and then an extension L/K'', then we may want to compare the extension fields of K' and those of K'', and it is convenient to treat L as an extension of K' via K-isomorphism $\tau : K' \to K''$. This will be very useful later, when we consider the separability of arbitrary finite extensions.

Math

We slightly extend the definition of extension fields.

Definition 7.1. Let K be a field. An **extension** F_τ/K is defined as a pair (F, τ) of a field F and a ring homomorphism $\tau : K \to F$. A **K-homomorphism** from F_τ to $F'_{\tau'}$ is a ring homomorphism $\varphi : F \to F'$ such that $\tau' = \varphi \circ \tau$. By a **subextension** L_τ/K of F_τ/K, we mean an intermediate field L of $F/\tau(K)$ and $\tau : K \to L$.

As τ is always an injection $F/\tau(K)$ is an extension in the previous sense. Also F is a K-vector space by the action via τ, and all the statements we have seen continue to hold. We sometimes suppress the notation τ when there is no danger of confusion.

We extend τ to $K[X] \ni P \mapsto \tau P \in F[X]$, and write $\mathrm{Root}_P(F_\tau) := \mathrm{Root}_{\tau P}(F)$ (see Exercise ix.7(i),(ii)). If $x \in \mathrm{Root}_P(F_\tau)$, then the map $f_x : K[X] \ni X \mapsto x \in F$ defines a K-homomorphism $f_x : K_P \ni \overline{X} \mapsto x \in F_\tau$. We restate Proposition 5.1:

Proposition 7.2. *The following maps are bijections that are inverse to each other:*

$$\mathrm{Root}_P(F_\tau) \ni x \longmapsto f_x \in \mathrm{Hom}_K(K_P, F_\tau),$$
$$\mathrm{Hom}_K(K_P, F_\tau) \ni f \longmapsto f(\overline{X}) \in \mathrm{Root}_P(F_\tau).$$

In particular, $|\mathrm{Hom}_K(K_P, F_\tau)| \leq \deg P = [K_P : K]$.

We say $P \in K[X] \setminus K$ **splits** in an extension $F = F_\tau/K$ if τP is a product of linear factors in $F[X]$. If $Q \mid P$ in $K[X]$ and P splits in F then Q splits in F. If P splits in F and $\mathrm{Hom}_K(F, F') \neq \emptyset$ for another extension F'/K, then P splits in F' as well.

Definition 7.3. Let $P \in K[X] \setminus K$ and F/K an extension. If P splits in an extension F'/K if and only if $\mathrm{Hom}_K(F, F') \neq \emptyset$, then we call F a **splitting field** of P over K.

Proposition 7.4. *For every $P \in K[X] \setminus K$, its splitting field over K exists and is unique up to K-isomorphisms. It is a finite extension of K.*

Proof. Any extension isomorphic to a splitting field is also a splitting field, as it is defined in terms of Hom sets. We prove the existence by induction on $\deg P$. Let Q be an irreducible factor of P, and let $\alpha \in K_Q$ its root. Then we have $P = (X - \alpha)R$ in $K_Q[X]$, and let F be a splitting field of R over K_Q (by induction hypothesis). Then F/K is finite by Proposition 2.4. If P splits in F', then there exists $\tau \in \mathrm{Hom}_K(K_Q, F')$ by Proposition 7.2 because $\mathrm{Root}_Q(F') \neq \emptyset$, and $\mathrm{Hom}_{K_Q}(F, F'_\tau) \neq \emptyset$ as R splits in F'. As $\mathrm{Hom}_{K_Q}(F, F'_\tau) \subset \mathrm{Hom}_K(F, F')$, we have $\mathrm{Hom}_K(F, F') \neq \emptyset$. If F'' is another splitting field of P over K, then $F \cong F''$ by Exercise 3.5. □

Proposition 7.5. *Suppose P splits in an extension F/K and $\mathrm{Root}_P(F) = \{x_1, \ldots, x_n\}$. Then $K(x_1, \ldots, x_n)/K$ is a splitting field of P, and it is the only subextension of F/K which is a splitting field of P.*

Proof. Note that P splits in $F' := K(x_1, \ldots, x_n)$. If F_0 is a splitting field of P, then take $\tau \in \mathrm{Hom}_K(F_0, F')$. As τ maps $\mathrm{Root}_P(F_0)$ onto $\mathrm{Root}_P(F') = \{x_1, \ldots, x_n\}$, it is surjective, thus $F_0 \cong F'$. If F_0 is moreover a subextension of F/K, then $\mathrm{Root}_P(F_0) = \mathrm{Root}_P(F) = \{x_1, \ldots, x_n\}$, thus $F' \subset F_0$ and $F' = F_0$. □

What we did

Let us construct a splitting field of $P(X) = X^3 - 2$ over $\mathbb{Q}$, inside $\mathbb{C}$ to be concrete. First we adjoin one root and get a cubic field $K = \mathbb{Q}(\sqrt[3]{2})$. This is isomorphic to $\mathbb{Q}_P = \mathbb{Q}[X]/(X^3 - 2)$. But K does not contain the other roots of P, namely $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$, as if you have only one edge of a regular triangle. So in $K[X]$ we get the factorization $P(X) = (X - \sqrt[3]{2})Q(X)$, where $Q(X) = X^2 + \sqrt[3]{2}X + \sqrt[3]{2}^2$. Now we adjoin a root of Q to K to get $F = K(\sqrt[3]{2}\omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega) = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$, in which P *splits*: $P(X) = (X - \sqrt[3]{2})(X - \sqrt[3]{2}\omega)(X - \sqrt[3]{2}\omega^2)$ in $F[X]$. The extension F/K was quadratic, hence we got an extension $F/\mathbb{Q}$ of degree 6. Proposition 7.4 says that this $F/\mathbb{Q}$ is uniquely determined by P — in this case there isn't much choice in the order of adjoining the roots, but if P has degree 100 you might get various factorizations in various order, but you will arrive at an isomorphic extension F/K.

Lecture 8. Algebraic closure (M. 25/10/10)

As far as you can get

Let us stick to the example $P(X) = X^3 - 2$, $K = \mathbb{Q}(\sqrt[3]{2})$ and $F = \mathbb{Q}(\sqrt[3]{2}, \omega)$. What is important is that $F/\mathbb{Q}$ is more symmetric than $K/\mathbb{Q}$; in fact it is *Galois*, i.e. there is an element $x \in F$, whose minimal polynomial P_x over $\mathbb{Q}$ has degree 6 and $F = \mathbb{Q}(x)$, and F contains all the conjugates of x. In fact, in Lecture 15 we will see that when P has no multiple roots its splitting field is *always* Galois. For this $F/\mathbb{Q}$, here is one way to look at this fact. Write $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ as α, β, γ to emphasize the symmetry — as P is irreducible in $\mathbb{Q}[X]$, we can in no way distinguish these three roots, they all have equal rights. The extension $K/\mathbb{Q}$ is not symmetric enough as it has only one root, and that is reflected in the fact that $\mathbb{Q}_P$ is realized as a subfield of $\mathbb{C}$ in three different ways: $K = \mathbb{Q}(\alpha), \mathbb{Q}(\beta)$ and $\mathbb{Q}(\gamma)$, which are different as subsets of $\mathbb{C}$, even though they are $\mathbb{Q}$-isomorphic. Now $F/\mathbb{Q}$ will have 6 different $\mathbb{Q}$-homomorphism into $\mathbb{C}$, but these 6 maps all have the same *image*, giving only *one subfield* of $\mathbb{C}$. Why? Recall that $F = \mathbb{Q}(\alpha, \beta, \gamma)$, so an element of $\mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{C})$ is determined by specifying the images of α, β, γ, but the images all have to be in $\mathrm{Root}_P(\mathbb{C}) = \{\alpha, \beta, \gamma\}$, therefore you are only permuting these three roots. (We will see that for *every* irreducible polynomial in $\mathbb{Q}[X]$ that has a root in F, all the other roots are in F as well, or else the roots will be intrinsically grouped into the ones that are obtained using P and the ones that are not; but such distinction cannot be made as the roots of an irreducible equation have "equal rights".) In this example $K \cong \mathbb{Q}_P$ does not know much about the equation P, other than that it has "a root"; but the extension $F/\mathbb{Q}$ *solves* the equation P in the sense that all the algebraic relations between the roots are written inside F, and any extension can only contain at most one subextension isomorphic to F, i.e. there is no other way to solve P. To make the *solving* more explicit, the internal structure of F is elucidated in terms of the Galois group, using the fundamental theorem.

In this lecture we digress and ask ourselves: could we keep on solving more and more equations over a field K until we solve them *all*? More precisely, if $P_1, P_2, \dots$ is the sequence of all irreducible polynomials in $K[X]$, make a splitting field F_1 of P_1, then F_2 of P_1P_2, and then F_3 of $P_1P_2P_3$, etc. to get a tower $F_1 \subset F_2 \subset F_3 \subset \cdots$ of extensions of K, whose union results in an infinite algebraic extension of K, in which all polynomials split? Well the answer is yes, except that if we want a statement over *general* fields, not just $\mathbb{Q}, \mathbb{F}_p$ or some explicitly given field, then there is a set-theoretic complication. When there are uncountably many irreducible polynomials in K, the above sequence of finite products does not seem to exhaust all of them; if we want to get around this, we might say we construct inductively a splitting field F_n of P_n over F_{n-1}, except that this will be a *transfinite induction*; it assumes that the index set of the polynomials is *well-ordered* so that the induction can be done; actually we need an additional axiom, the *axiom of choice*, to endorse this procedure. Here we use a statement that is equivalent to the axiom of choice, called *Zorn's lemma*. As this axiom is known to be independent from the standard axioms in set theory, purists may want to avoid using it; in fact over specific fields you can usually avoid it after making some effort. But for general theory's sake most mathematicians accept it.

MATH

Definition 8.1. A field F is called an **algebraically closed field** if every irreducible element of $F[X]$ is linear. Equivalently, it is a field whose algebraic extensions are all isomorphic to itself. An algebraic extension F/K is called an **algebraic closure** of K if F is algebraically closed.

Theorem 8.2. (Steinitz' theorem) *For any field K, its algebraic closure $\overline{K}$ exists uniquely up to K-isomorphism, and $\mathrm{Hom}_K(F, \overline{K}) \neq \emptyset$ for any algebraic extension F/K.*

Proof. Consider the set Λ of all pairs $\lambda = (P, i)$ where $P \in K[X]$ is an irreducible monic and $1 \leq i \leq \deg P$. Consider a variable $X_\lambda = X_{P,i}$ for each $\lambda \in \Lambda$, and the polynomial ring $A := K[X_\lambda \mid \lambda \in \Lambda]$ in all these variables (but note that each of its elements (polynomials) can contain only finitely many variables). For each irreducible monic $P \in K[X]$, consider the polynomial $P'(X) := P(X) - \prod_{i=1}^{\deg P}(X - X_{P,i}) \in A[X]$, and let $x_{P,i} \in A$ be the coefficient of X^i in $P'(X)$ for $0 \leq i < \deg P$.

Let I be the ideal of A generated by all $x_{P,i} \in A$ for all P. We first show $I \neq A$. Assume $I = A$, or $1 \in I$. Then:

$$\exists a_1, \ldots, a_n \in A, \quad \sum_{j=1}^{n} a_j x_{P_j, i_j} = 1 \in A.$$

Now let F be a splitting field of $P_1 \cdots P_n$. Then each P_j splits as $P_j(X) = \prod_{i=1}^{\deg P_j}(X - \alpha_{ji})$ in $F[X]$, with $\alpha_{ji} \in F$. Consider the "substitution" map $f : A \to F$ defined by $f(X_{P_j,i}) = \alpha_{ji}$ for $1 \leq j \leq n$ and $1 \leq i \leq \deg P_j$, and $f(X_\lambda) = 0$ for all the other X_λ. Then under this ring homomorphism f, the polynomial $P_j'[X] \in A[X]$ is sent to $P_j(X) - \prod_{i=1}^{\deg P_j}(X - \alpha_{ji}) = 0 \in F[X]$, thus we see that $f(x_{P_j,i}) = 0 \in F$ for all $1 \leq i \leq \deg P_j$. Therefore $1 = f(1) = f(\sum_j a_j x_{P_j,i_j}) = 0$ in F, a contradiction.

Hence take a maximal ideal Q of A containing I by Proposition xii.6 and consider the field $\overline{K} := A/Q$, which is an extension field of K. Let $\alpha_\lambda := X_\lambda \bmod Q \in \overline{K}$. Then every irreducible monic $P \in K[X]$ splits as $P(X) = \prod_i (X - \alpha_{P,i})$ in $\overline{K}[X]$. In particular α_λ is algebraic over K, and $\overline{K}/K$ is algebraic, as every element of $\overline{K}$ is a polynomial in α_λ. If $L/\overline{K}$ is algebraic, for every $x \in L$ its minimal polynomial lies in $K(\alpha_{\lambda_1}, \ldots, \alpha_{\lambda_m})$ for some $\lambda_1, \ldots, \lambda_m$, thus x is algebraic over K. As the minimal polynomial of x over K splits in $\overline{K}$, we have $x \in \overline{K}$, hence $L = \overline{K}$. Thus $\overline{K}$ is algebraically closed.

Now let F/K be algebraic, and let X be the set of all pairs (L, τ) where L is a subextension of F/K and $\tau \in \mathrm{Hom}_K(L, \overline{K})$. It is an ordered set if we define $(L_1, \tau_1) \leq (L_2, \tau_2) \iff L_1 \subset L_2,\ \tau_2|_{L_1} = \tau_1$. For any totally ordered subset Y of X, the element (L_Y, τ_Y), defined by $L_Y := \bigcup_{(L,\tau)\in Y} L$ and $\tau_Y|_L = \tau$ for $(L, \tau) \in Y$, is an upper bound of Y, hence X is inductive. Thus we can take a maximal element (M, ρ) of X by the Zorn's lemma (Theorem xii.5). For all $x \in F$, we have $\mathrm{Hom}_M(M(x), \overline{K}) \neq \emptyset$ by Proposition 7.2, as $\overline{K}$ is algebraically closed and the minimal polynomial of x over M splits in $\overline{K}$, therefore the maximality of (M, ρ) implies $M(x) = M$. Thus $M = F$, and $\mathrm{Hom}_K(F, \overline{K}) \neq \emptyset$. If F is an algebraic closure of K, then $\tau \in \mathrm{Hom}_K(F, \overline{K})$ makes $\overline{K}$ into an algebraic extension $\overline{K}_\tau/F$ (as $\overline{K}/K$ is algebraic), thus τ is an isomorphism. $\square$

Lecture 9. Cyclotomic extensions I: the group $\boldsymbol{\mu}_n$ (W. 27/10/10)

Background

In the next four lectures we deal with the *cyclotomic extensions*. It's not just that (1) they are the most beautiful examples of Galois extensions, but also (2) they are fairly general (for finite fields they cover all finite extensions, over rationals $\mathbb{Q}$ they cover all abelian extensions), (3) looking into their Galois groups is quite instructive, so you learn a lot by playing around with them, and (4) it is a basis of the technique of finding the Galois groups of polynomials over $\mathbb{Q}$ (well, a standard exam material).

Cyclotomic extensions are the finite extensions obtained by adjoining the *roots of unity*, i.e. the roots of $X^n - 1$, to a field. The fact that the set $\boldsymbol{\mu}_n$ of all roots of $X^n - 1$ forms a *group* under multiplication gives an additional structure to the equation, and gives a transparent view of how all the roots are related to each other. In fact the situation is as simple as it could be: the group $\boldsymbol{\mu}_n$ turns out to be cyclic, so all the roots are powers of one of the roots (a *primitive n-th root of unity*), and hence the cyclotomic extensions are simple. Moreover it turns out to be *Galois* when $X^n - 1$ actually has n distinct root, which is the case as long as the characteristic of the base field does not divide n (we show this in the next lecture).

Math

Definition 9.1. For a field K and an integer $n \geq 1$, a splitting field of $X^n - 1$ is denoted by $K(\boldsymbol{\mu}_n)$, and is called a **cyclotomic extension** of K. We denote the set of all roots of $X^n - 1$ (n**-th roots of unity**) in $K(\boldsymbol{\mu}_n)$ by $\boldsymbol{\mu}_n$.

By Proposition ix.8(ii), we have $|\boldsymbol{\mu}_n| \leq n$, and clearly $\boldsymbol{\mu}_n$ is a group under multiplication, i.e. it is a finite subgroup of $K(\boldsymbol{\mu}_n)^\times$ (the multiplicative group of $K(\boldsymbol{\mu}_n)$).

Definition 9.2. Let G be a **finite group**, i.e. a group of finite cardinality. For every $a \in G$, as there are identical elements among $1, a, a^2, \ldots$, there is a minimal $n \in \mathbb{N}$ with the property $a^n = 1$. This n is called the **order** of a.

Exercise 9.3. If the order of $a \in G$ is n, then $a^k = 1 \iff n \mid k$. Deduce $n \mid |G|$.

Definition 9.4. For an element a of a finite group G, the subset $\langle a \rangle = \{a^i \mid i \in \mathbb{N}\}$ of G is a subgroup of G, and is called the subgroup of G **generated by** a. When $G = \langle a \rangle$ for some $a \in G$, we call G a **cyclic group**, and a is called a **generator** of G. The order of a generator is equal to $|G|$. A cyclic group consisting of n elements (cyclic group of **order** n) is isomorphic to the addtive group of $\mathbb{Z}/(n)$ (often denoted by $\mathbb{Z}/n\mathbb{Z}$) by sending a generator to 1 mod n.

Exercise 9.5.
(i) The number of generators of a cyclic group of order n is $\varphi(n) = |\{1 \leq k \leq n-1 \mid (k, n) = 1\}|$ (**Euler's function**).
(ii) A cyclic group of order n has a unique subgroup of order d for each positive divisor d of n, and there are no other subgroups.

Proposition 9.6. *For a field K, every finite subgroup G of $K^\times$ is cyclic.*

Remark 9.7. Note that every element of a finite subgroup of $K^\times$ is a root of unity.

Proof. Take an element $x \in G$ which has the maximal order, and call its order n. We show that the order of any $y \in G$ is a divisor of n. If the order m of y does not divide n, there is a prime number p and its power p^j divides m but not n. So let $m = p^j m',\ n = p^k n',\ j > k,\ (p, m') = (p, n') = 1$. Then the order of $x^{p^k} y^{m'}$ is, by:

$$(x^{p^k} y^{m'})^i = 1 \Longrightarrow x^{p^k i} = y^{-im'}$$
$$\Longrightarrow \begin{cases} x^{p^j p^k i} = y^{-im} = 1 \Rightarrow n \mid p^{j+k} i \Rightarrow n' \mid i \\ 1 = x^{ni} = y^{-im'n'} \Rightarrow m \mid im'n' \Rightarrow p^j \mid i \end{cases} \Longrightarrow p^j n' \mid i,$$

equal to $p^j n'$, which contradicts the maximality of n. Therefore $m \mid n$, but now $x^{in/m}$ $(1 \le i \le m)$ gives m distinct roots of $X^m - 1$ in K, but by Proposition ix.8(ii), these are all the roots of $X^m - 1$ in K. Therefore $y = x^{in/m}$ for some i, and as y was arbitrary, x is a generator of G. □

Corollary 9.8. *The group $\boldsymbol{\mu}_n$ is cyclic, as it is a finite subgroup of $K(\boldsymbol{\mu}_n)^\times$.*

Lecture 10. Cyclotomic extensions II: the Galois group (F. 29/10/10)

Consider a field K and its cyclotomic extension $K(\boldsymbol{\mu}_n)$.

Proposition 10.1. *If* $(\operatorname{char} K, n) = 1$*, then* $|\boldsymbol{\mu}_n| = n$*, i.e.* $\boldsymbol{\mu}_n$ *is cyclic of order* n*.*

Proof. It suffices to show that $X^n - 1$ does not have a multiple root in $K(\boldsymbol{\mu}_n)$, but this follows readily from Exercise 10.3(ii) below, as it does not have common roots with its derivative nX^{n-1}, whose only root is 0 by $(\operatorname{char} K, n) = 1$. □

Definition 10.2. The K-linear map $D : K[X] \to K[X]$ characterized by the following is called the **derivation** of $K[X]$: (i) $D(1) = 0$, (ii) $D(X^n) = nX^{n-1}$ $(n \in \mathbb{Z}_{>0})$.

Exercise 10.3. (i) For $P, Q \in K[X]$, $D(PQ) = D(P)Q + D(Q)P$.
(ii) For $P \in K[X]$, $\alpha \in K$: a multiple root of $P \iff (X - \alpha) \mid P, D(P)$.

Now assume $(\operatorname{char} K, n) = 1$.

Definition 10.4. A generator of the cyclic group $\boldsymbol{\mu}_n$ (an element with order n) is called a **primitive n-th root of unity**. There are $\varphi(n)$ of them, and if we denote one of them by ζ, they are written as ζ^k, $k \in (\mathbb{Z}/(n))^\times$ (Exercise 9.5). This $(\mathbb{Z}/(n))^\times = \{k \bmod n \mid (k, n) = 1\}$ is the group of units of the ring $\mathbb{Z}/(n)$, and $|(\mathbb{Z}/(n))^\times| = \varphi(n)$.

Proposition 10.5. *Let* ζ *be a primitive* n*-th root of unity in* $K(\boldsymbol{\mu}_n)$*, and let* P_ζ *be its minimal polynomial over* K*.*

(i) $K(\boldsymbol{\mu}_n) = K(\zeta)$*, and* $K(\zeta)/K$ *is a Galois extension.*
(ii) *All the roots of* P_ζ *in* $K(\zeta)$ *are primitive* n*-th roots of unity.*

Proof. (i): As $\boldsymbol{\mu}_n = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$, the first part follows. Also, as P_ζ divides $X^n - 1 = \prod_{i=0}^{n-1}(X - \zeta^i)$, it has $\deg P_\zeta$ distinct roots in $K(\zeta)$. (ii): By $P_\zeta \mid X^n - 1$, all roots of P_ζ belong to $\boldsymbol{\mu}_n$. A non-primitive $\alpha \in \boldsymbol{\mu}_n$ of order $d < n$ is a root of $X^d - 1$. As ζ is not a root of $X^d - 1$, the P_ζ does not divide $X^d - 1$, i.e. P_ζ and $X^d - 1$ are relatively prime, and hence α is not a root of P_ζ. □

Definition 10.6. A Galois extension with an abelian Galois group is called an **abelian extension**.

Theorem 10.7. (Galois group of cyclotomic extensions) *There is an injective homomorphism as follows, and in particular* $K(\boldsymbol{\mu}_n)/K$ *is an abelian extension:*

$$\operatorname{Gal}(K(\boldsymbol{\mu}_n)/K) \ni (\zeta \mapsto \zeta^k) \longmapsto k \bmod n \in (\mathbb{Z}/(n))^\times.$$

Proof. By Proposition 5.2, $\operatorname{Gal}(K(\zeta)/K) \ni \sigma \longmapsto \sigma(\zeta) \in \operatorname{Root}_{P_\zeta}(K(\zeta))$ is a bijection, and we know by Proposition 10.5(ii) that $\operatorname{Root}_{P_\zeta}(K(\zeta))$ is contained in $\{\zeta^k \mid k \in (\mathbb{Z}/(n))^\times\}$. This gives an injection which does not depend on the choice of ζ, and as the composite of $\zeta \mapsto \zeta^k$ and $\zeta \mapsto \zeta^l$ is $\zeta \mapsto \zeta^{kl}$, it is a group homomorphism. □

Lecture 11. Example I: Finite fields (M. 1/11/10)

Proposition 11.1. *For a field F of characteristic $p > 0$, the map $\mathrm{Fr}_q : F \ni x \longmapsto x^q \in F$ for $q = p^f$ $(f \geq 1)$ is an injective homomorphism, and if F is a finite field then it is a field automorphism. (We call Fr_q the* q**-th power Frobenius map**.*)*

Proof. Consider $\mathrm{Fr}_p : F \ni x \longmapsto x^p \in F$. Then $(x+y)^p = x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^{p-i}y^i + y^p$, but as p is prime every $\binom{p}{i}$ is divisible by p. Hence $(x+y)^p = x^p + y^p$, and as $(xy)^p = x^p y^p$, this Fr_p is a ring homomorphism. As F is a field it is injective (Lemma 3.3), hence if F is finite it is bijective. The general case follows from $\mathrm{Fr}_q = (\mathrm{Fr}_p)^f$. □

Remark 11.2. When $K = \mathbb{F}_p$, $X^p - 1 = (X-1)^p$ shows that $\boldsymbol{\mu}_p = \{1\}$.

Proposition 11.3. *Let F be a finite field with $|F| = q$. Then F is an extension of $\mathbb{F}_p$ of degree f for some p and f, and $q = p^f$. Also $F^\times = \boldsymbol{\mu}_{q-1}$, i.e. if we take a generator ζ of the cyclic group $F^\times$ (a* **primitive root** *of F) then $F = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{q-2}\}$.*

Proof. As $|F| < \infty$, the prime field of F is $\mathbb{F}_p$ for some p and $[F : \mathbb{F}_p] < \infty$. If $[F : \mathbb{F}_p] = f$ then $|F| = p^f$. The latter part follows from Proposition 9.6. □

Theorem 11.4. *Let p be a prime. For each $f \geq 1$ there is a unique finite field $\mathbb{F}_q = \boldsymbol{\mu}_{q-1} \cup \{0\}$ with $q = p^f$ elements in $\overline{\mathbb{F}}_p$, and these fields exhaust all the finite fields of charactecteristic p.*

Proof. Let $\mathbb{F}_q = \boldsymbol{\mu}_{q-1} \cup \{0\}$ be the set of all roots of $X^q - X$ in $\overline{\mathbb{F}}_p$. As $(p, q-1) = 1$ we have $|\mathbb{F}_q| = q$ by Proposition 10.1. As $\mathbb{F}_q = \{x \in \overline{\mathbb{F}}_p \mid \mathrm{Fr}_q(x) = x\}$ we see that $\mathbb{F}_q$ is a subfield of $\overline{\mathbb{F}}_p$ by Proposition 11.1. By Proposition 11.3, every degree f extension $F/\mathbb{F}_p$ has to be isomorphic to $\mathbb{F}_q$, and is clearly unique as a subfield of $\overline{\mathbb{F}}_p$. □

Exercise 11.5. Show that $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ if and only if $m \mid n$. Draw a diagram of all the intermediate fields of the extension $\mathbb{F}_{4096}/\mathbb{F}_2$ of degree 12 and their inclusions, together with corresponding subgroups of the Galois group $\mathbb{Z}/12\mathbb{Z}$.

