

GALOIS THEORY MICHAELMAS 2009
(TU.TH.SA. 11AM, MR2)

TERUYOSHI YOSHIDA

CONTENTS

Notation	3
Preface	4
Part 1. Field Extensions	6
Lecture 1. Introduction, Adjoining roots (Th. 8/10/09)	6
Lecture 2. Field extensions (Sa. 10/10/09)	8
Lecture 3. K -homomorphisms (Tu. 13/10/09)	10
Lecture 4. Algebraic extensions, Simple extensions (Th. 15/10/09)	12
Lecture 5. Automorphisms of a field, Galois groups (Sa. 17/10/09)	14
Lecture 6. Splitting fields (Th. 22/10/09)	16
Lecture 7. Algebraic closure (Sa. 24/10/09)	18
Part 2. Galois Theory (1)	19
Lecture 8. Galois theory of simple extensions (Tu. 27/10/09)	19
Lecture 9. The group μ_n of roots of unity: Cyclicity (Th. 29/10/09)	21
Lecture 10. Galois theory of cyclotomic extensions (Sa. 31/10/09)	23
Lecture 11. Example I: Finite fields (Tu. 3/11/09)	24
Lecture 12. Example II: Cyclotomic fields (Th. 5/11/09)	25
Part 3. Galois Theory (2)	26

Date: November 28, 2009.

Lecture 13.	Separable extensions (1) (Sa. 7/11/09)	26
Lecture 14.	Separable extensions (2) (Tu. 10/11/09)	27
Lecture 15.	Galois extensions revisited (Th. 12/11/09)	28
Part 4.	Solving Equations	29
Lecture 16.	General equations, cubic equations (Sa. 14/11/09)	29
Lecture 17.	Kummer extensions (Tu. 17/11/09)	30
Lecture 18.	Galois groups of polynomials over \mathbb{Q} (Th. 19/11/09)	31
Lecture 19.	Soluble and radical extensions (Sa. 21/11/09)	32
Lecture 20.	Discriminants, quartics and examples (Sa. 28/11/09)	33
Part 5.	Beyond the Theory of Equations	34
Lecture 21.	Another proof of the Galois theory (Tu. 24/11/09)	34
Lecture 22.	Trace and norm (Th. 26/11/09)	35
Lecture 23.	Infinite Galois extensions (Tu. 1/12/09)	36
Appendix.	Galois groups of infinite Galois extensions	37
Preliminaries I: Linear Algebra		39
i.	Sets and Maps	39
ii.	Algebraic Systems — Structures	39
iii.	Basis and Dimension	43
iv.	Linear Maps — Morphisms	47
v.	Hom — Classification of Structures	50
vi.	Matrix Representation of Linear Maps — Representations of Structures	53
vii.	Determinants and Linear Equations	57
viii.	Direct Sum and Diagonalization — Decomposition of Structures	62
Preliminaries II: Rings and Modules		65
ix.	Prime Decomposition and Principal Ideal Domains	65

x.	Polynomial rings, Gauss' Lemma	69
xi.	Quotient Rings	70
xii.	Characteristic of a field	74
xiii.	Minimal polynomial of linear transformations	74
xiv.	Zorn's lemma	75
xv.	Modules and Algebras over Rings (optional)	76
	Index	78

NOTATION

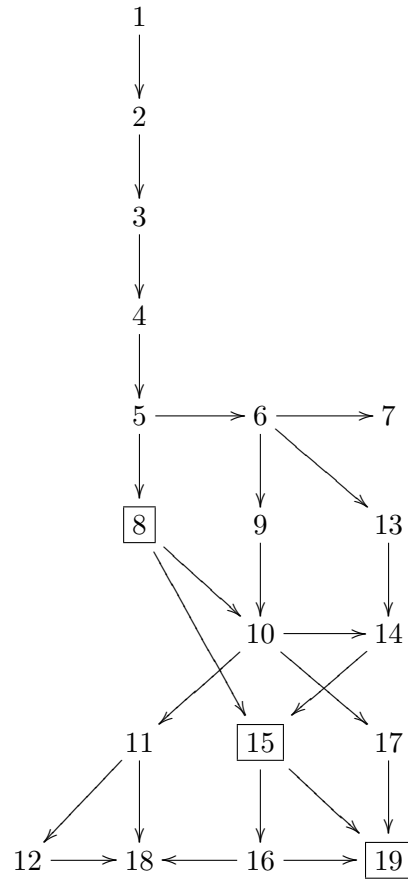
- \emptyset — The empty set (a set without any elements).
 $a \in A$ — a is an element of the set A . (Or: an element a of the set A .)
 $a \notin A$ — a is not an element of the set A . (Or: an element a not in the set A .)
 $|A|$ — The cardinality of the set A .
 $\exists x \in A$ — There exists an 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 .
 $\bigcup_{i=1}^n A_i = A_1 \cup \dots \cup A_n$.
 $\bigcap_{i=1}^n A_i = A_1 \cap \dots \cap A_n$.
 $A \setminus B$ — The set of elements of A not in B .
 $f : X \rightarrow Y$ — A map f from the set X to Y .
 $f : X \ni x \mapsto y \in Y$ — 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 $f : X \ni x \mapsto x \in X$.
 \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. Meant to be completed as lectures proceed.

Teruyoshi Yoshida
September 2009

LOGICAL ORDER



Part 1. Field Extensions

LECTURE 1. INTRODUCTION, ADJOINING ROOTS (TH. 8/10/09)

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 $\frac{-4\zeta}{(1-\zeta)^2}$, $\frac{1-\zeta}{1+3\zeta}$, $\frac{(1-\zeta)(1+3\zeta)}{-4\zeta^2}$. 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 $P \in K[X]$ be a monic irreducible polynomial. By Proposition x.3 and ix.24(i), (P) is a maximal ideal of $K[X]$, hence the quotient ring

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

is a field by Corollary xi.12(ii). As the subring K of $K[X]$ (constant polynomials) are mapped injectively into K_P by the canonical surjection $K[X] \rightarrow K_P$ (see Exercise 1.2), we can regard $K \subset K_P$, and the image \bar{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 $f : X \rightarrow Y$ and a subgroup/subring/ A -submodule X' of X , $\text{Ker}(f|_{X'}) = X' \cap \text{Ker } f$. Therefore, by the homomorphism theorem, $f(X') \cong X'/(X' \cap \text{Ker } f)$.

LECTURE 2. FIELD EXTENSIONS (SA. 10/10/09)

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} 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 xv.2), 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 always 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 satisfying $F \supset L \supset K$ 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 ix.13(i)).

Definition 2.2. The dimension of F as a vector space over K 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 $[F : K] = \infty$, F/K is called an **infinite extension**.

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

Proposition 2.4. $F \supset L \supset K \implies [F : K] = [F : L][L : K]$.

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

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 $\{1, \bar{X}, \bar{X}^2, \dots, \bar{X}^{n-1}\}$ 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 . \square

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 \bar{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

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

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 (TU. 13/10/09)

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 \bar{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 $f : F \rightarrow F'$ satisfies $f|_K = \text{id}$, f is called a **K -homomorphism**. The set of all K -homomorphisms from F to F' is denoted by $\text{Hom}_K(F, F')$. A bijective K -homomorphism is called a **K -isomorphism**. When there exists a K -isomorphism $F \rightarrow F'$, F and F' are said to be **isomorphic**, and we write $F \cong F'$. In particular, a K -isomorphism $F \rightarrow F$ is called a **K -automorphism** of F , and the group consisting of all K -automorphisms of F is denoted by $\text{Aut}_K(F)$.

Exercise 3.2. (i) If $f : F \rightarrow F'$ 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 $f : F \rightarrow F'$ between extension fields is injective, and the image is an intermediate field of F'/K .

Proof. As $\text{Ker } f$ is an ideal of F , it must be equal to F or 0 by Exercise ix.12. If $\text{Ker } f = F$ then $1 = f(1) = 0$ in F' , which is impossible as F' is not the zero ring. \square

Lemma 3.4. If $[F : K] = [F' : K] < \infty$ for two extension fields F, F' of K , any K -homomorphism $f : F \rightarrow F'$ is a K -isomorphism. In particular, $\text{Hom}_K(F, F) = \text{Aut}_K(F)$ for a finite extension F/K .

Proof. By Lemma 3.3 f is an injection and $F \cong \text{Im } f$, hence $[\text{Im } f : K] = [F : K]$. Therefore by Proposition 2.4, we have $[F' : \text{Im } f] = 1$, hence $F' = \text{Im } f$ by Example 2.3 and f is bijective. \square

Remark 3.5. In general, any injective linear map $f : F \rightarrow F'$ between two finite-dimensional vector spaces is bijective if $\dim F = \dim F'$, as the dimension formula (Theorem iv.12) gives $\dim(\text{Im } f) = \dim F = \dim F'$, and then use Lemma iv.9 to conclude $\text{Im } f = F'$.

 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 generalized¹.

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 \bar{X} of the equation $X^2 - 2$. So the fact that you can map \bar{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 $\bar{X} \in \mathbb{Q}[X]/(X^2 - 2X - 1)$ into $1 + \bar{X}$ or $1 - \bar{X}$ in $\mathbb{Q}[X]/(X^2 - 2)$. This can get more tricky for equations of higher degree!

¹Categorically 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. ALGEBRAIC EXTENSIONS, SIMPLE EXTENSIONS (Th. 15/10/09)

MUSINGS

Let me try to continue babbling on the difference between *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 occurrences. 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 $\text{Hom}_K(F, F')$ 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, $\text{Im } f_x$ is a subring of F , therefore a domain (Exercise ix.4(i)), hence by Corollary xi.12(i), $\text{Ker } f_x \in \text{Spec}(K[X])$.

Definition 4.1. If $\text{Ker } f_x \neq 0$ (resp. $\text{Ker } f_x = 0$), 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, $\text{Im } f_x$ is a K -subspace of F , therefore finite-dimensional over K by Lemma iv.9, and as $K[X]$ has infinite dimension over K , we have $\text{Ker } f_x \neq 0$. \square

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 $K[X] \cong \text{Im } f_x \subset F$, and by Exercise xv.9, the extension F/K has an intermediate extension $\text{Frac}(\text{Im } f_x)/K$, isomorphic to the fraction field $K(X)$ of $K[X]$ (called the **rational function field** over K). We write $K(x) := \text{Frac}(\text{Im } f_x)$, which is the minimal subextension of F/K containing x .

Now let $x \in F$ be algebraic over K . By Proposition x.3 and Exercise ix.18(i), $\text{Ker } f_x$ 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:

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

Definition 4.5. We call the monic generator P_x of $\text{Ker } f_x$ the **minimal polynomial** of x over K . It is irreducible. The subextension $\text{Im } f_x$ 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 $x \in F$.

Exercise 4.6. 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** as follows:

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

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 $x_i = e_i$. \square

LECTURE 5. AUTOMORPHISMS OF A FIELD, GALOIS GROUPS (SA. 17/10/09)

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 \bar{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 $\bar{X} \in K_P$ 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 $\text{Root}_P(F)$ 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 $\text{Hom}_K(K_P, F)$, 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* $\text{Aut}_K(F)$, 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 a finite extension. We fix an irreducible $P \in K[X]$, and consider the set $\text{Root}_P(F)$ 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 x.5.

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

$$\begin{aligned} \text{Root}_P(F) \ni x &\longmapsto f_x \in \text{Hom}_K(K_P, F), \\ \text{Hom}_K(K_P, F) \ni f &\longmapsto f(\bar{X}) \in \text{Root}_P(F). \end{aligned}$$

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

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

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

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

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

Proposition 5.2. *Assume $F \cong K_P$. For any $x \in \text{Root}_F(P)$, the map $\text{Aut}_K(F) \ni \sigma \mapsto \sigma(x) \in \text{Root}_P(F)$ is bijective. In particular, $|\text{Aut}_K(F)| \leq [F : K]$.*

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

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

(use Lemma 3.4 for the first equality), which, composed with the bijection $f \mapsto f(\bar{X})$ of Proposition 5.1, gives the desired bijection. The latter part follows from Proposition x.5, as $|\text{Root}_F(P)| \leq \deg P = [F : K]$. \square

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

When we write $F = K(x) \cong K_P$, F/K being Galois means that $|\text{Root}_P(F)| = [F : K] = \deg P$, i.e. P has $\deg P$ distinct roots in $F = K(x)$ (no multiple roots, and all the roots are expressible as a polynomial of x with coefficients in K), by Proposition 5.2.

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. SPLITTING FIELDS (TH. 22/10/09)

 IDEA

Now we can directly proceed to proving the fundamental theorem of Galois theory for simple extensions (Lecture 8), which turns out to cover all the separable extension when we have the primitive element theorem in Lecture 14. But before building up the general theory we will digress into the 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 — 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 $\iota : K' \rightarrow K''$. This will be very useful later, when we consider the separability of arbitrary finite extensions.

 MATH

Definition 6.1. Let K be a field. We slightly extend the definition of extension fields. An **extension** F_τ/K is defined as a pair (F, τ) of a field F and a ring homomorphism $\tau : K \rightarrow F$ (not necessarily the inclusion map of a subring). A K -homomorphism from F_τ to F'_τ is a ring homomorphism $\varphi : F \rightarrow F'$ such that $\tau' = \varphi \circ \tau$. By a **subextension** of F_τ/K we mean an intermediate field of $F/\tau(K)$.

Note that τ is always an injection and $F/\tau(K)$ 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 often 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 we write $\text{Root}_P(F_\tau) := \text{Root}_{\tau P}(F)$. We record the generalization of Proposition 5.1 to this setting:

Proposition 6.2. *We have a bijection $\text{Hom}_K(K_P, F_\tau) \ni f \mapsto f(\overline{X}) \in \text{Root}_P(F_\tau)$, with the inverse $x \mapsto (f_x : P \mapsto \tau P(x))$. In particular, $|\text{Hom}_K(K_P, F_\tau)| \leq \deg P = [K_P : K]$.*

Definition 6.3. Let $P \in K[X] \setminus K$ and F_τ an extension of K . We say P **splits** in F_τ if τP factors into a product of linear factors in $F[X]$. We call F a **splitting field** of P over K if, for all extensions F'/K , P splits in F' if and only if $\text{Hom}_K(F, F') \neq \emptyset$.

Exercise 6.4. If $Q \mid P$ in $K[X]$ and P splits in F then Q splits in F . If P splits in F and $\text{Hom}_K(F, F') \neq \emptyset$ for another extension F'/K , then P splits in F' as well.

Proposition 6.5. *Splitting fields exist, they are finite extensions of K and are unique up to K -isomorphisms.*

Proof. Any extension isomorphic to a splitting field is also a splitting field, as it is defined in terms of Hom sets. If F, F' are both splitting fields of P over K , then $\text{Hom}_K(F, F'), \text{Hom}_K(F', F) \neq \emptyset$, thus $[F : K] = [F' : K]$ by Lemma 3.3 and $F \cong F'$ by Lemma 3.4. We prove the existence by induction on $\deg P$. Let Q be an irreducible factor of P . Then we have $P = (X - \alpha)R$ in $K_Q[X]$ with $\alpha = \overline{X}$, 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 $\tau \in \text{Hom}_K(K_Q, F')$ by Proposition 6.2 because $\text{Root}_Q(F') \neq \emptyset$, and $\text{Hom}_{K_Q}(F, F'_\tau) \neq \emptyset$ as R splits in F' . As $\text{Hom}_{K_Q}(F, F'_\tau) \subset \text{Hom}_K(F, F')$, we have $\text{Hom}_K(F, F') \neq \emptyset$. \square

Proposition 6.6. *Suppose P splits in an extension F/K and $\text{Root}_P(F) = \{x_1, \dots, x_n\}$. Then $K(x_1, \dots, x_n)/K$ 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 $F' := K(x_1, \dots, x_n)$. If F_0 is a splitting field of P , then take $\tau \in \text{Hom}_K(F_0, F')$. As τ maps $\text{Root}_P(F_0)$ onto $\text{Root}_P(F') = \{x_1, \dots, x_n\}$, it is surjective, thus $F_0 \cong F'$. If F_0 is moreover a subextension of F/K , then $\text{Root}_P(F_0) = \text{Root}_P(F) = \{x_1, \dots, x_n\}$, thus $F' \subset F_0$ and $F' = F_0$. \square

LECTURE 7. ALGEBRAIC CLOSURE (SA. 24/10/09)

Definition 7.1. A field E is called an **algebraically closed field** if every irreducible element of $E[X]$ is linear. Equivalently, it is a field whose algebraic extensions are all isomorphic to itself. An algebraic extension E/K is called an **algebraic closure** of K if E is algebraically closed.

Theorem 7.2. (Steinitz' theorem) *Algebraic closures exist, and are unique up to K -isomorphisms. For every algebraic extension F/K , we have $\text{Hom}_K(F, \overline{K}) \neq \emptyset$.*

Proof. Consider the set A 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 $\lambda \in A$, and the polynomial ring $R := K[X_\lambda \mid \lambda \in A]$ 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 $P'(X) := P(X) - \prod_{i=1}^{\deg P} (X - X_{P,i}) \in R[X]$, and let $x_{P,i} \in R$ be the coefficient of X^i in $P'(X)$ for $0 \leq i < \deg P$. Let I be the ideal of R generated by all $x_{P,i} \in R$ for all P . We first show $I \neq R$. Assume $I = R$, or $1 \in I$. Then:

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

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 $f : R \rightarrow F$ 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 $P'_j[X] \in R[X]$ 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 R containing I by Proposition xiv.5 and consider the field $\overline{K} := R/Q$, which is naturally 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 $K(\alpha_{\lambda_1}, \dots, \alpha_{\lambda_m})$ for some $\lambda_1, \dots, \lambda_m$, 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 $\tau \in \text{Hom}_K(L, \overline{K})$. 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 xiv.4). For all $x \in F$, we have $\text{Hom}_M(M(x), \overline{K}) \neq \emptyset$ by Proposition 6.2, 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 $\text{Hom}_K(F, \overline{K}) \neq \emptyset$. If F is an algebraic closure of K , then $\tau \in \text{Hom}_K(F, \overline{K})$ makes \overline{K} into an algebraic extension \overline{K}_τ/F (as \overline{K}/K is algebraic), thus τ is an isomorphism. \square

Part 2. Galois Theory (1)

LECTURE 8. GALOIS THEORY OF SIMPLE EXTENSIONS (TU. 27/10/09)

 IDEA

Back to the Galois Theory. 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. We prove this for the *simple Galois* extensions (see Lecture 5 for the definition), i.e. the simple extensions $F = K(x)$ such that F contains all the $[F : K]$ 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 express this symmetry in the following language. For such extension F/K , its *Galois group* $\text{Gal}(F/K)$ is the group of automorphism of F over K as an extension field, that is the set of all K -homomorphisms $\sigma : F \rightarrow F$, 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 $\text{Gal}(F/K)$ as a subgroup of the group of all permutations of the set $\text{Root}_P(F)$, or the symmetric group S_n of n letters, if $n := [F : K]$. It can be a very small subgroup of S_n .

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 $\{\text{id}, \zeta \mapsto \zeta^2, \zeta \mapsto \zeta^3, \zeta \mapsto \zeta^4\} \cong \mathbb{Z}/4\mathbb{Z}$, there is a proper subgroup $\{\text{id}, \zeta \mapsto \zeta^4\} \cong \mathbb{Z}/2\mathbb{Z}$, 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 $\text{Gal}(F/K)$. That is why this correspondence is called the *fundamental theorem* of Galois theory.

