Lecture Notes On Abstract Algebra (Week 9)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

Contents

1 Lecture 15 (Oct 31, 2023): Applications of the Structure Theorem

1.1 Fundamental Theorem of Finite Abelian Groups

One application of the structure theorem on modules over PID is the decomposition of a finitely generated abelian group, in which case the ring R takes to be $\mathbb{Z}$.

The abelian groups $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/36\mathbb{Z}\oplus\mathbb{Z}/216\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/18\mathbb{Z}\oplus\mathbb{Z}/27\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$ have the same size, of order 15552 ($= 2^6\cdot 3^5$). Are they isomorphic? They are! Actually, they both isomorphic to

$$(\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z})\oplus(\mathbb{Z}/9\mathbb{Z}\oplus\mathbb{Z}/27\mathbb{Z})\,.$$

This can be explained by the Fundamental Theorem of Finite Abelian Groups.

Basic Observation An abelian group G is finite $\Longleftrightarrow$ G is a finitely generated torsion $\mathbb{Z}$-module.

Theorem 1.1 (Primary Decomposition of Finitely Generated Abelian Groups)**.** *Every finitely generated abelian group is isomorphic to a group of the form*

$$\mathbb{Z}^n\oplus\mathbb{Z}/q_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/q_t\mathbb{Z},$$

where the rank $n\geq 0$, and the numbers $q_1,\ldots,q_t$ are powers of (not necessarily distinct) prime numbers. The values of $n,q_1,\ldots,q_t$ are (up to rearranging the indices) uniquely determined by G.

Theorem 1.2 (Invariant Factor Decomposition of Finitely Generated Abelian Groups)**.** *Every finitely generated abelian group is isomorphic to a group of the form*

$$\mathbb{Z}^n\oplus\mathbb{Z}/d_1\mathbb{Z}\oplus\mathbb{Z}/d_2\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/d_m\mathbb{Z},$$

where $n \geq 0$ and $d_1|d_2|\cdots|d_m$. The rank n and the invariant factors $d_1, d_2, \ldots, d_m$ are uniquely determined by the group.

Corollary 1.1 (Fundamental Theorem of Finite Abelian Groups)**.** *Let G be a finite abelian group. Then G is isomorphic to a group of the form*

$$\mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{e_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_t^{e_t}\mathbb{Z},$$

where $p_1, p_2, \ldots, p_t$ are primes (not necessarily distinct). The numbers $p_1^{e_1}, p_2^{e_2}, \ldots, p_t^{e_t}$ are uniquely determined by G up to ordering and they are called the elementary divisors *of G.*

Corollary 1.2. *Every finite abelian group has a descending chain of subgroups such that each factor group is cyclic of prime order.*

Fact Let G be a free abelian group of rank n and H a subgroup of G.

1. The subgroup H is free with rank $\leq n$.
2. If $\text{rank}\,(H) = n$, then there exist a basis $g_1, g_2, \ldots, g_n$ of G and positive integers $d_1, d_2, \ldots, d_n$ such that $d_1 \mid d_2 \mid \cdots \mid d_n$ and $d_1 g_1, d_2 g_2, \ldots, d_n g_n$ form a basis of H. In particular, $[G : H] = d_1 d_2 \cdots d_n$.

The above fact is a corollary of Theorem 2.4 in last lecture.

For simplicity, we write C_n for a cyclic group of order n. That is, $C_n \cong \mathbb{Z}/n\mathbb{Z}$.

Example 1.1. Let

$$G_1 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/216\mathbb{Z},\ G_2 = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$$

be two finite abelian groups.

Then

$$\begin{aligned} G_1 &= C_2 \oplus C_{36} \oplus C_{216} \\ &\cong C_2 \oplus (C_{2^2} \oplus C_{3^2}) \oplus (C_{2^3} \oplus C_{3^3}) \\ &\cong (C_2 \oplus C_{2^2} \oplus C_{2^3}) \oplus (C_{3^2} \oplus C_{3^3})\,. \end{aligned}$$

Similarly,

$$\begin{aligned} G_2 &= C_4 \oplus C_{18} \oplus C_{27} \oplus C_8 \\ &\cong C_{2^2} \oplus (C_2 \oplus C_{3^2}) \oplus (C_{2^3} \oplus C_{3^3}) \\ &\cong (C_2 \oplus C_{2^2} \oplus C_{2^3}) \oplus (C_{3^2} \oplus C_{3^3})\,. \end{aligned}$$

This shows that $G_1 \cong G_2$ and they have the same elementary divisors: $2, 2^2, 2^3, 3^2, 3^3$. And their invariant factors are the same: $2, 2^2 \cdot 3^2, 2^3 \cdot 3^3$ or $2, 36, 216$.