By Proposition 11.3, every finite extension of finite fields is cyclotomic.

Theorem 11.6. *Every finite extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of finite fields of degree n is a Galois extension. Its Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a cyclic group of order n with a generator $\mathrm{Fr}_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$:*

$$\varphi_n : \mathbb{Z}/n\mathbb{Z} \ni 1 \bmod n \overset{\cong}{\longmapsto} \mathrm{Fr}_q \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$$

Proof. By Proposition 11.1, we see that $\mathrm{Fr}_q \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$. Taking a primitive root ζ of $\mathbb{F}_{q^n}$ by Proposition 11.3, its images $\zeta^{q^i} = \mathrm{Fr}_q^i(\zeta)$ for $0 \leq i < n$ are all distinct, hence Fr_q has order $n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$. Therefore $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois and Fr_q generates $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. □

Lecture 12. Example II: Cyclotomic fields (W. 3/11/10)

Lemma 12.1. *We can define the polynomial $\Phi_n(X) \in \mathbb{Z}[X]$ for $n \geq 1$ inductively by $X^n - 1 = \prod_{d|n} \Phi_d(X)$, where d runs through all positive divisors of n. Then $\deg \Phi_n = \varphi(n)$, and if $(\operatorname{char} K, n) = 1$, then $\mathrm{Root}_{\Phi_n}(K(\boldsymbol{\mu}_n))$ is the set of all primitive n-th roots of unity. (It is called the n-th cyclotomic polynomial.)*

Proof. Use induction in n. By induction hypothesis, the polynomial $\prod_{d|n, d<n} \Phi_d(X)$ is in $\mathbb{Z}[X]$ and its roots are precisely the n-th roots of unity that are not primitive, we have the claim by (if a polynomial in $\mathbb{Z}[X]$ is divisible in $\mathbb{Q}[X]$ by a monic in $\mathbb{Z}[X]$, its quotient also lies in $\mathbb{Z}[X]$, by the division algorithm). □

Example 12.2. The first few are: $\Phi_2(X) = X + 1,\ \Phi_3(X) = X^2 + X + 1,\ \Phi_4(X) = X^2 + 1,\ \Phi_5(X) = X^4 + X^3 + X^2 + X + 1,\ \Phi_6(X) = X^2 - X + 1, \ldots$.

Proposition 12.3. *Let $(\operatorname{char} K, n) = 1$. If the image of the canonical injection $\mathrm{Gal}(K(\boldsymbol{\mu}_n)/K) \to (\mathbb{Z}/(n))^\times$ in Theorem 10.7 has order m, then all irreducible factors of Φ_n in $K[X]$ have degree m.*

Proof. For any primitive n-th root of unity ζ, its minimal polynomial P_ζ over K is irreducible, divides $\Phi_n(X)$, and has degree $[K(\zeta) : K] = [K(\boldsymbol{\mu}_n) : K] = |\mathrm{Gal}(K(\boldsymbol{\mu}_n)/K)| = m$. As the roots of Φ_n are all primitive n-the roots of unity, all of its irreducible factors are of this form. □

Exercise 12.4. Let $(p, n) = 1$, and let f be the order of $p \bmod n$ in $(\mathbb{Z}/(n))^\times$. Then all irreducible factors of $\Phi_n(X)$ in $\mathbb{F}_p[X]$ have degree f.

Theorem 12.5. (Irreducibility of cyclotomic polynomials) *The canonical injection $\mathrm{Gal}(K(\boldsymbol{\mu}_n)/K) \to (\mathbb{Z}/(n))^\times$ in Theorem 10.7 is an isomorphism when $K = \mathbb{Q}$. Equivalently, the cyclotomic polynomial $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$.*

Proof. Let P be a (monic) irreducible factor of $\Phi_n(X)$ in $\mathbb{Q}[X]$. It is enough to show that if ζ is a root of P, then ζ^p is also a root of P for all primes p not dividing n, because such primes generate $(\mathbb{Z}/(n))^\times$ and it follows that all primitive n-th roots of unity ζ^a ($a \in (\mathbb{Z}/(n))^\times$) are roots of P. Assume that $\Phi_n = PQ$ and ζ is a root of P but ζ^p is a root of Q. Note that as Φ_n, P, Q are monic and $\Phi_n \in \mathbb{Z}[X]$, it follows that $P, Q \in \mathbb{Z}[X]$ by Gauss' Lemma (Proposition xi.2). Then ζ is a root of $Q(X^p)$, and as P is the minimal polynomial of ζ over $\mathbb{Q}$, we see that $P(X) \mid Q(X^p)$. Reducing modulo p, we see that $P(X) \bmod p$ divides $Q(X^p) \bmod p$ in $\mathbb{F}_p[X]$, but $Q(X^p) \bmod p = (Q(X) \bmod p)^p \in \mathbb{F}_p[X]$ by Proposition 11.1, thus $P(X) \bmod p$ and $Q(X) \bmod p$ are not coprime in $\mathbb{F}_p[X]$, which is false because $\Phi_n(X) \bmod p = (P(X) \bmod p)(Q(X) \bmod p)$ has no multiple roots in $\mathbb{F}_p(\boldsymbol{\mu}_n)$ by Proposition 10.1. □

Remark 12.6. This proof will look smarter if we can "reduce ζ modulo p" to get a primitive n-th root of unity over $\mathbb{F}_p$. For this we need to define the ring of integers $\mathbb{Z}[\zeta]$ of the number field $\mathbb{Q}(\boldsymbol{\mu}_n)$, and reduce ζ modulo the prime ideals of this ring.

Part 3. Galois Theory (2)

Lecture 13. Separable extensions I (F. 5/11/10)

Lemma 13.1. *If $F/K, E/K$ be two extensions and L a subextension of F/K, then:*

$$\mathrm{Hom}_K(F,E) = \coprod_{\tau\in\mathrm{Hom}_K(L,E)} \mathrm{Hom}_L(F,E_\tau).$$

Proof. If $\sigma \in \mathrm{Hom}_K(F,E)$ then $\tau := \sigma|_L \in \mathrm{Hom}_K(L,E)$, and $\sigma \in \mathrm{Hom}_L(F,E_\tau)$. Conversely $\mathrm{Hom}_L(F,E_\tau) \subset \mathrm{Hom}_K(F,E)$ for every $\tau \in \mathrm{Hom}_K(L,E)$. □

Lemma 13.2. *Let $F/L/K$ be finite with $F = L(x)$, and E/K arbitrary. Let P be the minimal polynomial of x over L. Then $|\mathrm{Hom}_K(F,E)| \le |\mathrm{Hom}_K(L,E)| \cdot [F:L]$, and the equality holds if and only if $|\mathrm{Root}_{\tau P}(E)| = \deg P$ for all $\tau \in \mathrm{Hom}_K(L,E)$.*

Proof. Use Lemma 13.1, $\mathrm{Hom}_L(F,E_\tau) \cong \mathrm{Root}_{\tau P}(E)$ (Proposition 7.2) and $\deg P = [F:L]$ (Proposition 2.7). □

Lemma 13.3. *If F/K is finite and E/K is arbitrary, then $|\mathrm{Hom}_K(F,E)| \le [F:K]$, and the following are equivalent:*

(i) $|\mathrm{Hom}_K(F,E)| = [F:K]$.
(ii) *Let $(L_i)_{0\le i\le n}$ be any sequence of subextensions of F/K such that $L_0 = K$, $L_n = F$ and $L_i = L_{i-1}(x_i)$. If Q_i is the minimal polynomial of x_i over L_{i-1}, then $|\mathrm{Root}_{\tau Q_i}(E)| = \deg Q_i$ for all $\tau \in \mathrm{Hom}_K(L_{i-1},E)$.*
(iii) *There exists a sequence (L_i) satisfying (ii).*
(iv) *Let L be a subextension of F/K and $x \in F$. If Q is the minimal polynomial of x over L, then $|\mathrm{Root}_{\tau Q}(E)| = \deg Q$ for all $\tau \in \mathrm{Hom}_K(L,E)$.*
(v) *If L, L' are subextensions of F/K with $L \subset L'$, then $|\mathrm{Hom}_L(L',E_\tau)| = [L':L]$ for all $\tau \in \mathrm{Hom}_K(L,E)$.*

Proof. By Proposition 4.8, writing $F = K(x_1,\dots,x_n)$ and $L_i := K(x_1,\dots,x_i)$ always gives a sequence (L_i) of the form in (ii). Thus iterating Lemma 13.2 and using Proposition 2.4 proves the inequality, (i)⇒(ii) and (iii)⇒(i). (ii)⇒(iii) is clear. (ii)⇒(iv): We can form $(L_i)_{0\le i\le n}$ with $L = L_{i-1}$ and $x = x_i$ for some i. (ii)⇒(v): We can form $(L_i)_{0\le i\le n}$ with $L = L_i$ and $L' = L_j$ for some i, j, then the same argument as (iii)⇒(i). (iv)⇒(ii): Clear. (v)⇒(i): Set $L = K$ and $L' = F$. □

Definition 13.4. (i) A polynomial $P \in K[X]\backslash K$ is called **separable** if $|\mathrm{Root}_P(E)| = \deg P$ for some extension E/K.
(ii) A finite extension F/K is called **separable** if $|\mathrm{Hom}_K(F,E)| = [F:K]$ for some extension E/K.

Proposition 13.5. *If $P \in K[X] \setminus K$ is separable, then $|\mathrm{Root}_P(E)| = \deg P$ whenever P splits in E.*

Proof. If $|\mathrm{Root}_P(E')| = \deg P$ then P splits in E'. If E is a splitting field of P, then an element of $\mathrm{Hom}_K(E,E')$ maps $\mathrm{Root}_P(E)$ onto $\mathrm{Root}_P(E')$, hence $|\mathrm{Root}_P(E)| = \deg P$. For general E'' where P splits, an element of $\mathrm{Hom}_K(E,E'')$ maps $\mathrm{Root}_P(E)$ into $\mathrm{Root}_P(E'')$ and thus $|\mathrm{Root}_P(E'')| = \deg P$. □

Lecture 14. Separable extensions II (M. 8/11/10)

Proposition 14.1. *Let F/K be a finite extension, and denote by P_x the minimal polynomial of $x \in F$ over K. The following are equivalent:*

(i) *P_x is separable (we say x is* **separable** *over K) for every $x \in F$.*
(ii) *If $F = K(x_1, \dots, x_n)$ and all P_{x_i} split in E/K, then $|\mathrm{Hom}_K(F, E)| = [F : K]$.*
(iii) *There exist $x_1, \dots, x_n \in F$ with $F = K(x_1, \dots, x_n)$ and all P_{x_i} separable.*
(iv) *F/K is separable.*

Proof. Write $P_i := P_{x_i}$. (i)⇒(ii): Let $L_i := K(x_1, \dots, x_i)$, and Q_i the minimal polynomial of x_i over L_{i-1}. Then $Q_i \mid P_i$ in $L_{i-1}[X]$, hence $\tau Q_i \mid P_i$ in $E[X]$ for all $\tau \in \mathrm{Hom}_K(L_{i-1}, E)$. (i) and Proposition 13.5 shows $|\mathrm{Root}_{P_i}(E)| = \deg P_i$, hence $|\mathrm{Root}_{\tau Q_i}(E)| = \deg Q_i$. Apply Lemma 13.3(iii)⇒(i). (ii)⇒(iv): Take E to be a splitting field of $P_1 \cdots P_n$. (iv)⇒(i): Lemma 13.3(i)⇒(iv) for $L = K$. (i)⇒(iii): Clear. (iii)⇒(iv): The same argument as (i)⇒(ii) for a splitting field E of $P_1 \cdots P_n$. □

Proposition 14.2. *An irreducible $P \in K[X] \setminus K$ is separable if and only if $D(P) \neq 0$. In particular, if $\mathrm{char}\, K = 0$, all irreducible $P \in K[X]$ are separable, and hence every finite extension of K is separable by Proposition 14.1(i)⇒(iv).*

Proof. If $D(P) = 0$, all roots of P are multiple roots in any field by Exercise 10.3(ii). If $D(P) \neq 0$, as $\deg D(P) < \deg P$ and $D(P) \notin (P)$ in $K[X]$, $(P) + (D(P)) = K[X] \ni 1$ as (P) is a maximal ideal (Proposition ix.8(i), Proposition vii.20(i)). If E is a splitting field of P, as $1 \in (P) + (D(P))$ remains true in $E[X]$, the linear factors of P cannot divide $D(P)$, i.e. there is no multiple root of P in E. □

Exercise 14.3.
(i) If $K = L(T)$ with $\mathrm{char}\, L = p$, then $X^p - T \in K[X]$ is irreducible but not separable, factoring into $(X - \sqrt[p]{T})^p$ in $K(\sqrt[p]{T})$.
(ii) Over a *finite* field, every finite extension is cyclotomic, Galois, hence separable. (If every finite extension of K is separable, we say K is a **perfect field**.)

Theorem 14.4. (The primitive element theorem) *Every separable finite extension F/K is simple.*

Proof. If K is a finite field, F is also finite, therefore $F^\times$ is a cyclic group by Proposition 9.6, hence its generator generates F/K. Assume K is infinite. We have $F = K(x_1, \dots, x_m)$ by Proposition 4.8, but induction on m and Lemma 13.3(i)⇒(v) shows that it suffices to prove when $m = 2$. Let $F = K(x, y)$, $[F : K] = n$, and $\mathrm{Hom}_K(F, E) = \{\sigma_1, \dots, \sigma_n\}$ for an E/K. As any element of $\mathrm{Hom}_K(F, E)$ is determined by the images of x, y, for $i \neq j$ we have $\sigma_i(x) \neq \sigma_j(x)$ or $\sigma_i(y) \neq \sigma_j(y)$. Consider a polynomial:

$$Q(X) = \prod_{i \neq j} \Big(\big(\sigma_i(x) - \sigma_j(x)\big)X + \big(\sigma_i(y) - \sigma_j(y)\big) \Big) \in E[X].$$

As K is infinite, there exists $z \in K$ that is not a root of Q. Putting $w = xz + y \in F$, we have $0 \neq Q(z) = \prod(\sigma_i(w) - \sigma_j(w))$, thus $\sigma_i(w) \neq \sigma_j(w)$ whenever $i \neq j$. Hence $\sigma_1, \dots, \sigma_n$ restricts to n distinct K-homomorphisms of $K(w)$ into E. But Proposition 5.1 shows $n \leq |\mathrm{Hom}_K(K(w), E)| \leq [K(w) : K]$, and $[K(w) : K] \leq [F : K] = n$ because $K(w) \subset F$, so these are all equalities and $F = K(w)$. □

Lecture 15. Galois theory II: completed (W. 10/11/10)

Definition 15.1. A finite extension F/K is **Galois** if $|\mathrm{Aut}_K(F)| = [F : K]$. [Equivalently: (a) $|\mathrm{Hom}_K(F, F)| = [F : K]$ (Lemma 3.4), (b) Definition 5.3 (Theorem 14.4).]

Theorem 15.2. *Let F/K be finite and P_x as in Proposition 14.1.*

(i) *F/K : Galois $\iff$ $|\mathrm{Root}_{P_x}(F)| = \deg P_x$ for all $x \in F$.*
(ii) **(Artin)** *F/K : Galois $\iff$ $K = F^G$ for some subgroup G of $\mathrm{Aut}_K(F)$.*
(iii) *A splitting field E/K of $P \in K[X]$ is Galois if all irreducible factors of P are separable. If F/K is separable, there is a finite E/F such that E/K is Galois.*

Proof. (i): $\Rightarrow$: Lemma 13.3(i)$\Rightarrow$(iv) for $L = K$ and $E = F$. $\Leftarrow$: Proposition 14.1(i)$\Rightarrow$(ii) for $E = F$. (ii): $\Rightarrow$: Theorem 6.2. $\Leftarrow$: For $x \in F$, let $\{x_1, \dots, x_m\} = \{\sigma(x) \mid \sigma \in G\}$ and $Q_x = \prod_{i=1}^m (X - x_i)$. Then $Q_x \in K[X]$ as $F^G = K$, thus $P_x \mid Q_x$. Apply (i). (iii): If $\mathrm{Root}_P(E) = \{x_1, \dots, x_n\}$, then $E = K(x_1, \dots, x_n)$ by Proposition 7.5. As P_{x_i} divide P, they are separable and split in E. Use Proposition 14.1(iii)$\Rightarrow$(ii). If $F = K(x_1, \dots, x_n)$ then P_{x_i} are separable by Proposition 14.1(iv)$\Rightarrow$(i). If E is a splitting field of the product of P_{x_i}, then $\mathrm{Hom}_K(F, E) = [F : K]$ by Proposition 14.1(i)$\Rightarrow$(ii). □

Exercise 15.3. The field E/K as in the proof of (iii) is the "minimal" extension E/K with $\mathrm{Hom}_K(F, E) = [F : K]$, and called the **Galois closure** of F/K.

Now we are ready to generalize the argument of Lecture 5. Assume L/K is finite and F/K is Galois, and consider the action we saw in Lecture 5:

$$\mathrm{Gal}(F/K) \times \mathrm{Hom}_K(L, F) \ni (\sigma, f) \longmapsto \sigma \circ f \in \mathrm{Hom}_K(L, F).$$

The generalization of Proposition 5.2 is as follows:

Proposition 15.4. *Assume $\mathrm{Hom}_K(L, F) \neq \emptyset$. Then for any $f \in \mathrm{Hom}_K(L, F)$, the map $\mathrm{Gal}(F/K) \ni \sigma \longmapsto \sigma \circ f \in \mathrm{Hom}_K(L, F)$ is surjective, and $|\mathrm{Hom}_K(L, F)| = [L : K]$.*

Proof. Assume L is a subextension of F/K and $f = \mathrm{id}$. Then the inverse image of $\tau \in \mathrm{Hom}_K(L, F)$ is $\mathrm{Hom}_L(F, F_\tau)$, but $|\mathrm{Hom}_L(F, F_\tau)| = [F : L]$ and $|\mathrm{Hom}_K(L, F)| = [L : K]$ by Lemma 13.3(i)$\Rightarrow$(v) for $E = F$. The general case follows because $L \cong f(L) \subset F$ by f, and $\mathrm{Hom}_K(f(L), F) \ni g \mapsto g \circ f \in \mathrm{Hom}_K(L, F)$ is bijective. □

Proposition 15.5. *Let F/K be Galois and $G = \mathrm{Gal}(F/K)$. If L is a subextension of F/K and $H = \mathrm{Gal}(F/L)$, then:*

(i) *$G \ni \sigma \longmapsto \sigma|_L \in \mathrm{Hom}_K(L, F)$ is surjective.*
(ii) *$\mathrm{Gal}(F/\sigma(L)) = \sigma H \sigma^{-1} = \{\sigma\tau\sigma^{-1} \mid \tau \in H\}$ $(\forall \sigma \in G)$.*
(iii) *$G \rhd H \iff \sigma(L) = L$ $(\forall \sigma \in G) \iff L/K$: Galois.*
(iv) *If L/K is Galois, then $G/H \ni \overline{\sigma} \longmapsto \sigma|_L \in \mathrm{Gal}(L/K)$ is an isomorphism.*

Proof. (i): Proposition 15.4. (ii): If $H' := \mathrm{Gal}(F/\sigma(L))$, then $\sigma H \sigma^{-1} \subset H'$. Similarly, $L = \sigma^{-1}(\sigma(L))$ gives $\sigma^{-1} H' \sigma \subset H$, hence $H' \subset \sigma H \sigma^{-1}$. (iii): By (ii) and Theorem 6.2, we have $\sigma H \sigma^{-1} = H$ $(\forall \sigma \in G) \iff \sigma(L) = L$ $(\forall \sigma \in G)$. This last condition means that the surjection (i) factors through $\mathrm{Hom}_K(L, L)$, thus $\mathrm{Hom}_K(L, L) = \mathrm{Hom}_K(L, F)$. Therefore L/K is Galois as $|\mathrm{Hom}_K(L, F)| = [L : K]$. (iv) By $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, F)$, the surjection (i) is a homomorphism with the kernel H. □

Part 4. Examples (2)

Lecture 16. General equations, cubics (F. 12/11/10)

Definition 16.1. Let K be a field and $P \in K[X]$ be a separable polynomial. The **Galois group** $\mathrm{Gal}(P)$ of P is defined as $\mathrm{Gal}(F/K)$ for a splitting field F of P over K, which is unique up to isomorphism by Propositions 7.4 and Theorem 15.2(iii).

Proposition 16.2. *Let $P \in K[X]$ be a separable polynomial with $\deg P = n$. Then $\mathrm{Gal}(P)$ is a subgroup of the automorphism group of $\mathrm{Root}_P(F)$, where F is a splitting field of P. In particular, a choice of ordering of the roots in $\mathrm{Root}_P(F)$ gives an injection $\mathrm{Gal}(P) \to S_n$, where $S_n := \mathrm{Aut}(\{1,\dots,n\})$ is the* **symmetric group in n letters** *(well-defined up to reordering of $\{1,\dots,n\}$, i.e. conjugation by an element of S_n).*

Proof. If $\mathrm{Root}_P(F) = \{x_1,\dots,x_n\}$, then $\mathrm{Gal}(F/K)$ acts on the set $\mathrm{Root}_P(F)$. As $F = K(x_1,\dots,x_n)$ by Proposition 7.5, an automorphism $\sigma \in \mathrm{Gal}(F/K)$ is determined by $\sigma(x_1),\dots,\sigma(x_n)$, thus $\mathrm{Gal}(F/K)$ is a subgroup of $\mathrm{Aut}(\mathrm{Root}_P(F))$. Once we label the elements of $\mathrm{Root}_P(F)$, we have $\mathrm{Aut}(\mathrm{Root}_P(F)) \cong \mathrm{Aut}(\{1,\dots,n\}) = S_n$. □

Proposition 16.3. *Let K be a field and $F = K(x_1,\dots,x_n) := \mathrm{Frac}(K[x_1,\dots,x_n])$ be a* **rational function field** *in n variables, where $x_1,\dots,x_n$ are indeterminates. Let $a_1,\dots,a_n$ be the elementary symmetric polynomials of x_i, namely $a_i := \sum_I x_{\lambda_1}\cdots x_{\lambda_i}$ where $I = \{\lambda_1,\dots,\lambda_i\}$ runs through all subsets of $\{1,\dots,n\}$ of cardinality i, and let $L := K(a_1,\dots,a_n)$ be the subfield of F consisting of all rational functions of a_i. If $P(X) = X^n + \sum_{i=1}^n (-1)^i a_i X^{n-i} \in L[X]$, then $\mathrm{Gal}(P) \cong S_n$.*

Proof. As $\mathrm{Root}_P(F) = \{x_1,\dots,x_n\}$ and $F = L(x_1,\dots,x_n)$, the F/L is a splitting field of P. Hence $\mathrm{Gal}(P) = \mathrm{Gal}(F/L) \subset G := \mathrm{Aut}(\{x_1,\dots,x_n\}) \cong S_n$. But G acts on F by K-automorphisms permuting $x_1,\dots,x_n$ and $L \subset F^G$, hence $G \subset \mathrm{Gal}(F/L)$. □

Remark 16.4. By Galois theory (Theorem 6.2), we have $L = F^G$ (the **symmetric function theorem** for rational functions).

Example 16.5. Let K be a field with $\mathrm{char}\, K \neq 2,3$ and $\boldsymbol{\mu}_3 \subset K$, and consider a general cubic $P(X) = X^3 - aX^2 + bX - c = (X-\alpha)(X-\beta)(X-\gamma)$ in $F = K(\alpha,\beta,\gamma)$, which is Galois over $L := K(a,b,c)$ with Galois group S_3. We look for $x \in F$ with $F = L(x)$, whose minimal polynomial Q over L (necessarily $\deg Q = 6$) has a simple form. For this we consider the **Lagrange resolvent** $x = \alpha + \zeta\beta + \zeta^2\gamma$ for a primitive cubic root of unity ζ. Then the images of x under the action of $\mathrm{Gal}(F/L) \cong S_3$ are:

$$\begin{aligned}\mathrm{Root}_Q(F) = \{\ & x = \alpha + \zeta\beta + \zeta^2\gamma, \quad \beta + \zeta\gamma + \zeta^2\alpha, \quad \gamma + \zeta\alpha + \zeta^2\beta,\\ & y := \alpha + \zeta\gamma + \zeta^2\beta, \quad \beta + \zeta\alpha + \zeta^2\gamma, \quad \gamma + \zeta\beta + \zeta^2\alpha\}.\end{aligned}$$

and $x^3 + y^3 = (x+y)(\zeta x + \zeta^2 y)(\zeta^2 x + \zeta y) = (2\alpha - \beta - \gamma)(2\gamma - \alpha - \beta)(2\beta - \alpha - \gamma) = (3\alpha - a)(3\beta - a)(3\gamma - a) = -27P(a/3) = -9ab + 2a^3 + 27c$ and $xy = \alpha^2 + \beta^2 + \gamma^2 - \alpha\beta - \beta\gamma - \gamma\alpha = a^2 - 3b$, thus we see that $Q(X) = X^6 + (9ab - 2a^3 - 27c)X^3 + (a^2 - 3b)^3$, which is solvable via $\sqrt{\ }$ and $\sqrt[3]{\ }$, and the original roots are recovered from x as

$$y = (a^2 - 3b)/x, \quad \alpha = (x + y + a)/3, \quad \beta = (\zeta x + \zeta^2 y + a)/3, \quad \gamma = (\zeta^2 x + \zeta y + a)/3.$$

Lecture 17. Kummer extensions (M. 15/11/10)

Definition 17.1. A Galois extension is called **cyclic** if its Galois group is cyclic.