 MATH

Proposition 8.1. *Let L be an intermediate field of a Galois extension F/K . Then F/L is also a Galois extension, and $\text{Gal}(F/L)$ is a subgroup of $\text{Gal}(F/K)$.*

Proof. Putting $F = K(x) \cong K_P$, we have $F = L(x)$, hence F/L is also simple. Let the kernel of $f_x : L[X] \rightarrow F$ be (Q) , to write $F \cong L_Q$, by definition we have $Q \mid P$, therefore Q has $\deg Q$ distinct roots in F and F/L is Galois. The latter part follows from the fact that every L -automorphism of F is also a K -automorphism. \square

Theorem 8.2. (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 $G = \text{Gal}(F/K)$. Then the map $A \ni L \mapsto \text{Gal}(F/L) \in B$ is bijective. More precisely, the following are inverse to each other (note $\Phi(L) = \text{Gal}(F/L)$):

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

Proof. By definition we 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. \square

Lemma 8.3. $|\Phi(L)| = [F : L]$, $|H| = [F : \Psi(H)]$.

Proof. The first equality $|\Phi(L)| = |\text{Gal}(F/L)| = [F : L]$ is trivial. 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 $[F : \Psi(H)] = \deg Q_x \leq \deg P = |H|$. \square

IDEA OF PROOF

Note that in Proposition 8.1, for a subfield L of F/K , it is the extension F/L that corresponds to a subgroup of $\text{Gal}(F/K)$, 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 $\text{Gal}(F/L)$ 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 $\{\sigma(x) \mid \sigma \in H\} \subset \text{Root}_P(F)$, where x is the generator of F . Thus it is exactly what we did for $X^4 + X^3 + X^2 + X + 1$.

LECTURE 9. THE GROUP μ_n OF ROOTS OF UNITY: CYCLICITY (TH. 29/10/09)

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 theory, 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 μ_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 μ_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 $n \geq 1$, the splitting field of $X^n - 1$ is denoted by $K(\mu_n)$, 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 $K(\mu_n)$ by μ_n .

By Proposition 9.5, we have $|\mu_n| \leq n$, and clearly μ_n is a group under multiplication, i.e. it is a finite subgroup of $K(\mu_n)^\times$ (the multiplicative group of $K(\mu_n)$).

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 $1, a, a^2, \dots$, 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 additive group of $\mathbb{Z}/(n)$ (often denoted by $\mathbb{Z}/n\mathbb{Z}$) by sending a generator to $1 \pmod n$.

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:

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

equal to $p^j n'$, which contradicts the maximality of n . Therefore $m \mid n$, but now $x^{in/m}$ ($1 \leq i \leq m$) gives m distinct roots of $X^m - 1$ in K , but by Proposition x.5, 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 . \square

Corollary 9.8. *The group μ_n is cyclic, as it is a finite subgroup of $K(\mu_n)^\times$.*

LECTURE 10. GALOIS THEORY OF CYCLOTOMIC EXTENSIONS (SA. 31/10/09)

Consider a field K and its cyclotomic extension $K(\mu_n)$.

Proposition 10.1. *If $(\text{char } K, n) = 1$, then $|\mu_n| = n$, i.e. μ_n is cyclic of order n .*

Proof. It suffices to show that $X^n - 1$ does not have a multiple root in $K(\mu_n)$, 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 $(\text{char } K, n) = 1$. \square

Definition 10.2. The K -linear map $D : K[X] \rightarrow K[X]$ 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 $(\text{char } K, n) = 1$.

Definition 10.4. A generator of the cyclic group μ_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 ζ in $K(\mu_n)$, and let P_ζ be its minimal polynomial over K .*

- (i) $K(\mu_n) = K(\zeta)$, 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 $\mu_n = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$, 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 μ_n . A non-primitive $\alpha \in \mu_n$ of order $d < n$ is a root of $X^d - 1$. As ζ is not a root of $X^d - 1$, 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 . \square

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 $K(\mu_n)/K$ is an abelian extension:*

$$\text{Gal}(K(\mu_n)/K) \ni (\zeta \mapsto \zeta^k) \longmapsto k \bmod n \in (\mathbb{Z}/(n))^\times.$$

Proof. By Proposition 5.2, $\text{Gal}(K(\zeta)/K) \ni \sigma \longmapsto \sigma(\zeta) \in \text{Root}_{P_\zeta}(K(\zeta))$ is a bijection, and we know by Proposition 10.5(ii) that $\text{Root}_{P_\zeta}(K(\zeta))$ 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 composition of $\zeta \mapsto \zeta^k$ and $\zeta \mapsto \zeta^l$ is $\zeta \mapsto \zeta^{kl}$, it is a group homomorphism. \square

LECTURE 11. EXAMPLE I: FINITE FIELDS (TU. 3/11/09)

Proposition 11.1. *For a field F of characteristic $p > 0$, the map $\text{Fr}_q : F \ni x \mapsto x^q \in F$ 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 $\text{Fr}_p : F \ni x \mapsto x^p \in F$. 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 $\text{Fr}_q = (\text{Fr}_p)^f$. \square

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

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 $F^\times = \mu_{q-1}$, i.e. if we take a generator ζ of the cyclic group F^\times (a primitive root of F) then $F = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{q-2}\}$.*

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. \square

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

Proof. Let $\mathbb{F}_q = \mu_{q-1} \cup \{0\}$ 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 $\mathbb{F}_q = \{x \in \overline{\mathbb{F}}_p \mid \text{Fr}_q(x) = x\}$ 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 $\overline{\mathbb{F}}_p$. \square

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 $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a cyclic group of order n with a generator $\text{Fr}_q : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$:*

$$\varphi_n : \mathbb{Z}/n\mathbb{Z} \ni 1 \pmod n \xrightarrow{\cong} \text{Fr}_q \in \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$$

Proof. By Proposition 11.1, we see that $\text{Fr}_q \in \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$. Taking a primitive root ζ of \mathbb{F}_{q^n} by Proposition 11.3, its images $\zeta^{q^i} = \text{Fr}_q^i(\zeta)$ 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 $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. \square

LECTURE 12. EXAMPLE II: CYCLOTOMIC FIELDS (TH. 5/11/09)

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 $(\text{char } K, n) = 1$, then $\text{Root}_{\Phi_n}(K(\boldsymbol{\mu}_n))$ 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 another polynomial in $\mathbb{Z}[X]$, its quotient also lies in $\mathbb{Z}[X]$). \square

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

Proposition 12.3. *Let $(\text{char } K, n) = 1$. If the image of the canonical injection $\text{Gal}(K(\boldsymbol{\mu}_n)/K) \rightarrow (\mathbb{Z}/(n))^\times$ 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 $[K(\zeta) : K] = [K(\boldsymbol{\mu}_n) : K] = |\text{Gal}(K(\boldsymbol{\mu}_n)/K)| = m$. As the roots of Φ_n are all primitive n -th roots of unity, all of its irreducible factors are of this form. \square

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 $\text{Gal}(K(\boldsymbol{\mu}_n)/K) \rightarrow (\mathbb{Z}/(n))^\times$ 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 x.10(i)). 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. \square

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 (1) (SA. 7/11/09)

Definition 13.1. (i) A polynomial $P \in K[X] \setminus K$ is called **separable** if $|\text{Root}_P(E)| = \deg P$ for some extension E/K .

(ii) A finite extension F/K is called **separable** if $|\text{Hom}_K(F, E)| = [F : K]$ for some extension E/K .

Proposition 13.2. *If $P \in K[X] \setminus K$ is separable, then $|\text{Root}_P(E)| = \deg P$ whenever P splits in E .*

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

Let $F/K, E/K$ be two extensions and L a subextension of F/K . If $\sigma \in \text{Hom}_K(F, E)$ then $\tau := \sigma|_L \in \text{Hom}_K(L, E)$, and $\sigma \in \text{Hom}_L(F, E_\tau)$. Conversely $\text{Hom}_L(F, E_\tau) \subset \text{Hom}_K(F, E)$ for every $\tau \in \text{Hom}_K(L, E)$. Therefore we have:

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

When $F = L(x)$ and the minimal polynomial of x over L is P , then by Proposition 6.2:

$$\text{Hom}_K(L(x), E) = \coprod_{\tau \in \text{Hom}_K(L, E)} \text{Hom}_L(L(x), E_\tau) \xrightarrow{\cong} \coprod_{\tau \in \text{Hom}_K(L, E)} \text{Root}_{\tau P}(E)$$

hence $|\text{Hom}_K(L(x), E)| \leq |\text{Hom}_K(L, E)| \cdot [F : L]$, and when both sides are finite, equality holds if and only if $|\text{Root}_{\tau P}(E)| = \deg P$ for all $\tau \in \text{Hom}_K(L, E)$.

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

- (i) $|\text{Hom}_K(F, E)| = [F : K]$.
- (ii) Let K_i ($0 \leq i \leq n$) be a sequence of subextensions of F/K with $K_0 = K$, $K_n = F$ and $K_i = K_{i-1}(x_i)$. If Q_i is the minimal polynomial of x_i over K_{i-1} , then $|\text{Root}_{\tau Q_i}(E)| = \deg Q_i$ for all $\tau \in \text{Hom}_K(K_{i-1}, E)$.
- (iii) There exists a sequence K_i ($0 \leq i \leq n$) satisfying (ii).
- (iv) If L is a subextension of F/K and $\tau \in \text{Hom}_K(L, E)$, then for every $x \in F$ we have $|\text{Root}_{\tau P}(E)| = \deg P$ for the minimal polynomial P of x over L .
- (v) If L, L' are subextensions of F/K with $L \subset L'$ and $\tau \in \text{Hom}_K(L, E)$, then $|\text{Hom}_L(L', E_\tau)| = [L' : L]$.

Proof. (i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i): repeat the above argument (and use Proposition 2.4). (ii) \Rightarrow (iv): We can form $\{K_i\}_{0 \leq i \leq n}$ with $L = K_{i-1}$ and $x = x_i$ for some i . (ii) \Rightarrow (v): We can form $\{K_i\}_{0 \leq i \leq n}$ with $L = K_i$ and $L' = K_j$ for some i, j . (iv) \Rightarrow (ii), (v) \Rightarrow (i): clear. \square

LECTURE 14. SEPARABLE EXTENSIONS (2) (Tu. 10/11/09)

Proposition 14.1. *The following are equivalent: (i) for every $x \in F$, its minimal polynomial P_x over K is separable (we say x is **separable** over K), (ii) if $F = K(x_1, \dots, x_n)$ then the minimal polynomials P_i of x_i over K are separable, (iii) if $F = K(x_1, \dots, x_n)$ and P_1, \dots, P_n splits in E/K , then $|\text{Hom}_K(F, E)| = [F : K]$, (iv) F/K is separable.*

Proof. (i) \Rightarrow (ii): clear. (ii) \Rightarrow (iii): We have $|\text{Root}_{P_i}(E)| = \deg P_i$ by Proposition 13.2, and as Q_i divides P_i in $K_{i-1}[X]$, we have $|\text{Root}_{\tau Q_i}(E)| = \deg Q_i$ for all i and τ . Apply Lemma 13.3(iii) \Rightarrow (i). (iii) \Rightarrow (iv): clear. (iv) \Rightarrow (i): Lemma 13.3(i) \Rightarrow (iv) for $L = K$. \square

Proposition 14.2. *An irreducible $P \in K[X]$ is separable if and only if $D(P) \neq 0$. In particular, if $\text{char } K = 0$, all irreducible $P \in K[X]$ are separable, and hence every finite extension of K is separable by Proposition 14.1(ii) \Rightarrow (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 x.3, Proposition ix.24(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 . \square

Exercise 14.3. (i) If $K = L(T)$ with $\text{char } L = p$, 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. (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. By Proposition 4.8, if we show the claim for $F = K(x, y)$, the general case follows by induction and Proposition 14.1(iii) \Rightarrow (i). Let $F = K(x, y)$, $[F : K] = n$, and for an E/K , we have $\text{Hom}_K(F, E) = \{\sigma_1, \dots, \sigma_n\}$. As any element of $\text{Hom}_K(F, E)$ is determined by 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:

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

As K is infinite, it contains an element z which is not a root of Q . Putting $w = xz + y$, we see that $i \neq j \implies \sigma_i(w) \neq \sigma_j(w)$, therefore $\sigma_1, \dots, \sigma_n$ restricts to n distinct K -homomorphisms of $K(w)$ into E . But Proposition 5.1 shows that $n \leq |\text{Hom}_K(K(w), E)| \leq [K(w) : K]$, and as $K(w) \subset F$, $[K(w) : K] \leq [F : K] = n$, so these are all equalities, hence $F = K(w)$. \square

Corollary 14.5. *A finite extension F/K is a **Galois extension** if $|\text{Aut}_K(F)| = [F : K]$ (with which we replace the previous Definition 5.3).*

LECTURE 15. GALOIS EXTENSIONS REVISITED (TH. 12/11/09)

- Proposition 15.1.** (i) A finite F/K is Galois if and only if $|\text{Root}_{P_x}(F)| = \deg P_x$ for every $x \in F$ and its minimal polynomial P_x over K .
(ii) A splitting field E/K of a separable $P \in K[X]$ is Galois. In particular, every finite separable extension F/K is contained in some Galois extension.

Proof. (i): Only if part is Lemma 13.3(i) \Rightarrow (iv) for $L = K$ and $E = F$. If part follows from Proposition 14.1(i) \Rightarrow (iii) for $E = F$. (ii): If $\text{Root}_P(E) = \{x_1, \dots, x_n\}$, then $E = K(x_1, \dots, x_n)$ by Proposition 6.6, and let $K_0 = K$, $K_i = K_{i-1}(x_i)$. The minimal polynomial Q_i of x_i over K_{i-1} divide P , hence Lemma 13.3(ii) \Rightarrow (i) shows $\text{Hom}_K(E, E) = [E : K]$, thus E/K is Galois by Lemma 3.4 and Corollary 14.5. \square

Exercise 15.2. For a finite separable F/K , the splitting field E/K of the minimal polynomial of x over K where $F = K(x)$ is the “minimal” Galois extension E/K containing F , 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:

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

The generalization of Proposition 5.2 is as follows:

Proposition 15.3. Assume $\text{Hom}_K(L, F) \neq \emptyset$. Then for any $f \in \text{Hom}_K(L, F)$, the map $\text{Gal}(F/K) \ni \sigma \longmapsto \sigma \circ f \in \text{Hom}_K(L, F)$ is surjective, and $|\text{Hom}_K(L, F)| = [L : K]$.

Proof. As $f(L) \subset F$ and $\text{Hom}_K(f(L), F) \ni g \mapsto g \circ f \in \text{Hom}_K(L, F)$ is bijective as $L \cong f(L)$ by f , it suffices to treat the case $L \subset F$. The inverse image of $\tau \in \text{Hom}_K(L, F)$ is $\text{Hom}_L(F, F_\tau)$. But $|\text{Hom}_L(F, F_\tau)| = [F : L]$ and $|\text{Hom}_K(L, F)| = [L : K]$ by Lemma 13.3(i) \Rightarrow (v) for $E = F$. \square

Proposition 15.4. Let F/K be Galois and $G = \text{Gal}(F/K)$, let L be a subextension of F/K and $H = \text{Gal}(F/L)$. Then

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

Proof. (i): Proposition 15.3. (ii): If $H' := \text{Gal}(F/\sigma(L))$, then $\sigma H \sigma^{-1} \subset H'$. Similarly, $L = \sigma^{-1}(\sigma(L))$ gives $\sigma^{-1} H' \sigma \subset H$, hence $H' \subset \sigma H \sigma^{-1}$. (ii) By (ii), $G \triangleright H \iff \sigma H \sigma^{-1} = H$ ($\forall \sigma \in G$) $\iff \sigma(L) = L$ ($\forall \sigma \in G$). This last condition means that the surjection (i) factors through $\text{Hom}_K(L, L)$, thus $\text{Hom}_K(L, L) = \text{Hom}_K(L, F)$. Therefore L/K is Galois as $|\text{Hom}_K(L, F)| = [L : K]$. (iii) By $\text{Gal}(L/K) = \text{Hom}_K(L, F)$, the surjection (i) is a homomorphism with the kernel H . \square

Part 4. Solving Equations

LECTURE 16. GENERAL EQUATIONS, CUBIC EQUATIONS (SA. 14/11/09)

Definition 16.1. Let K be a field and $P \in K[X]$ be a separable polynomial. The **Galois group** $\text{Gal}(P)$ of P is defined as $\text{Gal}(F/K)$ for a splitting field F of P over K , which is well-defined up to isomorphism by Propositions 6.5 and 15.1(ii).

Proposition 16.2. Let $P \in K[X]$ be a separable polynomial with $\deg P = n$. Then $\text{Gal}(P)$ is a subgroup of the automorphism group of $\text{Root}_P(F)$, where F is a splitting field of P . In particular, a choice of ordering of the roots in $\text{Root}_P(F)$ gives an injection $\text{Gal}(P) \rightarrow S_n$, where $S_n := \text{Aut}(\{1, \dots, n\})$ is the **symmetric group in n letters**.

Proof. If $\text{Root}_P(F) = \{x_1, \dots, x_n\}$, then $\text{Gal}(F/K)$ acts on the set $\text{Root}_P(F)$. As $F = K(x_1, \dots, x_n)$ by Proposition 6.6, an automorphism $\sigma \in \text{Gal}(F/K)$ is determined by $\sigma(x_1), \dots, \sigma(x_n)$, thus $\text{Gal}(F/K)$ is a subgroup of $\text{Aut}(\text{Root}_P(F))$. Once we label the elements of $\text{Root}_P(F)$, we have $\text{Aut}(\text{Root}_P(F)) \cong \text{Aut}(\{1, \dots, n\}) = S_n$. \square

Proposition 16.3. Let K be a field and $F = K(x_1, \dots, x_n) := \text{Frac}(K[x_1, \dots, x_n])$ 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 $L := K(a_1, \dots, a_n)$, the subfield of F consisting of all rational functions of a_i . If $P(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in L[X]$, then $\text{Gal}(P) \cong S_n$.

Proof. The group $G = S_n$ acts on F by K -automorphisms, permuting x_1, \dots, x_n . By Artin's theorem (Example Sheet 3, Problem 8), we know that F/F^G is a Galois extension with Galois group G , and $L \subset F^G$. As $\{x_1, \dots, x_n\} = \text{Root}_P(F)$, we see that $F = L(x_1, \dots, x_n)$ is a splitting field of P over L , thus $\text{Gal}(F/L)$ is a subgroup of S_n . Thus $L = F^G$ (the **fundamental theorem of symmetric functions**). \square

Let K be a field with $\text{char } K \neq 2, 3$ and $\mu_3 \subset K$, 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. This is done by considering 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 $\text{Gal}(F/L) \cong S_3$ are:

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

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 $\sqrt{\quad}$ and $\sqrt[3]{\quad}$, 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 (TU. 17/11/09)

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

Let n be a positive integer and K a field with $(\text{char } K, n) = 1$, and which contains the group of n -th roots of unity μ_n . 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 $\text{Root}_P(F) = \{\zeta^i x \in F \mid 0 \leq i \leq n-1\}$ 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:

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

Definition 17.2. For a field K with $(\text{char } K, n) = 1$, $\mu_n \subset K$, 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 $\text{char } K \neq 2$, every quadratic extension is a Kummer extension. (Note that $\mu_2 = \{\pm 1\} \subset K$.)