Example 1.2. We come to count the number of abelian groups of order 100,000. Since $100000 = 2^5 \cdot 5^5$, by structure theorem, every abelian group of order 100,000 is uniquely expressible as a direct sum of an abelian group of order 2^5 and an abelian group of order 5^5. For any prime p, also by structure theorem, the number of abelian groups of order p^5 is the number of sums of non-decreasing sequences of positive

integers which sum to the exponent 5. For 5, the possibilities are

$$\begin{aligned} 1+1+1+1+1 &= 5 \\ 1+1+1+2 &= 5 \\ 1+1+3 &= 5 \\ 1+2+2 &= 5 \\ 1+4 &= 5 \\ 2+3 &= 5 \\ 5 &= 5 \end{aligned}$$

That is, the abelian groups of order p^5 for prime p are

$$\begin{aligned} &C_p \oplus C_p \oplus C_p \oplus C_p \oplus C_p \\ &C_p \oplus C_p \oplus C_p \oplus C_{p^2} \\ &C_p \oplus C_p \oplus C_{p^3} \\ &C_p \oplus C_{p^2} \oplus C_{p^2} \\ &C_p \oplus C_{p^4} \\ &C_{p^2} \oplus C_{p^3} \\ &C_{p^5} \end{aligned}$$

Thus, there are 7 abelian groups of order 2^5, and 7 of order 5^5, and totally 49 abelian groups of order 100,000.

Remark 1.1.

1. We may say there are only 49 types of abelian groups of order 10^5. This means that there are 49 abelian groups of order 10^5 up to isomorphism.
2. Let p be a prime. If an abelian group G of p-power order is isomorphic to $C_{p^{e_1}} \oplus C_{p^{e_2}} \oplus \cdots \oplus C_{p^{e_n}}$ with $e_1 \leq e_2 \leq \cdots \leq e_n$, then we call $(p^{e_1}, p^{e_2}, \ldots, p^{e_n})$ the **type** of the p-group G. An abelian group of $(p, p, \ldots, p)$-type is called **elementary p-group**. An elementary abelian p-group can ba regarded as a module over the finite field $\mathbb{F}_p$.

1.2 Jordan Canonical Form

Another application of the structure theorem on modules over PID is the decomposition of a vector space under the action of a linear transformation, in which case the ring R takes to be $k[\lambda]$. That's the Jordan decomposition.

Basic Observation Let k be a field. Then V is a finitely generated torsion $k[\lambda]$-module $\iff$ V is a finite-dimensional k-vectorspace, affiliated with a k-linear transformation.

The polynomial ring $k[\lambda]$ is a typical PID. Let V be a finite-dimensional vector space over k, and T a k-linear endomorphism of V (i.e, a k-linear transformation of V). Let $k[\lambda] \to \mathrm{End}_k(V)$ be the unique ring homomorphism which sends and $a \mapsto \tau_a$ and $\lambda \mapsto T$ which implies that λ acts on V by T, where $a \in k$ and $\tau_a(v) = av$ for $v \in V$. This makes V into a $k[\lambda]$-module:

$$g(\lambda)\alpha = g(T)(\alpha).$$

To say that V is finite-dimensional is to say that it is finitely-generated as a k-module, so certainly is finitely-generated as a $k[\lambda]$-module. Thus, by the Invariant Factor Decomposition Theorem, we have

Theorem 1.3. *Let V be a finite-dimensional vector space over a field k and $\mathbb{T}$ a linear transformation of V. Then V becomes a $k[\lambda]$-module via $\mathbb{T}$.*

1. *There exist vectors $v_1, v_2, \dots v_r$ in V such that*

$$V = k[\lambda]v_1 \oplus k[\lambda]v_2 \oplus \cdots \oplus k[\lambda]v_r$$

and $\operatorname{ann}(v_i) = (d_i)$, where each d_i is a monic polynomial in $k[\lambda]$ and $d_1 \mid d_2 \mid \cdots \mid d_r$. Consequently, we have an isomorphism of $k[\lambda]$-modules:

$$V \cong k[\lambda]/(d_1) \oplus k[\lambda]/(d_2) \oplus \cdots \oplus k[\lambda]/(d_r).$$

where λ acts on V via T, and λ acts on the right-hand side by multiplication by λ. Furthermore, the monic polynomials $d_1, d_2, \dots, d_r$ are uniquely determined by $\mathbb{T}$. They are called the invariant factors of $\mathbb{T}$.

2. *There exist vectors $v_{11}, \dots, v_{1n_1}, \dots, v_{s1}, \dots, v_{sn_s}$ in V such that*

$$V = (k[\lambda]v_{11} \oplus \cdots \oplus k[\lambda]v_{1n_1}) \bigoplus \cdots \bigoplus (k[\lambda]v_{s1} \oplus \cdots \oplus k[\lambda]v_{sn_s}),$$

where $\operatorname{ann}(v_{ij}) = (p_i^{e_{ij}})$ and $p_1, \dots, p_s$ are distinct monic irreducible polynomial and $e_{i1} \le e_{i2} \le \cdots \le e_{in_i}$ for $i = 1, 2 \cdots s$. Consequently, we have an isomorphism of $k[\lambda]$-modules:

$$V \cong \left(k[\lambda]/\left(p_1^{e_{11}}\right) \oplus \cdots \oplus k[\lambda]/\left(p_1^{e_{1n_1}}\right)\right) \bigoplus \cdots \bigoplus \left(k[\lambda]/\left(p_s^{e_{s1}}\right) \oplus \cdots \oplus k[\lambda]/\left(p_s^{e_{sn_s}}\right)\right).$$

Moreover, the polynomials $p_1^{e_{11}}, \dots, p_s e_{1n_1}, \dots, p_s^{e_{s1}}, \dots, p_s e_{sn_s}$ are uniquely determined by $\mathbb{T}$. They are called the elementary divisors of $\mathbb{T}$.