Let n be a positive integer and K a field with $(\operatorname{char} K, n) = 1$, which contains the group of n-th roots of unity $\boldsymbol{\mu}_n$, i.e. $X^n - 1$ splits in K.

For $a \in K^\times$ such that $P(X) := X^n - a$ is irreducible in $K[X]$, we consider the extension $F = K(\sqrt[n]{a}) := K[X]/(X^n - a)$ obtained by adjoining a root of P (an n-th root of a). Denoting one root in F by $x = \sqrt[n]{a}$, and fixing a primitive n-th root of unity $\zeta = \zeta_n \in K$, we have $\operatorname{Root}_P(F) = \{\zeta^i x \in F \mid 0 \le i \le n-1\}$ as they are distinct by Proposition 10.1. Thus F/K is a Galois extension. We have the following isomorphism, which shows that it is a cyclic extension:

$$\operatorname{Gal}(F/K) \ni (\sqrt[n]{a} \mapsto \zeta^i \sqrt[n]{a}) \longmapsto i \bmod n \in \mathbb{Z}/n\mathbb{Z}.$$

Definition 17.2. For a field K with $(\operatorname{char} K, n) = 1$, $\boldsymbol{\mu}_n \subset K$, a cyclic extension of degree n of the form $F = K(\sqrt[n]{a}) \cong K[X]/(X^n - a)$ is called a **Kummer extension**.

Exercise 17.3. For every field K with $\operatorname{char} K \neq 2$, every quadratic extension is a Kummer extension. (Note that $\boldsymbol{\mu}_2 = \{\pm 1\} \subset K$.)

Theorem 17.4. (Kummer theory) *Let $n \ge 1$. Let K be a field with $(\operatorname{char} K, n) = 1$ and $\boldsymbol{\mu}_n \subset K$. Then every cyclic extension of degree n is a Kummer extension.*

Proof. Let F/K be cyclic of degree n, and choose a generator σ of $G = \operatorname{Gal}(F/K)$. Let Q be the minimal polynomial of σ considered as an endomorphism $\sigma \in \operatorname{End}(F)$ of F as a vector space over K. Then $\Lambda := \operatorname{Root}_Q(K)$ is the set of all eigenvalues of σ by Proposition xiv.17. As $\sigma^n = \mathrm{id}$ we have $Q \mid X^n - 1$, hence $\Lambda \subset \boldsymbol{\mu}_n$. Now Λ is a group under multiplication, because if $c, d \in \Lambda$ and $\sigma(x) = cx$, $\sigma(y) = dy$ for $x, y \in F^\times$, then $\sigma(xy) = \sigma(x)\sigma(y) = (cd)(xy)$, $\sigma(x^{-1}) = \sigma(x)^{-1} = c^{-1}x^{-1}$ imply $cd, c^{-1} \in \Lambda$. Thus $\Lambda = \boldsymbol{\mu}_d \subset \boldsymbol{\mu}_n$ for some $d \mid n$ (Exercise 9.5(ii)). As $Q \mid X^n - 1$, we have $Q = X^d - 1$. But σ has order n, hence $d = n$ and $\Lambda = \boldsymbol{\mu}_n$. Let $\zeta \in \boldsymbol{\mu}_n$ be a primitive n-th root of unity, and let $x \in F^\times$ be its eigenvector. Then $\sigma(x^n) = \sigma(x)^n = (\zeta x)^n = x^n$, hence $a := x^n \in F^G = K$ by Galois theory (Theorem 6.2). Therefore the minimal polynomial P of x over K divides $X^n - a$. But $\sigma^i(x) = \zeta^i x$ for $0 \le i \le n-1$ are all distinct, and as σ^i are K-isomorphisms, they are all roots of P. Thus $P = X^n - a$ and $F = K(x)$. □

Definition 17.5. A finite group G is called a **soluble group** if there exists a decreasing sequence (G_i) of subgroups $G = G_0 \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = \{1\}$ such that $G_{i-1} \rhd G_i$ and G_{i-1}/G_i is cyclic for all $1 \le i \le n$.

Lemma 17.6. (i) *If $G \rhd H$, then G : soluble $\iff$ H, G/H : soluble.*
(ii) *Finite abelian groups are soluble.*

Proof. (i): Let $p : G \to G/H$ be the canonical surjection. If (G_i) is a sequence for G, then $(H \cap G_i), (p(G_i))$ give the sequences for H and G/H. If $(H_i), (G_i)$ are sequences for H and G/H, combining (H_i) and $(p^{-1}(G_i))$ gives one for G. (ii): If $G \ni \sigma \neq 1$ and $H = \langle\sigma\rangle$, then H is cyclic and $|G/H| < |G|$. Use (i)$\Leftarrow$ and induction on $|G|$. □

Lecture 18. Soluble and radical extensions (W. 17/11/10)

Definition 18.1. A finite extension F/K is called a **soluble extension** if there is a finite E/F such that E/K is Galois with a soluble Galois group.

Proposition 18.2. (i) *A Galois F/K is soluble if and only if* $\mathrm{Gal}(F/K)$ *is soluble.*
(ii) *If L/K is soluble and F/L is abelian, then F/K is soluble.*

Proof. (i): If: clear. Only if: Proposition 15.5(iv) and Lemma 17.6(i)$\Rightarrow$. (ii): Let E/L be finite with E/K Galois (thus $|\mathrm{Hom}_K(L,E)| = [L:K]$) and $\mathrm{Gal}(E/K)$ soluble. By induction or Theorem 14.4, we can assume $F = L(x)$. Let P, Q be the minimal polynomial of x over K, L respectively, and E' be the splitting field of P over E. Then Q is separable as F/L is Galois, hence so is τQ for every $\tau \in \mathrm{Hom}_K(L,E)$ (use Proposition 14.2). As $\tau Q \mid P$, we have $|\mathrm{Hom}_K(F,E')| = [F:K]$ by Lemma 13.2, which shows $|\mathrm{Hom}_K(K(x),E')| = |\mathrm{Root}_P(E')| = \deg P$ by Lemma 13.3(i)$\Rightarrow$(iv). Let $\mathrm{Root}_P(E') = \{x_1,\dots,x_n\}$ so that $E' = E(x_1,\dots,x_n)$, and set $E_0 = E$, $E_n = E'$ and $E_i = E_{i-1}(x_i)$. If Q_i is the minimal polynomial of x_i over E_{i-1} and $\tau \in \mathrm{Hom}_K(E_{i-1},E')$, then $\tau Q_i \mid P$, thus $|\mathrm{Hom}_K(E',E')| = [E':K]$ by Lemma 13.3(iii)$\Rightarrow$(i) and E'/K is Galois. Fix i, pick $\tau \in \mathrm{Hom}_K(K(x),E')$ with $\tau(x) = x_i$ (Proposition 7.2) and extend to $\tau \in \mathrm{Hom}_K(F,E')$ by Lemma 13.3. Then $|\mathrm{Hom}_K(L,E)| = |\mathrm{Hom}_K(L,E')| = [L:K]$ shows $\tau(L) \subset E$. As τ gives $F \cong \tau(F)$, we have $\tau(F) = \tau(L)(x_i)$ and $\tau(F)/\tau(L)$ abelian. By $\tau(L) \subset E \subset E_{i-1}$, the next Lemma shows that E_i/E_{i-1} is abelian with $\mathrm{Gal}(E_i/E_{i-1})$ injecting to $\mathrm{Gal}(\tau(F)/\tau(L))$. Thus $\mathrm{Gal}(E'/K)$ is soluble by Lemma 17.6(ii) and (i)$\Leftarrow$. □

Lemma 18.3. *Let $E/L/K$ be finite extensions and $x \in E$. If $K(x)/K$ is Galois, then $L(x)/L$ is Galois and the map* $\mathrm{Gal}(L(x)/L) \ni \sigma \longmapsto \sigma|_{K(x)} \in \mathrm{Gal}(K(x)/K)$ *is injective. (The field $L(x)$ is the* **composite field** *of $K(x)$ and L in E.)*

Proof. As the minimal polynomial of x over L divides that of x over K, its roots are distinct and all belong to $K(x)$, hence $L(x)/L$ is Galois. The map is injective as $\sigma \in \mathrm{Gal}(L(x)/L)$ is determined by $\sigma(x)$. □

Definition 18.4. A finite extension F/K is called a **radical extension** if there is a finite E/F such that E/K is a succession of cyclotomic and Kummer extensions.

Theorem 18.5. *If* $\mathrm{char}\, K = 0$*, then F/K : radical $\iff$ F/K : soluble.*

Proof. $\Rightarrow$: Cyclotomic and Kummer extensions are abelian. Iterate Proposition 18.2(ii).
$\Leftarrow$: Let E/K be Galois with $\mathrm{Gal}(E/K)$ soluble. Take a sequence (G_i) for G and the corresponding subextensions $K = K_0 \subset \cdots \subset K_m = E$ (Theorem 6.2), both of which we subdivide (each step remains cyclic by Proposition 15.5(iv)) so that $K_i = K_{i-1}(x_i)$ for all i. Let $n_i := |G_{i-1}/G_i|$ and $n := n_1 \cdots n_m$. By Lemma 18.3 $K_i(\boldsymbol{\mu}_n)/K_{i-1}(\boldsymbol{\mu}_n)$ is Galois with the Galois group isomorphic to a subgroup of $\mathrm{Gal}(K_i/K_{i-1}) \cong G_{i-1}/G_i$ (Proposition 15.5(iv)), hence cyclic of degree dividing n_i (Exercise 9.5(ii)), therefore Kummer by Theorem 17.4. Thus $E(\boldsymbol{\mu}_n) = K_m(\boldsymbol{\mu}_n)/K$ is radical. □

Corollary 18.6. *A general equation of degree $n \geq 5$ is not solvable by iterated radicals.*

Proof. As A_n (Definition 19.1) is simple for $n \geq 5$, the group S_n is not soluble by Lemma 17.6(i)$\Rightarrow$. Now use Proposition 16.3, Proposition 18.2(i) and Theorem 18.5$\Rightarrow$. □

Lecture 19. Quartics, discriminants (F. 19/11/10)

Definition 19.1. (i) For every $\sigma \in S_n$ there is a partition $\{1,\dots,n\} = I_1 \amalg \cdots \amalg I_m$ with $|I_i| = n_i$ such that for each $I_i = \{a_1,\dots,a_{n_i}\}$ we have $\sigma(a_j) = a_{j+1}$ for $1 \le j \le n_i - 1$ and $\sigma(a_{n_i}) = a_1$. We denote $\sigma = (a_1 \cdots a_{n_1})(b_1 \cdots b_{n_2}) \cdots$, and say σ is of **cyclic type** $(n_1,\dots,n_m)$. (It corresponds to conjugacy classes.)

(ii) A group homomorphism $\mathrm{sgn} : S_n \to \mathbb{Z}/2\mathbb{Z}$ is defined by sending σ of cyclic type $(n_1,\dots,n_m)$ to $\sum_{i=1}^m (n_i - 1) \bmod 2$ (exercise). For all $n \ge 2$, the **alternating group** A_n is defined as $\mathrm{Ker}\,(\mathrm{sgn}) \lhd S_n$, a normal subgroup of index 2.

Definition 19.2. Let K be a field. If $P \in K[X]$ is separable and $\deg P = n$, then the injection $\mathrm{Gal}(P) \to S_n$ is determined up to conjugation in S_n by Proposition 16.2. Therefore, if $H \lhd S_n$, then we have a normal subgroup $\mathrm{Gal}(P) \cap H$ of $\mathrm{Gal}(P)$.

Example 19.3. When $n = 4$, the group S_4 is soluble. Define the **Klein 4-group** as $V_4 := \{1, (12)(34), (13)(24), (14)(23)\} \lhd S_4$, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $S_4/V_4 \cong S_3$, and we have $S_4 \rhd A_4 \rhd V_4 \rhd \mathbb{Z}/2\mathbb{Z} \rhd \{1\}$ and the successive indices are $2, 3, 2, 2$. Let $P \in K[X]$ be a separable quartic with a splitting field F/K and $\mathrm{Root}_P(F) = \{\alpha, \beta, \gamma, \delta\}$. As $a = \alpha + \beta + \gamma + \delta \in K$, by subtracting $a/4$ from all roots we assume $a = 0$. Let $x = \alpha + \beta,\ y = \alpha + \gamma,\ z = \alpha + \delta$. Then

$$\alpha = (x + y + z)/2, \quad \beta = (x - y - z)/2, \quad \gamma = (-x + y - z)/2, \quad \delta = (-x - y + z)/2$$

and $F = K(x, y, z)$. As $x = \alpha + \beta = -(\gamma + \delta)$, etc., $\{\pm x, \pm y, \pm z\}$ are all distinct, and we have 3 distinct elements of F:

$$x^2 = -(\alpha + \beta)(\gamma + \delta), \quad y^2 = -(\alpha + \gamma)(\beta + \delta), \quad z^2 = -(\alpha + \delta)(\beta + \gamma),$$

the action of $\mathrm{Gal}(P) \subset S_4$ on $\{\alpha, \beta, \gamma, \delta\}$ induces its action on $\{x^2, y^2, z^2\}$ (this realizes $S_3 \cong S_4/V_4$), and the subgroup of automorphisms fixing all x^2, y^2, z^2 is $\mathrm{Gal}(P) \cap V_4$. Thus the subextension of F/K corresponding to $\mathrm{Gal}(P) \cap V_4$ is $L = K(x^2, y^2, z^2)$, and F/L is at most biquadratic. The extension L/K is a splitting field of the cubic equation $Q \in K[X]$ with $\mathrm{Root}_Q(L) = \{x^2, y^2, z^2\}$, which is called the **resolvent cubic** of P.

Exercise 19.4. For $P(X) = X^4 + pX^2 + qX + r$, its resolvent cubic is $Q(X) = X^3 + 2pX^2 + (p^2 - 4r)X - q^2$.

Proposition 19.5. *Let $P \in K[X]$ be separable with $\deg P = n$, and F/K its splitting field. If $\mathrm{char}\, K \ne 2$, then the subextension corresponding to $\mathrm{Gal}(P) \cap A_n$ is $K(\sqrt{\Delta_P})$, where the* **discriminant** *$\Delta_P \in K$ of P is defined as $\Delta_P := \prod_{i<j}(x_i - x_j)^2 \in K$ where $\mathrm{Root}_P(F) = \{x_1,\dots,x_n\}$. Therefore $\mathrm{Gal}(P) \subset A_n$ if and only if Δ_P is a square in K.*

Proof. As Δ_P is fixed under the action of $\mathrm{Gal}(P)$, it lies in K, and $\Delta_P \ne 0$ as P is separable. Let L/K be the subextension corresponding to $\mathrm{Gal}(P) \cap A_n$. As $\sqrt{\Delta_P} := \prod_{i<j}(x_i - x_j)$ is fixed under the action of $\mathrm{Gal}(P) \cap A_n$ it is in L, and if $\sigma \in \mathrm{Gal}(P) \setminus A_n$ then $\sigma(\sqrt{\Delta_P}) = -\sqrt{\Delta_P} \ne \sqrt{\Delta_P}$, hence it generates L/K. □

Exercise 19.6. Let $\mathrm{char}\, K \ne 2, 3$ and $\boldsymbol{\mu}_3 \subset K$, and consider a cubic $P(X) = X^3 - aX^2 + bX - c = (X - \alpha)(X - \beta)(X - \gamma)$ with $a, b, c \in K$. If P is irreducible then $\mathrm{Gal}(P) \cong A_3$ or S_3, and the two cases occur according to whether $\Delta_P \in K$ is a square or not. The extension $K(\sqrt{\Delta_P})$ is obtained by adjoining a root of the minimal polynomial $X^2 + (9ab - 2a^3 - 27c)X + (a^2 - 3b)^3$ of the cube of Lagrange resolvent.

Lecture 20. Galois groups over $\mathbb{Q}$ (M. 22/11/10)

Proposition 20.1. *Let $P \in K[X]$ be separable with $\deg P = n$. Then P is irreducible if and only if the Galois group $\mathrm{Gal}(P)$ is transitive as a subgroup of S_n. (A subgroup $G \subset S_n$ is* **transitive** *if for every $i, j \in \{1, \dots, n\}$ there exists $\sigma \in G$ with $\sigma(i) = j$.)*

Proof. If $P = QR$ in $K[X]$, then elements of $\mathrm{Gal}(P)$ cannot send roots of Q to roots of R, thus not transitive on $\mathrm{Root}_P(F)$. If P is irreducible, then by $S_n \cong \mathrm{Aut}\big(\mathrm{Root}_P(F)\big) \cong \mathrm{Aut}\big(\mathrm{Hom}_K(K_P, F)\big)$ (Proposition 5.1), the transitivity is Proposition 15.4. □

Example 20.2.
(i) If a cyclic subgroup of S_n is transitive then it has order n. (The Galois groups over finite fields.)
(ii) Transitive subgroups of S_3 are $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ and S_3.
(iii) Transitive subgroups of S_4 are, up to conjugation: $\mathbb{Z}/4\mathbb{Z}$, $V_4 = \{1, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_8, A_4 and S_4.
(iv) Transitive subgroups of S_5 are, up to conjugation: $\mathbb{Z}/5\mathbb{Z}$, D_{10}, $F_{20} = \langle (12345), (1)(2453) \rangle$ (the **Frobenius group** of order 20), A_5 and S_5.

Let x_i, a_i be as in Proposition 16.3. Let $A := \mathbb{Z}[a_1, \dots, a_n]$ and $B := \mathbb{Z}[x_1, \dots, x_n]$ be the polynomial rings, so that $L = \mathbb{Q}(a_1, \dots, a_n)$ and $F = \mathbb{Q}(x_1, \dots, x_n)$ are their fields of fractions. Recall the action of $S_n \cong \mathrm{Gal}(F/L)$ on $x_1, \dots, x_n$, i.e. $\sigma(x_i) := x_{\sigma(i)}$ for $\sigma \in S_n$, thus S_n acts on B and F. Consider the following polynomial (the minimal polynomial of a "generic resolvent"), where T_i are auxiliary variables:

$$R := \prod_{\sigma \in S_n} R_\sigma, \quad R_\sigma := X - \big(\sigma(x_1)T_1 + \cdots + \sigma(x_n)T_n\big) \in B[T_1, \dots, T_n][X].$$

Then the coefficients are invariant under S_n, therefore in L (Remark 16.4), thus in $B \cap L = A$ (Lemma xi.4), i.e. $R \in A[T_1, \dots, T_n][X]$. Now let K be a field and $P = X^n + \sum_{i=1}^n (-1)^i b_i X^{n-i} \in K[X]$ be separable. Let E/K be its splitting field so that $G := \mathrm{Gal}(P) = \mathrm{Gal}(E/K) \subset S_n$ and $\mathrm{Root}_P(E) = \{y_1, \dots, y_n\}$. Consider a G-equivariant ring homomorphism $\tau : B \to E$ defined by $\tau(x_i) = y_i$. It restricts to $A \to K$ with $\tau(a_i) = b_i$. Thus $\tau R_\sigma \in E[T_1, \dots, T_n][X]$ for each σ, and $\tau R \in K[T_1, \dots, T_n][X]$. Let Q be an irreducible factor of τR in $K(T_1, \dots, T_n)[X]$. If $\tau R_\sigma \mid Q$ then $\tau R_{\rho\sigma} \mid Q$ for all $\rho \in G$, thus $\tau R_{G\sigma} := \prod_{\rho \in G} \tau R_{\rho\sigma} \mid Q$. But $\tau R_{G\sigma} \in K[T_1, \dots, T_n][X]$ because the coefficients are invariant under G and $E^G = K$, thus $\tau R_{G\sigma} = Q$. As $\tau R = \prod_{\sigma \in G \backslash S_n} \tau R_{G\sigma}$, this is the irreducible factorization of τR in $K(T_1, \dots, T_n)[X]$.

Proposition 20.3. *Let $P \in \mathbb{Z}[X]$ be a separable monic polynomial and let p be a prime such that $P \bmod p \in \mathbb{F}_p[X]$ is also separable. If $P \bmod p = Q_1 \cdots Q_m$ is the factorization into irreducibles in $\mathbb{F}_p[X]$ and $\deg Q_i = n_i$, then $\mathrm{Gal}(P)$ contains an element of cyclic type $(n_1, \dots, n_m)$. (The proof of Theorem 12.5 used this structure.)*

Proof. The τ corresponding to P gives $\tau R \in \mathbb{Z}[T_1, \dots, T_n][X]$, whose factorization in $\mathbb{Q}(T_1, \dots, T_n)[X]$, which is the same as the factorization in $\mathbb{Z}[T_1, \dots, T_n][X]$ (it is a UFD by Proposition xi.3, so use Gauss' Lemma (Proposition xi.2)), gives $\mathrm{Gal}(P)$. The $\overline{\tau}$ corresponding to $P \bmod p$ gives $\overline{\tau}R = \tau R \bmod p \in \mathbb{F}_p[T_1, \dots, T_n][X]$, and it factorizes further than τR, thus $\mathrm{Gal}(P \bmod p)$ is a subgroup of $\mathrm{Gal}(P)$ up to conjugation. The p-th power Frobenius map gives the desired element in $\mathrm{Gal}(P \bmod p)$. □

Part 5. Beyond the Theory of Equations

Lecture 21. Another proof of the Galois theory (W. 24/11/10)

Proposition 21.1. (Dedekind) *Let F, E be fields and $\sigma_1, \dots, \sigma_n : F \to E$ be mutually distinct field homomorphisms. Then they are linearly independent over E in the E-vector space of all additive group homomorphisms from F to E. In other words, if $c_1, \dots, c_n \in E$ and $\sum_{i=1}^n c_i\sigma_i(x) = 0$ for all $x \in F$, then $c_1 = \cdots = c_n = 0$.*

Proof. Assume otherwise and take the minimal k such that $\{\sigma_1, \dots, \sigma_k\}$ is linearly dependent, i.e. there exist $c_j \in E$ with $\sum_{j=1}^k c_j\sigma_j = 0$ and $c_k \neq 0$. As $\sigma_k \neq 0$, there is a $t < k$ with $c_t \neq 0$. As $\sigma_t \neq \sigma_k$, choose $x \in F$ with $\sigma_t(x) \neq \sigma_k(x)$. For all $y \in F$ we have $\sum_{j=1}^k c_j\sigma_j(x)\sigma_j(y) = \sum_{j=1}^k c_j\sigma_j(xy) = 0$, i.e. $\sum_{j=1}^k c_j\sigma_j(x)\sigma_j = 0$. Hence

$$\sum_{j=1}^{k-1} c_j\big(\sigma_j(x) - \sigma_k(x)\big)\sigma_j = \sum_{j=1}^{k} c_j\sigma_j(x)\sigma_j - \sigma_k(x)\sum_{j=1}^{k} c_j\sigma_j = 0,$$

which contradicts the minimality of k because $\sigma_t(x) - \sigma_k(x) \neq 0$. □

Corollary 21.2. *Let F/K be finite. (cf. Lemma 13.3, Definition 15.1.)*

(i) *If E/K is an extension, then $|\mathrm{Hom}_K(F, E)| \leq [F : K]$.*
(ii) *If F/K is Galois and L/K is its subextension, then F/L is Galois.*

Proof. (i): By Proposition 21.1 $\mathrm{Hom}_K(F, E)$ is a linearly independent set in the E-vector space of all K-linear maps from F to E, which has dimension $[F : K]$ over E. Use Proposition iv.6(i). (ii): Use (i), Lemma 13.1 and Proposition 2.4. □

Proposition 21.3. (Artin) *If H is a subgroup of $\mathrm{Aut}(F)$, then $[F : F^H] \leq |H|$.*

Proof. Assume otherwise, and let $H = \{\sigma_1, \dots, \sigma_m\}$ with $m < n = [F : F^H]$. Take a basis $\{x_1, \dots, x_n\}$ of F over F^H. Then the system of equations $\sum_{j=1}^n c_j\sigma_i(x_j) = 0$ $(1 \leq i \leq m)$ has a solution $c_j \in F$ which is not all zero (Proposition xv.3(ii)). Take the minimal k such that there exist $c_j \in F$ with $\sum_{j=1}^k c_j\sigma_i(x_j) = 0$ with $c_k \neq 0$. We can assume $c_k = 1$ by dividing all c_j by c_k. As $x_1, \dots, x_k$ are linearly independent over F^H, there is a $t < k$ with $c_t \notin F^H$ (look at $\sigma_1 = \mathrm{id}$), so choose $\sigma \in H$ with $\sigma(c_t) \neq c_t$. As H is a group, applying σ to the system of equations gives $\sum_{j=1}^k \sigma(c_j)\sigma_i(x_j) = 0$ $(1 \leq i \leq m)$. As $\sigma(c_k) = \sigma(1) = 1 = c_k$, we have

$$\sum_{j=1}^{k-1}\big(\sigma(c_j) - c_j\big)\sigma_i(x_j) = \sum_{j=1}^{k}\sigma(c_j)\sigma_i(x_j) - \sum_{j=1}^{k} c_j\sigma_i(x_j) = 0 \quad (1 \leq i \leq m),$$

which contradicts the minimality of k because $\sigma(c_t) - c_t \neq 0$. □

Proof of Theorem 6.2. We have $|\Phi(L)| = [F : L]$ by Corollary 21.2(ii). Therefore, as $H \subset \Phi(\Psi(H))$, we have $|H| \leq |\Phi(\Psi(H))| = [F : \Psi(H)]$. As $L \subset \Psi(\Phi(L))$, we have $[F : L] = |\Phi(L)| \leq [F : \Psi(\Phi(L))] \leq [F : L]$, thus $\Psi \circ \Phi = \mathrm{id}$. By Proposition 21.3, we have $|H| \leq |\Phi(\Psi(H))| = [F : \Psi(H)] \leq |H|$, thus $\Phi \circ \Psi = \mathrm{id}$. □

Lecture 22. Trace and norm* (not lectured)

We denote by $\mathrm{Hom}_{K\text{-vs}}(F,E)$ etc. the set of all K-linear maps as K-vector spaces.