Theorem 17.4. (Kummer theory) Let K be a field with $(\text{char } K, n) = 1$ and $\mu_n \subset K$. Then every cyclic extension is a Kummer extension.

Proof. Let F/K be cyclic, and choose a generator σ of $G = \text{Gal}(F/K)$. Let Q be the minimal polynomial of σ considered as an endomorphism $\sigma \in \text{End}(L)$ of L as a vector space over K . Then $\Lambda := \text{Root}_Q(K)$ is the set of all eigenvalues of σ by Proposition xiii.3. As $\sigma^n = \text{id}$ we have $Q \mid X^n - 1$, hence $\Lambda \subset \mu_n$. Now Λ is a group under multiplication, because if $c, d \in \Lambda$ and $\sigma(x) = cx$, $\sigma(y) = dy$ for $x, y \in L^\times$, 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 $\Lambda = \mu_d \subset \mu_n$ for some $d \mid n$ (Exercise 9.5(ii)) and $Q = X^d - 1$. But $\sigma^d \neq \text{id}$ unless $d = n$, thus $\Lambda = \mu_n$. Let $\zeta \in \mu_n$ be a primitive n -th root of unity, and let $x \in L^\times$ be its eigenvector. Then $\sigma(x^n) = \sigma(x)^n = (\zeta x)^n = x^n$, hence $a := x^n \in F^G = K$ by the fundamental theorem of Galois theory. Therefore the minimal polynomial P of x over K divides $X^n - a$. But $\sigma^i(x) = \zeta^i x$ for $0 \leq i \leq n-1$ are all distinct, and as σ^i are K -isomorphisms, they are all roots of P . Therefore $P(X) = X^n - a$ and $F = K(x)$. \square

Definition 17.5. (i) A finite group G is called a **soluble group** if there exists a decreasing sequence of subgroups $G = G_0 \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = \{1\}$ such that $G_{i-1} \triangleright G_i$ and G_{i-1}/G_i is cyclic for all $1 \leq i \leq n$.
(ii) A finite extension F/K is called a **soluble extension** if it is contained in a Galois extension E/K with a soluble Galois group.

LECTURE 18. GALOIS GROUPS OF POLYNOMIALS OVER \mathbb{Q} (TH. 19/11/09)

Let P be a separable polynomial over a field K with $\deg P = n$. By Proposition 16.2, we can consider $\text{Gal}(P)$ as a subgroup of S_n (which is well-defined up to reordering of $\{1, \dots, n\}$, i.e. conjugation by an element of S_n).

Definition 18.1. (i) A subgroup $G \subset S_n$ is called **transitive** if for every $i, j \in \{1, \dots, n\}$ there exists $\sigma \in G$ such that $\sigma(i) = j$.
(ii) For every $\sigma \in S_n$ there is a partition $\{1, \dots, n\} = I_1 \amalg \dots \amalg I_m$ 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 $1 \leq j \leq n_i - 1$ and $\sigma(a_{n_i}) = a_1$. We denote $\sigma = (a_1 \dots a_{n_1})(b_1 \dots b_{n_2}) \dots$, and say that σ is of **cyclic type** (n_1, \dots, n_m) .

Proposition 18.2. *Let $P \in K[X]$ be a separable polynomial with $\deg P = n$. Then P is irreducible if and only if the Galois group $\text{Gal}(P)$ is transitive as a subgroup of S_n .*

Proof. If $P = QR$ in $K[X]$, then elements of $\text{Gal}(P)$ cannot send a root of Q to a root of R , hence $\text{Gal}(P)$ is not transitive. If P is irreducible, for $x_i, x_j \in \text{Root}_P(F)$ where F is a splitting field of P , we can extend any element $\tau \in \text{Hom}_K(K(x_i), F)$ defined by $\tau(x_i) = x_j$ to an element of $\text{Gal}(F/K)$ by Proposition 15.4(i). \square

Let K, F, L and $P \in L[X]$ as in Proposition 16.3. Consider the following polynomial in $F[T_1, \dots, T_n][X]$ (the minimal polynomial of a “generic resolvent”), where T_i are auxiliary variables:

$$R_P(X) = \prod_{\sigma \in S_n} R_\sigma, \quad R_\sigma := X - (\sigma(x_1)T_1 + \dots + \sigma(x_n)T_n). \quad (\text{recall } \sigma(x_i) = x_{\sigma(j)})$$

Then the coefficients are invariant under the action of $S_n = \text{Gal}(F/L)$ on x_1, \dots, x_n , thus $R_P \in L[T_1, \dots, T_n][X]$, whose coefficients are actually in $\mathbb{Z}[a_1, \dots, a_n] \subset L$.

Now we let a_i be elements of K , so that $L = K$ and F is a splitting field of $P \in K[X]$ with $G = \text{Gal}(F/K)$. Let Q be an irreducible factor of R_P in $K(T_1, \dots, T_n)[X]$. If $R_\sigma \mid Q$ then $R_{\tau\sigma} \mid Q$ for all $\tau \in G$, thus $R_{G\sigma} := \prod_{\tau \in G\sigma} R_\tau \mid Q$. But $R_{G\sigma} \in K(T_1, \dots, T_n)[X]$ because the coefficients are invariant under the action of G , thus $R_{G\sigma} = Q$. As $R_P = \prod_{\sigma \in G \backslash S_n} R_{G\sigma}$, this is the irreducible factorization of R_P in $K(T_1, \dots, T_n)[X]$, hence in $K[T_1, \dots, T_n][X]$ by Gauss’ Lemma.

Proposition 18.3. *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 $P \bmod p = Q_1 \dots Q_m$ is the factorization into irreducibles in $\mathbb{F}_p[X]$ and $\deg Q_i = n_i$, then $\text{Gal}(P)$ contains an element of cyclic type (n_1, \dots, n_m) . (The proof of Theorem 12.5 used this structure.)*

Proof. As above $\text{Gal}(P)$ is read off from the factorization of $R_P \in \mathbb{Z}[T_1, \dots, T_n][X]$. It is clear that $R_{(P \bmod p)} = R_P \bmod p \in \mathbb{F}_p[T_1, \dots, T_n][X]$, and it factorizes further than R_P , thus $\text{Gal}(P \bmod p)$ is a subgroup of $\text{Gal}(P)$ up to conjugation. The p -th power Frobenius map gives the desired element in $\text{Gal}(P \bmod p)$. \square

LECTURE 19. SOLUBLE AND RADICAL EXTENSIONS (SA. 21/11/09)

Exercise 19.1. (i) If $G \triangleright H$, then $G : \text{soluble} \iff H, G/H : \text{soluble}$.

(ii) If F/K is soluble, then its Galois closure has a soluble Galois group.

Lemma 19.2. (i) *Finite abelian groups are soluble.*

(ii) *If L/K is soluble and F/L is abelian, then F/K is soluble.*

Proof. (i): For a finite abelian group G , taking any $\sigma \neq 1$ and $H := \langle \sigma \rangle$, we have $G \triangleright H \triangleright \{1\}$ and $|G/H| < |G|$. Repeating this, we obtain a desired sequence. (ii): Let L/K be a subextension of a Galois extension E/K with $\text{Gal}(E/K)$ soluble. Let $F = L(x)$ and let $x = x_1, \dots, x_n$ be the roots of the minimal polynomial of x over K . Then $E' = E(x_1, \dots, x_n)$ is Galois over K and contains F . Let $E = E_0$, $E' = E_n$ and $E_i = E_{i-1}(x_i)$ for $1 \leq i \leq n$. If E_i/E_{i-1} is abelian for all i , then $\text{Gal}(E'/K)$ is soluble by (i) and Exercise 19.1(i). Take $\tau \in \text{Hom}_K(F, E')$ such that $\tau(x) = x_i$ (by extending $\tau \in \text{Hom}_K(K(x), E')$ corresponding to x_i). Then $F = L(x)$ implies $\tau(F) = \tau(L)(x_i)$, and the isomorphism $\text{Gal}(F/L) \ni \sigma \mapsto \tau\sigma\tau^{-1} \in \text{Gal}(\tau(F)/\tau(L))$ shows that $\tau(F)/\tau(L)$ is abelian. As $\tau(L) \subset E \subset E_{i-1}$, the next Lemma shows that E_i/E_{i-1} is Galois with $\text{Gal}(E_i/E_{i-1})$ isomorphic to a subgroup of $\text{Gal}(\tau(F)/\tau(L))$, hence is abelian. \square

Lemma 19.3. *Let $F = K(x)/K$ and L/K be subextensions of a finite extension E/K . The **composite field** of F and L in E is defined as $FL := L(x)$. If F/K is Galois, then FL/L is Galois and the map $\text{Gal}(FL/L) \ni \sigma \mapsto \sigma|_F \in \text{Gal}(F/K)$ is injective.*

Proof. As the minimal polynomial of x over L divides that of x over K , its roots all belong to F if F/K is Galois, which shows that $L(x)/L$ is Galois. The map is injective because $\sigma \in \text{Gal}(L(x)/L)$ is determined by $\sigma(x)$. \square

Definition 19.4. A finite extension obtained as a succession of cyclotomic extensions and Kummer extensions is called a **radical extension**.

Theorem 19.5. *If $\text{char } K = 0$, a finite extension is soluble if and only if it is a subextension of a radical extension.*

Proof. Radical extensions are soluble by an iterated application of Lemma 19.2(ii). Conversely, if F/K is a soluble Galois extension, then take a sequence $\text{Gal}(F/K) = G_0 \triangleright \dots \triangleright G_m = \{1\}$, and let $K = K_0 \subset \dots \subset K_m = F$ be the corresponding subextensions. Let n_i be the order of each cyclic group G_{i-1}/G_i ($1 \leq i \leq m$), and put $n = n_1 \cdots n_m$. By Lemma 19.3, the extension $K_i(\mu_n)/K_{i-1}(\mu_n)$ is cyclic with its Galois group isomorphic to a subgroup of $\text{Gal}(K_i/K_{i-1})$, hence its degree divides $[K_i : K_{i-1}] = n_i$ (Exercise 9.5(ii)). Therefore Theorem 17.4 shows that $K_i(\zeta)/K_{i-1}(\zeta)$ is a Kummer extension, hence $F(\mu_n) = K_m(\mu_n)$ is a radical extension of K . \square

Corollary 19.6. *A general equation of degree $n \geq 5$ is not solvable by iterated radicals, because S_n is not soluble for $n \geq 5$.*

LECTURE 20. DISCRIMINANTS, QUARTICS AND EXAMPLES (SA. 28/11/09)

If $P \in K[X]$ be separable and $\deg P = n$, then the injection $\text{Gal}(P) \rightarrow S_n$ is determined up to conjugation in S_n by Proposition 16.2. Thus for a normal subgroup $H \triangleleft S_n$, the normal subgroup $\text{Gal}(P) \cap H$ of $\text{Gal}(P)$ is well-defined.

Exercise 20.1. A group homomorphism $\text{sgn} : S_n \rightarrow \mathbb{Z}/2\mathbb{Z}$ is defined by sending σ of cyclic type (i_1, \dots, i_r) to $\sum_{j=1}^r (i_j - 1) \pmod 2$.

Definition 20.2. For all $n \geq 2$, the **alternating group** A_n is defined as $\text{Ker}(\text{sgn}) \triangleleft S_n$, a normal subgroup of index 2.

Proposition 20.3. Let $P \in K[X]$ be separable with $\deg P = n$, and F/K its splitting field. The subextension corresponding to $\text{Gal}(P) \cap A_n$ 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 $\text{Root}_P(F) = \{x_1, \dots, x_n\}$. Therefore $\text{Gal}(P) \subset A_n$ if and only if Δ_P is a square in K .

Proof. As Δ_P is fixed under the action of $\text{Gal}(P)$, hence lies in K . Let L/K be the subextension corresponding to $\text{Gal}(P) \cap A_n$. As $\sqrt{\Delta_P} := \prod_{i < j} (x_i - x_j)$ is fixed under the action of $\text{Gal}(P) \cap A_n$ it is in L , and if $\text{Gal}(P)$ is not contained in A_n then $\sqrt{\Delta_P}$ is not fixed by $\text{Gal}(P)$, hence it generates L/K . \square

Example 20.4. 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 $\text{Gal}(P) \cong A_3$ or S_3 by Proposition 18.2, and the two cases occur according to whether $\Delta_P \in K$ is a square or not. If $\text{char } K \neq 2, 3$ and $\mu_3 \subset K$, then 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.

When $n = 4$, the group S_4 is solvable. Define $V_4 := \{1, (12)(34), (13)(24), (14)(23)\} \triangleleft S_4$ (the **Klein 4-group**), which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $S_4/V_4 \cong S_3$, and we have $S_4 \triangleright A_4 \triangleright V_4 \triangleright \mathbb{Z}/2\mathbb{Z} \triangleright \{1\}$ and the successive indices are 2, 3, 2, 2. Consider a quartic $P(X) \in K[X]$ with a splitting field F/K and $\text{Root}_P(F) = \{\alpha, \beta, \gamma, \delta\}$. As $a = \alpha + \beta + \gamma + \delta \in K$, if we subtract $a/4$ from all roots and 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 we have

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

the action of $\text{Gal}(P) \subset S_4$ on $\{\alpha, \beta, \gamma, \delta\}$ induces its action on $\{x^2, y^2, z^2\}$, and the stabilizers of x^2, y^2, z^2 are all equal to $\text{Gal}(P) \cap V_4$ (this realizes $S_3 \cong S_4/V_4$). Thus the subextension of F/K corresponding to $\text{Gal}(P) \cap V_4$ 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 $\text{Root}_Q(L) = \{x^2, y^2, z^2\}$, which is called the **resolvent cubic** of P .

Exercise 20.5. For $P(X) = X^4 + pX^2 + qX + r$, its resolvent cubic is $Q(X) = X^3 + 2pX^2 + (p^2 - 4r)X - q^2$.

Part 5. Beyond the Theory of Equations

LECTURE 21. ANOTHER PROOF OF THE GALOIS THEORY (Tu. 24/11/09)

Proposition 21.1. (Artin's Lemma) *Let F, E be fields and $\sigma_1, \dots, \sigma_n : F \rightarrow E$ 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 $c_1 = \dots = c_n = 0$.*

Proof. Assume otherwise, and take the smallest k such that $\{\sigma_1, \dots, \sigma_k\}$ is linearly dependent, i.e. there exists $c_i \in E$ with $\sum_{i=1}^k c_i \sigma_i = 0$ and $c_k \neq 0$. Note that there exists a $j < k$ with $c_j \neq 0$ because $\sigma_k \neq 0$. For $x, y \in F$ we have $\sum_{i=1}^k c_i \sigma_i(x) \sigma_i(y) = \sum_{i=1}^k c_i \sigma_i(xy) = 0$, i.e. $\sum_{i=1}^k c_i \sigma_i(x) \sigma_i = 0$. Hence

$$\sum_{i=1}^{k-1} c_i (\sigma_i(x) - \sigma_k(x)) \sigma_i = \sum_{i=1}^k c_i \sigma_i(x) \sigma_i - \sigma_k(x) \sum_{i=1}^k c_i \sigma_i = 0,$$

which contradicts the minimality of k once we choose x such that $\sigma_j(x) \neq \sigma_k(x)$, which is certainly possible as $\sigma_j \neq \sigma_k$. \square

Corollary 21.2. *Let F/K be a finite separable extension with $[F : K] = n$, and $\text{Hom}_K(F, E) = \{\sigma_1, \dots, \sigma_n\}$ for an extension E/K . Then a subset $\{x_1, \dots, x_n\} \subset F$ is a K -basis for F if and only if $\det(\sigma_i(x_j)) \neq 0$ in E .*

Proof. Assume $\det(\sigma_i(x_j)) \neq 0$. If $\sum_{j=1}^n c_j x_j = 0$ for $c_i \in K$, then $\sum_{j=1}^n c_j \sigma_i(x_j) = 0$ for all i , thus all c_j are zero and $\{x_1, \dots, x_n\}$ is a K -basis. If $\det(\sigma_i(x_j)) = 0$, then there exists $c_i \in E$, not all equal to zero, such that $\sum_{i=1}^n c_i \sigma_i(x_j) = 0$ for all j . If $\{x_1, \dots, x_n\}$ were a K -basis, then $\sum_{i=1}^n c_i \sigma_i = 0$, which contradicts Artin's Lemma. \square

Similar argument gives a direct proof of the fundamental theorem of Galois theory (Theorem 8.2) without using the primitive element theorem. Recall that for a Galois extension F/K it was reduced (see Lemma 8.3) to proving $|H| \geq [F : F^H]$ for a subgroup $H \subset \text{Gal}(F/K)$. 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 . The system of linear equation $\sum_{i=1}^n c_i \sigma_j(x_i) = 0$ ($1 \leq j \leq m$) has a solution $c_1, \dots, c_n \in F$ where not all c_i are zero. Take the smallest k such that there exists $c_i \in F$ with $\sum_{i=1}^k c_i \sigma_j(x_i) = 0$ and $c_k \neq 0$. We can assume $c_k = 1$ by dividing all c_i by c_k . As x_1, \dots, x_k are linearly independent over F^H there is a $j < k$ such that $c_j \notin F^H$. Then there exists $\sigma \in H$ such that $\sigma(c_j) \neq c_j$. As H is a group, applying σ to the system of linear equations gives $\sum_{i=1}^n \sigma(c_i) \sigma_j(x_i) = 0$ ($1 \leq j \leq m$). Subtracting the original equations give

$$\sum_{i=1}^{k-1} (\sigma(c_i) - c_i) \sigma_j(x_i) = 0 \quad (1 \leq j \leq m),$$

which contradicts the minimality of k because $\sigma(c_j) \neq c_j$.

LECTURE 22. TRACE AND NORM (TH. 26/11/09)

Definition 22.1. Let F/K be a finite separable extension. For $x \in F$, consider the multiplication map $m_x : F \ni y \mapsto xy \in F$ as an endomorphism of F as a K -vector space. Then its trace and determinant are the elements of K , called the **trace** $T_{F/K}(x)$ and **norm** $N_{L/K}(x)$.

Clearly the trace $T_{F/K} : F \rightarrow K$ is a K -linear map, and the norm $N_{F/K} : F^\times \rightarrow K^\times$ is a group homomorphism.

Proposition 22.2. Let F/K be a finite separable extension with $[F : K] = n$, and $\text{Hom}_K(F, E) = \{\sigma_1, \dots, \sigma_n\}$ 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, the trace $T_{F/K} : F \rightarrow K$ is surjective.

Proof. Let $\{e_1, \dots, e_n\}$ be the K -basis of F . The matrix representation in $GL_n(K)$ of $m_x \in \text{End}_K(V)$ is diagonalized in $GL_n(E)$ with the diagonal entries $\sigma_1(x), \dots, \sigma_n(x)$ by the matrix $(\sigma_i(e_j))$, which is invertible by Corollary 21.2. \square

Proposition 22.3. 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 $\text{Hom}_K(F, E) = [F : K]$. Then the proposition follows from the decomposition $\text{Hom}_K(F, E) = \prod_{\tau \in \text{Hom}_K(L, E)} \text{Hom}_L(F, E_\tau)$ (see Lecture 13). \square

- inseparable case?
- dual basis
- Hilbert 90

LECTURE 23. INFINITE GALOIS EXTENSIONS (TU. 1/12/09)

In the following we will fix an algebraic closure of \bar{K} of a field K , and regard any algebraic extension of K as an intermediate field of \bar{K}/K .

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 $\text{Aut}_K(F)$ of all K -automorphisms of F is called the **Galois group** of F/K , and denoted by $\text{Gal}(F/K)$.

For example, the union K^{sep} of all finite separable extensions of K inside \bar{K} is a Galois extension of K by the next lemma and Proposition 15.2:

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 (see Remark ?? – the extension field obtained by the procedure of Proposition 14.1(ii)) coincides with LL' , it is a Galois extension. The latter part follows from the injectivity of the group homomorphism $\text{Gal}(LL'/K) \ni \sigma \mapsto (\sigma|_L, \sigma|_{L'}) \in \text{Gal}(L/K) \oplus \text{Gal}(L'/K)$. \square

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

Exercise 23.4. (i) By Lemma 23.2, the union K_{ab} of all abelian extensions of K contained in \bar{K} is a Galois extension of K . This is called the **maximal abelian extension** of K .

(ii) The union $K(\mu_\infty) = \bigcup_{n \geq 1} K(\mu_n)$ of all cyclotomic extensions of K contained in \bar{K} is a Galois extension of K . This is called the **maximal cyclotomic extension** of K . We have $K(\mu_\infty) \subset K_{ab}$ by Theorem 10.7.

Proposition 23.5. *Let F/K be a Galois extension, and a finite extension L/K be its intermediate field. Then:*

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

Proof. (i) Write $F = \bigcup L'$ as a union of finite Galois extensions L'/K . Then by Lemma 19.3 LL'/L is Galois and $F = \bigcup LL'$, hence F/L is Galois. For each L' , by the latter part of Proposition 14.1 we have $\text{Gal}(L'/K) = \text{Hom}_K(L', \bar{K})$, hence $\text{Gal}(F/K) = \text{Hom}_K(F, \bar{K})$. Therefore if we extend an arbitrary element of $\text{Hom}_K(L, F)$ to an element of $\text{Hom}_K(\bar{K}, \bar{K})$ by Theorem 7.2(ii) and restrict it to F we get an element of $\text{Gal}(F/K)$, hence the surjectivity.

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

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:

$$(x_1, \dots, x_n)(y_1, \dots, y_n) = (x_1y_1, \dots, x_ny_n),$$

$$(\text{ resp. and } (x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)),$$

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:

$$\text{Gal}(F/K) \ni \sigma \mapsto (\sigma|_L) \in \left\{ (\sigma_L)_{L \in \Lambda} \mid L \subset L' \implies \sigma_{L'}|_L = \sigma_L \right\} \subset \prod_{L \in \Lambda} \text{Gal}(L/K).$$

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

Proof. The group homomorphism is defined as $\text{Hom}_K(L, F) = \text{Gal}(L/K)$ 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 $\sigma \in \text{Gal}(F/K)$ by $x \in L \implies \sigma(x) = \sigma_L(x)$, hence it is also surjective. \square

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 $\text{Ker}(G \rightarrow G_\lambda)$ gives the basis of open neighborhoods of 1. The Galois group $\text{Gal}(F/K)$ 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:

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

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

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 $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N} \setminus \{0\}$). 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:

$$\widehat{\mathbb{Z}} = \left\{ (a_n)_{n \geq 1} \mid m \mid n \implies a_n \equiv a_m \pmod{m} \right\} \subset \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}.$$

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 $\mathbb{Z} \ni 1 \mapsto (1)_{n \geq 1} \in \widehat{\mathbb{Z}}$ 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 $\widehat{\mathbb{Z}} \ni (a_n)_{n \geq 1} \mapsto a_n \in \mathbb{Z}/n\mathbb{Z}$ 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 $\text{Fr}_q \in \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ to \mathbb{F}_{q^m} for $m \mid n$ we get $\text{Fr}_q \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. This defines, by Proposition 23.8, the **Frobenius map** as an element of the absolute Galois group as follows:

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

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:

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

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

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

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

Preliminaries I: Linear Algebra

i. SETS AND MAPS

Definition i.1. (i) A **map** $f : X \rightarrow Y$ from the set X to the set Y is a correspondence sending each element x of X to an element $y = f(x)$ of Y . When we want to make the correspondence explicit, we write as

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

- (ii) The map $\text{id}_X : X \ni x \mapsto x \in X$ is called the **identity map** of X .
- (iii) For two maps $f : X \rightarrow Y$ and $g : Y \rightarrow Z$, the map $X \ni x \mapsto g(f(x)) \in Z$ 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 of X is called the **image** of f and denoted by $\text{Im } f$.
- (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 $i_{X'} : X' \ni x \mapsto x \in X$ is called the **inclusion map**. For a map $f : X \rightarrow Y$, the map $f|_{X'} : X' \ni x \mapsto f(x) \in Y$ is called the **restriction** of f to X' . We have $f|_{X'} = f \circ i_{X'}$. In this case, we say that f is an **extension** of $f|_{X'}$.

Definition i.2. (i) A map f is called a **surjection** if $\text{Im } f = Y$.

- (ii) A map f is called an **injection** if it satisfies $f(x) = f(y) \implies x = y$.
- (iii) A map f is called a **bijection** if it is a surjection and an injection.
- (iv) For a bijection f , we define a map $f^{-1} : Y \rightarrow X$ by

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

and call it the **inverse map** of f . Conversely, if there exists a map $f^{-1} : Y \rightarrow X$ satisfying $f^{-1} \circ f = \text{id}_X$ and $f \circ f^{-1} = \text{id}_Y$, 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, \dots, X_n , the set consisting of n -tuples (x_1, \dots, x_n) of elements $x_i \in X_i$ is called the **direct product** of X_1, \dots, X_n , and denoted by

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

ii. ALGEBRAIC SYSTEMS — STRUCTURES

ii.1. **Operations, groups/rings/fields.** Let A be a set, and let x, y, z, \dots 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) $x * (y * z) = (x * y) * z$;
- (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 $*$.)

Example ii.3. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ has two operations $+$ (**addition**) and \times (or \cdot , **multiplication**). The identity of $+$ is 0, and that of \times is 1.

Example ii.4. 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 by 0, and the identity for multiplication by 1. (The identity 0 of addition is called the **zero element**.)

The name “addition” is only used for commutative operations.

Example ii.5. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have addition and multiplication.

Definition ii.6. Let A be a set with the 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.7. 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.8. 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 the operation 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.9. (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.10. If we define an addition by $(x, y) \mapsto x + y - 1$ on the set \mathbb{Z} , it also becomes an additive group.

Definition ii.11. 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) $x(y + z) = xy + xz$;
- (iii) $(x + y)z = xz + yz$.

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

Example ii.12. (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 $A[X_1, \dots, X_n]$ of all polynomials in n variables X_1, \dots, 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 $\{0, 1, \dots, n - 1\}$ 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 $\mathbb{Z} \bmod n$, and denoted by $\mathbb{Z}/(n)$.
- (v) The set of all continuous functions $C(\mathbb{R})$ on \mathbb{R} is a commutative ring with respect to the usual (valuewise) addition and multiplication of functions.

Exercise ii.13. (i) For a ring A , $0 = 1$ 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:

$$\text{Addition: } (x, y) \mapsto xy, \quad \text{Multiplication: } (x, y) \mapsto x^{\log y}.$$

Definition ii.14. (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 the multiplication (Example ii.9(iv)), and is called the **unit group** or **group of units** 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**.

Exercise ii.15. $\mathbb{Z}^\times = \{1, -1\}$, $\mathbb{R}[X]^\times = \mathbb{R}^\times$.

Example ii.16. (i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.

(ii) For a prime number p , the residue class ring $\mathbb{Z}/(p)$ of $\mathbb{Z} \bmod p$ is a field, and is denoted by \mathbb{F}_p . A field consisting of finite number of elements is called a **finite field**.

Definition ii.17. (i) If a subset A' of a group A is again a group under the operation $(e, *)$ of A (in particular $e \in A'$), 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.18. A' is a subgroup of A if and only if $x * y^{-1} \in A'$ for all $x, y \in A'$.

- Example ii.19.** (i) \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} .
(ii) \mathbb{R} is a subring of $\mathbb{R}[X]$.

ii.2. Vector spaces over K .

Definition ii.20. Let V be a set, and A a set with a multiplication. A map

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

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

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

Definition ii.21. Let K be a field. When a set V which has an addition and an action of K satisfies the following, it is called a **vector space** over K , or a **K -vector space**:

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

- Example ii.22.** (i) The additive group 0 consisting of one element 0 is a vector space over any field.
(ii) A field K is a vector space over K , by regarding its multiplication as an action on itself.
(iii) For an integer $n \geq 1$, the set K^n of n -tuples of elements of K is a vector space if we define the addition and the action of K componentwise:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n);$$

$$c(a_1, \dots, a_n) = (ca_1, \dots, ca_n).$$

More generally, for any vector space V over K , the set V^n of n -tuples of elements in V is a vector space under the componentwise addition and K -action.

- (iv) The polynomial ring $K[X]$ over a field K is a vector space over K .
(v) 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} .
(vi) 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} .

Definition ii.23. If a subset V' of a vector space V over K is again a vector space over K by the addition and the action of K on V , V' is called a **subspace** of V .

Exercise ii.24. A subset $V' \subset V$ is a subspace if and only if it satisfies the following conditions:

- (i) $x, y \in V' \implies x - y \in V'$;
(ii) $a \in K, x \in V' \implies ax \in V'$.

- Example ii.25.** (i) For any vector space V , 0 and V are subspaces of V .
 (ii) If we consider \mathbb{C} as a vector space over \mathbb{R} , then \mathbb{R} is a subspace of \mathbb{C} .
 (iii) More generally, if a field K is a subring of a ring L , then L is naturally a vector space over K , and K is a subspace of L . (A ring with a vector space structure over K is called a **K -algebra**.)

ii.3. **A -modules.**

Definition ii.26. Let A be a ring. When a set V which has an addition and an action of A satisfies the following, it is called an **A -module**:

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

- Example ii.27.** (i) The additive group 0 consisting of one element 0 is a modular space 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.
 (iv) For a field K , a vector space over K means a K -module.
 (v) 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 K componentwise:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n);$$

$$c(a_1, \dots, a_n) = (ca_1, \dots, ca_n).$$

- (vi) 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 ii.28. If a subset V' of an A -module V is again an A -module by the addition and the action of A on V , V' is called an **A -submodule** of V .

Definition ii.29. When we consider a commutative ring A as an A -module, an A -submodule of A is called an **ideal** of A .

- Exercise ii.30.** (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. BASIS AND DIMENSION

iii.1. **Linear relation and bases.** Let K be a field, and V a vector space over K .

Definition iii.1. Let X be a subset of V .

- (i) A finite sum of the form $\sum_{i=1}^n a_i x_i$ ($a_i \in K$, $x_i \in X$) is called a **linear combination** of elements of X with coefficients in K . 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.

Lemma iii.2. *The following are equivalent:*

- (i) *There exists a linear relation $\sum_{i=1}^n a_i x_i = 0$ where the coefficient a_1 of x_1 is non-zero.*
(ii) *x_1 can be expressed as a linear combination of x_2, \dots, x_n .*

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

iii.1.1. *Linear independence / generating set.*

- Definition iii.3.** (i) When there is no non-trivial linear relation among the elements 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.
(ii) If all $x \in V$ can be written as a linear combination of elements in X , we say that V is **generated** by X , and X is called a **generating set** of V .

Lemma iii.4. *Let X be linearly independent. For any $y \in V$, if y is expressed as a linear combination of elements of X , the expression 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 expressions, their difference gives a non-trivial linear relation among elements of X . \square

Proposition iii.5. *Let $X \subset Y$.*

- (i) *Y : linearly independent $\implies X$: linearly independent.*
(ii) *X : generates $V \implies Y$: generates V .*

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

Proposition iii.6. *Let $x \notin X$, $Y = X \cup \{x\}$.*

- (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 iii.2.

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

Definition iii.7. A linear independent generating set of V is called a **basis** of V .

Example iii.8. In K^n , if we denote by e_i the element whose i -th component is 1 and the rest are 0, $\{e_1, \dots, e_n\}$ is a basis of K^n . This is called a **canonical basis** of K^n .

iii.2. Existence of a basis and dimension.

iii.2.1. Existence of a basis.

Definition iii.9. A vector space V is **finitely generated** if there is a generating set of V of finite cardinality.

Lemma iii.10. *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 iii.6(i), all the elements of S are linear combinations of elements of T , hence by Lemma iii.6(ii), T is a basis of V . \square

This lemma gives the following:

Theorem iii.11. *A finitely generated vector space has a basis of finite cardinality.*

iii.2.2. *Existence of the dimension.* Let V be a finitely generated vector space over K , and fix a basis $T = \{x_1, \dots, x_n\}$ of V (whose existence is assured by Theorem iii.11).

Lemma iii.12. *If $S = \{y_1, \dots, y_k\} \subset V$ ($k \leq n$) is linearly independent, we can renumber the indices of $x_i \in T$ so that $U = \{y_1, \dots, y_k, x_{k+1}, \dots, x_n\}$ 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 $U' = \{y_1, \dots, y_{k-1}, x_k, \dots, x_n\}$ by the inductive hypothesis. As U' is a basis, we can write y_k (uniquely, by Lemma iii.4) as a linear combination of elements of U' as:

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

which gives a linear relation:

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

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 $U = U' \setminus \{x_k\} \cup \{y_k\}$ is a basis of V .

As U' is linearly independent, $U' \setminus \{x_k\}$ is linearly independent. By the uniqueness of expression (1), y_k cannot be a linear combination of $U' \setminus \{x_k\}$, hence $U' \setminus \{x_k\} \cup \{y_k\} = U$ is linearly independent by Lemma iii.6(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 $U = U' \cup \{y_k\} \setminus \{x_k\}$ by Lemma iii.2(i) \Rightarrow (ii). Hence $U' \cup \{y_k\} \setminus \{x_k\} = U$ generates V by iii.6(ii). \square

Proposition iii.13. *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 iii.12. 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 iii.6(i).

(ii) A subset U of S gives a basis of V by Lemma iii.10, hence using (i) we see that $|T| = n \leq |U|$. Hence $|S| \geq |U| \geq n$, and if $|S| = n$ we have $S = U$. \square

By this proposition we obtain:

Theorem iii.14. *All bases of V have the same number of elements.*

- Definition iii.15.**
- (i) The cardinality of a basis, which is unique by the above theorem, is called the **dimension** of V , and denoted by $\dim_K V$ or $\dim V$.
 - (ii) A finitely generated vector space over K is called **finite-dimensional**. Otherwise it is called **infinite-dimensional** and we formally write $\dim V = \infty$.

Remark iii.16. The vector space 0 is finite-dimensional as it has the empty set as a basis, and $\dim 0 = 0$. Conversely $\dim V = 0 \implies V = 0$.

- Exercise iii.17.**
- (i) K^n is has dimension n as vector space over K , and in general, V^n has dimension $n \dim V$.
 - (ii) $K[X]$ is infinite-dimensional vector space over K .
 - (iii) If we denote $K[X]_{\deg \leq n}$ for the set of all polynomials in X with degree not greater than n , then it is a $(n + 1)$ -dimensional vector space over K , and $\{1, X, X^2, \dots, X^n\}$ gives its basis.
 - (iv) The set of all sequences $\{a_n\}_{n \in \mathbb{N}}$ of real numbers satisfying $a_{n+2} = a_n + a_{n+1}$ is a 2-dimensional vector space over \mathbb{R} .
 - (v) \mathbb{C} is a 2-dimensional vector space over \mathbb{R} .
 - (vi) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, $\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$ are both 2-dimensional vector spaces over \mathbb{Q} .
 - (vii) The \mathbb{R} -vector space $C(\mathbb{R})$ of all continuous functions on \mathbb{R} is infinite-dimensional.
 - (viii) If we write $C^\infty(\mathbb{R})$ for the set of all functions on \mathbb{R} that are differentiable arbitrary many times, then it is an infinite-dimensional vector space over \mathbb{R} .

(The above two examples are seen to be infinite-dimensional using the Lemma iv.9 from $\mathbb{R}[X] \subset C^\infty(\mathbb{R}) \subset C(\mathbb{R})$.)

iv. LINEAR MAPS — MORPHISMS

iv.1. **Linear maps.** Let K be a field.

Definition iv.1. For two vector spaces V, W over K , a map $f : V \rightarrow W$ is called a **K -linear map** if satisfies the following conditions:

- (i) $f(x + y) = f(x) + f(y) \quad (\forall x, y \in V)$;
- (ii) $f(ax) = af(x) \quad (\forall a \in K, \forall x \in V)$.

In particular, K -linear map $f : V \rightarrow V$ is called a **linear transformation** of V .

- Exercise iv.2.**
- (i) The identity map $\text{id}_V : V \rightarrow V$ is K -linear.
 - (ii) The composite of two K -linear maps is again K -linear.
 - (iii) The restriction $f|_{V'} : V' \rightarrow W$ of a K -linear map $f : V \rightarrow W$ to a subspace $V' \subset V$ is again K -linear.

Definition iv.3. A K -linear map is called an **isomorphism** if it is bijective. When an isomorphism $f : V \rightarrow W$ exists, we say that V and W are **isomorphic**, and write $V \cong W$.

Exercise iv.4. The identity, the inverse of an isomorphism, the composite of two isomorphisms are all again isomorphisms.

Exercise iv.5. The complex conjugate map $\mathbb{C} \ni x \mapsto \bar{x} \in \mathbb{C}$ of \mathbb{C} is an isomorphism of vector spaces over \mathbb{R} , but not a \mathbb{C} -linear map of vector spaces over \mathbb{C} .

Definition iv.6. For a K -linear map $f : V \rightarrow W$, the subset $\{x \in V \mid f(x) = 0\}$ of V is called the **kernel** of f and denoted by $\text{Ker } f$.

Proposition iv.7. For a K -linear map $f : V \rightarrow W$, $\text{Ker } f$ and $\text{Im } f$ are subspaces of V and W , respectively.

Proof. $\text{Ker } f$ is a subspace of V because:

$$\begin{aligned} f(x_1) = 0, f(x_2) = 0 &\implies f(x_1 - x_2) = f(x_1) - f(x_2) = 0, \\ f(x) = 0 &\implies f(ax) = af(x) = 0. \end{aligned}$$

$\text{Im } f$ is a subspace of Y because:

$$\begin{aligned} y_1 = f(x_1), y_2 = f(x_2) &\implies y_1 - y_2 = f(x_1) - f(x_2) = f(x_1 - x_2), \\ y = f(x) &\implies ay = af(x) = f(ax). \end{aligned}$$

□

Proposition iv.8. A K -linear map $f : V \rightarrow W$ is injective if and only if $\text{Ker } f = 0$.