Definition 22.1. Let F/K be finite and $x \in F$. Let $m_x : F \ni y \mapsto xy \in F$ be the x-multiplication map viewed as an element of $\mathrm{End}_{K\text{-vs}}(F)$. Its trace and determinant (elements in K) are called the **trace** $T_{F/K}(x)$ and the **norm** $N_{L/K}(x)$ of x.

Clearly the trace $T_{F/K} : F \to K$ is a K-linear map, and the norm $N_{F/K} : F^\times \to K^\times$ is a group homomorphism by Proposition xiii.5(i),(ii).

Lemma 22.2. *Let F/K be finite separable with $[F:K] = n$, and $\mathrm{Hom}_K(F,E) = \{\sigma_1, \dots, \sigma_n\}$ for an extension E/K. Then a subset $X = \{x_1, \dots, x_n\} \subset F$ is a K-basis of F if and only if $\big(\sigma_i(x_j)\big) \in \mathrm{GL}_n(E)$ ($\Leftrightarrow \det\big(\sigma_i(x_j)\big) \neq 0$ by Proposition xvi.14(ii)).*

Proof. If X is a basis of F, then its dual basis $X^* := \{x_1^*, \dots, x_n^*\}$ is an E-basis of $\mathrm{Hom}_K(F,E)$. As $\mathrm{Hom}_K(F,E)$ is also an E-basis by Proposition 21.1 and $\sigma_i = \sum_{j=1}^n \sigma_i(x_j)x_j^*$, we have $(\sigma_i(x_j)) \in GL_n(E)$. If $(\sigma_i(x_j)) \in GL_n(E)$ and $\sum_{j=1}^n c_j x_j = 0$ for $c_j \in K$, then $\sum_{j=1}^n c_j \sigma_i(x_j) = 0$ shows $c_j = 0$ by Proposition xvi.15(ii). □

Proposition 22.3. *Let F/K be finite separable with $[F:K] = n$, and $\mathrm{Hom}_K(F,E) = \{\sigma_1, \dots, \sigma_n\}$ for an extension E/K. Then we have*

$$T_{F/K}(x) = \sum_{i=1}^n \sigma_i(x), \quad N_{F/K}(x) = \prod_{i=1}^n \sigma_i(x).$$

In particular, $T_{F/K} : F \to K$ is not a zero map by Proposition 21.1, hence surjective.

Proof. Note that $T_{F/K}(x), N_{F/K}(x)$ are trace/determinant of $m_x^* \in \mathrm{End}_{K\text{-vs}}(F^*)$, which are also those of the E-linear map $m_x^* : \mathrm{Hom}_{K\text{-vs}}(F,E) \ni f \mapsto f \circ m_x \in \mathrm{Hom}_{K\text{-vs}}(F,E)$. With respect to its basis $\mathrm{Hom}_K(F,E)$ (Proposition 21.1), it is represented by a diagonal matrix with entries $\sigma_1(x), \dots, \sigma_n(x)$, because $m_x^*(\sigma_j) = \sigma_j \circ m_x = (y \mapsto xy \mapsto \sigma_j(xy) = \sigma_j(x)\sigma_j(y)) = \sigma_j(x) \cdot \sigma_j$. □

Proposition 22.4. *Let F/K be finite separable and L/K its subextension. Then:*

$$T_{F/K} = T_{L/K} \circ T_{F/L}, \quad N_{F/K} = N_{L/K} \circ N_{F/L}.$$

Proof. Take an extension E/K with $\mathrm{Hom}_K(F,E) = [F:K]$. The proposition follows from the decomposition $\mathrm{Hom}_K(F,E) = \coprod_{\tau \in \mathrm{Hom}_K(L,E)} \mathrm{Hom}_L(F, E_\tau)$ (Lemma 13.1). □

- inseparable case?
- dual basis
- Hilbert 90

Lecture 23. Infinite Galois extensions* (not lectured)

Let K be a field.

Definition 23.1. An algebraic extension F/K is called a **Galois extension** if it is a union of finite Galois extensions of K. In this case the group $\mathrm{Aut}_K(F)$ of all K-automorphisms of F is called the **Galois group** of F/K, and denoted by $\mathrm{Gal}(F/K)$.

Fix an algebraic closure of $\overline{K}$ of K. The union K^{sep} of all finite separable extensions of K inside $\overline{K}$ is a Galois extension of K by the next lemma and Theorem 15.2(iii):

Lemma 23.2. *The composite LL'/K of two finite Galois extensions $L/K, L'/K$ is a Galois extension. If $L/K, L'/K$ are both abelian, so is LL'/K.*

Proof. As the Galois closure of LL'/K (Exercise 15.3) coincides with LL', it is a Galois extension. The latter part follows from the injectivity of the group homomorphism $\mathrm{Gal}(LL'/K) \ni \sigma \longmapsto (\sigma|_L, \sigma|_{L'}) \in \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)$. □

Definition 23.3. We call K^{sep} the **separable closure** of K, and its Galois group $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ the **absolute Galois group** of K. If K is perfect then $K^{\mathrm{sep}} = \overline{K}$.

Exercise 23.4.
(i) By Lemma 23.2, the union K^{ab} of all abelian extensions of K inside $\overline{K}$ is a Galois extension of K (the **maximal abelian extension** of K).
(ii) The union $K(\boldsymbol{\mu}_\infty) = \bigcup_{n\geq 1} K(\boldsymbol{\mu}_n)$ of all cyclotomic extensions of K inside $\overline{K}$ is a Galois extension of K (the **maximal cyclotomic extension** of K). We have $K(\boldsymbol{\mu}_\infty) \subset K^{\mathrm{ab}}$ by Theorem 10.7.

Proposition 23.5. *Let F/K be a Galois extension, and L/K its finite subextension.*

(i) *F/L is Galois and $\mathrm{Gal}(F/K) \ni \sigma \longmapsto \sigma|_L \in \mathrm{Hom}_K(L, F)$ is surjective.*
(ii) *If L/K is also Galois, then $H = \mathrm{Gal}(F/L)$ is a normal subgroup of $G = \mathrm{Gal}(F/K)$, and we have a group isomorphism: $G/H \ni \overline{\sigma} \longmapsto \sigma|_L \in \mathrm{Gal}(L/K)$.*

Proof. (i) Write $F = \bigcup L'$ as a union of finite Galois extensions L'/K. Then LL'/L is Galois by Lemma 18.3 and $F = \bigcup LL'$, hence F/L is Galois. For each L', by the latter part of Proposition 14.1 we have $\mathrm{Gal}(L'/K) = \mathrm{Hom}_K(L', \overline{K})$, hence $\mathrm{Gal}(F/K) = \mathrm{Hom}_K(F, \overline{K})$. Therefore if we extend an arbitrary element of $\mathrm{Hom}_K(L, F)$ to an element of $\mathrm{Hom}_K(\overline{K}, \overline{K})$ by Theorem 8.2(ii) and restrict it to F we get an element of $\mathrm{Gal}(F/K)$, hence the surjectivity.

(ii) By the latter part of Proposition 14.1 we have $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, F)$ hence the surjection in (i) is a group homomorphism, and as H is its kernel it is normal. The second part follows from the homomorphism theorem. □

Appendix. Galois groups of infinite Galois extensions

Definition 23.6. For a family $\{X_i\}_{i\in\Lambda}$ of groups (resp. rings), indexed by the elements of a set Λ, if we define componentwise operations on the product set $\prod_{i\in\Lambda} X_i$ as:

$$(x_i)(y_i) = (x_iy_i), \quad (\text{ resp. and } (x_i)+(y_i) = (x_i+y_i)\ ),$$

then it becomes a group (resp. ring). This $\prod_{i\in\Lambda} X_i$ is called the **direct product** of groups (resp. rings).

Exercise 23.7. An integral domain cannot be isomorphic to a direct product of more than one rings.

Proposition 23.8. *For an infinite Galois extension F/K, if we denote the set of all intermediate finite Galois extensions of F/K by Λ, then we have the following group isomorphism:*

$$\mathrm{Gal}(F/K) \ni \sigma \longmapsto (\sigma|_L) \in \left\{\ (\sigma_L)_{L\in\Lambda} \;\middle|\; L\subset L' \Longrightarrow \sigma_{L'}|_L = \sigma_L\ \right\} \subset \prod_{L\in\Lambda} \mathrm{Gal}(L/K).$$

The set in the right hand side is a subgroup of the direct product, and is called an **inverse limit** $\varprojlim \mathrm{Gal}(L/K)$ *of* $\{\mathrm{Gal}(L/K)\}_{L\in\Lambda}$.

Proof. The group homomorphism is defined as $\mathrm{Hom}_K(L,F) = \mathrm{Gal}(L/K)$ for each $L\in\Lambda$. As $F = \bigcup L$, an element σ is determined by $(\sigma|_L)_{L\in\Lambda}$, hence the map is injective. Conversely any element $(\sigma_L)_{L\in\Lambda}$ of the right hand side defines an element $\sigma\in\mathrm{Gal}(F/K)$ by $x\in L \Longrightarrow \sigma(x) = \sigma_L(x)$, hence it is also surjective. □

Remark 23.9. A group G equipped with an isomorphism with the inverse limit $\varprojlim G_\lambda$ of an inverse system $\{G_\lambda\}$ of finite groups is called a **profinite group**, and this isomorphism gives a natural topology **(profinite topology)** such that $\mathrm{Ker}\,(G\to G_\lambda)$ gives the basis of open neighborhoods of 1. The Galois group $\mathrm{Gal}(F/K)$ is naturally a profinite group by Proposition 23.8, and there is a bijective correspondence between its closed subgroups and the subextensions of F/K (in particular, open subgroups correspond to finite subextensions).

Example: The absolute Galois group of finite fields. We begin with the following corollary of Theorem 11.6.

Corollary 23.10. *For any positive integer m,n with $m \mid n$ we have a commutative diagram:*

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow[\cong]{\varphi_n} & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ \downarrow & & \downarrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow[\cong]{\varphi_m} & \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \end{array}$$

where the right vertical map is the natural restriction $\sigma\longmapsto\sigma|_{\mathbb{F}_{q^m}}$ and the left vertical map is the natural surjection $1 \bmod n \longmapsto 1 \bmod m$.

We would like to represent the fact (Corollary 23.10) that there are isomorphisms between Galois groups and cyclic groups for all finite extensions simultaneously and

compatibly, using the absolute Galois group. We will introduce the inverse limit of $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}\backslash\{0\}$). This is defined from the cyclic groups by the same procedure as we found the Galois group of infinite Galois extension in Proposition 23.8.

Definition 23.11. We define the **profinite completion** $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$ as follows:

$$\widehat{\mathbb{Z}} = \left\{ (a_n)_{n\geq 1} \;\middle|\; m \mid n \Longrightarrow a_n \equiv a_m \bmod m \right\} \subset \prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z}.$$

Exercise 23.12.
(i) $\prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z}$ is a ring by componentwise addition and multiplication, and $\widehat{\mathbb{Z}}$ is its subring.
(ii) The natural map $\mathbb{Z} \ni 1 \longmapsto (1)_{n\geq 1} \in \widehat{\mathbb{Z}}$ is an injective ring homomorphism which identifies $\mathbb{Z}$ with a subring of $\widehat{\mathbb{Z}}$.
(iii) For each $n \geq 1$ there is a natural surjection $\widehat{\mathbb{Z}} \ni (a_n)_{n\geq 1} \longmapsto a_n \in \mathbb{Z}/n\mathbb{Z}$ with kernel $(n) \subset \widehat{\mathbb{Z}}$. (Use (ii).)

In what follows, we regard $\widehat{\mathbb{Z}}$ as an additive group, and also $\mathbb{Z} \subset \widehat{\mathbb{Z}}$, in particular $1 = (1)_{n\geq 1} \in \widehat{\mathbb{Z}}$.

Now we consider the absolute Galois group of $\mathbb{F}_q$. By the definition of Frobenius map, if we restrict $\mathrm{Fr}_q \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ to $\mathbb{F}_{q^m}$ for $m \mid n$ we get $\mathrm{Fr}_q \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. This defines, by Proposition 23.8, the **Frobenius map** as an element of the absolute Galois group as follows:

$$\mathrm{Fr}_q = (\mathrm{Fr}_q)_{n\geq 1} \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \subset \prod_{n\geq 1} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q).$$

Hence defining $\varphi((a_n)_{n\geq 1}) = (\varphi_n(a_n))_{n\geq 1}$ by means of Corollary 23.10, we have:

Theorem 23.13. *For any finite field $\mathbb{F}_q$, there is an isomorphism:*

$$\varphi : \widehat{\mathbb{Z}} \ni 1 \longmapsto \mathrm{Fr}_q \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q).$$

Proposition 23.14. *For a finite field $\mathbb{F}_q$ and a positive integer n, the diagram below is commutative:*

$$\begin{array}{ccccc}
\widehat{\mathbb{Z}} & \xrightarrow{\quad n \quad} & \widehat{\mathbb{Z}} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\
\cong\downarrow\varphi & & \cong\downarrow\varphi & & \cong\downarrow\varphi_n \\
\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^n}) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)
\end{array}$$

where the lower left horizontal map is the natural inclusion, the upper left horizontal map is the multiplication by n. The horizontal maps on the right is the canonical surjection to the quotient group by the image of the horizontal maps on the left.

Proof. The first part follows from $\mathrm{Fr}_{q^n} = (\mathrm{Fr}_q)^n$ and the definitions. The second part follows from $\widehat{\mathbb{Z}}/(n) \cong \mathbb{Z}/n\mathbb{Z}$ (Exercise 23.12(iii)). □

Preliminaries I: Linear Algebra

i. Sets and Maps

Definition i.1. (i) A **map** $f : X \to Y$ from a set X to a set Y is a correspondence sending each element x of X to an element $y = f(x)$ of Y. We write:

$$f : X \ni x \longmapsto y \in Y.$$

(ii) The map $\mathrm{id}_X : X \ni x \longmapsto x \in X$ is called the **identity map** of X.
(iii) For two maps $f : X \to Y$ and $g : Y \to Z$, the map $X \ni x \longmapsto g(f(x)) \in Z$ is called the **composite** of f and g, and denoted by $g \circ f$.
(iv) For a subset $X' \subset X$, the subset $\{f(x) \mid x \in X'\}$ of Y is called an **image** of X', and denoted by $f(X')$. In particular, the image $f(X)$ of X is called the **image** of f and denoted by $\mathrm{Im}\, f$.
(v) For a subset $Y' \subset Y$, the subset $\{x \mid f(x) \in Y'\}$ of X is called the **inverse image** of Y', and denoted by $f^{-1}(Y')$. In particular, for $y \in Y$, the inverse image $\{x \mid f(x) = y\}$ of $\{y\}$ is called the **inverse image** of y and denoted by $f^{-1}(y)$.
(vi) For a subset $X' \subset X$, the map $i_{X'} : X' \ni x \longmapsto x \in X$ is called the **inclusion map**. For a map $f : X \to Y$, the map $f|_{X'} : X' \ni x \longmapsto f(x) \in Y$ is called the **restriction** of f to X'. We have $f|_{X'} = f \circ i_{X'}$. In this case, we say f is an **extension** of $f|_{X'}$.

Definition i.2. (i) A map f is called a **surjection** if $\mathrm{Im}\, f = Y$.
(ii) A map f is called an **injection** if it satisfies $f(x) = f(y) \Longrightarrow x = y$.
(iii) A map f is called a **bijection** if it is a surjection and an injecton.
(iv) For a bijection f, we define a map $f^{-1} : Y \to X$ by

$$f(x) = y \iff x = f^{-1}(y)$$

and call it the **inverse map** of f. Conversely, if there exists a map $f^{-1} : Y \to X$ satisfying $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_Y$, then f is a bijection.

Definition i.3. For two sets X, Y, the set consisting of all pairs (x, y) of an element x of X and an element y of Y is called the **direct product** and denoted by $X \times Y$. Similarly, for sets $X_1, \ldots, X_n$, the set consisting of n-tuples $(x_1, \ldots, x_n)$ of elements $x_i \in X_i$ is called the **direct product** of $X_1, \ldots, X_n$, and denoted by

$$\prod_{i=1}^{n} X_i = X_1 \times \cdots \times X_n.$$

In particular, for a set X, its n-fold direct product $X \times \cdots \times X$, the set of ordered n-tuples of elements of X, is denoted by X^n. For a family of sets $\{X_i\}_{\lambda \in \Lambda}$ indexed by a set Λ, their direct product $\prod_{i \in \Lambda} X_i$ is defined as the set of all sequences $(x_i)_{i \in \Lambda}$ of elements $x_i \in X_i$.

ii. Groups, rings and fields

Let A be a set, and let $x, y, z, \ldots$ denote arbitrary elements of A.

Definition ii.1. Assume $A \neq \emptyset$. A pair $(e, *)$ of an element $e \in A$ and a map:

$$* : A \times A \ni (x, y) \longmapsto x * y \in A$$

is called an **operation** on A when it satisfies the following conditions:

(i) $x * (y * z) = (x * y) * z$ **(associative)**,
(ii) $e * x = x * e = x$. (We call e the **identity** for this operation.)

An operation is called **commutative** if in addition it satisfies:

(iii) $x * y = y * x$.

Exercise ii.2. For a set with an operation $(e, *)$, the identity is uniquely determined by $*$, because if e' satisfies (ii) we get $e = e * e' = e'$. (So we often denote an operation $(e, *)$ just by $*$, although we always assume the existence of an identity.)

Example ii.3. $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ has two operations $+$ (**addition**) and $\times$ (or $\cdot$, **multiplication**). The identity of $+$ is 0, and that of $\times$ is 1. The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have addition and multiplication, extending those of $\mathbb{N}$.

We will define an operation written as $+$ (**addition**) or one written as $\times$ (or $\cdot$, **multiplication**) on other sets as well. We will always denote the identity for addition (resp. multiplication) by 0 (resp. 1). (The identity 0 of addition is called the **zero element**.) *The name "addition" is only used for commutative operations.*

Definition ii.4. Let A be a set with an operation $*$. For $x \in A$, an element $x^{-1} \in A$ satisfying the following, if it exists, is called an **inverse** of x:

$$x * x^{-1} = x^{-1} * x = e.$$

The element x is called **invertible** if an inverse exists.

Exercise ii.5. If y, y' are both inverse elements of x, we have $y' = y' * (x * y) = (y' * x) * y = y$, hence the inverse element of x is unique if exists.

Definition ii.6. If the inverse of x exists for all $x \in A$, the set A is said to be a **group** under the operation $*$. When the operation is commutative, A is called a **commutative group** or an **abelian group**. When $*$ is denoted by $+$, we call it an **additive group**, and we denote the inverse of x by $-x$, and write $x - y$ for $x + (-y)$.

Example ii.7.
(i) We write 0 for the additive group consisting of one element 0.
(ii) The set of all vectors on a real plane is an additive group.
(iii) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all additive groups.
(iv) For any set A with an operation $*$, if $x, y \in A$ are invertible then $x * y$ also is, because $(y^{-1} * x^{-1}) * (x * y) = e$. Hence the subset $A^{\times} \subset A$ consisting of all invertible elements of A is a group with respect to $*$.

Exercise ii.8. If we define an addition by $(x, y) \longmapsto x + y - 1$ on the set $\mathbb{Z}$, it also becomes an additive group.

Definition ii.9. If a set A with an addition and a multiplication satisfies the following, it is called a **ring**:

(i) A is an additive group,
(ii) $x(y+z) = xy + xz$ **(left-distributive)**,
(iii) $(x+y)z = xz + yz$ **(right-distributive)**.

If the multiplication is commutative, we call A a **commutative ring**.

Example ii.10. (i) The ring consisting of one element 0 is denoted by 0, and called a **zero ring**.
(ii) $\mathbb{Z}$ is a commutative ring.
(iii) The set $\mathbb{R}[X]$of all polynomials in one variable X with coefficients in $\mathbb{R}$ is a commutative ring (**polynomial ring** in one variable over $\mathbb{R}$). In general, for any commutative ring A, we can consider the set $A[X]$ of all polynomials in X with coefficients in A or the set $A[X_1, \ldots, X_n]$ of all polynomials in n variables $X_1, \ldots, X_n$, and they all become commutative rings.
(iv) For an integer $n > 1$, if we define an addition and a multiplication on the set $\{0, 1, \ldots n-1\}$ by the residue of the sum or the product after dividing by n, we obtain a commutative ring. This ring is called a **residue class ring** of $\mathbb{Z}$ mod n, and denoted by $\mathbb{Z}/(n)$.

Exercise ii.11. (i) If A is a ring, then $0 = 1$ in $A \iff A = 0$.
(ii) On the set $\mathbb{R}_{>0}$ of all positive real numbers, we can define a commutative ring structure as follows:

$$\text{addition: } (x, y) \longmapsto xy, \quad \text{multiplication: } (x, y) \longmapsto x^{\log y}.$$

Definition ii.12. (i) An element $a \in A$ of a ring A is called a **unit** when it has an inverse with respect to the multiplication. The set $A^\times$ of all units of A is a group under multiplication (Example ii.7(iv)), and is called the **group of units** or the **multiplicative group** of A.
(ii) If all the elements except for 0 are units in a commutative ring $A \neq 0$, the ring A is called a **field**.

Example ii.13. (i) $\mathbb{Z}^\times = \{1, -1\}$, $\mathbb{R}[X]^\times = \mathbb{R}^\times$.
(ii) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.
(iii) For a prime number p, the residue class ring $\mathbb{Z}/(p)$ of $\mathbb{Z}$ mod p is a field, denoted by $\mathbb{F}_p$. A field consisting is called a **finite field** if its cardinality is finite.

Definition ii.14. (i) If a subset A' of a group A is again a group under the operation of A (in particular $e \in A'$), then A' is called a **subgroup** of A.
(ii) If a subset A' of a ring A is again a ring under the operation $(0, +)$ and $(1, \times)$ of A (in particular $0, 1 \in A'$), A' is called a **subring** of A.

Exercise ii.15. A' is a subgroup of A if and only if $x * y^{-1} \in A'$ for all $x, y \in A'$.

Example ii.16. $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is in turn a subring of $\mathbb{R}$, which is in turn a subring of $\mathbb{C}$. $\mathbb{R}$ is a subring of $\mathbb{R}[X]$.

iii. Modules

Definition iii.1. Let V be a set, and A a set with a multiplication. A map

$$A \times V \ni (a, x) \longmapsto ax \in V$$

satisfying the following is called an **action** of A on V:

(i) $a(bx) = (ab)x$,
(ii) $1x = x$.

Definition iii.2. Let A be a ring. When a set M which has an addition and an action of A satisfies the following, it is called a (left) A**-module**:

(i) M is an additive group;
(ii) $a(x + y) = ax + ay$ for all $a \in A$ and $x, y \in M$;
(iii) $(a + b)x = ax + bx$ for all $a, b \in A$ and $x \in M$.

If A is a field, an A-module is called a **vector space** over A, or an A**-vector space**.

Example iii.3.
(i) The additive group 0 consisting of one element 0 is a module over any ring. It is the only module over the zero ring.
(ii) A ring A is an A-module, by regarding its multiplication as an action on itself.
(iii) Any additive group has an action of $\mathbb{Z}$ and is a $\mathbb{Z}$-module in a unique way.
(iv) For an integer $n \geq 1$, the set A^n of n-tuples of elements of A is an A-module vector space if we define the addition and the action of A componentwise:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n);$$
$$c(a_1, \ldots, a_n) = (ca_1, \ldots, ca_n).$$

More generally, for any A-module M, the set M^n is an A-module under the componentwise addition and A-action.
(v) If A is a subring of a ring B, then (1) B is naturally an A-module, and (2) every B-module is naturally an A-module. (A ring with an A-module structure is called an A**-algebra**.)
(vi) The subset $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ of $\mathbb{R}$ is a vector space over $\mathbb{Q}$. The subset $\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$ of $\mathbb{C}$ is a vector space over $\mathbb{Q}$.
(vii) The subset $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ of $\mathbb{Q}(\sqrt{2})$, the subset $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$ of $\mathbb{Q}(\sqrt{-1})$ are $\mathbb{Z}$-modules.

Definition iii.4. If a subset M' of an A-module M is again an A-module by the addition and the action of A on M, M' is called an A**-submodule** of M. When A is a field, we say M' is a **subspace** of M.

Exercise iii.5. A subset $M' \subset M$ is an A-submodule if and only if it satisfies the following conditions:

(i) $x, y \in M' \Longrightarrow x - y \in M'$;
(ii) $a \in A,\ x \in M' \Longrightarrow ax \in M'$.