Proof. Rewrite the definition $f(x) = f(y) \implies x = y$ of the injection as $f(x - y) = 0 \implies x - y = 0$. □

iv.2. Dimension formula.

Lemma iv.9. *A subspace V' of a finite-dimensional vector space V is again finite-dimensional and $\dim V' \leq \dim V$. If $\dim V' = \dim V$ then $V' = V$.*

Proof. By Proposition iii.13(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 iii.6(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 iii.13(i), hence $V' = V$. \square

In the following, we assume that vector spaces V, W over K are finite-dimensional.

Proposition iv.10. *Let $f : V \rightarrow W$ be a K -linear map.*

- (i) *If f is surjective, X generates $V \implies f(X)$ generates W .*
- (ii) *If f is injective, X : linearly independent $\implies f(X)$: linearly independent.*
- (iii) *If f is an isomorphism, X : a basis of $V \iff f(X)$: a basis of W .*

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 :

$$\sum_{i=1}^n a_i f(x_i) = 0 \implies f\left(\sum_{i=1}^n a_i x_i\right) = 0.$$

Hence, if f is injective and X is linearly independent, it must be a trivial relation.

(iii) Combine (i),(ii) and use $X = f^{-1}(f(X))$. \square

Corollary iv.11. *For a K -linear map $f : V \rightarrow W$:*

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

Theorem iv.12. (dimension formula) *For a K -linear map $f : V \rightarrow W$:*

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

Proof. Let $\dim V = n$, $\dim(\text{Ker } f) = k$ and $l = n - k$ and take a basis $\{y_1, \dots, y_k\}$ of $\text{Ker } f$. Then we can take a basis of V of the form $T = \{y_1, \dots, y_k, x_1, \dots, x_l\}$ by Lemma iii.12. Let V' be the subspace of V generated by $\{x_1, \dots, x_l\}$, and restrict f to $f|_{V'} : V' \rightarrow W$. As T is linearly independent $\text{Ker } f|_{V'} = \text{Ker } f \cap V' = 0$, hence $f|_{V'}$ is injective (Proposition iv.8), and any element in the image of V is the image of an element of V' , hence $f|_{V'}$ is a surjection onto $\text{Im } f$. Therefore $V' \cong \text{Im } f$ and $\dim(\text{Im } f) = \dim V' = l$. \square

Corollary iv.13. For a linear transformation $f : V \rightarrow V$,

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

Proof. $f: \text{injective} \iff \dim(\text{Ker } f) = 0 \iff \dim(\text{Im } f) = \dim V \iff f: \text{surjective}$. (These equivalences come from respectively Proposition iv.8, dimension formula (Theorem iv.12) and Lemma iv.9.) \square

Exercise iv.14. (i) For a vector space over K and $a \in K$, **a -multiplication:**

$V \ni x \mapsto ax \in V$ is a K -linear map, and an isomorphism if $a \neq 0$.

(ii) $\mathbb{C} \ni x \mapsto x + \bar{x} \in \mathbb{R}$ is a surjective \mathbb{R} -linear map.

(iii) The map of **substituting** $x \in K$ into polynomials with K -coefficients $K[X] \ni P(X) \mapsto P(x) \in K$ is a surjective K -linear map.

(iv) Taking derivatives of polynomials with \mathbb{R} -coefficients $\mathbb{R}[X] \ni P(X) \mapsto P'(X) \in \mathbb{R}[X]$ is a surjective \mathbb{R} -linear map, and its kernel is the subspace \mathbb{R} consisting of all constant functions. (The derivative can be defined on polynomial rings over any field K by $X^n \mapsto nX^{n-1}$. See Definition 10.2.)

(v) The **differentiation** $\frac{d}{dx} : C^\infty(\mathbb{R}) \ni f \mapsto f' \in C^\infty(\mathbb{R})$ is a surjective \mathbb{R} -linear

map, and $\text{Ker} \left(\frac{d}{dx} \right)$ is the subspace \mathbb{R} of all constant functions. For more

general **differential operator**, such as $\frac{d}{dx} - \text{id} : C^\infty(\mathbb{R}) \ni f \mapsto f' - f \in C^\infty(\mathbb{R})$ is an \mathbb{R} -linear map, and its kernel is the subspace consisting of solutions of the differential equation (such as $f' = f$).

(vi) If we denote by $C([0, 1])$ the set of all continuous function on the closed segment $[0, 1]$, the **integration** $C([0, 1]) \ni f \mapsto \int_0^1 f(x)dx \in \mathbb{R}$ is a surjective \mathbb{R} -linear map.

iv.3. Homomorphisms.

Definition iv.15. (i) Let X, Y be sets with operations $(e_X, *_X), (e_Y, *_Y)$ respectively. A map $f : X \rightarrow Y$ is called 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 $f : X \rightarrow Y$ is called **A -equivariant** if it satisfies $f(ax) = af(x)$.

Definition iv.16. (i) A homomorphism $f : X \rightarrow Y$ between groups X, Y is called a **group homomorphism**.

(ii) A homomorphism $f : X \rightarrow Y$ between rings X, Y , with respect to both addition and multiplication, is called a **ring homomorphism**.

(iii) An A -equivariant homomorphism $f : X \rightarrow Y$ between A -modules X, Y is called an **A -homomorphism**.

Exercise iv.17. (i) The identity map is a homomorphism.

(ii) The composite of two homomorphisms is again a homomorphism.

(iii) For any ring X , there is a unique ring homomorphism $\mathbb{Z} \rightarrow X$.

(iv) For any ring X , there is a unique ring homomorphism $X \rightarrow 0$.

- (v) Any ring homomorphism $f : X \rightarrow Y$ gives a group homomorphism $f|_{X^\times} : X^\times \rightarrow Y^\times$.
- (vi) For a field K , a K -homomorphism means a K -linear map.

Definition iv.18. A homomorphism which is a bijection is called an **isomorphism**. When an isomorphism $f : X \rightarrow Y$ exists, we say that X and Y are **isomorphic**, and write $X \cong Y$.

Exercise iv.19. The identity, the inverse of an isomorphism, the composite of two isomorphisms are all again isomorphisms.

- Definition iv.20.**
- (i) For a group homomorphism $f : X \rightarrow Y$, the subset $\{x \in X \mid f(x) = e_Y\}$ of X is called the **kernel** of f and denoted by $\text{Ker } f$.
 - (ii) For a ring homomorphism or an A -homomorphism $f : X \rightarrow Y$, the subset $\{x \in X \mid f(x) = 0\}$ of X is called the **kernel** and denoted by $\text{Ker } f$.

- Exercise iv.21.**
- (i) For a group homomorphism $f : X \rightarrow Y$, $\text{Ker } f$, $\text{Im } f$ are subgroups of X, Y respectively.
 - (ii) For a ring homomorphism $f : X \rightarrow Y$, $\text{Ker } f$ is an ideal of X , and $\text{Im } f$ is a subring of Y .
 - (iii) For an A -homomorphism $f : X \rightarrow Y$, $\text{Ker } f$, $\text{Im } f$ are A -submodules of X, Y respectively.

- Exercise iv.22.** (i) If we denote the group defined in Exercise ii.10 by \mathbb{Z}' , the map from \mathbb{Z} :

$$\mathbb{Z} \ni x \mapsto x + 1 \in \mathbb{Z}'$$

gives an isomorphism of additive groups.

- (ii) For $n \geq 1$, a map which takes $x \in \mathbb{Z}$ to the residue \bar{x} after dividing by n :

$$\mathbb{Z} \ni x \mapsto \bar{x} \in \mathbb{Z}/(n)$$

gives a surjective ring homomorphism, and its kernel is (n) .

- (iii) The map from the polynomial ring $\mathbb{R}[X]$ over \mathbb{R} to \mathbb{C} defined by substituting $\sqrt{-1}$ into X :

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

is a surjective ring homomorphism, and its kernel is the set $(X^2 + 1)$ of all polynomials that are divisible by $X^2 + 1$.

v. Hom — CLASSIFICATION OF STRUCTURES

v.1. Hom, End. Let K be a field.

Definition v.1. For vector spaces V_1, V_2 over K , the set of all K -linear maps from V_1 to V_2 is denoted by $\text{Hom}_K(V_1, V_2)$ (or simply $\text{Hom}(V_1, V_2)$). The sum $f_1 + f_2$ and scalar multiple af for $f, f_1, f_2 \in \text{Hom}_K(V_1, V_2)$ is defined as

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

which makes $\text{Hom}_K(V_1, V_2)$ into a vector space over K . In particular, the set of linear transformations $\text{Hom}(V, V)$ of V is denoted by $\text{End}(V)$.

As the composite of K -linear maps was again K -linear, there is a map:

$$\text{Hom}(V_1, V_2) \times \text{Hom}(V_2, V_3) \ni (g, f) \mapsto f \circ g \in \text{Hom}(V_1, V_3),$$

which clearly satisfies $f \circ (g \circ h) = (f \circ g) \circ h$.

Definition v.2. In $\text{End}(V)$, the composite:

$$\text{End}(V) \times \text{End}(V) \ni (g, f) \mapsto f \circ g \in \text{End}(V)$$

is an operation on $\text{End}(V)$ with the identity being the identity map $\text{id} \in \text{End}(V)$. This gives a (non-commutative) ring structure on $\text{End}(V)$, and this ring is called the **endomorphism ring** of V .

Exercise v.3. Check that $\text{End}(V)$ satisfies the definition of rings.

Exercise v.4. $\text{End}(V)$ turns out to have dimension $(\dim V)^2$ as a vector space over K , and is an example of a K -algebra.

As the inverse with respect to the multiplication of $\text{End}(V)$ is none other than the inverse map, therefore $f \in \text{End}(V)$ is a unit if and only if f is an isomorphism.

Definition v.5. The unit group $\text{End}(V)^\times$ (the group of all the isomorphisms $f : V \rightarrow V$) of $\text{End}(V)$ is called the **automorphism group** of V and denoted by $\text{Aut}(V)$.

Exercise v.6. If we fix an $f \in \text{Hom}(V_1, V_2)$, for any W , there are K -linear maps:

$$\begin{aligned} f^* : \text{Hom}(V_2, W) \ni g &\mapsto g \circ f \in \text{Hom}(V_1, W), \\ f_* : \text{Hom}(W, V_1) \ni g &\mapsto f \circ g \in \text{Hom}(W, V_2). \end{aligned}$$

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

v.2. $\text{Hom}(K^n, V)$ — **representation by bases.** Let V be a vector space over K . For any element $x \in V$, there is a K -linear map K :

$$\varphi_x : K \ni a \mapsto ax \in V.$$

More generally, for any n -tuples $X = \{x_1, \dots, x_n\} \in V^n$ of elements in V , there is a K -linear map:

$$\varphi_X : K^n \ni (a_1, \dots, a_n) \mapsto a_1x_1 + \dots + a_nx_n \in V.$$

This gives a K -linear map $V^n \ni X \mapsto \varphi_X \in \text{Hom}(K^n, V)$, and its inverse is given by

$$\text{Hom}(K^n, V) \ni \varphi \mapsto (\varphi(e_1), \dots, \varphi(e_n)) \in V^n,$$

where $\{e_1, \dots, e_n\}$ is the canonical basis of Example iii.8.

Proposition v.7. By the above bijection, $V^n \cong \text{Hom}(K^n, V)$.

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

Lemma v.8. For a subset $X \subset V$ consisting of n distinct elements, let $\varphi_X : K^n \rightarrow V$ be the K -linear map defined above.

- (i) X : linearly independent $\iff \varphi_X$: injective.
- (ii) X : generates V $\iff \varphi_X$: surjective.
- (iii) X : basis of V $\iff \varphi_X$: an isomorphism.

By the above, we have:

Proposition v.9. *Let $\text{Basis}(V)$ be the set of all bases of V consisting of n elements (considered as an ordered set, i.e. we distinguish the permuted bases), and $\text{Isom}(K^n, V)$ be the set of all isomorphisms from K^n to V . Then there is a bijection:*

$$\text{Basis}(V) \ni X \mapsto \varphi_X \in \text{Isom}(K^n, V).$$

In other words, fixing a basis X of V consisting of n elements is equivalent to fixing an isomorphism $f : K^n \rightarrow V$. In particular, as a basis exists for any finite-dimensional vector spaces:

Theorem v.10. *If V is an n -dimensional vector space over K , then $K^n \cong V$. In particular, if V, W are finite-dimensional vector spaces, $V \cong W \iff \dim V = \dim W$.*

Proof. The first part follows from the existence of a basis. As for the second part, \Rightarrow follows from Corollary iv.11(iii), and \Leftarrow is because if $\dim V = \dim W = n$ then $K^n \cong V$, $K^n \cong W$. \square

v.3. Change of bases. Let V be a n -dimensional vector space over K . As the composite of two isomorphisms is again an isomorphism, the group $\text{Aut}(V)$ acts on $\text{Isom}(K^n, V)$ as follows:

$$\text{Aut}(V) \times \text{Isom}(K^n, V) \ni (f, \varphi) \mapsto f \circ \varphi \in \text{Isom}(K^n, V).$$

Under the bijection $\text{Isom}(K^n, V) \ni \varphi \mapsto X = \{\varphi(e_1), \dots, \varphi(e_n)\} \in \text{Basis}(V)$ of Proposition v.9, we have $f \circ \varphi \mapsto f(X)$, so if we consider the above action as an action on $\text{Basis}(V)$, we get:

$$\text{Aut}(V) \times \text{Basis}(V) \ni (f, X) \mapsto f(X) \in \text{Basis}(V).$$

Proposition v.11. (change of bases) *Let $X = \{x_1, \dots, x_n\} \in \text{Basis}(V)$.*

- (i) *For any $f \in \text{Aut}(V)$, $f(X) = \{f(x_1), \dots, f(x_n)\}$ is again a basis of V .*
- (ii) *For any basis X' of V , there is a unique $f \in \text{Aut}(V)$ satisfying $f(X) = X'$.*
- (iii) *$\text{Aut}(V) \ni f \mapsto f(X) \in \text{Basis}(V)$ is a bijection.*

Proof. (i): Clear by the above action. (ii): By the bijection of Proposition v.9, $f(X) = X' \iff f \circ \varphi_X = \varphi_{X'} \iff f = \varphi_{X'} \circ \varphi_X^{-1}$. (iii) follows immediately from (i),(ii). \square

$f = \varphi_{X'} \circ \varphi_X^{-1}$ is represented by the following diagram:

$$\begin{array}{ccc} & K^n & \\ \varphi_X \swarrow & & \searrow \varphi_{X'} \\ V & \xrightarrow{f} & V \end{array}$$

(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. (In this case, $f \circ \varphi_X = \varphi_{X'}$.)

v.4. **Categories.**

Definition v.12. A **category** \mathcal{C} is defined as follows:

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

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

called the **composition** of morphisms.

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

Definition v.13. (i) A morphism $f \in \text{Hom}_{\mathcal{C}}(X, Y)$ of \mathcal{C} is called an **isomorphism** of \mathcal{C} if there exists a $g \in \text{Hom}_{\mathcal{C}}(Y, X)$ satisfying

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

- (ii) When an isomorphism $f \in \text{Hom}_{\mathcal{C}}(X, Y)$ exists, we say that X and Y are **isomorphic** in \mathcal{C} , and write $X \cong_{\mathcal{C}} Y$.

Example v.14. The **category of sets** **Sets** has sets as objects and maps as morphisms. The **category of vector spaces** \mathbf{Vect}_K has K -vector spaces as objects and K -linear maps as morphisms. Similarly we can define the category **Groups** of groups and group homomorphisms, **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** means \mathbf{Vect}_K (Example ii.27(iv), iv.17(vi)).

Exercise v.15. For an object $X \in \mathcal{C}$ of a category \mathcal{C} , the set $\text{Aut}_{\mathcal{C}}(X)$ of all isomorphisms $f : X \rightarrow X$ is a group under the composition.

vi. MATRIX REPRESENTATION OF LINEAR MAPS — REPRESENTATIONS OF STRUCTURES

vi.1. **Matrices.** Let K be a field, and $n, m \geq 1$ be integers.

As giving a K -linear map $f \in \text{Hom}(K^n, K^m)$ is equivalent to giving $f(e_1), \dots, f(e_n)$, if we set, for $1 \leq j \leq n$,

$$f(e_j) = (a_{1j}, \dots, a_{mj}),$$

the map f is uniquely represented by the mn numbers $a_{ij} \in K$ ($1 \leq i \leq m, 1 \leq j \leq n$).

Definition vi.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:

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

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

Proposition vi.2. As K -vector spaces, $\text{Hom}(K^n, K^m) \cong M_{m,n}(K)$.

By Proposition v.7, we have $\text{Hom}(K^n, K^m) \cong (K^m)^n \cong K^{mn}$ as K -vector spaces, hence $M_{m,n}(K)$ is a mn -dimensional vector space. There is an obvious canonical basis on $M_{m,n}(K)$:

Definition vi.3. 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}) .

Clearly $\{(1_{ij})\}_{1 \leq i \leq m, 1 \leq j \leq n}$ gives a basis of $M_{m,n}(K)$.

Moreover, if we compose $g \in \text{Hom}(K^n, K^m)$ and $f \in \text{Hom}(K^m, K^l)$ we get $f \circ g \in \text{Hom}(K^n, K^l)$, but if we represent f , g , $f \circ g$ respectively by $(a_{ij}) \in M_{l,m}(K)$, $(b_{jk}) \in M_{m,n}(K)$, $(c_{ik}) \in M_{l,n}(K)$, we have:

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

Hence we define:

Definition vi.4. For $(a_{ij}) \in M_{l,m}(K)$, $(b_{jk}) \in M_{m,n}(K)$, the matrix $(c_{ik}) \in M_{l,n}(K)$ defined by $c_{ik} = \sum_{j=1}^m a_{ij} b_{jk}$ is called the **product** of (a_{ij}) , (b_{jk}) and written as $(c_{ik}) = (a_{ij})(b_{jk})$.

Note that associativity of additions and compositions of matrices follow from those for $\text{Hom}(K^n, K^m)$. In particular, the set of all n by n matrices, corresponding to the endomorphism ring $\text{End}(K^n) = \text{Hom}(K^n, K^n)$ of K^n , has a ring structure.

Definition vi.5. An n by n matrix is called a **square matrix** of degree n , and the set $M_{n,n}(K)$ of all square matrices of degree n over K is denoted simply by $M_n(K)$. This is

a ring by the entrywise addition and the product, and the identity of the multiplication is the following matrix:

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

This (δ_{ij}) is 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 is the matrix representing the identity map $\text{id} \in \text{End}(K^n)$. Similarly, we can represent the automorphism group $\text{Aut}(K^n)$ of K^n by matrices.

Definition vi.6. A square matrix $\alpha \in M_n(K)$ is called **invertible** when 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 set of all n by n invertible matrices is the unit group of the ring $M_n(K)$. This group is called the **general linear group** of degree n over K , and is denoted by $GL_n(K) = M_n(K)^\times$.

Exercise vi.7. When $n = 1$, $M_1(K) \cong K$, $GL_1(K) \cong K^\times$. For $n > 1$, $M_n(K)$ is a non-commutative ring, and $GL_n(K)$ is a non-commutative group.

vi.2. Matrix representation of linear maps. Let V_1, V_2 be finite-dimensional vector spaces over K , and let their dimension be n, m respectively.

If we fix a basis $Y = \{y_j\}$ of V_1 and a basis $X = \{x_i\}$ of V_2 , they give isomorphisms $\varphi_Y : K^n \rightarrow V_1$, $\varphi_X : K^m \rightarrow V_2$. For any $f \in \text{Hom}(V_1, V_2)$, if we let $f' = \varphi_X^{-1} \circ f \circ \varphi_Y$, there is a following commutative diagram:

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

By this correspondence, we have an isomorphism:

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

Definition vi.8. For a K -linear map $f \in \text{Hom}(V_1, V_2)$, the matrix $(a_{ij}) \in M_{m,n}(K)$ representing f' is called the **representation matrix** of f with respect to bases $Y = \{y_j\}, X = \{x_i\}$.

Exercise vi.9. 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 vi.10. The representation matrix of an isomorphism is invertible. The identity and inverse maps are represented respectively by identity and inverse matrices.

Exercise vi.11. Fix the bases $Z = \{z_i\}, Y = \{y_j\}, X = \{x_k\}$ for the K -vector spaces $V_1 \cong K^n, V_2 \cong K^m, V_3 \cong K^l$ and let the representation matrices of $f \in \text{Hom}(V_2, V_3), g \in \text{Hom}(V_1, V_2)$ with respect to these bases be $(a_{ij}) \in M_{l,m}(K), (b_{jk}) \in M_{m,n}(K)$ respectively. Then the composite $f \circ g \in \text{Hom}(V_1, V_3)$ is represented by the product $(c_{ik}) = (a_{ij})(b_{jk})$:

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

vi.3. Change of bases for matrix representations.

Lemma vi.12. Let $(p_{ij}) \in GL_n(K)$ be the representation matrix of $f \in \text{Aut}(V)$ with respect to the basis $X = \{x_i\}$, and let $f(X) = X'$. Then we have a commutative diagram:

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

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

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

as $f = \varphi_{X'} \circ \varphi_X^{-1}$, we obtain the lemma. \square

Remark vi.13. If we set $X' = \{x'_j\} = f(X)$ then $x'_j = \sum_{i=1}^n p_{ij}x_i$ by Exercise vi.9.

Let V_1, V_2 be K -vector spaces with dimension respectively n, m , and fix the bases $Y = \{y_j\}, X = \{x_i\}$ respectively of V_1, V_2 . Consider the change of basis $g_1(Y) = Y', g_2(X) = X'$ under $g_1 \in \text{Aut}(V_1), g_2 \in \text{Aut}(V_2)$, and let $\eta = (q_{ij}), \xi = (p_{ij}) \in GL_n(K)$ respectively be the representation matrices of g_1, g_2 with respect to Y, X .

Proposition vi.14. If we let $\alpha = (a_{ij})$ (resp. $\alpha' = (a'_{ij})$) be the representation matrix of a K -linear map $f \in \text{Hom}(V_1, V_2)$ with respect to Y, X (resp. Y', X'). Then:

$$\alpha' = \xi^{-1}\alpha\eta.$$

Proof. By Lemma vi.12, consider the commutative diagram:

$$\begin{array}{ccccccc}
 K^n & \xrightarrow{\eta} & K^n & \xrightarrow{\alpha} & K^m & \xrightarrow{\xi^{-1}} & K^m \\
 \searrow \varphi_{Y'} & & \swarrow \varphi_Y & & \searrow \varphi_X & & \swarrow \varphi_{X'} \\
 & & V_1 & \xrightarrow{f} & V_2 & &
 \end{array}$$

□

Corollary vi.15. *Let V be an n -dimensional vector space. Let the image of the basis $X = \{x_i\}$ under $g \in \text{Aut}(V)$ be $X' = g(X)$, and let $\xi = (p_{jk})$ be the representation matrix of g with respect to X . If we denote the representation matrix of an $f \in \text{End}(V)$ with respect to X (resp. X') by $\alpha = (a_{ij})$ (resp. $\alpha' = (a'_{ij})$), then:*

$$\alpha' = \xi^{-1}\alpha\xi.$$

Exercise vi.16. Represent the following linear maps with respect to the given bases.

- (i) For a K -vector space V and $a \in K$, the a -multiplication $V \ni x \mapsto ax \in V$ has the same representation matrix for any bases.
- (ii) The \mathbb{R} -linear map $\mathbb{C} \ni x \mapsto x + \bar{x} \in \mathbb{R}$, the basis $\{1, \sqrt{-1}\}$ of \mathbb{C} , the basis $\{1\}$ of \mathbb{R} .
- (iii) The \mathbb{R} -linear map $\mathbb{C} \ni x \mapsto (a + b\sqrt{-1})x \in \mathbb{C}$ ($a, b \in \mathbb{R}$), the basis $\{1, \sqrt{-1}\}$ of \mathbb{C} .
- (iv) The \mathbb{Q} -linear map $\mathbb{Q}(\sqrt{2}) \ni x \mapsto \sqrt{2}x \in \mathbb{Q}(\sqrt{2})$, the basis $\{1, \sqrt{2}\}$ of $\mathbb{Q}(\sqrt{2})$.
- (v) The same map, with respect to the basis $\{1 + \sqrt{2}, 1 - \sqrt{2}\}$ of $\mathbb{Q}(\sqrt{2})$, and check that the formula of Corollary vi.15 holds.
- (vi) The substitution map $K[X]_{\text{deg} \leq n} \ni P(X) \mapsto P(x) \in K$ for $x \in K$, the basis $\{1, X, X^2, \dots, X^n\}$ of $K[X]_{\text{deg} \leq n}$, the basis $\{1\}$ of K .
- (vii) The derivative map $\mathbb{R}[X]_{\text{deg} \leq n} \ni P(X) \mapsto P'(X) \in \mathbb{R}[X]_{\text{deg} \leq n-1}$, the basis $\{1, X, X^2, \dots, X^n\}$ of $\mathbb{R}[X]_{\text{deg} \leq n}$, the basis $\{1, X, X^2, \dots, X^{n-1}\}$ of $\mathbb{R}[X]_{\text{deg} \leq n-1}$. (For the definition of $K[X]_{\text{deg} \leq n}$, see Exercise iii.17.)

vii. DETERMINANTS AND LINEAR EQUATIONS

vii.1. Determinants.

vii.1.1. Volume Forms.

Definition vii.1. A map $\Phi : V^n \rightarrow K$ is called an n -fold **multilinear form** on V 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) $\Phi(x_1, \dots, ax_i, \dots, x_n) = a\Phi(x_1, \dots, x_i, \dots, x_n)$ ($\forall a \in K$).

If moreover it satisfies

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

then Φ is called a **alternating multilinear form**. The set of all alternating n -fold multilinear forms on V is a K -vector space by the addition and scalar multiplication on their values.

Lemma vii.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 $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ (**permutation**):

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

(Here $s(\sigma) = \prod_{1 \leq j < i \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \in \{\pm 1\}$ is called the **sign** of σ .)

- (iii) If $y_j = \sum_{i=1}^n a_{ij}x_i$ ($1 \leq j \leq n$), then:

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

(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.)

$$\begin{aligned} \text{(iii): } \Phi(y_1, \dots, y_n) &= \Phi\left(\sum_{i=1}^n a_{i1}x_i, \dots, \sum_{i=1}^n a_{in}x_i\right) = \sum_{i_1, \dots, i_n} a_{i_1 1} \cdots a_{i_n n} \Phi(x_{i_1}, \dots, x_{i_n}) \\ &= \left(\sum_{\sigma \in S_n} s(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n}\right) \Phi(x_1, \dots, x_n). \quad \square \end{aligned}$$

Definition vii.3. For an n -dimensional K -vector space V , an alternating n -fold multilinear form on V is called a **volume form** on V , and we denote the set of all volume forms on V by $\text{Vol}(V)$.

Proposition vii.4. $\text{Vol}(V)$ is a 1-dimensional vector space over K .

Proof. Fix a basis $\{x_1, \dots, x_n\}$ of V . Then the K -linear map:

$$\text{Vol}(V) \ni \Phi \longmapsto \Phi(x_1, \dots, x_n) \in K$$

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

vii.1.2. *Determinants.* Take an $f \in \text{End}(V)$. For a $\Phi \in \text{Vol}(V)$,

$$\Phi \circ f : V^n \ni (x_1, \dots, x_n) \mapsto \Phi(f(x_1), \dots, f(x_n)) \in K$$

is again an alternating n -fold multilinear form, i.e. a volume form. Thus we have a map:

$$\text{Vol}(V) \ni \Phi \mapsto \Phi \circ f \in \text{Vol}(V)$$

which is clearly K -linear, hence an a -multiplication for some $a \in K$ by Proposition vii.4.

Definition vii.5. The element $\det f \in K$ satisfying $\Phi \circ f = (\det f) \cdot \Phi$ is called the **determinant** of f .

Proposition vii.6. (i) $\det(\text{id}) = 1$, $\det(f \circ g) = \det f \cdot \det g$.

(ii) $f \in \text{Aut}(V) \implies \det f \neq 0$.

(iii) $\det : \text{Aut}(V) \rightarrow K^\times$ is a surjective group homomorphism.

Proof. (i): $\Phi \circ (f \circ g) = (\Phi \circ f) \circ g$, $\Phi \circ \text{id} = \Phi$.

(ii): $f \in \text{Aut}(V) \implies \exists g \in \text{End}(V)$, $f \circ g \implies \det f \cdot \det g = 1 \implies \det f \neq 0$.

(iii): (i),(ii) show that it is a group homomorphism. For any $a \in K^\times$, if we consider an $f \in \text{Aut}(V)$ mapping a basis $X = \{x_1, \dots, x_n\}$ to $X' = \{ax_1, x_2, \dots, x_n\}$, then $\det f = a$. \square

Remark vii.7. As $\Phi \circ (f + g) \neq (\Phi \circ f) + (\Phi \circ g)$, \det is not a K -linear map from $\text{End}(V)$ to K .

vii.1.3. *The main theorem for volume forms and determinants.*

Proposition vii.8. For $\Phi \in \text{Vol}(V) \setminus \{0\}$ and $X \in V^n$, $\Phi(X) \neq 0 \iff X \in \text{Basis}(V)$.

Proof. \implies : If $X \notin \text{Basis}(V)$, X is linearly dependent by Proposition iii.13(i), hence some x_i is a non-trivial linear combination of other x_j 's, and $\Phi(X) = 0$ as Φ is alternating multilinear form.

\Leftarrow : As $\Phi \neq 0$, there exists $X_0 \in V^n$ such that $\Phi(X_0) \neq 0$. BBy \implies we have $X_0 \in \text{Basis}(V)$, hence by Proposition v.11(ii), we have $f(X_0) = X$ for $f = \varphi_X \circ \varphi_{X_0}^{-1} \in \text{Aut}(V)$. Hence $\Phi(X) = (\Phi \circ f)(X_0) = (\det f) \cdot \Phi(X_0)$ and Proposition vii.6(ii) gives $\Phi(X) \neq 0$. \square

Theorem vii.9. For $f \in \text{End}(V)$, $f \in \text{Aut}(V) \iff \det f \neq 0$.

Proof. \implies is just Proposition vii.6(ii). We will show \Leftarrow . Take a $\Phi \in \text{Vol}(V) \setminus \{0\}$ and $X_0 \in V^n$ with $\Phi(X_0) \neq 0$. If we let $f(X_0) = X$, then $\Phi(X) = (\Phi \circ f)(X_0) = (\det f)\Phi(X_0) \neq 0$. Proposition vii.8 shows that $X_0, X \in \text{Basis}(V)$, hence $f = \varphi_X \circ \varphi_{X_0}^{-1} \in \text{Aut}(V)$ (Proposition v.11(ii)). \square

vii.2. Matrix representation of the determinant.

Proposition vii.10. *Let (a_{ij}) be the matrix representation of $f \in \text{End}(V)$ with respect to the 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 we let $X = \{x_1, \dots, x_n\}$, then $f(x_j) = \sum_{i=1}^n a_{ij} x_i$. For any $\Phi \in \text{Vol}(V)$, Lemma vii.2(iii) shows $(\Phi \circ f)(X) = \Phi(f(X)) = \left(\sum_{\sigma \in S_n} s(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} \right) \Phi(X)$. \square

Definition vii.11. We define the **determinant** of $\alpha = (a_{ij}) \in M_n(K)$ as follows:

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

Exercise vii.12. (i) $\det(\delta_{ij}) = 1$, $\det(\alpha\beta) = \det \alpha \det \beta$. (Proposition vii.6(i))
(ii) $\alpha \in GL_n(K) \iff \det \alpha \neq 0$. (Proposition vii.6(ii))
(iii) $\det({}^t \alpha) = \det \alpha$.

vii.3. System of linear equations. Let K be a field, and 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:

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

Proposition vii.13. *Assume $m = n$. Then $(a_{ij})(X_j) = (b_i)$ has a unique solution (X_j) if $\det(a_{ij}) \neq 0$.*

Proof. By Exercise vii.12(ii), $(a_{ij}) \in GL_n(K)$ and $(X_j) = (a_{ij})^{-1}(b_i)$. \square

Proposition vii.14. *Consider the system of equations $(a_{ij})(X_j) = (0)$.*

- (i) *Assume $m = n$. Then there exists a solution $(X_j) \neq (0) \iff \det(a_{ij}) = 0$.*
- (ii) *Assume $m < n$. Then there always exists a solution $(X_j) \neq (0)$.*

Proof. If we let $a_j = (a_{1j}, \dots, a_{mj})$, then the system of equations $(a_{ij})(X_j) = (0)$ is none other than the linear relation $\sum_{j=1}^n a_j X_j = 0$ in K^m , hence

There exists a solution $(X_j) \neq (0) \iff \{a_1, \dots, a_n\}$: linearly dependent.

Therefore (i) is a restatement of Proposition vii.8, (ii) that of Proposition iii.13(i). \square

vii.4. **Cofactor and inverse matrix.**

Exercise vii.15. Let $(a_{ij}) \in M_n(K)$ be a matrix.

- (i) Assume that the j_0 -th column of (a_{ij}) satisfies $a_{ij_0} = \sum_k b_i^k x_k$, and let (a_{ij}^k) be a matrix obtained by replacing the j_0 -th column of (a_{ij}) by (b_i^k) . Then $\det(a_{ij}) = \sum_k \det(a_{ij}^k) x_k$.
- (ii) If we exchange two different columns of (a_{ij}) , the determinant is multiplied by (-1) .
- (iii) If two different columns of (a_{ij}) are identical, then the determinant is 0.

Definition vii.16. The (i, j) -**cofactor** Δ_{ij} of (a_{ij}) is defined by multiplying $(-1)^{i+j}$ to the determinant of $n - 1$ by $n - 1$ square matrix obtained by removing the i -th row and the j -th column from $\alpha = (a_{ij})$. The matrix $\Delta_\alpha = (\Delta_{ij}) \in M_n(K)$ is called the **cofactor matrix** of α .

Proposition vii.17. $\alpha \Delta_\alpha = \Delta_\alpha \alpha = \det \alpha \cdot (\delta_{ij})$. In particular, $\alpha^{-1} = (\det \alpha)^{-1} \Delta_\alpha$.

Proof. First we show that the (j_0, j_0) -entry of $\Delta_\alpha \alpha$ is equal to $\det \alpha$. Let (a_{ij}^k) be the matrix obtained from $\alpha = (a_{ij})$ by replacing the (k, j_0) -entry by 1 and all the other entries in the j_0 -th column by 0. Following the exercise vii.15(i), we get $\det(a_{ij}^k) = \sum_k \det(a_{ij}^k) a_{kj_0}$. Let (b_{ij}^k) be the matrix obtained from (a_{ij}^k) by repeating the exchange with the neighboring row/column on the k -th row and the j_0 -th column until the (k, j_0) -entry moves to the (n, n) -entry. By this procedure the determinant is multiplied by $(-1)^{n-k} (-1)^{n-j_0} = (-1)^{k+j_0}$ (Exercise vii.15(ii)), and as the n -th row of (b_{ij}^k) is all 0 except for the (n, n) -entry which is 1:

$$\begin{aligned} \det(a_{ij}^k) &= (-1)^{k+j_0} \det(b_{ij}^k) = (-1)^{k+j_0} \sum_{\sigma} s(\sigma) \prod_{i=1}^n b_{i\sigma(i)}^k \\ &= (-1)^{k+j_0} \sum_{\sigma(n)=n} s(\sigma) \prod_{i=1}^{n-1} b_{i\sigma(i)}^k = \Delta_{j_0 k}. \end{aligned}$$

Hence $\det(a_{ij}) = \sum_k \Delta_{j_0 k} a_{kj_0}$.

Then we show that the (j_1, j_2) -entries for $(j_1 \neq j_2)$ are all 0. If we denote by (a'_{ij}) the matrix obtained from (a_{ij}) by replacing the j_1 -th column by the j_2 -th column, by Exercise vii.15(iii) we have $\det(a'_{ij}) = 0$, and its cofactors for the j_1 -th column coincide with the ones for (a_{ij}) . Therefore by the above result:

$$0 = \det(a'_{ij}) = \sum_k \Delta_{j_1 k} a'_{kj_1} = \sum_k \Delta_{j_1 k} a_{kj_2}.$$

For the $\alpha \Delta_\alpha$, it is shown in exactly the same way using the expansion with respect to rows (Exercise vii.12(iii)). □

viii. DIRECT SUM AND DIAGONALIZATION — DECOMPOSITION OF STRUCTURES

viii.1. Direct sum.

viii.1.1. Direct sum of vector spaces.

Definition viii.1. Let V_1, V_2 be two vector spaces over K . We can define the componentwise operation on the direct product set $V_1 \times V_2$ to make it into a K -vector space:

$$\begin{aligned}(x_1, x_2) + (y_1, y_2) &= (x_1 + y_1, x_2 + y_2), \\ a(x_1, x_2) &= (ax_1, ax_2).\end{aligned}$$

The vector space thus obtained is denoted by $V_1 \oplus V_2$ and called the **direct sum** of V_1, V_2 . Similarly we can define the componentwise operations on the direct product set $V_1 \times \cdots \times V_n$ of n vector spaces V_1, \dots, V_n :

$$\begin{aligned}(x_1, \dots, x_n) + (y_1, \dots, y_n) &= (x_1 + y_1, \dots, x_n + y_n), \\ a(x_1, \dots, x_n) &= (ax_1, \dots, ax_n),\end{aligned}$$

and this vector space is denoted by $\bigoplus_{i=1}^n V_i = V_1 \oplus \cdots \oplus V_n$ and called the **direct sum** of V_1, \dots, V_n . In particular, direct sum $V \oplus \cdots \oplus V$ of n copies of V is denoted by V^n (defined in Exercise ii.22(iii)).

The following two maps are injective K -linear maps (**natural injection**):

$$\begin{aligned}i_1 : V_1 \ni x_1 &\longmapsto (x_1, 0) \in V_1 \oplus V_2, \\ i_2 : V_2 \ni x_2 &\longmapsto (0, x_2) \in V_1 \oplus V_2.\end{aligned}$$

We regard V_1, V_2 as subspaces of $V_1 \oplus V_2$ by these injections.