Example iii.6.
(i) If M is an A-module, then 0 and M are A-submodules of M.
(ii) If we consider $\mathbb{C}$ as a vector space over $\mathbb{R}$, then $\mathbb{R}$ is a subspace of $\mathbb{C}$.
(iii) If a ring A is a subring of B, then A is an A-submodule of B.

Definition iii.7. When we consider a ring A as a (left) A-module, an A-submodule of A is called a (left) **ideal** of A.

Exercise iii.8. (i) For $n \in \mathbb{Z}$, the set $(n) = \{an \mid a \in \mathbb{Z}\}$ of all multiples of n is an ideal of $\mathbb{Z}$.
(ii) A field K has only two ideals, namely 0 and K.

iii.1. **Generating sets of modules.**

Definition iii.9. Let A be a ring, M an A-module, and X a subset of M.

(i) A finite sum of the form $\sum_{i=1}^{n} a_i x_i$ ($a_i \in A,\ x_i \in X$) is called a **linear combination** of elements of X with coefficients in A. We consider 0 as a linear combination of 0 elements of X, and define 0 as the linear combination of $\emptyset$.
(ii) A relation $\sum_{i=1}^{n} a_i x_i = 0$ expressing 0 as a linear combination of X is called a **linear relation** among the elements of X. In particular, when all the coefficients a_i are 0, it is called a **trivial** linear relation.
(iii) When there is no non-trivial linear relation among the elments of X, the subset X is called **linearly independent**. If it is not linearly independent, it is called **linearly dependent**. The empty set is linearly independent.
(iv) If all $x \in M$ can be written as linear combinations of elements in X, we say that M is **generated** by X, and X is called a **generating set** of M.
(v) The subset of M consisting of all the elements which are linear combinations of elements of X is clearly an A-submodule of M, and is called the A-submodule **generated by** X.
(vi) If M has a linearly independent generating set, M is called a **free A-module**, and a linearly independent generating set is called a **basis** of M.

Example iii.10. In A^n, if we denote by e_i the element whose i-th component is 1 and the rest are 0, then $\{e_1, \ldots, e_n\}$ is a basis of A^n, called the **canonical basis** of A^n.

Lemma iii.11. *Let $X \subset M$ be linearly independent. For any $x \in M$, if x is expressed as a linear combination of elements of X, the expresssion is unique (i.e. if we consider the coefficients of the elements of X that do not appear in the expression as 0, then the coefficients are uniquely determined).*

Proof. If there are two different expresssions, their difference gives a non-trivial linear relation among elements of X. □

Proposition iii.12. *Let $X \subset Y \subset M$.*

(i) *Y: linearly independent $\Longrightarrow$ X: linearly independent.*
(ii) *X: generates M $\Longrightarrow$ Y: generates M.*

Proof. A linear combination of elements of X is also that of Y. □

Exercise iii.13. The A-submodule N generated by X is the minimal A-submodule of M containing X, as any A-submodule of M containing X also contains N.

Definition iii.14. An A-module M is **finite** or **finitely generated** if there is a generating set of M of finite cardinality. The module 0 is finite, being generated by $\emptyset$.

iv. Vector spaces

iv.1. **Existence of a basis.** Let K be a field, and V a vector space over K.

Lemma iv.1. *The following are equivalent:*

(i) *There exists a linear relation* $\sum_{i=1}^{n} a_i x_i = 0$ *with* $a_1 \neq 0$.
(ii) x_1 *can be expressed as a linear combination of* $x_2, \ldots, x_n$.

Proof. (i)⇒(ii): $x_1 = \sum_{i=2}^{n} \left(-\frac{a_i}{a_1}\right) x_i$. (ii)⇒(i): Subtract x_1 from both sides. □

Lemma iv.2. *Let* $X \subset V$, *and* $Y = X \cup \{x\}$ *for* $x \in V \setminus X$.

(i) *If* X *is linearly independent and* x *is not a linear combination of elements of* X, *then* Y *is linearly independent.*
(ii) *If* Y *generates* V *and* x *is a linear combination of* X, *then* X *generates* V.

Proof. (i) If X is linearly independent, in any nontrivial linear relation among elements of Y, the coefficient of x must be nonzero, hence x is a linear combination of elements of Y by Lemma iv.1.

(ii) A linear combination of elements written as linear combinations of elements of X is again a linear combination of elements of X. □

Lemma iv.3. *Assume that* V *is finitely generated. For any generating set* S *of* V *of finite cardinality, there is a subset of* S *which is a basis of* V.

Proof. Let T be a linearly independent subset of S whose cardinality is maximal among such subsets. Then by maximality and Lemma iv.2(i), all the elements of S are linear combinations of elements of T, hence by Lemma iv.2(ii), T is a basis of V. □

Thus we have proved:

Theorem iv.4. *A finitely generated vector space has a basis of finite cardinality.*

iv.2. **Existence of the dimension.** Let V be a finitely generated vector space over K, and fix a basis $T = \{x_1, \ldots, x_n\}$ of V (whose existence is assured by Theorem iv.4).

Lemma iv.5. *If* $S = \{y_1, \ldots, y_k\} \subset V$ $(k \leq n)$ *is linearly independent, we can renumber the indices of* $x_i \in T$ *so that* $U = \{y_1, \ldots, y_k, x_{k+1}, \ldots, x_n\}$ *is a basis of* V.

Proof. (i) We argue by induction on k. It is clear when $k = 0$. For a general k, take a basis $U' = \{y_1, \ldots, y_{k-1}, x_k, \ldots, x_n\}$ by the inductive hypothesis. As U' is a basis, we can write y_k (uniquely, by Lemma iii.11) as a linear combination of elements of U' as:

$$y_k = \sum_{i=1}^{k-1} a_i y_i + \sum_{i=k}^{n} b_i x_i, \tag{1}$$

which gives a linear relation:

$$\sum_{i=1}^{k-1} a_i y_i - y_k + \sum_{i=k}^{n} b_i x_i = 0. \tag{2}$$

If the coefficients b_i of $x_k, \dots, x_n$ are all 0, it contradicts the linear independence of S. Hence we renumber the indices so that the coefficient b_k of x_k is non-zero. We will show that $U = U' \backslash \{x_k\} \cup \{y_k\}$ is a basis of V.

As U' is linearly independent, $U' \backslash \{x_k\}$ is linearly independent. By the uniqueness of expression (1), y_k cannot be a linear combination of $U' \backslash \{x_k\}$, hence $U' \backslash \{x_k\} \cup \{y_k\} = U$ is linearly independent by Lemma iv.2(i).

As U' generates V, $U' \cup \{y_k\}$ generates V. As $b_k \neq 0$ in the relation (2), x_k is a linear combination of elements of $U = U' \cup \{y_k\} \backslash \{x_k\}$ by Lemma iv.1(i)⇒(ii). Hence $U' \cup \{y_k\} \backslash \{x_k\} = U$ generates V by iv.2(ii). □

Proposition iv.6. *Assume that there is a basis $T = \{x_1, \dots, x_n\}$ of V with finite number of elements.*

(i) *If S is a linearly independent subset of V, then $|S| \leq n$. If moreover $|S| = n$, then S is a basis.*
(ii) *If S generates V, then $|S| \geq n$. If moreover $|S| = n$, then S is a basis.*

Proof. (i) The second part follows from the case $k = n$ of Lemma iv.5. If $|S| > n$, any subset of S with n elements is a basis of V, hence the rest of S are linear combination of them and contradicts the linear independence of S by Lemma iv.2(i).

(ii) A subset U of S gives a basis of V by Lemma iv.3, hence using (i) we see that $|T| = n \leq |U|$. Hence $|S| \geq |U| \geq n$, and if $|S| = n$ we have $S = U$. □

By this proposition we obtain:

Theorem iv.7. *If V is finitely generated, then all bases of V have the same number of elements, called the* **dimension** *of V and denoted by $\dim_K V$ or $\dim V$ (We call them* **finite-dimensional***; otherwise it is called* **infinite-dimensional** *and we formally write $\dim V = \infty$).*

Proposition iv.8. *A subspace V' of a finite-dimensional K-vector space V is again finite-dimensional and $\dim V' \leq \dim V$. If $\dim V' = \dim V$ then $V' = V$.*

Proof. By Proposition iv.6(i), any linearly independent subset of V' has cardinality not greater than $\dim V$, hence there is one with maximal cardinality, say T. By maximality and Lemma iv.2(i), any other element of V' is a linear combination of T, i.e. T generates V', hence a basis of V'. Therefore $\dim V' = |T| \leq \dim V$, and if $|T| = \dim V$ then T is a basis of V by Proposition iv.6(i), hence $V' = V$. □

Remark iv.9. The vector space 0 is finite-dimensional as it has the empty set as a basis, and $\dim 0 = 0$. Conversely $\dim V = 0 \Longrightarrow V = 0$.

Exercise iv.10.
(i) $\dim_K(K^n) = n$, and in general V^n has dimension $n \dim V$.
(ii) The polynomial ring $K[X]$ is an infinite-dimensional vector space over K.
(iii) The set $K[X]_{\deg<n}$ of all polynomials in X with degree less than n is an n-dimensional vector space over K, and $\{1, X, X^2, \dots, X^{n-1}\}$ gives its basis.
(iv) $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$.
(v) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, $\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$ are both 2-dimensional vector spaces over $\mathbb{Q}$.

v. Morphisms

v.1. **Homomorphisms.**

Definition v.1. (i) If X, Y are sets with operations $(e_X, *_X), (e_Y, *_Y)$, a map $f : X \to Y$ is a **homomorphism** if $f(x *_X y) = f(x) *_Y f(y)$ and $f(e_X) = f(e_Y)$.
(ii) For a set A with a multiplication and sets X, Y with actions of A, a map $f : X \to Y$ is called **A-equivariant** if it satisfies $f(ax) = af(x)$.

Definition v.2. (i) If X, Y are groups, a homomorphism $f : X \to Y$ is called a **group homomorphism**.
(ii) If X, Y are rings, a homomorphism $f : X \to Y$ with respect to both addition and multiplication is called a **ring homomorphism**.
(iii) If A is a ring and X, Y are A-modules, an A-equivariant homomorphism $f : X \to Y$ is called an **A-homomorphism**, or an **A-linear map**.

Example v.3. (i) The identity map $\mathrm{id}_X : X \to X$ is a homomorphism.
(ii) The composite of two homomorphisms is again a homomorphism.
(iii) The restriction $f|_{X'} : X' \to Y$ of a homomorphism $f : X \to Y$ to a subgroup (resp. subring, A-submodule) X' of X is again a homomorphism.
(iv) For any ring X, there is a unique ring homomorphism $\mathbb{Z} \to X$.
(v) For any ring X, there is a unique ring homomorphism $X \to 0$.
(vi) A ring homomorphism f gives a group homomorphism $f|_{X^\times} : X^\times \to Y^\times$.
(vii) If A is a commutative ring, for an A-module M and $a \in A$, the **a-multiplication** $M \ni x \longmapsto ax \in M$ is an A-linear map.
(viii) The map of **substituting** $x \in A$ into polynomials with A-coefficients $A[X] \ni P(X) \mapsto P(x) \in A$ is surjective, an A-linear map, and a ring homomorphism.
(ix) The complex conjugate $\mathbb{C} \ni x \longmapsto \overline{x} \in \mathbb{C}$ is an automorphism of $\mathbb{C}$ as an $\mathbb{R}$-vector space, but not $\mathbb{C}$-linear. $\mathbb{C} \ni x \longmapsto x + \overline{x} \in \mathbb{R}$ is surjective and $\mathbb{R}$-linear.

v.2. **Categories.**

Definition v.4. A **category** $\mathscr{C}$ is defined as follows:

(i) There is a notion of X being an **object** of $\mathscr{C}$. We write $X \in \mathscr{C}$.
(ii) For any $X, Y \in \mathscr{C}$, there is a set $\mathrm{Hom}_{\mathscr{C}}(X, Y)$ of **morphisms** from X to Y. (A morphism $f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$ is denoted by $f : X \to Y$.)
(iii) $\mathrm{Hom}_{\mathscr{C}}(X, Y) \cap \mathrm{Hom}_{\mathscr{C}}(X', Y') = \emptyset$ unless $X = X'$ and $Y = Y'$.
(iv) For $X, Y, Z \in \mathscr{C}$, there is a map called the **composition** of morphisms:

$$\mathrm{Hom}_{\mathscr{C}}(X, Y) \times \mathrm{Hom}_{\mathscr{C}}(Y, Z) \ni (f, g) \longmapsto g \circ f \in \mathrm{Hom}_{\mathscr{C}}(X, Z),$$

satisfying the **associativity** $h \circ (g \circ f) = (h \circ g) \circ f$.
(v) For all $X \in \mathscr{C}$, there is an **identity morphism** $\mathrm{id}_X \in \mathrm{Hom}_{\mathscr{C}}(X, X)$ of X such that for all $Y \in \mathscr{C}$ and $f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$, we have $f \circ \mathrm{id}_X = \mathrm{id}_Y \circ f = f$.

Definition v.5. (i) A morphism $f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$ of $\mathscr{C}$ is called an **isomorphism** of $\mathscr{C}$ if there exists a $g \in \mathrm{Hom}_{\mathscr{C}}(Y, X)$ (the **inverse** f^{-1} of f) satisfying

$$g \circ f = \mathrm{id}_X, \quad f \circ g = \mathrm{id}_Y.$$

(ii) If an isomorphism $f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$ exists, we say X and Y are **isomorphic** in $\mathscr{C}$, and write $X \cong Y$. If $X \cong Y$ and $Y \cong Z$, then $Y \cong X$ and $X \cong Z$.

Example v.6. The **category of sets Sets** has sets as objects and maps as morphisms. Similarly we can define the category **Groups** of groups and group homorphisms, **Rings** of rings and ring homomorphisms, and A-**Mod** of A-modules and A-homomorphisms for a ring A. For a field K, the category K-**Mod** is the **category of K-vector spaces** $\mathbf{Vect}_K$, and $\mathbf{Ab} = \mathbb{Z}$-**Mod** is the category of abelian groups. There is a category **Top** of topological spaces and continuous maps.

Definition v.7. For an object $X \in \mathscr{C}$ of a category $\mathscr{C}$, a morphism $f : X \to X$ is called an **endomorphism** of X, and an **automorphism** of X if it is an isomorphism. The set $\mathrm{End}_{\mathscr{C}}(X) = \mathrm{Hom}_{\mathscr{C}}(X, X)$ of all endomorphisms of X has an operation $\circ$ with the identity id_X. The set $\mathrm{Aut}_{\mathscr{C}}(X)$ of all automorphisms of X is a group under $\circ$, called the **automorphism group** of X.

Exercise v.8. Let $\mathscr{C} =$ **Groups**, **Rings** or A-**Mod**, and $f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$. Then f is an isomorphism if and only if it is a bijection of sets. For every $Z \in \mathscr{C}$, there are maps:

$$f^* : \mathrm{Hom}(Y, Z) \ni g \longmapsto g \circ f \in \mathrm{Hom}(X, Z),$$
$$f_* : \mathrm{Hom}(Z, X) \ni g \longmapsto f \circ g \in \mathrm{Hom}(Z, Y).$$

We have f: an isomorphism $\iff$ f^*: bijective for all Z $\iff$ f_*: bijective for all Z.

v.3. **Basis as morphisms.** Let A be a ring, and M an A-module. For every $x \in M$, the map $\varphi_x : A \ni a \longmapsto ax \in M$ is A-linear. More generally, every element $X = (x_1, \ldots, x_n) \in M^n$ gives an A-linear map:

$$\varphi_X : A^n \ni (a_1 \ldots, a_n) \longmapsto a_1 x_1 + \cdots + a_n x_n \in M.$$

Proposition v.9. *The following maps are bijections of sets, inverse to each other:*

$$M^n \ni X \longmapsto \varphi_X \in \mathrm{Hom}(A^n, M),$$
$$\mathrm{Hom}(A^n, M) \ni \varphi \longmapsto (\varphi(e_1), \ldots, \varphi(e_n)) \in M^n,$$

where $\{e_1, \ldots, e_n\}$ is the canonical basis of A^n (Example iii.10).

Proof. Immediate from the definitions. □

Therefore, giving a A-linear map from A^n to M is equivalent to choosing n elements (ordered) from M. Using this correspondence, we can translate the definition of linear independence, generating sets and bases as follows.

Lemma v.10. *Let $X = (x_1, \ldots, x_n) \in M^n$ with all x_i distinct, and consider X as a subset $\{x_1, \ldots, x_n\} \subset M$. Let $\varphi_X : A^n \to M$ be the A-linear map defined above.*

(i) *X: linearly independent $\iff$ φ_X: injective.*
(ii) *X: generates M $\iff$ φ_X: surjective.*
(iii) *X: basis of M $\iff$ φ_X: an isomorphism.*

Proposition v.11. *Let $\mathrm{Basis}_n(M) \subset M^n$ be the set of all bases of M consisting of n elements (considered as an ordered set, i.e. we distinguish the permuted bases), and $\mathrm{Isom}(A^n, M)$ be the set of all isomorphisms from A^n to M. Then there is a bijection:*

$$\mathrm{Basis}_n(M) \ni X \longmapsto \varphi_X \in \mathrm{Isom}(A^n, M).$$

If V is an n-dimensional K-vector space for a field K, then $K^n \cong V$.

As composing two isomorphisms gives an isomorphism, the group $\mathrm{Aut}(M)$ acts on $\mathrm{Isom}(A^n, M)$ as follows:

$$\mathrm{Aut}(M) \times \mathrm{Isom}(A^n, M) \ni (f, \varphi) \longmapsto f \circ \varphi \in \mathrm{Isom}(A^n, M).$$

The bijection $\mathrm{Isom}(A^n, M) \ni \varphi \longmapsto X = \big(\varphi(e_1), \dots, \varphi(e_n)\big) \in \mathrm{Basis}_n(M)$ of Proposition v.11 gives $f \circ \varphi \longmapsto f(X)$, so we can consider the above as an action on $\mathrm{Basis}_n(M)$:

$$\mathrm{Aut}(M) \times \mathrm{Basis}_n(M) \ni (f, X) \longmapsto f(X) \in \mathrm{Basis}_n(M).$$

Proposition v.12. (change of bases) *Let M be a free A-module, and fix a basis $X = (x_1, \dots, x_n) \in \mathrm{Basis}_n(M)$.*

(i) *If $f \in \mathrm{Aut}(M)$, then $f(X) = \big(f(x_1), \dots, f(x_n)\big)$ is again a basis of M.*
(ii) *For any basis X' of M, there is a unique $f \in \mathrm{Aut}(M)$ satisfying $f(X) = X'$.*
(iii) *$\mathrm{Aut}(M) \ni f \longmapsto f(X) \in \mathrm{Basis}_n(M)$ is a bijection.*

Proof. (i): Clear by the above action. (ii): By the bijection of Proposition v.11, $f(X) = X' \iff f \circ \varphi_X = \varphi_{X'} \iff f = \varphi_{X'} \circ \varphi_X^{-1}$. (iii) follows from (i),(ii). □

v.4. **Bases and morphisms.** Let A be a ring.

Proposition v.13. *Let $f : M \to N$ be an A-linear map, and X be a subset of M.*

(i) *If f is surjective, then X generates $M \Longrightarrow f(X)$ generates N.*
(ii) *If f is injective, then X: linearly independent $\Longrightarrow f(X)$: linearly independent.*
(iii) *If f is an isomorphism, then X: a basis of $M \iff f(X)$: a basis of N.*

Proof. (i) The image under f of linear combination of elements of X is a linear combination of elements of $f(X)$. (ii) A linear relation among the elements of $f(X)$ is an image under f of a linear relation among the elements of X:

$$\sum_{i=1}^{n} a_i f(x_i) = 0 \Longrightarrow f\Big(\sum_{i=1}^{n} a_i x_i\Big) = 0.$$

Hence, if f is injective and X is linearly independent, it must be a trivial relation. (iii) Combine (i),(ii) and use $X = f^{-1}(f(X))$. □

Corollary v.14. *Let K be a field and V, W be finite-dimensional K-vector spaces. For a K-linear map $f : V \to W$:*

(i) *f: surjective $\Longrightarrow \dim V \geq \dim W$.*
(ii) *f: injective $\Longrightarrow \dim V \leq \dim W$.*
(iii) *f: an isomorphism $\Longrightarrow \dim V = \dim W$.*

Theorem v.15. *If V, W are finite-dimensional, then $V \cong W \iff \dim V = \dim W$.*

Proof. $\Rightarrow$: Corollary v.14(iii). $\Leftarrow$: if $\dim V = \dim W = n$ then $K^n \cong V$, $K^n \cong W$. □

vi. Kernels, rank-nullity

Definition vi.1. For a group homomorphism $f : X \to Y$, the subset $\{x \in X \mid f(x) = e_Y\}$ of X is called the **kernel** of f and denoted by $\operatorname{Ker} f$. For a ring homomorphism or an A-linear map $f : X \to Y$, its **kernel** is that as additive groups.

Exercise vi.2. An A-linear map $f : X \to Y$ is injective if and only if $\operatorname{Ker} f = 0$.

Proposition vi.3. *Consider a homomorphism $f : X \to Y$ of groups/rings/A-modules.*

(i) *For groups,* $\operatorname{Ker} f$, $\operatorname{Im} f$ *are subgroups of* X, Y *respectively.*
(ii) *For rings,* $\operatorname{Ker} f$ *is an ideal of* X *and* $\operatorname{Im} f$ *is a subring of* Y.
(iii) *For A-modules,* $\operatorname{Ker} f$, $\operatorname{Im} f$ *are A-submodules of* X, Y *respectively.*

Proof. (i) By the following:

$$f(x_1) = 0,\ f(x_2) = 0 \Longrightarrow f(x_1 - x_2) = 0,$$
$$y_1 = f(x_1),\ y_2 = f(x_2) \Longrightarrow y_1 - y_2 = f(x_1 - x_2).$$

(ii) By (i) and the following:

$$f(x_2) = 0 \Longrightarrow f(x_1x_2) = f(x_1)f(x_2) = 0,$$
$$y_1 = f(x_1),\ y_2 = f(x_2) \Longrightarrow y_1y_2 = f(x_1x_2),\ f(1) = 1.$$

(iii) By (i) and the following:

$$f(x) = 0 \Longrightarrow f(ax) = af(x) = 0,$$
$$y = f(x) \Longrightarrow ay = af(x) = f(ax).$$

□

Example vi.4. Taking derivatives of polynomials with $\mathbb{R}$-coefficients $\mathbb{R}[X] \ni P(X) \longmapsto P'(X) \in \mathbb{R}[X]$ is a surjective $\mathbb{R}$-linear map, and its kernel is the subspace $\mathbb{R}$ consisting of all constant functions.

Theorem vi.5. (rank-nullity) *Let K be a field. For a K-linear map $f : V \to W$ between finite-dimensional K-vector spaces:*

$$\dim V = \dim(\operatorname{Ker} f) + \dim(\operatorname{Im} f).$$

Proof. Let $\dim V = n$, $\dim(\operatorname{Ker} f) = k$ and $l = n - k$ and take a basis $\{y_1, \ldots, y_k\}$ of $\operatorname{Ker} f$. Then we can take a basis of V of the form $T = \{y_1, \ldots, y_k, x_1, \ldots, x_l\}$ by Lemma iv.5. Let V' be the subspace of V generated by $\{x_1, \ldots, x_l\}$, and restrict f to $f|_{V'} : V' \to W$. As T is linearly independent $\operatorname{Ker} f|_{V'} = \operatorname{Ker} f \cap V' = 0$, hence $f|_{V'}$ is injective (Proposition vi.2), and any element in the image of V is the image of an element of V', hence $f|_{V'}$ is a surjection onto $\operatorname{Im} f$. Therefore $V' \cong \operatorname{Im} f$ and $\dim(\operatorname{Im} f) = \dim V' = l$. □

Corollary vi.6. *Let $f : V \to W$ be K-linear with $\dim V = \dim W < \infty$, then:*

$$f\text{: an isomorphism} \iff f\text{: injective} \iff f\text{: surjective.}$$

Proof. f: injective $\iff \dim(\operatorname{Ker} f) = 0 \iff \dim(\operatorname{Im} f) = \dim V \iff f$: surjective. (Use respectively Proposition vi.2, Theorem vi.5 and Lemma iv.8.) □

Preliminaries II: Rings

vii. Prime factorization and PIDs

In what follows, by *rings* we always mean *commutative rings* unless otherwise stated.

vii.1. **Domains and prime factorization.** Let A be a ring, and $a, b, c, \ldots \in A$.

Definition vii.1. An element b is **divisible** by a if $\exists c \in A,\ b = ac$, and we write $a \mid b$. We say a is a **divisor** of b, and b is a **multiple** of a. If $a \mid b$ and $b \mid a$, then a and b are called **associate** to each other.

Definition vii.2. If $a, b \neq 0$ and $ab = 0$, then a, b are called **zero divisors**. If there is no zero divisor in a ring $A \neq 0$, the ring A is called an **integral domain**, or a **domain**.

Exercise vii.3. (i) A subring of a domain is a domain. Every field is a domain.
(ii) In a domain, if $a \neq 0$, then $ab = ac \Longrightarrow b = c$.
(iii) If A is a domain, a, b : associate $\iff \exists c \in A^\times,\ b = ac$.

In the rest of this section, let A be a domain.

Definition vii.4. (i) A divisor of a is called **proper** if it is not a unit nor an associate of a.
(ii) An element of A, which is neither 0 nor a unit, is called **irreducible** if it does not have any proper divisors.
(iii) An element $p \in A$, which is neither 0 nor a unit, is called **prime** if it satisfies $p \mid ab \Longrightarrow p \mid a$ or $p \mid b$.