Exercise viii.2. For any vector space W ,

$$\text{Hom}(V_1 \oplus V_2, W) \ni f \longmapsto (f \circ i_1, f \circ i_2) \in \text{Hom}(V_1, W) \oplus \text{Hom}(V_2, W)$$

gives an isomorphism. In other words, when there are two K -linear maps $f_1 : V_1 \rightarrow W$, $f_2 : V_2 \rightarrow W$, if we define a K -linear map by $f : V_1 \oplus V_2 \rightarrow W$ by $f(x_1, x_2) = f_1(x_1) + f_2(x_2)$, this gives the unique K -linear map which satisfies $f \circ i_1 = f_1$, $f \circ i_2 = f_2$.

Exercise viii.3. $\dim(V_1 \oplus V_2) = \dim V_1 + \dim V_2$.

viii.1.2. Direct sum of K -linear maps.

Definition viii.4. For two K -linear maps $f_1 : V_1 \rightarrow W_1$, $f_2 : V_2 \rightarrow W_2$, the K -linear map:

$$V_1 \oplus V_2 \ni (x_1, x_2) \longmapsto (f_1(x_1), f_2(x_2)) \in W_1 \oplus W_2$$

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

Exercise viii.5. If we denote the natural injections by $i_k^V : V_k \rightarrow V_1 \oplus V_2$, $i_k^W : W_k \rightarrow W_1 \oplus W_2$ ($k = 1, 2$), the direct sum $f = f_1 \oplus f_2$ is the unique K -linear map satisfying the following property:

$$f \circ i_1^V = i_1^W \circ f_1, \quad f \circ i_2^V = i_2^W \circ f_2.$$

viii.1.3. *Direct sum decomposition.*

Definition viii.6. (i) For two subspaces V_1, V_2 of V , if the K -linear map:

$$V_1 \oplus V_2 \ni (x_1, x_2) \mapsto x_1 + x_2 \in V$$

is an isomorphism, we write $V = V_1 \oplus V_2$ and it is called a **direct sum decomposition** of V .

(ii) Let V, W be both decomposed into direct sums as $V = V_1 \oplus V_2$, $W = W_1 \oplus W_2$. For a K -linear map $f : V \rightarrow W$, if there are K -linear maps $f_1 : V_1 \rightarrow W_1$, $f_2 : V_2 \rightarrow W_2$ such that $f|_{V_1} = f_1$, $f|_{V_2} = f_2$, we write $f = f_1 \oplus f_2$ and it is called a **direct sum decomposition** of f .

Remark viii.7. $\text{Hom}(V_1, W_1) \oplus \text{Hom}(V_2, W_2) \ni (f_1, f_2) \mapsto f_1 \oplus f_2 \in \text{Hom}(V_1 \oplus V_2, W_1 \oplus W_2)$ is not a surjection, therefore there are maps f which are not decomposed into direct sum.

Exercise viii.8. When $f = f_1 \oplus f_2$, there is a following commutative diagram:

$$\begin{array}{ccc} V_1 \oplus V_2 & \xrightarrow{\cong} & V \\ f_1 \oplus f_2 \downarrow & & \downarrow f \\ W_1 \oplus W_2 & \xrightarrow{\cong} & W \end{array}$$

Exercise viii.9. Let V be an n -dimensional vector space over K , and $X = \{x_1, \dots, x_n\}$ be its basis. If we write $V_i = \{ax_i \mid a \in K\}$ for the subspace generated by $\{x_i\}$:

$$\bigoplus_{i=1}^n V_i = V_1 \oplus \dots \oplus V_n \ni (y_1, \dots, y_n) \mapsto \sum_{i=1}^n y_i \in V$$

is an isomorphism, i.e. gives a direct sum decomposition of V into V_1, \dots, V_n . Conversely, for any direct sum decomposition of V into n pieces of 1-dimensional subspaces V_i , choosing a basis (a non-zero element) of V_i gives a basis of V .

viii.2. **The category of linear transformations and diagonalization.**

Definition viii.10. We will consider the pairs (V, φ) consisting of a finite dimensional K -vector space V and its linear transformation $\varphi \in \text{End}(V)$.

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

Example viii.11. When V is 1-dimensional, any $\varphi \in \text{End}(V)$ 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**.

Remark viii.12. We are using the term “pairs”, but as φ determines V , we can consider φ as the only essential object.

Definition viii.13. (i) For a pair (V, φ) , we call a pair (W, ψ) consisting of a subspace W of V and $\psi \in \text{End}(W)$ a **subpair** of (V, φ) if $\varphi|_W = \psi$, and we write $(W, \psi) \subset (V, \varphi)$. An inclusion $i : W \rightarrow V$ gives a morphism of pairs $i : (W, \psi) \rightarrow (V, \varphi)$. In particular the subpairs which are elementary, **elementary subpairs**, will be important.

- (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, φ_1) , (V_2, φ_2) of (V, φ) satisfy $V = V_1 \oplus V_2$, $\varphi = \varphi_1 \oplus \varphi_2$, we write $(V, \varphi) = (V_1, \varphi_1) \oplus (V_2, \varphi_2)$ and call it a **direct sum decomposition** of (V, φ) .

Proposition viii.14. For a pair (V, φ) and $c \in K$:

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

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

$$\begin{aligned} \exists (V_0, c) \subset (V, \varphi) &\iff \exists x \in V \setminus \{0\} \quad \varphi(x) = cx \iff \text{Ker}(\varphi - c \cdot \text{id}) \neq 0 \\ &\iff \varphi - c \cdot \text{id} \notin \text{Aut}(V) \iff \det(\varphi - c \cdot \text{id}) = 0 \end{aligned}$$

(The latter two equivalences follow respectively from Corollary iv.13 and Theorem vii.9.) \square

Definition viii.15. For a pair (V, φ) , the polynomial in one variable X with K -coefficients $P_\varphi(X) = \det(\varphi - X \cdot \text{id})$ is called the **characteristic polynomial** of (V, φ) , and its roots are called **eigenvalues** of (V, φ) .

For an eigenvalue c of (V, φ) , an $x \in V \setminus \{0\}$ satisfying $\varphi(x) = cx$ (a basis of an elementary subpair) is called an **eigenvector** of (V, φ) for the eigenvalue c .

Proposition viii.16. 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) .

Proof. \Rightarrow : If $(V, \varphi) = (V_1, c_1) \oplus \cdots \oplus (V_n, c_n)$, 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 $\{x_1, \dots, x_n\}$ consisting of eigenvectors of (V, φ) , if we let c_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 $\varphi = c_1 \oplus \cdots \oplus c_n$. \square

Definition viii.17. A pair (V, φ) satisfying the above condition is called **diagonalizable** or **semisimple**.

Exercise viii.18. If we consider c -multiplication for $c \in K$, any $x \in V \setminus \{0\}$ is an eigenvector for the eigenvalue c , hence (V, c) is diagonalizable.

Exercise viii.19. When $(V, \varphi) = (V_1, c_1) \oplus \cdots \oplus (V_n, c_n)$, if we represent φ with respect to the basis consisting of non-zero elements $x_i \in V_i$, then we obtain a matrix of the following form (called a **diagonal matrix**):

$$\text{diag}(c_1, \dots, c_n) = \begin{pmatrix} c_1 & 0 & \cdots & 0 \\ 0 & c_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & c_n \end{pmatrix}.$$

Preliminaries II: Rings and Modules

ix. PRIME DECOMPOSITION AND PRINCIPAL IDEAL DOMAINS

In the rest of this book, by *rings* we always mean *commutative rings* unless otherwise stated. Let A be a ring, and a, b, c, \dots denote elements of A .

ix.1. Integral domains and prime decomposition.

ix.1.1. Domains and divisibility.

Definition ix.1. Let A be a ring, and a, b, c, \dots denote the elements of A .

- (i) An element b is **divisible** by a if $\exists c \in A$, $b = ac$, and we write $a \mid b$.
- (ii) If $a \mid b$, we say that a is a **divisor** of b , and b is a **multiple** of a .
- (iii) A divisor of 1 is called a **unit**. The set of all units of A is denoted by A^\times .
- (iv) When $a \mid b$ and $b \mid a$, we say that a and b are **associate** to each other.

Exercise ix.2. The unit group of a field A is $A^\times = A \setminus \{0\}$.

Definition ix.3. 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 ix.4. (i) A subring of a domain is also a domain.

- (ii) In a domain, if $a \neq 0$, then $ab = ac \implies b = c$.
- (iii) A field is a domain.

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

Definition ix.5. (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 $p \mid ab \implies p \mid a$ 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 we can identify the associate elements 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 ix.6. If A is a domain, a, b : associate $\iff \exists c \in A^\times, b = ac$.

Exercise ix.7. (i) The units of \mathbb{Z} are ± 1 , and irreducibles of \mathbb{Z} are prime numbers $\times(\pm 1)$.

(ii) A field does not have any prime nor irreducible elements.

Proposition ix.8. *In a domain, all primes are irreducible.*

Proof. If a prime p decomposes 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 $p = pcb$. By Exercise ix.4(ii), we have $cb = 1$, which shows that b is a unit. Therefore p does not have any proper divisors. \square

ix.1.2. *Prime Decomposition.*

Proposition ix.9. *In a domain, the decomposition 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 ix.4(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. \square

Definition ix.10. If every element of a domain A , except 0 and units, is a product of primes, A is called a **unique factorization domain (UFD)**.

The decomposition of an element into a product of primes is unique up to associate (Proposition ix.9).

Definition ix.11. Two elements a, b of a UFD A are said to be **relatively prime** or **coprime** to each other if no prime is a divisor of both elements.

ix.2. **Ideals.**

ix.2.1. *Ideals and principal 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 ii.27(ii)). Recall that an A -submodule of A is called an **ideal** of A (Definition ii.29).

Exercise ix.12. Ideals of a field A are only 0 and A .

Exercise ix.13. If A is a subring of B , (i) B is naturally an A -module, and (ii) every B -module is naturally an A -module.

Definition ix.14. 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 ix.15. (i) $a = 0 \iff (a) = 0$.
 (ii) $a \in A^\times \iff (a) = A$.
 (iii) For an ideal I , $(a) \subset I \iff a \in I$.

Exercise ix.16. (principal ideals and divisibility)

(i) $(a) \supset (b) \iff a \mid b$.
 (ii) $(a) = (b) \iff a, b : \text{associate}$.

If we assume A is a domain, we have:

(iii) $A \neq (a) \supsetneq (b) \iff a : \text{a proper divisor of } b$.
 (iv) $(a) = (b) \iff b = ac, c \in A^\times$.

ix.2.2. *Prime ideals and maximal ideals.*

Definition ix.17. An ideal $I \subsetneq A$ is called:

(i) **prime** if the following holds: $a, b \notin I \implies ab \notin I$,
 (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 $\text{Spec}(A)$ (resp. $\text{m-Spec}(A)$).

Exercise ix.18. (i) $A = 0 \implies \text{Spec}(A) = \emptyset$.
 (ii) $A : \text{domain} \iff 0 \in \text{Spec}(A)$.
 (iii) In a domain, $A \ni a : \text{prime} \iff (a) \in \text{Spec}(A) \setminus \{0\}$.
 (iv) If A is a subring of B , then $Q \in \text{Spec}(B) \implies Q \cap A \in \text{Spec}(A)$.
 (v) More generally, for a ring homomorphism $f : A \rightarrow B$, $Q \in \text{Spec}(B) \implies f^{-1}(Q) \in \text{Spec}(A)$.

Definition ix.19. For ideals I_1, I_2 of A , the set $\{x + y \mid x \in I_1, y \in I_2\}$ is another ideal of A , and contains both I_1 and I_2 . This ideal is called the **sum** of I_1 and I_2 , and denoted by $I_1 + I_2$.

Example ix.20. 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 ix.21. $\text{m-Spec}(A) \subset \text{Spec}(A)$.

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. \square

ix.3. Principal ideal domains.

Definition ix.22. A domain is called a **principal ideal domain (PID)** if all of its ideals are principal.

Example ix.23. A field is a PID.

Proposition ix.24. Let A be a PID, and $a \in A$. Then:

- (i) a : irreducible $\iff (a) \in \mathfrak{m}\text{-Spec}(A)$,
- (ii) a : irreducible $\iff a$: prime.

Proof. (i) Follows from Exercise ix.16(iii).

(ii) \Leftarrow : Proposition ix.8. \Rightarrow : Use (i), Proposition ix.21, and Exercise ix.18(i). \square

Proposition ix.25. 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, \dots , by Exercise ix.16(iii) we have $(a_i) \subsetneq (a_{i+1})$ ($\forall i \in \mathbb{N}$). On the other hand, consider the ideal $I = \bigcup_{i=0}^{\infty} (a_i)$ of A (see Exercise ix.26 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 $(a) \subset (a_i) \subsetneq (a_{i+1}) \subset (a)$ is a contradiction. \square

Exercise ix.26. For an increasing sequence $I_0 \subset I_1 \subset I_2 \subset \dots$ of ideals in A , the union $I = \bigcup_{i=0}^{\infty} I_i$ is an ideal of A .

Theorem ix.27. $\text{PID} \implies \text{UFD}$.

Proof. Follows from Proposition ix.25 and Proposition ix.24(ii). \square

ix.4. Euclidean domains.

Definition ix.28. A domain A is called a **euclidean domain** if there exists a map $f : A \rightarrow \mathbb{N} \cup \{-\infty\}$ satisfying the following condition:

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

Exercise ix.29. (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 ix.30. $\text{Euclidean domain} \implies \text{PID}$.

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 $I = (a)$. \square

Theorem ix.31. (Fundamental theorem of arithmetic) \mathbb{Z} is a PID, therefore a UFD.

Proof. Follows from Exercise ix.29(i), Proposition ix.30 and Theorem ix.27. \square

x. POLYNOMIAL RINGS, GAUSS' LEMMA

x.1. **Polynomial ring over a field.** Let A be a ring.

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

- Exercise x.2.** (i) If A is a subring of B , $A[X]$ is naturally a subring of $B[X]$.
 (ii) $A : \text{domain} \implies A[X] : \text{domain}, \ A[X]^\times = A^\times$.

In the following, K denotes a field.

Proposition x.3. $K : \text{field} \implies K[X] : \text{PID}$.

Proof. Follows from Exercise ix.29(ii) and Theorem ix.30. \square

Exercise x.4. As $K[X]^\times = K^\times = K \setminus \{0\}$, every $P \in K[X] \setminus \{0\}$ is associate to some monic polynomial with the same degree. Therefore, every ideal of $K[X]$ is generated by a monic polynomial.

Proposition x.5. The number of roots of $P \in K[X] \setminus \{0\}$ is not greater than $\deg P$.

Proof. For $a \in K, P \in K[X]$, we have $P = (X - a)Q + R, \ \deg R < 1$ (Exercise ix.29(ii)). As $\deg R < 1$ means $R \in K$, by substituting X by a , we have $P(a) = R$. Therefore:

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

and the number of roots of P is equal to the number of monics with degree one that divides P . As $K[X]$ is a UFD, considering the uniqueness of prime decomposition (factorization into irreducibles) of P , which factors into a constant and monic polynomials, this number is at most $\deg P$. \square

Definition x.6. For a root $a \in K$ of $P \in K[X]$, the maximal integer n satisfying $(X - a)^n \mid P$ is called the **multiplicity**, and a root with multiplicity greater than one is called a **multiple root**.

x.2. **Fraction fields and polynomial rings over UFD.** Let A be a domain.

Definition x.7. 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. If we denote the quotient set by K and the equivalence class of (a, b) by $\frac{a}{b}$, we can define

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

independently on the choice of representatives and K becomes a field. This field is called the **fraction field** of A , and denoted by $\text{Frac}(A)$. The map $A \ni x \mapsto \frac{x}{1} \in K$ is an injective ring homomorphism (with which we always regard A as a subring of K).

Example x.8. \mathbb{Q} is (defined as!) the fraction field of \mathbb{Z} .

Exercise x.9. For a subring A of a field K , the fraction field of A is contained in K . In particular, the fraction field of a field K is K itself.

Proposition x.10. (i) **(Gauss' Lemma)**
(ii) **(Eisenstein's irreducibility criterion)**

xi. QUOTIENT RINGS

xi.1. **Quotient algebraic systems.**

Definition xi.1. Let X be a set. Suppose we know, for every pair of elements x, y of X , a relation $x \sim y$ holds or not. The relation \sim is called an **equivalence relation** if the following conditions are satisfied:

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

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 \bar{x} , and x is called a **representative element** of the class \bar{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 xi.2. (i) For a subgroup Y of an additive group X , if we define a relation \sim in X as:

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

it is an equivalence relation, and we can define a natural addition on the quotient set of X by \sim (denoted by X/Y) by the addition of representative elements, and it is an additive group.

- (ii) For an ideal Y of a ring X , we can define a natural multiplication on the additive group X/Y by multiplication of representative elements, and it becomes a ring.
- (iii) For an A -submodule Y of an A -module X , we can define a natural A -action on the additive group X/Y by A -action on representative elements, and it becomes an A -module.

Proof. (i) First, the relation \sim is an equivalence relations because

$$\begin{aligned} x - x &= 0 \in Y, \\ x - y \in Y &\implies y - x = -(x - y) \in Y, \\ x - y, y - z \in Y &\implies x - z = (x - y) + (y - z) \in Y \end{aligned}$$

hold. Secondly,

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

shows that the operation $\bar{x} + \bar{y} = \overline{x + y}$ on X/Y is well-defined regardless of the choice of representative elements (and $\bar{0}$ is the zero element) which gives the addition on X/Y , and it is a group as $\overline{-x}$ gives the inverse element of \bar{x} .

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

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

holds, and hence $\bar{x} \cdot \bar{y} = \overline{xy}$ is well-defined regardless of the choice of representatives (and $\bar{1}$ is the unity), and X/Y becomes a ring.

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

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

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

Definition xi.3. The X/Y in Proposition xi.2(i),(ii),(iii) are called respectively **quotient group**, **quotient ring**, **quotient A -module** of X by Y . The surjection $X \rightarrow X/Y$ defined by $x \mapsto \bar{x}$ is called the **canonical surjection**. It is a homomorphism by definition. We also write \bar{x} as $x \bmod Y$.

Exercise xi.4. $X/0 \cong X$, $X/X \cong 0$.

Example xi.5. (i) For an ideal (n) ($n \geq 1$) of \mathbb{Z} , the quotient ring $\mathbb{Z}/(n) = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ is “the ring of residues of integers divided by n ”. We also denote $\bar{k} = k \bmod (n)$ as $k \bmod n$.

- (ii) The quotient ring of $\mathbb{R}[X]$ by the ideal $(X^2 + 1)$ is isomorphic to \mathbb{C} by the following ring isomorphism (in fact, it is the formal definition of the complex numbers):

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

Exercise xi.6. For general (non-commutative) group G and its subgroup H , in order to define the quotient group G/H , it is necessary for H to satisfy the following condition:

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

A subgroup H satisfying this condition is called a **normal subgroup** of G , and we denote it as $G \triangleright H$.

xi.2. Homomorphism theorem.

Proposition xi.7. Consider a homomorphism $f : X \rightarrow Y$ of groups/rings/ A -modules.

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

Proof. (i) By the following:

$$\begin{aligned} f(x_1) = 0, f(x_2) = 0 &\implies f(x_1 - x_2) = 0, \\ y_1 = f(x_1), y_2 = f(x_2) &\implies y_1 - y_2 = f(x_1 - x_2). \end{aligned}$$

(ii) By (i) and the following:

$$\begin{aligned} f(x_2) = 0 &\implies f(x_1 x_2) = f(x_1) f(x_2) = 0, \\ y_1 = f(x_1), y_2 = f(x_2) &\implies y_1 y_2 = f(x_1 x_2), f(1) = 1. \end{aligned}$$

(iii) By (i) and the following:

$$\begin{aligned} f(x) = 0 &\implies f(ax) = af(x) = 0, \\ y = f(x) &\implies ay = af(x) = f(ax). \end{aligned}$$

□

Theorem xi.8. (Homomorphism theorem) For a (group/ring/ A -) homomorphism $f : X \rightarrow Y$, there is a canonical isomorphism $X/\text{Ker } f \cong \text{Im } f$.

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

$$\bar{x} = \bar{y} \iff x - y \in \text{Ker } f \iff f(x) = f(y),$$

therefore the map:

$$\bar{f} : X/\text{Ker } f \ni \bar{x} \mapsto f(x) \in \text{Im } f$$

is well-defined and injective. As \bar{f} is clearly surjective, it is bijective. Also, as f is a homomorphism, the bijection \bar{f} is a homomorphism by:

$$\begin{aligned}\bar{f}(\bar{x} + \bar{y}) &= \bar{f}(\overline{x + y}) = f(x + y) = f(x) + f(y) = \bar{f}(\bar{x}) + \bar{f}(\bar{y}), \\ \bar{f}(\bar{0}) &= f(0) = 0,\end{aligned}$$

therefore a group isomorphism. Similarly when f is a ring (resp. A -) homomorphism, we see that the bijection \bar{f} is a ring (resp. A -) homomorphism, therefore it is a ring (resp. A -) isomorphism. \square

Exercise xi.9. For homomorphism $f : X \rightarrow Y$ of general (non-commutative) groups, $\text{Ker } f$ is a normal subgroup of X and $\text{Im } f$ is a subgroup of Y , and $X/\text{Ker } f \cong \text{Im } f$.

xi.3. Ideals and quotient rings. For an A -homomorphism $f : X \rightarrow Y$ between A -modules, let S be the set of all A -submodules of X that contain $\text{Ker } f$, and T the set of all A -submodules of $\text{Im } f$. As the image of an A -submodule of X is always an A -submodule of $\text{Im } f$, and the inverse image of an A -submodule of $\text{Im } f$ is always an A -submodule of X containing $\text{Ker } f$, we have the following two maps:

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

Proposition xi.10. *The two maps Φ, Ψ are inverse to each other, and therefore both isomorphisms.*

Proof. These maps clearly preserve the inclusion relations, and as $f(f^{-1}(J)) = J$, we have $\Phi \circ \Psi = \text{id}$. 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 $x - y \in \text{Ker } f \subset I$ shows that $x = y + (x - y) \in I$, we have $f^{-1}(f(I)) \subset I$, hence $\Psi \circ \Phi = \text{id}$. \square

Proposition xi.11. *For a surjective homomorphism $f : A \rightarrow B$, above Φ, Ψ give one-to-one correspondence between (i) the prime ideals of A that contain $\text{Ker } f$ and the prime ideals of B , and (ii) the maximal ideals of A that contain $\text{Ker } f$ and the maximal ideals of B .*

Proof. That maximals correspond to each other follows from the fact that Φ, Ψ preserve the inclusion relations. Also, for $P \in \text{Spec}(A)$, let $a, b \notin f(P)$, and choosing $a' \in f^{-1}(a)$, $b' \in f^{-1}(b)$, as

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

we see that $f(P) \in \text{Spec}(B)$. That $Q \in \text{Spec}(B) \implies f^{-1}(Q) \in \text{Spec}(A)$ is Exercise ix.18(v). \square

Corollary xi.12. (i) $I \in \text{Spec}(A) \iff A/I : \text{domain}$.
(ii) $I \in \text{m-Spec}(A) \iff A/I : \text{field}$.

Proof. Using Proposition xi.11 on the canonical surjection $A \ni a \mapsto \bar{a} \in A/I$, we see that $I \subset A$ and $0 \subset A/I$ correspond with each other, therefore the corollary follows from Exercise ix.18(ii). \square

Example xi.13. 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.16(ii)).

xii. CHARACTERISTIC OF A FIELD

Let K be a field. The image of the natural ring homomorphism $\varphi : \mathbb{Z} \rightarrow K$ (defined 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 xi.12(i)).

Definition xii.1. When $\text{Ker } \varphi = 0$, K is said to have **characteristic 0**, and when $\text{Ker } \varphi = (p)$ for a prime p , K is said to have **characteristic p** . The characteristic of K is denoted by $\text{char } K$.

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

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

(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 .)

xiii. MINIMAL POLYNOMIAL OF LINEAR TRANSFORMATIONS

Let K be a field, V an n -dimensional vector space over K . The ring of endomorphisms $\text{End}(V)$ of V is a K -algebra which is non-commutative ring in general and has dimension n^2 as a vector space over K (Exercise v.4).

For any $\varphi \in \text{End}(V)$, consider the ring homomorphism of “substituting φ into polynomials with coefficients in K ”:

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

(set $f_\varphi(1) = \text{id}$ to make it into a ring homomorphism). This f_φ is K -linear and $\text{Im } f_\varphi$ is finite-dimensional, being a subspace of $\text{End}(V)$ (Lemma iv.9), and as $K[X]$ is infinite-dimensional, $\text{Ker } f_\varphi \neq 0$. Therefore, by Proposition x.3, $\text{Ker } f_\varphi$ is a principal ideal (Q_φ) generated by $Q_\varphi \neq 0$, and $\text{Im } f_\varphi$ is a subring of $\text{End}(V)$ isomorphic to $K[X]/(Q_\varphi)$.

Definition xiii.1. The monic generator Q_φ (Exercise x.4) of $\text{Ker } f_\varphi$ is called the **minimal polynomial** of f over K .

Remark xiii.2. This Q_φ has minimal degree among the polynomials with coefficients in K which have φ as a “root”, but it is not necessarily irreducible.

Proposition xiii.3. For $c \in K$, c : an eigenvalue of $\varphi \iff Q_\varphi(c) = 0$.

Proof. Recall that, by Proposition viii.14 and Corollary iv.13,

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

\Rightarrow : If $Q_\varphi(c) \neq 0$, $Q_\varphi \notin (X-c)$ in $K[X]$, and as $(X-c) \in \text{m-Spec}K[X]$, $(Q_\varphi) + (X-c) = K[X]$. Hence there exist R_1, R_2 such that $Q_\varphi R_1 + (X-c)R_2 = 1$. Then $f_\varphi(R_2)$ gives the inverse of $f_\varphi(X-c) = \varphi - c \cdot \text{id}$ in $\text{End}(V)$, hence $\varphi - c \cdot \text{id} \in \text{Aut}(V)$. \Leftarrow : If $Q_\varphi(c) = 0$, we can write $Q_\varphi = (X-c) \cdot R$, so by applying f_φ , $0 = (\varphi - c \cdot \text{id}) \circ f_\varphi(R)$. Now if $\varphi - c \cdot \text{id} \in \text{Aut}(V)$, we can multiply its inverse $\psi = (\varphi - c \cdot \text{id})^{-1}$ to get $0 = f_\varphi(R)$, hence $Q_\varphi \mid R$, which contradicts $\deg R < \deg Q_\varphi$. \square

Remark xiii.4. The same proposition holds for the **characteristic polynomial** P_φ of φ (Proposition viii.14), 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.)

xiv. ZORN'S LEMMA

Definition xiv.1. Let X be a set. Suppose we know, for every pair of elements x, y of X , a relation $x \leq y$ holds or not. We call X an **ordered set** by the order \leq if the following conditions are satisfied:

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

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

Exercise xiv.2. (i) We usually consider a subset of an ordered set with the naturally inherited order.

(ii) For a set X and a set Y whose elements are subsets of X , we can define a natural order by inclusions on Y , by $A \leq B \iff A \subset B$ for $A, B \in Y$.

Definition xiv.3. Let X be an ordered set.

- (i) An element $x \in X$ with the property $x \leq y \implies x = y$ is called a **maximal element** of X .
- (ii) For a subset $Y \subset X$ and $x \in X$, if $y \leq x$ for all $y \in Y$, x is called an **upper bound** of Y .
- (iii) If $X \neq \emptyset$ and all non-empty totally ordered subset of X has an upper bound in X , X is called **inductive**.

Theorem xiv.4. (Zorn's lemma) Any inductive ordered set has a maximal element.

Proposition xiv.5. 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 ix.26), therefore has a maximal element. \square

Remark xiv.6. We used the axiom of choice in the proof of Proposition ix.25 when we took an infinite sequence (if we wanted to prove it for euclidean domains and not general PID's, we did not need it). Rewrite this proof by using the Zorn's lemma.

xv. MODULES AND ALGEBRAS OVER RINGS (OPTIONAL)

xv.1. Generating sets of modules.

Definition xv.1. Let A be a ring, M an A -module, 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 elements 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 .

Exercise xv.2. 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 .

Exercise xv.3. (i) 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.
(ii) For a ring A and its ideal I ($\neq 0$, $\neq A$), the quotient ring A/I is not a free A -module (as there it has no linearly independent element).

Definition xv.4. An A -module M is **finitely generated** if there is a generating set of M of finite cardinality. The module 0 is finitely generated as it is generated by \emptyset .

xv.2. Algebras over rings.

Definition xv.5. Let A be a ring.

- (i) If a ring B is also an A -module and the A -homomorphism $A \ni a \mapsto a \cdot 1 \in B$ is a ring homomorphism, B is called an **A -algebra**.

- (ii) A ring homomorphism $B \rightarrow B'$ between A -algebras is called an **A -algebra homomorphism** or **morphism of A -algebras** if it is also an A -homomorphism of A -modules.

We denote the **category of A -algebras** and A -algebra homomorphisms by $A\text{-Alg}$ and its set of morphisms by $\text{Hom}_{A\text{-Alg}}(B, B')$, so that we can distinguish it from the set of A -homomorphisms $\text{Hom}_A(B, B') = \text{Hom}_{A\text{-Mod}}(B, B')$. A morphism of A -algebras is an **isomorphism** if it is an isomorphism either as sets, rings, or A -modules.

Remark xv.6. This definition makes sense for non-commutative rings B as well (but it is better to assume that A is commutative): e.g. $\text{End}_A(M) := \text{Hom}_A(M, M)$ for an A -module M is a non-commutative A -algebra in general (we have seen the case over a field in K in Definition v.2).

- Example xv.7.**
- (i) Any ring has a unique structure of \mathbb{Z} -algebra, and every ring homomorphism is a morphism of \mathbb{Z} -algebras. Therefore $\mathbb{Z}\text{-Alg} = \mathbf{Rings}$.
 - (ii) A field extension L of K is a K -algebra, and K -homomorphisms are K -algebra homomorphisms between the extension fields.
 - (iii) Polynomial rings $A[X]$, $A[X_1, \dots, X_n]$ are A -algebras.
 - (iv) 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.
 - (v) If A is a subring of a ring B , then B is an A -algebra (Exercise ix.13(i)).
 - (vi) Defining an A -algebra structure on a ring B is equivalent to specify a ring homomorphism $A \ni a \mapsto a \cdot 1 \in B$.
 - (vii) If a subring of an A -algebra B is an A -submodule, it is called an **A -subalgebra**. The image of an A -algebra homomorphism $B \rightarrow B'$ is an A -subalgebra of B' .
 - (viii) If B is an A -algebra, every B -module is naturally an A -module (compare Exercise ix.13(ii)). In particular, every B -algebra is naturally an A -algebra.

Definition xv.8. If an A -algebra is finitely generated as an A -module, it is called a **finite A -algebra**. (This is the same as *finite extensions* (Definition 2.2) in the case of extension fields.)

Exercise xv.9. Let A be a domain. Every ring homomorphism $f : A \rightarrow X$ satisfying $f(A \setminus \{0\}) \subset X^\times$ extends uniquely to an A -algebra morphism $\text{Frac}(A) \rightarrow X$.

INDEX

- A -algebra, 76
- A -algebra homomorphism, 77
- A -equivariant, 49
- A -homomorphism, 49
- A -module, 43
- A -subalgebra, 77
- A -submodule, 43
- K -algebra, 43
- K -linear map, 47

- abelian extension, 23
- abelian group, 40
- absolute Galois group, 36
- action, 42
- addition, 40
- addition (for \mathbb{N}), 40
- additive group, 40
- adjoining a root, 7
- algebra, 76
- algebra homomorphism, 77
- algebraic (element), 13
- algebraic (extension), 13
- algebraic closure, 18
- algebraic number field, 9
- algebraically closed field, 18
- alternating group, 33
- alternating multilinear form, 58
- antisymmetric law, 75
- associate, 65
- associativity (of morphisms), 53
- automorphism group, 51

- basis, 45
- basis (free module), 76
- bijection, 39

- canonical basis (of K^n), 45
- canonical surjection, 71
- category, 53
- category of A -algebras, 77
- category of A -modules, 53
- category of groups, 53
- category of rings, 53
- category of sets, 53
- category of vector spaces, 53
- change of bases, 52
- characteristic (field), 74
- characteristic polynomial, 64
- cofactor, 61
- cofactor matrix, 61
- commutative, 40
- commutative diagram, 53
- commutative group, 40
- commutative ring, 41
- composite, 39
- composite field, 32
- composition (of morphisms), 53
- coprime, 66
- cyclic extension, 30
- cyclic group, 21
- cyclic type (element of S_n), 31
- cyclotomic extension, 21
- cyclotomic polynomial, 25

- derivation, 23
- determinant (linear transformation), 59
- determinant (matrix), 60
- diagonal matrix, 65
- diagonalizable, 64
- dimension, 46
- dimension formula, 48
- direct product (group/ring), 37
- direct product (set), 39
- direct sum (linear map), 62
- direct sum (pair), 64
- direct sum (vector space), 62
- direct sum decomposition (linear map), 63
- direct sum decomposition (pair), 64
- direct sum decomposition (vector space), 63
- discriminant, 33
- divisible, 65
- divisor, 65
 - proper —, 65
- domain, 65

- eigenvalue, 64
- eigenvector, 64
- Eisenstein's irreducibility criterion, 70
- elementary pair, 64
- elementary subpair, 64
- endomorphism ring, 51
- entry, 54
- equivalence class, 70
- equivalence relation, 70
- equivariant, 49
- euclidean domain, 68
- Euler's function, 21
- extension, 8, 16, 39
- extension degree, 9
- extension field, 8

- field, 41

- finite (algebra), 77
- finite extension, 9
- finite field, 41
- finite group, 21
- finite-dimensional, 46
- finitely generated (module), 76
- finitely generated (vector space), 45
- fraction field, 70
- free (module), 76
- Frobenius map, 24, 38
- fundamental theorem of arithmetic, 69
- fundamental theorem of Galois theory, 20
- fundamental theorem of symmetric functions, 29

- Galois closure, 28
- Galois extension, 15, 27
- Galois extension (infinite), 36
- Galois group, 15
- Galois group (infinite), 36
- Galois group (polynomial), 29
- Gauss' Lemma, 70
- general linear group, 55
- generate, 44
- generate (module), 76
- generated by (field), 13
- generated by (finite group), 21
- generated by (submodule), 76
- generating set, 44
- generating set (module), 76
- generator (finite group), 21
- group, 40
- group homomorphism, 49

- homomorphism, 49
- homomorphism (algebra), 77
- homomorphism theorem, 72

- ideal, 43, 66
- identity, 40
- identity map, 39
- identity matrix, 55
- identity morphism, 53
- image, 39
- inclusion map, 39
- inductive, 75
- infinite extension, 9
- infinite-dimensional, 46
- injection, 39
- integral domain, 65
- intermediate field, 8
- inverse, 40
- inverse image, 39
- inverse map, 39
- inverse matrix, 55
- invertible (in general), 40
- invertible matrix, 55
- irreducibility of cyclotomic polynomials, 25
- irreducible (element), 65
- isomorphic, 47, 50
- isomorphic (as extensions), 10
- isomorphic (object), 53
- isomorphism, 47, 50, 63
- isomorphism (algebra), 77
- isomorphism (object), 53

- K -automorphism (of extensions), 10
- K -homomorphism (of extensions), 10
- K -isomorphism (of extensions), 10
- kernel (group), 50
- kernel (rings, A -modules), 50
- kernel (vector space), 47
- Klein 4-group, 33
- Kronecker's delta, 55
- Kummer extension, 30

- linear combination, 43
- linear combination (module), 76
- linear map, 47
- linear relation, 44
- linear relation (module), 76
- linear transformation, 47
- linearly dependent, 44
- linearly dependent (module), 76
- linearly independent, 44
- linearly independent (module), 76

- map, 39
- matrix, 54
- matrix element, 54
- maximal (ideal), 67
- maximal abelian extension, 36
- maximal cyclotomic extension, 36
- maximal element, 75
- minimal polynomial, 13, 74
- module, 43
- monic, 69
- morphism, 53
- morphism (algebra), 77
- morphism (pair), 63
- multilinear form, 57
- multiple, 65
- multiple root, 70
- multiplication, 40
- multiplication (for \mathbb{N}), 40
- multiplicity, 70

- norm, 35

- normal subgroup, 72
- object, 53
- operation, 40
- order (cyclic group), 21
- order (element of a finite group), 21
- ordered set, 75
- perfect field, 27
- permutation, 58
- PID, 68
- polynomial ring, 41, 69
- prime (element), 65
- prime (ideal), 67
- prime field, 74
- primitive n -th root of unity, 23
- primitive element theorem, 27
- primitive root, 24
- principal ideal, 67
- principal ideal domain (PID), 68
- product, 54
- profinite completion (of \mathbb{Z}), 38
- profinite topology, 37
- quotient A -module, 71
- quotient group, 71
- quotient ring, 71
- quotient set, 70
- radical extension, 32
- rational function field, 13
- rational function field (n variables), 29
- reflexive law, 70, 75
- relatively prime (UFD), 66
- representation matrix, 55
- representative element, 70
- residue class ring, 41
- resolvant cubic, 33
- restriction, 39
- ring, 41
- ring homomorphism, 49
- root, 69
- roots of unity, 21
- semisimple, 64
- separable (element), 27
- separable (extension), 26
- separable (polynomial), 26
- separable closure, 36
- sign (permutation), 58
- soluble extension, 30
- soluble group, 30
- split (polynomial), 17
- splitting field, 17
- square matrix, 54
- Steinitz' theorem, 18
- subalgebra, 77
- subextension, 8, 16
- subfield, 8
- subgroup, 41
- submodule, 43
- subpair, 64
- subring, 42
- subspace, 42
- sum (ideals), 67
- surjection, 39
- symmetric group, 58
- symmetric group (in n letters), 29
- symmetric law, 70
- totally ordered set, 75
- trace, 35
- transcendental (element), 13
- transitive, 31
- transitive law, 70, 75
- trivial (linear relation), 44, 76
- unique factorization domain (UFD), 66
- unit, 41, 65
- unit group, 41
- upper bound, 75
- vector space, 42
- volume form, 58
- zero divisor, 65
- zero element, 40
- zero ring, 41
- Zorn's lemma, 75