If a, b are associates, we have $x \mid a \iff x \mid b$, and also $a \mid x \iff b \mid x$, therefore the associate elements are not distinguished as far as the divisibility is concerned. In particular, an associate of a unit (resp. irreducible, prime) element is also a unit (resp. irreducible, prime).

Exercise vii.5. (i) The irreducibles of $\mathbb{Z}$ are prime numbers $\times(\pm 1)$.
(ii) A field does not have any prime nor irreducible elements.

Proposition vii.6. *In a domain, all primes are irreducible.*

Proof. If a prime p factorizes as $p = ab$, as $p \mid ab$ we have $p \mid a$ or $p \mid b$. Without loss of generality assume $p \mid a$. Then $a = pc$ for some c, therefore $p = pcb$. Then $cb = 1$ by Exercise vii.3(ii), thus b is a unit. Therefore p does not have any proper divisor. □

Proposition vii.7. *In a domain, the factorization of an element into a product of primes, if exists, is unique up to associate.*

Proof. It is enough to show that, for primes p_i, q_j $(1 \leq i \leq n,\ 1 \leq j \leq m)$, if $p_1 \cdots p_n$ and $q_1 \cdots q_m$ are associates, then $n = m$ and by appropriately changing the order p_i and q_i are associates. We prove this by induction on $\max\{n, m\}$. It is trivial when $\max\{n, m\} = 1$, so assume $\max\{n, m\} > 1$, say $n > 1$. Then $p_1 \mid q_1 \cdots q_m$, and as p_1 is prime, there exists a j with which we have $p_1 \mid q_j$, but as p_1, q_j are primes and therefore irreducibles, p_1, q_j must be associates. Therefore, by Exercise vii.3(ii), $p_2 \cdots p_n$ and $q_1 \cdots q_{j-1} q_{j+1} \cdots q_m$ are associates, but as $\max\{n-1, m-1\} < \max\{n, m\}$ the proposition is proven by the inductive hypothesis. □

Definition vii.8. If every element of a domain A, except 0 and units, is a product of primes, A is called a **unique factorization domain (UFD)**. (Indeed the factorization is unique up to associate by Proposition vii.7.)

Definition vii.9. If A is a UFD and $a_1, \dots, a_n \in A$, then for a prime p let p^m be its maximal power dividing all of $a_1, \dots, a_n$. Then $p^m \neq 1$ for only finitely many p up to associates, and their product, well-defined up to associates, is called the **greatest common divisor (GCD)** of $a_1, \dots, a_n$. We say a, b are **coprime** if their GCD is 1.

vii.2. **Principal ideals, maximal and prime ideals.** Let A be a ring. In the following, we always regard A as an A-module by means of the multiplication of A. (Example iii.3(ii)). Recall that an A-submodule of A is called an **ideal** of A (Definition iii.7).

Definition vii.10. For $a \in A$, the set $\{ax \mid x \in A\}$ of all multiples of a is an ideal of A. We denote this ideal by (a), and call it the **principal ideal** generated by a.

Exercise vii.11. For a ring A, its ideal is free if and only if it is a principal ideal generated by an element which is not a zero divisor.

Exercise vii.12. (i) $a = 0 \iff (a) = 0$.
(ii) $a \in A^\times \iff (a) = A$.
(iii) For an ideal I, $(a) \subset I \iff a \in I$.
(iv) $(a) \supset (b) \iff a \mid b$.
(v) $(a) = (b) \iff a, b$: associate.

If we assume A is a domain, we have:

(vi) $A \neq (a) \supsetneqq (b) \iff a$: a proper divisor of b.
(vii) $(a) = (b) \iff b = ac,\ c \in A^\times$.

Definition vii.13. An ideal $I \subsetneqq A$ is called:

(i) **prime** if the following holds: $a, b \notin I \Longrightarrow ab \notin I$,
(ii) **maximal** if no ideal other than A contains I as a proper subset.

The set of all prime (resp. maximal) ideals of A is denoted by $\mathrm{Spec}(A)$ (resp. m-$\mathrm{Spec}(A)$).

Exercise vii.14. (i) $A = 0 \Longrightarrow \mathrm{Spec}(A) = \emptyset$.
(ii) A : field $\iff 0 \in$ m-$\mathrm{Spec}(A)$. A : domain $\iff 0 \in \mathrm{Spec}(A)$.
(iii) In a domain, $A \ni a$: prime $\iff (a) \in \mathrm{Spec}(A) \backslash \{0\}$.
(iv) If A is a subring of B, then $Q \in \mathrm{Spec}(B) \Longrightarrow Q \cap A \in \mathrm{Spec}(A)$. More generally, if $f : A \to B$ is a ring homomorphism, then $Q \in \mathrm{Spec}(B) \Longrightarrow f^{-1}(Q) \in \mathrm{Spec}(A)$.

Definition vii.15. For ideals I_1, I_2 of A, the set $\{x + y \mid x \in I_1,\ y \in I_2\}$ is an ideal of A, containing I_1 and I_2. It is called the **sum** of I_1 and I_2, and denoted by $I_1 + I_2$.

Example vii.16. In $A = \mathbb{Z}$, $(6) + (15) = (3)$. (In general, $(a) + (b)$ is a principal ideal generated by the g.c.d. of a, b.)

Proposition vii.17. m-$\mathrm{Spec}(A) \subset \mathrm{Spec}(A)$.

Proof. If a maximal ideal I is not prime, as $I \neq A$, $\exists a, b \notin I,\ ab \in I$. Then $I + (b)$ contains I as a proper subset, therefore equals A. Hence $\exists d \in I,\ \exists c \in A,\ I + (b) \ni 1 = d + bc$, and as $ad, ab \in I$ we have $a = ad + abc \in I$, a contradiction. □

vii.3. **Principal ideal domains.**

Definition vii.18. A domain is called a **principal ideal domain (PID)** if all of its ideals are principal.

Example vii.19. A field is a PID.

Proposition vii.20. *Let A be a PID, and $a \in A$. Then:*

(i) *a: irreducible* $\iff$ $(a) \in$ m-Spec(A),
(ii) *a: irreducible* $\iff$ *a : prime.*

Proof. (i) Follows from Exercise vii.12(vi).

(ii) $\Leftarrow$: Proposition vii.6. $\Rightarrow$: Use (i), Proposition vii.17, and Exercise vii.14(iii). □

Proposition vii.21. *In a PID, every element, except 0 and units, is decomposed as a product of irreducible elements.*

Proof. Let S be the set of products of irreducible elements in A. Assume $\exists a_0 \notin S,\ a_0 \neq 0,\ a_0 \notin A^\times$. As a_0 is not an irreducible, it is a product of two proper divisors. If they both belong to S then $a_0 \in S$, so at least one of them, say a_1, does not belong to S. By repeating the same procedure on a_1 we get $a_2 \notin S$, a proper divisor of a_1. Continuing to get a sequence $a_0, a_1, a_2, \cdots$, by Exercise vii.12(vi) we have $(a_i) \subsetneqq (a_{i+1})$ $(\forall i \in \mathbb{N})$. On the other hand, consider the ideal $I = \bigcup_{i=0}^{\infty}(a_i)$ of A (see Exercise vii.22 below). As A is a PID, $I = (a)$ for some $a \in A$. As $a \in I$ we have $a \in (a_i)$ for some i, but then $(a) \subset (a_i) \subsetneqq (a_{i+1}) \subset (a)$ is a contradiction. □

Exercise vii.22. For an increasing sequence $I_0 \subset I_1 \subset I_2 \subset \cdots$ of ideals in A, the union $I = \bigcup_{i=0}^{\infty} I_i$ is an ideal of A.

Theorem vii.23. *PID $\Longrightarrow$ UFD.*

Proof. Follows from Proposition vii.21 and Proposition vii.20(ii). □

vii.4. **Euclidean domains.**

Definition vii.24. A domain A is called a **Euclidean domain** if there exists a map $f : A \to \mathbb{N} \cup \{-\infty\}$ satisfying the following condition:

$$a, b \in A,\ a \neq 0 \Longrightarrow \exists q, r \in A\ \ b = aq + r,\ f(r) < f(a).$$

Exercise vii.25. (i) $\mathbb{Z}$ is Euclidean. In fact, $f(x) = |x|$ satisfies the condition.
(ii) For a field K, a one-variable polynomial ring $K[X]$ with coefficients in K is Euclidean. In fact, $f(P) = \deg P$ suffices.

Proposition vii.26. *Euclidean domain $\Longrightarrow$ PID.*

Proof. For an ideal $I \neq 0$ of a Euclidean domain A, take a non-zero element a of I such that $f(a)$ is minimal. Then $\forall b \in I$, $\exists q, r \in A\ \ b = aq + r,\ f(r) < f(a)$, but as $r = b - aq \in I$, we have $r = 0$ by minimality of $f(a)$, therefore b is a multiple of a, hence $I = (a)$. □

Theorem vii.27. (Prime factorization of integers) *$\mathbb{Z}$ is a PID, therefore a UFD.*

Proof. Follows from Exercise vii.25(i), Proposition vii.26 and Theorem vii.23. □

viii. Quotient rings

viii.1. **Quotient structures.**

Definition viii.1. Let X be a set, and Z a subset of $X \times X$. We write $x \sim y$ when $(x, y) \in Z$, and call it a **relation** on X. It is called an **equivalence relation** if the following conditions are satisfied:

(i) $x \sim x$ **(reflexive)**,
(ii) $x \sim y \Longrightarrow y \sim x$ **symmetric**,
(iii) $x \sim y,\ y \sim z \Longrightarrow x \sim z$ **(transitive)**.

For an element $x \in X$, a subset $\{y \in X \mid x \sim y\}$ of X is called an **equivalence class** of x, and is denoted $\overline{x}$, and x is called a **representative (element)** of the class $\overline{x}$. By (i),(ii),(iii), X is partitioned into mutually disjoint equivalence classes. The set of equivalence classes is called the **quotient set** of X by the relation $\sim$.

Proposition viii.2. (i) *If Y is a subgroup of an additive group X, the relation*

$$x \sim y \iff x - y \in Y$$

is an equivalence relation, whose quotient set is denoted by X/Y. The addition of representatives defines an addition on X/Y, which becomes an additive group.

(ii) *If Y is an ideal of a ring X, then the multiplication of representatives defines a multiplication on X/Y, which becomes a ring.*

(iii) *If Y is an A-submodule of an A-module X, then the A-action on the representatives defines an A-action on X/Y, which becomes an A-module.*

Proof. (i) First, the relation $\sim$ is an equivalence relations because $x - x = 0 \in Y$,

$$\begin{aligned} x - y \in Y &\implies y - x = -(x - y) \in Y, \\ x - y, y - z \in Y &\implies x - z = (x - y) + (y - z) \in Y. \end{aligned}$$

Secondly, the operation $\overline{x} + \overline{y} = \overline{x + y}$ on X/Y is well-defined regardless of the choice of representatives (and $\overline{0}$ is the zero element) because

$$\begin{aligned} x \sim x',\ y \sim y' &\implies x - x',\ y - y' \in Y \\ &\implies (x + y) - (x' + y') = (x - x') + (y - y') \in Y \\ &\implies x + y \sim x' + y'. \end{aligned}$$

Thus we have the addition on X/Y, and it is a group as $\overline{-x}$ gives the inverse of $\overline{x}$.

(ii) Also for the multiplication, as Y is an ideal of X,

$$\begin{aligned} x \sim x',\ y \sim y' &\implies x - x',\ y - y' \in Y \\ &\implies xy - x'y' = (x - x')y + x'(y - y') \in Y \\ &\implies xy \sim x'y'. \end{aligned}$$

Thus $\overline{x} \cdot \overline{y} = \overline{xy}$ is well-defined with $\overline{1}$ as the identity, and X/Y becomes a ring.

(iii) Also for the A-action, as Y is an A-submodule of X, we have

$$x \sim x' \Longrightarrow x - x' \in Y \Longrightarrow ax - ax' = a(x - x') \in Y \Longrightarrow ax \sim ax',$$

thus the A-action $a\overline{x} = \overline{ax}$ is well-defined, and X/Y becomes an A-module. □

Definition viii.3. The X/Y in Proposition viii.2(i),(ii),(iii) are called respectively **quotient group**, **quotient ring**, **quotient A-module** of X by Y. The surjection $X \to X/Y$ defined by $x \longmapsto \overline{x}$ is called the **canonical surjection**, which is clearly a homomorphism with the kernel Y. We also write $\overline{x}$ as $x \bmod Y$.

Example viii.4. (i) $X/0 \cong X$, $X/X \cong 0$.

(ii) For an ideal (n) $(n \geq 1)$ of $\mathbb{Z}$, the quotient ring $\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ is "the ring of residues modulo n". We also denote $\overline{k} = k \bmod (n)$ as $k \bmod n$.

Theorem viii.5. (The homomorphism theorem) *For a (group/ring/A-) homomorphism $f : X \to Y$, there is a canonical isomorphism $X/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$.*

Proof. For a homomorphism f, if we denote by $\overline{x}$ the equivalence class of x in $X/\mathrm{Ker}\, f$:

$$\overline{x} = \overline{y} \iff x - y \in \mathrm{Ker}\, f \iff f(x) = f(y),$$

therefore the map:

$$\overline{f} : X/\mathrm{Ker}\, f \ni \overline{x} \longmapsto f(x) \in \mathrm{Im}\, f$$

is well-defined and injective. As $\overline{f}$ is clearly surjective, it is bijective. Also, as f is a homomorphism, the bijection $\overline{f}$ is a homomorphism by $\overline{f}(\overline{0}) = f(0) = 0$ and:

$$\overline{f}(\overline{x} + \overline{y}) = \overline{f}(\overline{x+y}) = f(x+y) = f(x) + f(y) = \overline{f}(\overline{x}) + \overline{f}(\overline{y}),$$

thus a group isomorphism. Similarly if f is a ring (resp. A-) homomorphism, then the bijection $\overline{f}$ is a ring (resp. A-) homomorphism, hence a ring (resp. A-) isomorphism. □

Example viii.6. The map from $\mathbb{R}[X]$ to $\mathbb{C}$ defined as substituting $\sqrt{-1}$ into X:

$$\mathbb{R}[X] \ni P(X) \longmapsto P(\sqrt{-1}) \in \mathbb{C}$$

is a surjective ring homomorphism, whose kernel is the ideal $(X^2 + 1)$. Thus we have the following ring isomorphism (in fact this is the definition of $\mathbb{C}$):

$$\mathbb{R}[X]/(X^2+1) \ni a + b\overline{X} \longmapsto a + b\sqrt{-1} \in \mathbb{C}.$$

Exercise viii.7. For a general (non-commutative group) G and its subgroup H, in order to define the quotient group G/H, we need the following condition on H:

$$x \in G,\ y \in H \Longrightarrow x * y * x^{-1} \in H.$$

Such a subgroup is called a **normal subgroup** of G, and we write $G \rhd H$. If $f : X \to Y$ is a homomorphism of general groups, then $\mathrm{Ker}\, f$ is a normal subgroup of X and $\mathrm{Im}\, f$ is a subgroup of Y, and $X/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$.

viii.2. **Ideals and quotient rings.** For an A-homomorphism $f : X \to Y$ between A-modules, let S be the set of all A-submodules of X that contain $\mathrm{Ker}\, f$, and T the set of all A-submodules of $\mathrm{Im}\, f$. As the image of an A-submodule of X is always an A-submodule of $\mathrm{Im}\, f$, and the inverse image of an A-submodule of $\mathrm{Im}\, f$ is always an A-submodule of X containing $\mathrm{Ker}\, f$, we have the following two maps:

$$\Phi : S \ni I \longmapsto f(I) \in T,$$
$$\Psi : T \ni J \longmapsto f^{-1}(J) \in S.$$

Proposition viii.8. *The two maps Φ, Ψ are inverse to each other, hence bijective.*

Proof. These maps clearly preserve the inclusion relations, and as $f(f^{-1}(J)) = J$, we have $\Phi \circ \Psi = \mathrm{id}$. Also, observing that $\Psi \circ \Phi(I) = f^{-1}(f(I)) \supset I$, as we have $f(x) \in f(I)$ for all $x \in f^{-1}(f(I))$, $\exists y \in I,\ f(y) = f(x)$. Therefore, as $x - y \in \mathrm{Ker}\, f \subset I$ shows that $x = y + (x - y) \in I$, we have $f^{-1}(f(I)) \subset I$, hence $\Psi \circ \Phi = \mathrm{id}$. □

Proposition viii.9. *For a surjective homomorphism $f : A \to B$, above Φ, Ψ give one-to-one correspondence between (i) the prime ideals of A that contain* $\mathrm{Ker}\, f$ *and the prime ideals of B, and (ii) the maximal ideals of A that contain* $\mathrm{Ker}\, f$ *and the maximal ideals of B.*

Proof. As Φ, Ψ preserve the inclusion relations, the maximals correspond to maximals. We have $P \in \mathrm{Spec}(A) \Longrightarrow f(P) \in \mathrm{Spec}(B)$, because if $a, b \notin f(P)$, then choosing $a' \in f^{-1}(a),\ b' \in f^{-1}(b)$, we have

$$a', b' \notin P \Longrightarrow a'b' \notin P \Longrightarrow ab = f(a'b') \notin f(P).$$

Exercise vii.14(iv) shows $Q \in \mathrm{Spec}(B) \Longrightarrow f^{-1}(Q) \in \mathrm{Spec}(A)$. □

Corollary viii.10. *Let A be a ring, and I be an ideal of A.*

(i) $I \in \mathrm{Spec}(A) \iff A/I$ *: domain.*
(ii) $I \in \text{m-Spec}(A) \iff A/I$ *: field.*

Proof. Applying Proposition viii.9 to the canonical surjection $A \ni a \longmapsto \overline{a} \in A/I$, we see that $I \subset A$ and $0 \subset A/I$ correspond. Now use Exercise vii.14(ii). □

Example viii.11. Considering the quotient ring $\mathbb{Z}/(n)$ of $\mathbb{Z}$ by an ideal (n) $(n \geq 1)$,

$$\mathbb{Z}/(n) : \text{field} \iff \mathbb{Z}/(n) : \text{domain} \iff n : \text{prime}.$$

When n is a prime p, the field $\mathbb{Z}/(p)$ is denoted by $\mathbb{F}_p$ (Example ii.13(ii)).

viii.3. **Characteristic of a field.** Let K be a field. The image of the unique ring homomorphism $\varphi : \mathbb{Z} \to K$ (dtermined by $1 \mapsto 1$) is, being a subring of the field, a domain, and hence the kernel of φ is a prime ideal of $\mathbb{Z}$ (Corollary viii.10(i)).

Definition viii.12. When $\mathrm{Ker}\, \varphi = 0$, K is said to have **characteristic 0**, and when $\mathrm{Ker}\, \varphi = (p)$ for a prime p, K is said to have **characteristic** p. The characteristic of K is denoted by $\mathrm{char}\, K$.

Identifying $\mathbb{Z}$ or $\mathbb{F}_p$ with a subring of K by homomorphism theorem,

$$\mathrm{char}\, K = 0 \iff \mathbb{Z} \cong \mathrm{Im}\, \varphi \subset K \iff K : \text{an extension field of } \mathbb{Q},$$
$$\mathrm{char}\, K = p \iff \mathbb{F}_p \cong \mathrm{Im}\, \varphi \subset K \iff K : \text{an extension field of } \mathbb{F}_p.$$

(Thus an arbitrary field can be regarded as an extension field of $\mathbb{Q}$ or $\mathbb{F}_p$. In each case, we call $\mathbb{Q}, \mathbb{F}_p$ the **prime field** of K.)

ix. Algebras over rings

ix.1. **Algebras over rings.**

Definition ix.1. Let A be a ring. A pair (B, τ) of a ring B and a ring homomorphism $\tau : A \to B$ is called an **A-algebra**. We often omit τ from the notation. By a **morphism** $f : (B, \tau) \to (B', \tau')$ of A-algebras we mean a ring homomorphism $f : B \to B'$ such that $\tau' = f \circ B$. We denote the **category of A-algebras** and A-algebra homomorphisms by A-**Alg** and its set of morphisms by $\mathrm{Hom}_{A\text{-}\mathbf{Alg}}(B, B')$.

Equivalently, an A-algebra is a ring B which is also an A-module, such that the A-linear map $A \ni a \longmapsto a \cdot 1 \in B$ is a ring homormorphism. A ring homomorphism between A-algebras is a morphism of A-algebras if it is also an A-linear map. The set $\mathrm{Hom}_{A\text{-}\mathbf{Alg}}(B, B')$ is a subset of the set of A-linear maps $\mathrm{Hom}_A(B, B') = \mathrm{Hom}_{A\text{-}\mathbf{Mod}}(B, B')$. In A-**Alg**, a morphism is an isomorphism if and only if it is an isomorphism either as sets, rings, or A-modules.

Remark ix.2. This definition makes sense for non-commutative rings B as well (but it is better to assume that A is commutative): e.g. $\mathrm{End}_A(M) := \mathrm{Hom}_A(M, M)$ for an A-module M is an A-algebra but non-commutative in general (Section xiii.2).

Example ix.3.
(i) Every ring has a unique structure of $\mathbb{Z}$-algebra, and every ring homomorphism is a morphism of $\mathbb{Z}$-algebras. Therefore $\mathbb{Z}$-**Alg** = **Rings**.
(ii) An extension field F of K (Definition 2.1) is a K-algebra, and K-homomorphisms (Definition 3.1) between extension fields are morphisms of K-algebras.
(iii) Polynomial rings $A[X]$, $A[X_1, \ldots, X_n]$ are A-algebras (next subsection). More generally, if A is a subring of a ring B, then B is an A-algebra.
(iv) If B is an A-algebra, every B-module is naturally an A-module (compare Example iii.3(v)). In particular, every B-algebra is naturally an A-algebra.
(v) A quotient ring A/I for an ideal $I \subset A$ is an A-algebra. More generally, for any A-algebra B, its quotient rings are A-algebras.
(vi) If a subring of an A-algebra (B, τ) contains the image $\tau(A)$ of A, (or equivalent ly, is an A-submodule), it is called an **A-subalgebra** of B. The image of a morphism of A-algebras $B \to B'$ is an A-subalgebra of B'.

Definition ix.4. If an A-algebra is finitely generated as an A-module, it is called a **finite** A-algebra. (In the case of extension fields, a *finite extension* (Definition 2.2).)

Exercise ix.5. For a ring A and its ideal I ($\neq 0$, $\neq A$), the quotient ring A/I is a finite A-algebra, but not a free A-module (it has no linearly independent element).

ix.2. **Polynomial rings.** Let A be a ring.

Definition ix.6.
(i) The set $A[X]$ of all polynomials of one variable X with coefficients in A is a ring with the usual addition and multiplication, and called the **polynomial ring** over A. We naturally consider A as a subring of $A[X]$. The ring of multivariable polynomials $A[X_1, \ldots, X_n]$ for $n \geq 1$ is defined similarly.
(ii) An element $P \in A[X]$ is called **monic** if its coefficient of the highest term is 1.
(iii) An element $a \in A$ is called a **root** of $P \in A[X]$ if $P(a) = 0$.

Exercise ix.7. (i) Let (B, τ) be an A-algebra. We extend τ to $A[X] \ni P \mapsto \tau P \in B[X]$, where $\tau P \in B[X]$ is obtained by applying τ to the coefficients of P, and $(B[X], \tau)$ is an $A[X]$-algebra. If A is a subring of B, $A[X]$ is a subring of $B[X]$.

(ii) For every A-algebra (B, τ), a morphism of A-algebras $f : A[X] \to B$ is uniquely determined by $x = f(X) \in B$, and it has to be the morphism of "substituting x" (cf. Example v.3(viii)):

$$f_x : A[X] \ni P(X) \longmapsto \tau P(x) \in B.$$

As $x \in B$ can be arbitrary, the map $x \mapsto f_x$ gives the inverse to the bijection:

$$\mathrm{Hom}_{A\text{-}\mathbf{Alg}}(A[X], B) \ni f \longmapsto f(X) \in B.$$

(iii) If A is a domain, then $A[X]$ is a domain and $A[X]^\times = A^\times$.

Proposition ix.8. *Let K be a field.*

(i) *The ring $K[X]$ is a PID. Every ideal of $K[X]$ is generated by a monic.*
(ii) *The number of roots of $P \in K[X]\backslash\{0\}$ is not greater than* $\deg P$.

Proof. (i) The first part follows from Exercise vii.25(ii) and Theorem vii.26. As $K[X]^\times = K^\times = K\backslash\{0\}$, every $P \in K[X]\backslash\{0\}$ is associate to a monic with the same degree.

(ii) For $a \in K$, we have $P = (X - a)Q + R$, $\deg R < 1$ (Exercise vii.25(ii)). As $\deg R < 1$ means $R \in K$, by substituting X by a, we have $P(a) = R$. Therefore:

$$a : \text{root of } P \iff R = 0 \iff (X - a) \mid P,$$

hence the number of roots of P is equal to the number of monics with degree one diving P. As $K[X]$ is a UFD, it is at most $\deg P$ by the uniqueness of prime factorization. □

Definition ix.9. The **multiplicity** of a root $a \in K$ of $P \in K[X]$ is the maximal integer n satisfying $(X - a)^n \mid P$. A root is called a **multiple root** if $n > 1$.

ix.3. **Field of fractions.** Let A be a domain.

Definition ix.10. In the product set $A \times (A \setminus \{0\})$, the relation $\sim$ defined as

$$(a, b) \sim (c, d) \iff ad = bc$$

is an equivalence relation. Denoting the equivalence class of (a, b) by $\frac{a}{b}$, the operations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

on the quotient set $\mathrm{Frac}(A)$ are well defined (independent of the choice of representatives) and $\mathrm{Frac}(A)$ becomes a field, called the **field of fractions** of A. We have an injective ring homomorphism $A \ni x \longmapsto \frac{x}{1} \in \mathrm{Frac}(A)$, with which we regard $\mathrm{Frac}(A)$ as an A-algebra, or even A as a subring of $\mathrm{Frac}(A)$.

Example ix.11. $\mathbb{Q}$ is (defined as!) the field of fractions of $\mathbb{Z}$.

Exercise ix.12. The A-algebra $\mathrm{Frac}(A)$ is determined up to a unique isomorphism by the following property: every ring homomorphism $f : A \to B$ satisfying $f(A\backslash\{0\}) \subset B^\times$ extends uniquely to a morphism $\mathrm{Frac}(A) \to B$ of A-algebras. In other words, every A-algebra (B, τ) with $\tau(A \setminus \{0\}) \subset B^\times$ is a $\mathrm{Frac}(A)$-algebra in a unique way. In particular, if a field K is an A-algebra, then there is a unique morphism $\mathrm{Frac}(A) \to K$ of A-algebras, necessarily injective. The fraction field of a field K is K itself.

x. Noetherian rings (for Section xi only)

Definition x.1. A ring A is called **noetherian** if all of its ideals are finite A-modules.

Example x.2. PID is noetherian.

Proposition x.3. *For a ring A, the following are equivalent:*

(i) *A is noetherian;*
(ii) *For any chain $I_0 \subset I_1 \subset I_2 \subset \cdots$ of ideals of A, there exists $k \in \mathbb{N}$ and $I_k = I_{k+1} = \cdots$.*
(iii) *Any nonempty set X consisting of ideals of A has a maximal element with respect to the inclusions.*

Proof. (i)⇒(ii): For a chain $I_0 \subset I_1 \subset I_2 \subset \cdots$, the union $I = \bigcup_{i=0}^{\infty} I_i$ is an ideal of A, hence finite. Take an I_k which contains the finite generating set of I. (ii)⇒(iii): If X does not have a maximal element, for all $I_0 \in X$, there is an $I_1 \in X$ with $I_0 \subset I_1$ and $I_0 \neq I_1$. Repeating this, we obtain a chain $I_0 \subset I_1 \subset I_2 \subset \cdots$ with $I_i \neq I_{i+1}$ for all i. (iii)⇒(i): Take any ideal I of A. The set X of all finite ideals contained in I is nonempty as $0 \in X$, hence has a maximal element J by (iii). If $J \neq I$, there is an $a \in I \setminus J$ and $J \subset J + (a) \in X$ which contradicts the maximality by $J \neq J + (a)$. Hence $J = I$ and I is finite. □

Proposition x.4. *Let A be a noetherian ring. Let M be an A-module and N its A-submodule. If M is finite, then so is N.*

Proof. We prove by induction on the cardinality n of a generating set of M. If $n = 1$, there is a surjective A-homomorphism $f : A \ni a \longmapsto ax \in M$ for the generator x of M, hence $N = f(J)$ for some ideal J of A by Proposition viii.8. As A is noetherian J is finite, and the images under f of the generators of J generates N.

For $n > 1$, let $x_1, \ldots, x_n$ be a generating set of M. Consider $M' = \{ax_1 \mid a \in A\}$ and the surjective A-homomorphism $f : M \to M/M'$. As $f(x_2), \ldots, f(x_n)$ generates M/M', the A-submodule $f(N)$ of M/M' is finite by the inductive hypothesis. Also the kernel of the surjective A-homomorphism $f|_N : N \to f(N)$ is $N \cap M'$, which is, being an A-submodule of M', finite by the case $n = 1$. Take a generating set $y_1, \ldots, y_k$ of $N \cap M'$ and a generating set $f(y_{k+1}), \ldots, f(y_m)$ of $f(N)$, and for any $x \in N$, write $f(x) \in f(N)$ as $\sum_{i=k+1}^{m} a_i f(y_i)$ and write $x - \sum_{i=k+1}^{m} a_i y_i \in \operatorname{Ker} f|_N = N \cap M'$ as $\sum_{i=1}^{k} a_i y_i$. Then $x = \sum_{i=1}^{m} a_i y_i$, which shows that $y_1, \ldots, y_m$ generates N. □

Theorem x.5. (Hilbert's basis theorem) *If A is noetherian, then so is $A[X]$. (In particular, so is $A[X_1, \ldots, X_n]$; e.g. $\mathbb{Z}[X_1, \ldots, X_n]$ or $K[X_1, \ldots, X_n]$ for a field K.)*

Proof. If I is an ideal of $A[X]$ that is not finitely generated, then we can inductively choose $P_1, P_2, \ldots$ so that if I_{i-1} is the ideal generated by $P_1, \ldots, P_{i-1}$ and $I_0 := 0$ then $P_i \in I \setminus I_i$ and $\deg P_i$ is minimal in $I \setminus I_{i-1}$. In particular $i < j$ implies $\deg P_i \leq \deg P_j$. Let a_i be the leading coefficient of P_i, and J the ideal of A generated by all a_i. As A is noetherian J is generated by $a_1, \ldots, a_{n-1}$ for some n and $a_n = \sum_{i=1}^{n-1} x_i a_i$ for $x_i \in A$. Let $d_i := \deg P_n - \deg P_i$ and $Q := \sum_{i=1}^{n-1} x_i X^{d_i} P_i \in I_{n-1}$. Then $P_n - Q \notin I_{n-1}$, but the leading coefficients of P_n, Q agree and $\deg(P_n - Q) < \deg P_n$, contradiction. □

xi. Polynomial rings over UFDs (for Lectures 12, 20 only)

Lemma xi.1. *Let A be a UFD. For $P = \sum_{i=0}^{n} a_i X^i \in A[X]\setminus\{0\}$, its* **content** *$c(P) \in A$ is the GCD of $a_0, \dots, a_n$ (well-defined up to associates). Then $c(PQ) = c(P)c(Q)$.*

Proof. If $a \in A$ then $c(aP) = a \cdot c(P)$. If $c(P) = a$ then $a^{-1}P \in A[X]$ and $c(a^{-1}P) = 1$. Thus it suffices to show $c(P) = c(Q) = 1 \Longrightarrow c(PQ) = 1$. Let $P = \sum_{i=0}^{m} a_i X^i$, $Q = \sum_{j=0}^{n} b_j X^j$, and $PQ = \sum_{k=0}^{m+n} c_k X^k$ with $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. For any prime $p \in A$, choose i and j minimal such that $a_i, b_j \notin (p)$. Then $a_i b_j \notin (p)$, and in the formula for c_{i+j} every term is in (p) except for $a_i b_j$, hence $c_{i+j} \notin (p)$. Thus $c(PQ) = 1$. □

Proposition xi.2. (Gauss' Lemma) *Let A be a UFD and $K = \mathrm{Frac}(A)$. If $P \in A[X]$ is not divisible by any non-unit of A, then:*

$$P\text{: irreducible in } A[X] \iff P \text{ : irreducible in } K[X].$$

Proof. $\Leftarrow$: If P is irreducible in $K[X]$, then $P = QR$ in $A[X]$ implies Q (or R) is in $A[X] \cap K^\times = A \cap K^\times$, thus $Q \in A^\times$ by hypothesis. $\Rightarrow$: If $P \in A[X]$ is reducible in $K[X]$, i.e. $P = QR$ for $Q, R \in K[X] \setminus K$, then by clearing the denominators we have $aP = bQ'R'$ where $a, b \in A \setminus \{0\}$ and $Q', R' \in A[X]$ with $c(Q') = c(R') = 1$. Hence $a \cdot c(P) = c(aP) = c(bQ'R') = b \cdot c(Q'R') = b$, therefore $a \mid b$. Thus $P = (b/a)Q'R'$ is reducible in $A[X]$. □

Proposition xi.3. *If A is a UFD, then the polynomial ring $A[X]$ is also a UFD. (In particular, so is $A[X_1, \dots, X_n]$; e.g. $\mathbb{Z}[X_1, \dots, X_n]$ or $K[X_1, \dots, X_n]$ for a field K.)*

Proof. A prime p of A is a prime of $A[X]$, because if $p \mid PQ$ for $P, Q \in A[X]$ then $p \mid c(PQ) = c(P)c(Q)$, thus $p \mid c(P)$ (or $p \mid c(Q)$), i.e. $p \mid P$. Let $K = \mathrm{Frac}(A)$. If $P \in A[X]$ is a prime of $K[X]$ and $c(P) = 1$ then P is a prime of $A[X]$, because if $P \mid QR$ for $Q, R \in A[X]$, then $P \mid Q$ (or $P \mid R$) in $K[X]$, hence $aQ = bPS$ for some $a, b \in A \setminus \{0\}$ and $S \in A[X]$ with $c(S) = 1$, thus $b/a = c(Q) \in A$ and $P \mid (a/b)Q \mid Q$ in $A[X]$. Prime decompostion of $P \in A[X] \setminus \{0\}$ in $K[X]$ gives $aP = bP_1 \cdots P_n$ where $a, b \in A \setminus \{0\}$ and $P_i \in A[X]$ are primes in $K[X]$ with $c(P_i) = 1$. Then $b/a = c(P) \in A$, and we have $P = cP_1 \cdots P_n$ with $c \in A$. Now factoring c into primes in A gives a prime factorization of P in $A[X]$ (recall $A[X]^\times = A^\times$ by Exercise ix.7(iii)). □

Lemma xi.4. *Let R be a UFD and $K := \mathrm{Frac}(R)$. Let $B := R[x_1, \dots, x_n]$ be the polynomial ring in n variables. Let $a_1, \dots, a_n \in B$ be the elementary symmetric polynomials of x_i (Proposition 16.3) and $A := R[a_1, \dots, a_n] \subset B$. If $L := \mathrm{Frac}(A) = K(a_1, \dots, a_n)$ and $F := \mathrm{Frac}(B) = K(x_1, \dots, x_n)$, then $B \cap L = A$ in F.*

Proof. As $x_i \in B$ are all roots of $P := X^n + \sum_{i=1}^{n} (-1)^i a_i X^{n-i} \in A[X]$, the x_i^n is an A-linear combination of $1, x_i, \dots, x_i^{n-1}$, and B is a finite A-module generated by $\{x_1^{d_1} \cdots x_n^{d_n} \mid 0 \le d_i < n\}$. For $x \in B$, the A-submodule of B generated by $\{1, x, x^2, \dots\}$ is a finite A-module by Proposition x.4 (as A is noetherian by Theorem x.5), hence generated by $1, x, \dots, x^{m-1}$ for some m and $x^m = \sum_{i=1}^{m-1} a_i x^i$ for $a_i \in A$. As A is a UFD (Proposition xi.3), if $x \in B \cap L$ then $x = \frac{a}{b}$ with $a, b \in A$ coprime, but $a^m = \sum_{i=1}^{m-1} a_i a^i b^{m-i}$ shows $b \mid a^m$, thus $b \in A^\times$ and $x \in A$. □

xii. Zorn's lemma (for Lecture 8 only)

Theorem xii.1. (The axiom of choice) *Let $\{X_i\}_{i\in\Lambda}$ be a family of sets indexed by a set Λ. If $X_i \neq \emptyset$ for every $i \in \Lambda$, then $\prod_{i\in\Lambda} X_i \neq \emptyset$.*

We state two equivalent reformulations of the axiom of choice (treated in Part IID Logic and Set Theory).

Definition xii.2. Let X be a set and $\leq$ a relation on X (Definition viii.1). We call X a (**partially**) **ordered set** with the **order** $\leq$ if the following are satisfied:

(i) $x \leq x$ **(reflexive)**,
(ii) $x \leq y,\ y \leq x \Longrightarrow x = y$ **(antisymmetric)**,
(iii) $x \leq y,\ y \leq z \Longrightarrow x \leq z$ **(transitive)**.

If moreover for all pairs $x, y \in X$ either $x \leq y$ or $y \leq x$ holds, then X is called a **totally ordered set**.

Example xii.3.
(i) $\mathbb{N}, \mathbb{Z}$ and $\mathbb{R}$ are totally ordered.
(ii) A subset of an ordered set has a naturally inherited order.
(iii) For a set X and a set Y whose elements are subsets of X, we can define a natural order on Y by inclusion, i.e. $A \leq B \iff A \subset B$ for $A, B \in Y$.

Definition xii.4. Let X be an ordered set.

(i) An element $x \in X$ satisfying $x \leq y \Longrightarrow x = y$ is called a **maximal element** of X. An $x \in X$ satisfying $y \leq x \Longrightarrow x = y$ is called a **minimal element** of X.
(ii) Let $Y \subset X$ be a subset. An element $x \in X$ is called an **upper bound** of Y if $y \leq x$ for all $y \in Y$.
(iii) If $X \neq \emptyset$ and all non-empty totally ordered subset of X has an upper bound in X, then X is called **inductive**.

Theorem xii.5.
(i) **(Zorn's lemma)** *Every inductive set has a maximal element.*
(ii) **(The well-ordering principle)** *Every set can be* **well-ordered***, i.e. can define an order on it so that its every non-empty subset has a minimal element.*

Proposition xii.6. *For a ring A and an ideal $I \neq A$, there exists a maximal ideal which contains I. In particular (taking $I = 0$),* $\text{m-Spec}(A) \neq \emptyset$ *if $A \neq 0$.*

Proof. The set of all ideals containing I and not equal to A is inductive with the order by inclusions (shown as in Exercise vii.22), therefore has a maximal element. □

Exercise xii.7. The axiom of choice was used in the proofs of Proposition vii.21, Proposition x.3(ii)⇒(iii) and Theorem x.5 to choose infinite sequences (it is not needed to prove Proposition vii.21 for Euclidean domains). Rewrite these proofs using the Zorn's lemma.

Proposition xii.8. *Every vector space V has a basis.*

Proof. The set of all linearly independent subsets of V is inductive with the order by inclusions, hence has a maximal element, which has to be a generating set of V. □

Preliminaries III: More Linear Algebra

xiii. Determinants (for Section xiv only)

xiii.1. **Volume Forms.** Let A be a ring, and M be an A-module.

Definition xiii.1. Let $M_1, \dots, M_n, N$ be A-modules. A map $\Phi : M_1 \times \cdots \times M_n \to N$ is called a **A-multilinear map** if it satisfies the following conditions:

(i) $\Phi(x_1, \dots, x_i + y_i, \dots, x_n) = \Phi(x_1, \dots, x_i, \dots, x_n) + \Phi(x_1, \dots, y_i, \dots, x_n)$;
(ii) $\Phi(x_1, \dots, ax_i, \dots, x_n) = a\Phi(x_1, \dots, x_i, \dots, x_n) \quad (\forall a \in A)$.

The set $\mathrm{Lin}(M_1, \dots, M_n; N)$ of all such maps is an A-module by the operations on their values. It is called a **(multilinear) form** if $N = A$, and an **n-fold** form on M if $M = M_1 = \cdots = M_n$. An n-fold form Φ on M is called **alternating** if it satisfies

(iii) $\Phi(x_1, \dots, x_n) = 0$ if $x_i = x_j$ for $i \neq j$.

If $M \cong A^n$, then an alternating n-fold form on M is called a **volume form** on M, and we denote the A-module of all volume forms on M by $\mathrm{Vol}(M)$.

Lemma xiii.2. *For an alternating multilinear form Φ:*

(i) $\Phi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -\Phi(x_1, \dots, x_j, \dots, x_i, \dots, x_n)$.
(ii) *For a bijection $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$* **(permutation)***:*

$$\Phi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = s(\sigma)\Phi(x_1, \dots, x_n).$$

(Here $s(\sigma) = \prod_{1 \le j < i \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \in \{\pm 1\}$ is called the **sign** *of σ.)*
(iii) *If $y_j = \sum_{i=1}^n a_{ij} x_i$ $(1 \le j \le n)$, then:*

$$\Phi(y_1, \dots, y_n) = \Big(\sum_{\sigma \in S_n} s(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} \Big) \Phi(x_1, \dots, x_n).$$

(Here S_n is the set of all permutations σ of $\{1, \dots, n\}$ and called the **symmetric group** *of n letters.)*

Proof. (i): Using (i),(iii) of the definition, LHS $= \Phi(x_1, \dots, x_i + x_j, \dots, x_j, \dots, x_n)$, RHS $= \Phi(x_1, \dots, x_i + x_j, \dots, x_i, \dots, x_n)$, hence LHS+RHS $= \Phi(x_1, \dots, x_i + x_j, \dots, x_i + x_j, \dots, x_n) = 0$.

(ii): Apply (i) repeatedly. (The sign is seen to coincide with the given formula by repeating the exchange of (i) from $x_{\sigma(n)}$ until there are no indices greater or equal to $\sigma(n)$ in the left hand side.)

(iii): $\Phi(y_1, \dots, y_n) = \Phi\Big(\sum_{i=1}^n a_{i1} x_i, \dots, \sum_{i=1}^n a_{in} x_i \Big) = \sum_{i_1, \dots, i_n} a_{i_1 1} \cdots a_{i_n n} \Phi(x_{i_1}, \dots, x_{i_n})$
$= \Big(\sum_{\sigma \in S_n} s(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} \Big) \Phi(x_1, \dots, x_n)$. □

Proposition xiii.3. *We have $\mathrm{Vol}(M) \cong A$ as A-modules.*

Proof. Fix a basis $(x_1, \dots, x_n)$ of M. Then the A-linear map:

$$\mathrm{Vol}(M) \ni \Phi \longmapsto \Phi(x_1, \dots, x_n) \in A$$

is an isomorphism, because Lemma xiii.2(iii) shows that the value of Φ for all $(y_1, \dots, y_n)$ is determined by the value $\Phi(x_1, \dots, x_n) \in A$ which we can choose arbitrarily. □

xiii.2. **Determinants.** Let A be a ring. For A-modules M, N, the set $\mathrm{Hom}(M, N)$ of all A-linear maps from M to N is an A-module if we define $f_1 + f_2, af$ for $a \in M$ and $f, f_1, f_2 \in \mathrm{Hom}(M, N)$ as

$$(f_1 + f_2)(x) = f_1(x) + f_2(x), \quad (af)(x) = af(x).$$

This makes the maps f^*, f_* of Exercise v.8 A-linear. If we consider the composition $\circ$ on $\mathrm{End}(M) = \mathrm{Hom}(M, M)$ as a multiplication, then $\mathrm{End}(M)$ is a ring, non-commutative in general (in fact an A-algebra), called the **endomorphism ring** of M. Note that the group $\mathrm{End}(M)^\times$ is equal to $\mathrm{Aut}(M)$.

Now let $M \cong A^n$. Then $\mathrm{End}(M)$ is an A-algebra (non-commutative in general) and $\mathrm{End}(M) \cong A^{n^2}$ as an A-module (the bijection in Proposition v.9 is A-linear). Take $f \in \mathrm{End}(M)$. For a $\Phi \in \mathrm{Vol}(M)$,

$$\Phi \circ f : M^n \ni (x_1, \dots, x_n) \longmapsto \Phi(f(x_1), \dots, f(x_n)) \in A$$

is again a volume form. Thus we have a map:

$$\mathrm{Vol}(M) \ni \Phi \longmapsto \Phi \circ f \in \mathrm{Vol}(M)$$

which is A-linear, hence an a-multiplication for some $a \in A$ by Proposition xiii.3.

Definition xiii.4. The element $\det f \in A$ satisfying $\Phi \circ f = (\det f) \cdot \Phi$ is called the **determinant** of f.

Proposition xiii.5. (i) $\det(\mathrm{id}) = 1$, $\det(f \circ g) = \det f \cdot \det g$.
(ii) $f \in \mathrm{Aut}(M) \Longrightarrow \det f \in A^\times$.
(iii) $\det : \mathrm{Aut}(M) \to A^\times$ *is a surjective group homomorphism.*

Proof. (i): $\Phi \circ (f \circ g) = (\Phi \circ f) \circ g$, $\Phi \circ \mathrm{id} = \Phi$. (ii): $f \in \mathrm{Aut}(M) \Rightarrow \det f \cdot \det(f^{-1}) = 1$. (iii): It is a group homomorphism by (i),(ii). For $a \in A^\times$, if we consider an $f \in \mathrm{Aut}(M)$ mapping a basis $X = (x_1, \dots, x_n)$ to $X' = (ax_1, x_2 \dots, x_n)$, then $\det f = a$. □

Remark xiii.6. As $\Phi \circ (f + g) \neq (\Phi \circ f) + (\Phi \circ g)$, the map $\det : \mathrm{End}(M) \to A$ is not A-linear.

Theorem xiii.7. *Let K be a field, and V a K-vector space with $\dim_K V = n$.*

(i) *If $\Phi \in \mathrm{Vol}(V) \setminus \{0\}$ and $X \in M^n$, then $\Phi(X) \neq 0 \iff X \in \mathrm{Basis}(V)$.*
(ii) *If $f \in \mathrm{End}(V)$, then $f \in \mathrm{Aut}(V) \iff \det f \neq 0$.*

Proof. (i): $\Rightarrow$: If $X \notin \mathrm{Basis}(V)$, then X is linearly dependent by Proposition iv.6(i), hence some x_i is a non-trivial linear combination of other x_j's, and $\Phi(X) = 0$ as Φ is alternating. $\Leftarrow$: As $\Phi \neq 0$, there exists $X_0 \in V^n$ such that $\Phi(X_0) \neq 0$. By $\Rightarrow$ we have $X_0 \in \mathrm{Basis}(V)$, hence by Proposition v.12(ii), we have $f(X_0) = X$ for $f = \varphi_X \circ \varphi_{X_0}^{-1} \in \mathrm{Aut}(V)$. Hence $\Phi(X) = (\Phi \circ f)(X_0) = (\det f) \cdot \Phi(X_0)$ and Proposition xiii.5(ii) gives $\Phi(X) \neq 0$.

(ii): $\Rightarrow$: Proposition xiii.5(ii). $\Leftarrow$: Take a $\Phi \in \mathrm{Vol}(V) \setminus \{0\}$ and $X_0 \in V^n$ with $\Phi(X_0) \neq 0$. If we let $f(X_0) = X$, then $\Phi(X) = (\Phi \circ f)(X_0) = (\det f)\Phi(X_0) \neq 0$. (i) shows that $X_0, X \in \mathrm{Basis}(V)$, hence $f = \varphi_X \circ \varphi_{X_0}^{-1} \in \mathrm{Aut}(V)$ (Proposition v.12(ii)). □

xiv. Diagonalization (for Lecture 17 only)

xiv.1. **Direct sum.** Let A be a ring.

Definition xiv.1. Let $M_1, \dots, M_n$ be A-modules. We define componentwise operations on the direct product set $M_1 \times \cdots \times M_n$:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n),$$
$$a(x_1, \dots, x_n) = (ax_1, \dots, ax_n).$$

This is an A-module, denoted by $\bigoplus_{i=1}^n M_i = M_1 \oplus \cdots \oplus M_n$ and called the **direct sum** of $M_1, \dots, M_n$. In particular, the direct sum $M \oplus \cdots \oplus M$ of n copies of M is denoted by M^n (Exercise iii.3(iii)). In the following, we treat the case $n = 2$ for simplicity.

The following two maps are injective A-linear maps (**canonical injections**):

$$i_1 : M_1 \ni x_1 \longmapsto (x_1, 0) \in M_1 \oplus M_2, \quad i_2 : M_2 \ni x_2 \longmapsto (0, x_2) \in M_1 \oplus M_2.$$

We regard M_1, M_2 as subspaces of $M_1 \oplus M_2$ by these injections. We have:

Lemma xiv.2. *For any A-module N, the A-linear map*

$$\mathrm{Hom}(M_1 \oplus M_2, N) \ni f \longmapsto (f \circ i_1,\ f \circ i_2) \in \mathrm{Hom}(M_1, N) \oplus \mathrm{Hom}(M_2, N)$$

is an isomorphism, whose inverse is given by

$$\mathrm{Hom}(M_1, N) \oplus \mathrm{Hom}(M_2, N) \ni (f_1, f_2) \longmapsto f \in \mathrm{Hom}(M_1 \oplus M_2, N),$$

where $f(x_1, x_2) := f_1(x_1) + f_2(x_2)$.

Definition xiv.3. For $f_1 \in \mathrm{Hom}(M_1, N_1)$ and $f_2 \in \mathrm{Hom}(M_2, N_2)$, the map:

$$M_1 \oplus M_2 \ni (x_1, x_2) \longmapsto (f_1(x_1), f_2(x_2)) \in N_1 \oplus N_2$$

is A-linear, denoted by $f_1 \oplus f_2$, and called the **direct sum** of f_1, f_2.

Exercise xiv.4. If f_1, f_2 are isomorphisms, then so is $f_1 \oplus f_2$. In particular, if $M_1 \cong A^n$ and $M_2 \cong A^m$, then $M_1 \oplus M_2 \cong A^{m+n}$.

Exercise xiv.5. If $i_k^M : M_k \to M_1 \oplus M_2,\ i_k^N : N_k \to N_1 \oplus N_2$ $(k = 1, 2)$ are canonical injections, then $f = f_1 \oplus f_2$ is the unique A-linear map satisfying the following:

$$f \circ i_1^M = i_1^N \circ f_1, \quad f \circ i_2^M = i_2^N \circ f_2.$$

Definition xiv.6. Let M_1, M_2 be A-submodules of M. If the A-linear map

$$M_1 \oplus M_2 \ni (x_1, x_2) \longmapsto x_1 + x_2 \in M$$

is an isomorphism, we write $M = M_1 \oplus M_2$ (a **direct sum decomposition** of M). Let $M = M_1 \oplus M_2,\ N = N_1 \oplus N_2$ and $f \in \mathrm{Hom}(M, N)$. If there are $f_k \in \mathrm{Hom}(M_k, N_k)$ $(k = 1, 2)$ with $f|_{M_k} = f_k$, then we write $f = f_1 \oplus f_2$.

Remark xiv.7. There are maps f which are not decomposed into direct sums, i.e. the map $\mathrm{Hom}(M_1, N_1) \oplus \mathrm{Hom}(M_2, N_2) \ni (f_1, f_2) \longmapsto f_1 \oplus f_2 \in \mathrm{Hom}(M_1 \oplus M_2, N_1 \oplus N_2)$ is not surjective.

Exercise xiv.8. Let $M \cong A^n$ and $X = \{x_1, \dots, x_n\}$ be its basis. If we write $M_i = \{ax_i \mid a \in A\}$ for the submodule generated by $\{x_i\}$, then

$$\bigoplus_{i=1}^{n} M_i = M_1 \oplus \cdots \oplus M_n \ni (y_1, \dots, y_n) \longmapsto \sum_{i=1}^{n} y_i \in M$$

is an isomorphism, i.e. gives a direct sum decomposition of M into $M_1, \dots, M_n$. Conversely, for any direct sum decomposition of M into n pieces of submodules M_i with $M_i \cong A$, choosing a basis of M_i gives a basis of M.

xiv.2. **Linear transformations and diagonalization.** Let K be a field.

Definition xiv.9. We will consider the pairs (V, φ) consisting of a finite dimensional K-vector space V and its linear transformation $\varphi \in \mathrm{End}(V)$.

(i) For two pairs (V, φ), (W, ψ), we will call a K-linear map $f \in \mathrm{Hom}(V, W)$ a **morphism** of pairs when it satisfies $f \circ \varphi = \psi \circ f$, and write $f : (V, \varphi) \to (W, \psi)$.
(ii) If a morphism f of pairs is an isomorphism as a K-linear map, then its inverse f^{-1} is also a morphism of pairs, and we call f an **isomorphism** of pairs.

Example xiv.10. When V is 1-dimensional, any $\varphi \in \mathrm{End}(V)$ is an a-multiplication for some $a \in K$. In this case we write (V, φ) as (V, a) and call it an **elementary pair**.

Definition xiv.11. (i) For a pair (V, φ), we call a pair (W, ψ) consisting of a subspace W of V and $\psi \in \mathrm{End}(W)$ a **subpair** of (V, φ) if $\varphi|_W = \psi$, and we write $(W, \psi) \subset (V, \varphi)$. An inclusion $i : W \to V$ gives a morphism of pairs $i : (W, \psi) \to (V, \varphi)$. In particuar we will study the **elementary subpairs**.
(ii) For two pairs (V_1, φ_1), (V_2, φ_2), we denote $(V_1 \oplus V_2,\ \varphi_1 \oplus \varphi_2)$ by $(V_1, \varphi_1) \oplus (V_2, \varphi_2)$, and call it the **direct sum** of (V_1, φ_1), (V_2, φ_2).
(iii) If two subpairs $(V_1, \varphi_1), (V_2, \varphi_2)$ of (V, φ) satisfy $V = V_1 \oplus V_2,\ \varphi = \varphi_1 \oplus \varphi_2$, we write $(V, \varphi) = (V_1, \varphi_1) \oplus (V_2, \varphi_2)$, a **direct sum decomposition** of (V, φ).

Proposition xiv.12. *For a pair (V, φ) and $a \in K$:*

$$(V, \varphi) \text{ has an elementary subpair of the form } (V_0, a) \iff \det(\varphi - a \cdot \mathrm{id}) = 0.$$

Proof. As a subspace V_0 with $\dim V_0 = 1$ is generated by some non-zero $x \in V$:

$$\begin{aligned} \exists (V_0, a) \subset (V, \varphi) &\iff \exists x \in V \backslash \{0\}\ \ \varphi(x) = ax \iff \mathrm{Ker}\,(\varphi - a \cdot \mathrm{id}) \neq 0 \\ &\iff \varphi - a \cdot \mathrm{id} \notin \mathrm{Aut}(V) \iff \det(\varphi - a \cdot \mathrm{id}) = 0 \end{aligned}$$

(The last two equivalences follow respectively from Corollary vi.6, Theorem xiii.7.) □

Definition xiv.13. For a pair (V, φ), the polynomial in one variable X with K-coefficients $P_\varphi(X) = \det(\varphi - X \cdot \mathrm{id})$ is called the **characteristic polynomial** of (V, φ). If (V_0, a) is an elementary subpair of (V, φ), then a is called an **eigenvalue** of (V, φ), and a non-zero element of V_0 is called an **eigenvector** of (V, φ) for the eigenvalue a.

Proposition xiv.14. *The following are equivalent:*

(i) *(V, φ) decomposes into direct sum of n elementary subpairs.*
(ii) *There is a basis of V consisting of eigenvectors of (V, φ).*

A pair (V, φ) satisfying this condition is called **diagonalizable** *or* **semisimple**.

Proof. $\Rightarrow$: If $(V,\varphi) = (V_1, a_1) \oplus \cdots \oplus (V_n, a_n)$, a non-zero element $x_i \in V_i$ from each V_i gives a basis consisting of eigenvectors of (V,φ).

$\Leftarrow$: For a basis $\{x_1, \ldots, x_n\}$ consisting of eigenvectors of (V,φ), if we let a_i be the eigenvalue of x_i and V_i be the subspace generated by $\{x_i\}$, then by the direct sum decomposition $V = V_1 \oplus \cdots \oplus V_n$ of V, we have $\varphi = a_1 \oplus \cdots \oplus a_n$. □

Exercise xiv.15. If we consider a-multiplication for $a \in K$, any $x \in V\backslash\{0\}$ is an eigenvector for the eigenvalue a, hence (V, a) is diagonalizable.

xiv.3. **Eigenvalues and minimal polynomials.** For $\varphi \in \mathrm{End}(V)$, consider the ring homomorphism of "substituting φ into polynomials with coefficients in K":

$$f_\varphi : K[X] \ni P \longmapsto P(\varphi) \in \mathrm{End}(V)$$

(set $f_\varphi(1) = \mathrm{id}$ to make it into a ring homomorphism). This f_φ is K-linear and $\mathrm{Im}\, f_\varphi$ is finite-dimensional, being a subspace of $\mathrm{End}(V)$ (Lemma iv.8), and as $K[X]$ is infinite-dimensional, $\mathrm{Ker}\, f_\varphi \neq 0$. Therefore, by Proposition ix.8(i), $\mathrm{Ker}\, f_\varphi$ is a principal ideal (Q_φ) generated by $Q_\varphi \neq 0$, and $\mathrm{Im}\, f_\varphi$ is a subring of $\mathrm{End}(V)$ isomorphic to $K[X]/(Q_\varphi)$.

Definition xiv.16. The monic generator Q_φ (Proposition ix.8(ii)) of $\mathrm{Ker}\, f_\varphi$ is called the **minimal polynomial** of f over K. (It has minimal degree among the polynomials with coefficients in K which have φ as a "root", but is not necessarily irreducible.)

Proposition xiv.17. *If $a \in K$, then a : an eigenvalue of $\varphi \iff Q_\varphi(a) = 0$.*

Proof. Recall that, by Proposition xiv.12 and Corollary vi.6,

$$a : \text{an eigenvalue of } \varphi \iff \mathrm{Ker}\,(\varphi - a\cdot\mathrm{id}) \neq 0 \iff \varphi - a\cdot\mathrm{id} \notin \mathrm{Aut}(V).$$

$\Rightarrow$: If $Q_\varphi(a) \neq 0$ then $Q_\varphi \notin (X-a)$ in $K[X]$. As $(X-a) \in \text{m-Spec}(K[X])$, we have $(Q_\varphi) + (X-a) = K[X]$. Hence there exist $R_1, R_2 \in K[X]$ with $Q_\varphi R_1 + (X-a)R_2 = 1$. Applying f_φ, we have $(\varphi - a\cdot\mathrm{id}) \circ R_2(\varphi) = \mathrm{id}_V$, thus $\varphi - a\cdot\mathrm{id} \in \mathrm{Aut}(V)$.

$\Leftarrow$: If $Q_\varphi(a) = 0$, then $Q_\varphi = (X-a)\cdot R$ for some $R \in K[X]$, so by applying f_φ, we have $0 = (\varphi - a\cdot\mathrm{id}) \circ R(\varphi)$. Now if $\varphi - a\cdot\mathrm{id} \in \mathrm{Aut}(V)$, composing its inverse shows $0 = R(\varphi)$, hence $Q_\varphi \mid R$, which contradicts $\deg R < \deg Q_\varphi$. □

Remark xiv.18. The same proposition holds for the characteristic polynomial P_φ of φ (Proposition xiv.12), but in general $Q_\varphi \neq P_\varphi$. ($Q_\varphi \mid P_\varphi$ by definition, and they have same sets of roots, but their multiplicities can be different.)

xv. Matrices (for Lecture 21 only)

Let K be a field and $n, m \geq 1$ be integers. By Proposition v.9, a K-linear map $f \in \mathrm{Hom}(K^n, K^m)$ is determined by $f(e_1), \ldots, f(e_n)$, where e_i are the canonical basis of K^n (Example iii.10). If we set $f(e_j) = (a_{1j}, \ldots, a_{mj})$ for $1 \leq j \leq n$, then f is uniquely represented by the mn elements $a_{ij} \in K$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$.

Definition xv.1. The arrangement of mn elements in K in the following form is called an m by n **matrix** over K:

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

The a_{ij} is called the (i,j)**-entry** of the matrix (a_{ij}). A matrix with all entries equal to 0 is denoted by 0. The set of all m by n matrices over K is denoted by $M_{m,n}(K)$.

Thus we have a bijection:

$$\mathrm{Hom}(K^n, K^m) \ni f \longmapsto (a_{ij}) \in M_{m,n}(K).$$

Addition and scalar multiplication on $\mathrm{Hom}(K^n, K^m)$ corresponds to the entrywise addition and scalar multiplications of matrices. Therefore we define the K-vector space structure on $M_{m,n}(K)$ by entrywise operations.

Proposition xv.2. *We have* $\mathrm{Hom}(K^n, K^m) \cong M_{m,n}(K)$ *as K-vector spaces.*

By Proposition v.9, we have $\mathrm{Hom}(K^n, K^m) \cong (K^m)^n \cong K^{mn}$ as K-vector spaces, hence $M_{m,n}(K)$ is mn-dimensional. This gives a canonical basis for $M_{m,n}(K)$: a matrix with only (i,j)-entry equal to 1 and rest of the entries equal to 0 is called a **matrix element** and denoted by (1_{ij}).

Consider a system of m linear equations with n variables with coefficients in K:

$$\sum_{j=1}^{n} a_{ij} X_j = b_i \quad (a_{ij}, b_i \in K,\ 1 \leq i \leq m,\ m \leq n).$$

We will write the above equation using the matrix $(a_{ij}) \in M_{m,n}(K)$ as follows:

$$(a_{ij})(X_j) = (b_i).$$

If (a_{ij}) correspond to $f \in \mathrm{Hom}_K(K^n, K^m)$, then $a_j = (a_{1j}, \ldots, a_{mj}) = f(e_j)$ for $1 \leq j \leq n$ and the equation is $f((X_j)) = (b_i)$. Thus $(X_j) \in K^n$ is a solution if and only if $(X_j) \in f^{-1}((b_i))$.

Proposition xv.3. *Consider* $(a_{ij})(X_j) = (0)$ *and let* $a_j = (a_{1j}, \ldots, a_{mj})$.

(i) *There is a solution* $(X_j) \neq (0)$ *if and only if* $\{a_1, \ldots, a_n\}$ *is linearly dependent.*
(ii) *Assume* $m < n$. *Then there always exists a solution* $(X_j) \neq (0)$.

Proof. If (a_{ij}) correspond to $f \in \mathrm{Hom}_K(K^n, K^m)$, then the equation is $f((X_j)) = f(\sum_{j=1}^n X_j e_j) = \sum_{j=1}^n X_j a_j = 0$. (ii) follows from (i) and Proposition iv.6(i). □

xvi. Matrices and linear maps (for Lecture 22 only)

xvi.1. **Product of matrices.** If $f \in \mathrm{Hom}(K^m, K^l)$, $g \in \mathrm{Hom}(K^n, K^m)$ and $f \circ g \in \mathrm{Hom}(K^n, K^l)$ correspond to $(a_{ij}) \in M_{l,m}(K)$, $(b_{jk}) \in M_{m,n}(K)$ and $(c_{ik}) \in M_{l,n}(K)$, then we have:

$$c_{ik} = \sum_{j=1}^{m} a_{ij} b_{jk}.$$

Definition xvi.1. For $(a_{ij}) \in M_{l,m}(K)$, $(b_{jk}) \in M_{m,n}(K)$, the matrix $(c_{ik}) \in M_{l,n}(K)$ with $c_{ik} := \sum_{j=1}^{m} a_{ij} b_{jk}$ is called their **product**, written as $(c_{ik}) = (a_{ij})(b_{jk})$.

The associativity and distributivity of addition and multiplication follow from those for $\mathrm{Hom}(K^n, K^m)$. In particular, the set $M_n(K) := M_{n,n}(K)$ of all n by n matrices is a ring, isomorphic to the endomorphism ring $\mathrm{End}(K^n) = \mathrm{Hom}(K^n, K^n)$ of K^n.

Definition xvi.2. An n by n matrix is called a **square matrix** of degree n. The set $M_n(K) := M_{n,n}(K)$ of all square matrices of degree n over K is a ring by the entrywise addition and the product, and the multiplicative identity is the matrix

$$(\delta_{ij}) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

called the **identity matrix**. The symbol δ_{ij} (**Kronecker's delta**) is generally used for the (i, j)-entry of the identity matrix.

The identity matrix corresponds to the identity map $\mathrm{id} \in \mathrm{End}(K^n)$. The automorphism group $\mathrm{Aut}(K^n)$ corresponds to the group of units in $M_n(K)$.

Definition xvi.3. A square matrix $\alpha \in M_n(K)$ is called **invertible** if there exists an $\alpha^{-1} \in M_n(K)$ which satisfies $\alpha\alpha^{-1} = \alpha^{-1}\alpha = (\delta_{ij})$, in which case α^{-1} is called the **inverse matrix** of α. The group $M_n(K)^\times$ of all n by n invertible matrices is called the **general linear group** of degree n over K, and is denoted by $\mathrm{GL}_n(K)$.

If $n = 1$, then $M_1(K) \cong K$ and $\mathrm{GL}_1(K) \cong K^\times$. If $n > 1$, then $M_n(K)$ is a non-commutative ring and $\mathrm{GL}_n(K)$ is a non-commutative group.

xvi.2. **Matrices representing linear maps.** Let V_1, V_2 be vector spaces over K of dimensions n, m respectively. Choosing a basis $Y = (y_j)$ of V_1 and a basis $X = (x_i)$ of V_2, we have isomorphisms $\varphi_Y : K^n \to V_1$, $\varphi_X : K^m \to V_2$ (Lemma v.10(iii)). If $f \in \mathrm{Hom}(V_1, V_2)$, defining $f' = \varphi_X^{-1} \circ f \circ \varphi_Y$, we have a commutative diagram:

$$\begin{array}{ccc} K^n & \xrightarrow{f'} & K^m \\ {\scriptstyle\varphi_Y}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\varphi_X} \\ V_1 & \xrightarrow{f} & V_2 \end{array}$$

(A diagram consisting of sets and arrows representing the maps between the sets is called a **commutative diagram** if for any two sets the composite of maps along a path between those two sets does not depend on the path.)

By this correspondence, we have an isomorphism:

$$\mathrm{Hom}(V_1, V_2) \ni f \longmapsto f' \in \mathrm{Hom}(K^n, K^m) \cong M_{m,n}(K)$$

Definition xvi.4. The matrix $(a_{ij}) \in M_{m,n}(K)$ corresponding to f' is called the matrix **representing** f with respect to bases $Y = (y_j)$ and $X = (x_i)$.

Exercise xvi.5. The entries of the representation matrix of f with respect to bases $Y = (y_j),\ X = (x_i)$ are the coefficients a_{ij} $(1 \leq i \leq m,\ 1 \leq j \leq n)$ appearing in:

$$f(y_j) = \sum_{i=1}^{m} a_{ij} x_i \quad (a_{ij} \in K).$$

Exercise xvi.6. The matrix representing an isomorphism is invertible. The identity and inverse maps are represented respectively by identity and inverse matrices.

Exercise xvi.7. Fix the bases $Z = (z_i),\ Y = (y_j)$ and $X = (x_k)$ for the K-vector spaces $V_1 \cong K^n,\ V_2 \cong K^m$ and $V_3 \cong K^l$. Let the matrices $(a_{ij}) \in M_{l,m}(K),\ (b_{jk}) \in M_{m,n}(K)$ represent $f \in \mathrm{Hom}(V_2, V_3),\ g \in \mathrm{Hom}(V_1, V_2)$ with respect to these bases. Then $f \circ g \in \mathrm{Hom}(V_1, V_3)$ is represented by the product $(c_{ik}) = (a_{ij})(b_{jk})$:

$$\begin{array}{ccccc} K^n & \xrightarrow{g'} & K^m & \xrightarrow{f'} & K^l \\ {\scriptstyle\varphi_Z}\downarrow{\scriptstyle\cong} & & {\scriptstyle\varphi_Y}\downarrow{\scriptstyle\cong} & & {\scriptstyle\varphi_X}\downarrow{\scriptstyle\cong} \\ V_1 & \xrightarrow{g} & V_2 & \xrightarrow{f} & V_3 \end{array}$$

Lemma xvi.8. *Let $(p_{ij}) \in \mathrm{GL}_n(K)$ be the matrix representing $f \in \mathrm{Aut}(V)$ with respect to the basis $X = (x_i)$, and $f(X) = X'$. Then we have a commutative diagram:*

$$\begin{array}{ccc} K^n & \xrightarrow{(p_{ij})} & K^n \\ & {\scriptstyle\varphi_{X'}}\searrow \quad \swarrow{\scriptstyle\varphi_X} & \\ & V & \end{array}$$

Proof. By definition of the representation matrix, we have a commutative diagram:

$$\begin{array}{ccc} K^n & \xrightarrow{(p_{ij})} & K^n \\ {\scriptstyle\varphi_X}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\varphi_X} \\ V & \xrightarrow{f} & V \end{array}$$

As $f = \varphi_{X'} \circ \varphi_X^{-1}$ (see proof of Proposition v.12), we obtain the lemma. □

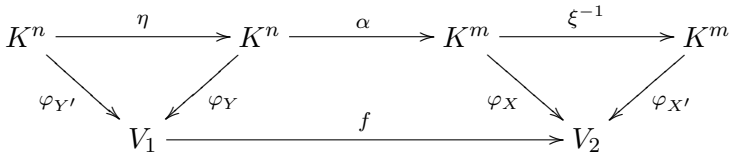
Remark xvi.9. If we set $X' = (x'_j) = f(X)$ then $x'_j = \sum_{i=1}^{n} p_{ij} x_i$ by Exercise xvi.5.

Let V_1, V_2 be K-vector spaces of dimensions n, m respectively. Let $Y = (y_j),\ X = (x_i)$ be the basis of V_1, V_2 respectively. Consider the change of basis $g_1(Y) = Y',\ g_2(X) =$

X' under $g_1 \in \mathrm{Aut}(V_1)$, $g_2 \in \mathrm{Aut}(V_2)$, and let $\eta = (q_{ij})$, $\xi = (p_{ij}) \in \mathrm{GL}_n(K)$ respectively be the matrices representing g_1, g_2 with respect to Y, X.

Proposition xvi.10. *Let $\alpha = (a_{ij}) \in M_n(K)$ (resp. $\alpha' = (a'_{ij})$) be the matrix representing $f \in \mathrm{Hom}(V_1, V_2)$ with respect to Y, X (resp. Y', X'). Then $\alpha' = \xi^{-1}\alpha\eta$.*

Proof. By Lemma xvi.8, consider the commutative diagram:



□

Corollary xvi.11. *Let V be an n-dimensional vector space. Let the image of the basis $X = (x_i)$ under $g \in \mathrm{Aut}(V)$ be $X' = g(X)$, and let $\xi = (p_{jk}) \in \mathrm{GL}_n(K)$ be the representation matrix of g with respect to X. If we denote the matrix representing $f \in \mathrm{End}(V)$ with respect to X (resp. X') by $\alpha = (a_{ij})$ (resp. $\alpha' = (a'_{ij})$), then $\alpha' = \xi^{-1}\alpha\xi$.*

xvi.3. **Determinants.**

Proposition xvi.12. *Let (a_{ij}) be the matrix representing $f \in \mathrm{End}(V)$ with respect to a basis X of V. Then:*

$$\det f = \sum_{\sigma \in S_n} s(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n}.$$

Proof. If $X = (x_1, \ldots, x_n)$, then $f(x_j) = \sum_{i=1}^n a_{ij} x_i$. For any $\Phi \in \mathrm{Vol}(V)$, Lemma xiii.2(iii) shows $(\Phi \circ f)(X) = \Phi(f(X)) = \Big(\sum_{\sigma \in S_n} s(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n}\Big)\Phi(X)$. □

Definition xvi.13. We define the **determinant** of $\alpha = (a_{ij}) \in M_n(K)$ as follows:

$$\det \alpha = \det(a_{ij}) = |(a_{ij})| = \sum_{\sigma \in S_n} s(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n}.$$

Proposition xiii.5 gives the following:

Proposition xvi.14. (i) $\det(\delta_{ij}) = 1$, $\det(\alpha\beta) = \det\alpha \det\beta$.
(ii) $\alpha \in \mathrm{GL}_n(K) \iff \det\alpha \neq 0$.

Proposition xvi.15. *Consider the systems of linear equations for $(a_{ij}) \in M_n(K)$.*

(i) *$(a_{ij})(X_j) = (b_i)$ has a unique solution $(X_j) \in K^n$ if $\det(a_{ij}) \neq 0$.*
(ii) *$(a_{ij})(X_j) = (0)$ has a solution $(X_j) \neq (0)$ if and only if $\det(a_{ij}) = 0$.*

Proof. (i): By Proposition xvi.14(ii), $(a_{ij}) \in \mathrm{GL}_n(K)$ and $(X_j) = (a_{ij})^{-1}(b_i)$. (ii): If (a_{ij}) correspond to $f \in \mathrm{End}(K^n)$ and $X = \big(f(e_1), \ldots, f(e_n)\big)$, then for any $\Phi \in \mathrm{Vol}(V)$ we have $\Phi(X) = (\Phi \circ f)(e_1, \ldots, e_n) = (\det f) \cdot \Phi(e_1, \ldots, e_n) = (\det(a_{ij})) \cdot \Phi(e_1, \ldots, e_n)$. Now use Theorem xiii.7(i) and Proposition xv.3(i). □

xvii. Traces (for Lecture 22 only)

xvii.1. **Dual modules.** Let A be a ring, and M be an A-module.

Definition xvii.1. The A-module $M^\vee := \mathrm{Hom}(M, A)$ is called the **dual** of M. If $f \in \mathrm{Hom}(M, N)$, then $f^\vee := \mathrm{Hom}(N^\vee, M^\vee)$ is defined by $f^\vee(\alpha) = \alpha \circ f$. As $(f \circ g)^\vee = g^\vee \circ f^\vee$, if f is an isomorphism then so is $f^\vee$.

By Proposition v.9, we have an isomorphism $(A^n)^\vee \ni \alpha \mapsto (\alpha(e_i)) \in A^n$. If $M \cong A^n$ and $X = (x_i)$ is a basis of M, then the isomorphism $\varphi_X : A^n \ni e_i \mapsto x_i \in M$ gives $\varphi_X^\vee : M^\vee \cong (A^n)^\vee$, and composing with the above gives $\psi_X : M^\vee \ni \alpha \mapsto (\alpha(x_i)) \in A^n$. By Proposition v.11, the isomorphism $\psi_X^{-1} \in \mathrm{Isom}(A^n, M^\vee)$ corresponds to a basis $X^\vee = (x_j^\vee)$ of $M^\vee$, satisfying $x_j^\vee(x_i) = \delta_{ij}$. It is called the **dual basis** of X.

xvii.2. **Traces.** Let $\mathrm{Lin}(M, N) := \mathrm{Lin}(M, N; A)$ be the A-module of all bilinear forms on M, N. If $f : M \cong M'$ then $\mathrm{Lin}(M', N) \cong \mathrm{Lin}(M, N)$, and $\mathrm{Lin}(A, N) \cong N^\vee$.

Lemma xvii.2. *For $f \in M_1^\vee$ and $x \in M_2$, define $f \otimes x \in \mathrm{Hom}(M_1, M_2)$ by $(f \otimes x)(y) := f(y)x$. Then $\Phi : M_1^\vee \times M_2 \ni (f, x) \longmapsto f \otimes x \in \mathrm{Hom}(M_1, M_2)$ is bilinear. In particular, we have an A-linear map:*

$$\Phi^* : \mathrm{Hom}(M_1, M_2)^\vee \ni \alpha \longmapsto \alpha \circ \Phi \in \mathrm{Lin}(M_1^\vee, M_2).$$

Proof. Immediate from the definition. □

Proposition xvii.3. *Let $M_1 \cong A^n$.*

(i) $\mathrm{Lin}(M_1, M_2) \cong (M_2^\vee)^n$.
(ii) $\Phi^* : \mathrm{Hom}(M_1, M_2)^\vee \longrightarrow \mathrm{Lin}(M_1^\vee, M_2)$ *is an isomorphism.*

Definition xvii.4. Define the **canonical pairing** $c \in \mathrm{Lin}(M^\vee, M)$ by $c(f, x) := f(x)$. If $M \cong A^n$, then the element $\mathrm{tr} \in \mathrm{End}(M)^\vee$ satisfying $\Phi^*(\mathrm{tr}) = c$ is called the **trace**.

Index