Each direct summand $V_i = k[\lambda]v_i$ in the first part of Theorem 1.3 is a cylic k-vector space and is essentially $\mathbb{T}$-invariant. If $\deg d_i(\lambda) = n_i$, then

$$V_i = \{a_0 v_i + a_1 \mathbb{T} v_i + \cdots + a_{n-1}\mathbb{T}^{n_i - 1} v_i \mid a_0, a_1, \dots, a_{n-1} \in F\},\ \dim_F V_i = n_i.$$

The restriction of $\mathbb{T}$ on V_i induces a linear transformation whose characteristic polynomial is $d_i(\lambda)$.

The second part can be explained in the same way.

Breaking V up into $k[\lambda]$-module summands isomorphic to

$$N = k[\lambda]/(p(\lambda)^e),$$

where $p(\lambda)$ is monic irreducible in $k[\lambda]$, is the finest reasonable decomposition to expect. Each such N corresponds to a $\mathbb{T}$-invariant k-vectorspace of the form $W = k[\lambda]\alpha$ with $\operatorname{ann}(\alpha) = (p(\lambda)^e)$. Hence $\dim_k W = e \deg p(\lambda)$ and the characteristic polynomial of $\mathbb{T}|_W$, the linear transformation restricted on W, is just $p(\lambda)^e$.

Though we have not chosen a basis nor written matrices, this $k[\lambda]$-module decomposition of the original k-vectorspace V is a **Jordan canonical form** (Jordan标准型) of $\mathbb{T}$. The monic polynomials $d_i(\lambda)$ that occur are the *invariant divisors* of $\mathbb{T}$ and the monic polynomials $p_j(\lambda)^{e_{ij}}$ with $e_{ij} \neq 0$ are the *elementary divisors*.

Example 1.3. A $k[\lambda]$-module of the form

$$V = k[\lambda]/(f(\lambda))$$

with (not necessarily irreducible) monic

$$f(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots a_1\lambda + a_0$$

in $k[\lambda]$ of degree n is called a cyclic module for $k[\lambda]$, since it can be generated by a single element, as we shall see here. A reasonable choice of k-basis is $1, \lambda, \lambda^2, \ldots, \lambda^{n-1}$ and

$$\dim_k V = \dim_k (k[\lambda]/(f(\lambda))) = \deg f(\lambda).$$

The multiplication by λ is an endomorphism $\mathbb{T}$ of the $k[\lambda]$-module V. It is a linear transformation of the n-dimensional k-vector space V. Notice that

$$\mathbb{T}\lambda^i = \lambda^{i+1} \bmod \lambda^n = \begin{cases} \lambda^{i+1}, & \text{if } 0 \le i \le n-2, \\ -(a_0 + a_1\lambda + \cdots + a_{n-1}\lambda^{n-1}), & \text{if } i = n-1. \end{cases}$$

Then

$$T = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -a_{n-2} \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix} \tag{1}$$

is the matrix of $\mathbb{T}$ with respect to the basis $1, \lambda, \lambda^2, \ldots, \lambda^{n-1}$. The matrix T in (1) is the **rational canonical form** of $\mathbb{T}$. In particular, the characteristic polynomial of $\mathbb{T}$ is $f(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots a_1\lambda + a_0$. We have discussed the rational canonical form of $\mathbb{T}$ for the case $k = \mathbb{Q}$ in *Linear Algebra*. Notice, as a $k[\lambda]$-module, V is torsion and cyclic (hence only one generator); as a k-module, V is free and each basis has n vectors, since $\dim_k V = n$.

In terms of languages in vector space, the above discussion shows that *there is an ordered k-basis $v, \mathbb{T}v, \mathbb{T}^2v, \ldots, \mathbb{T}^{n-1}v$ such that the associated representing matrix of $\mathbb{T}$ is the rational canonical form as in* (1).

If k is an algebraic closed fields (for example, $k = \mathbb{C}$), then an indecomposable $k[\lambda]$-module is of the form

$$V = k[\lambda]/((\lambda - a)^n),$$

where $a \in k$. Clearly V is a cyclic $k[\lambda]$-module. But V is not a cyclic k-module unless $n = 1$. Take a k-basis for V:

$$1, \lambda - a, (\lambda - a)^2, \ldots, (\lambda - a)^{n-1}.$$

The multiplication by λ is an endomorphism $\mathbb{T}$ of the $k[\lambda]$-module V. Since $(\lambda - a)^n = 0$ holds in $k[\lambda]/((\lambda - a)^n)$, we have

$$\mathbb{T}(\lambda - a)^i = \lambda(\lambda - a)^i \bmod (\lambda - a)^n = \begin{cases} a(\lambda - a)^i + (\lambda - a)^{i+1}, & \text{if } i < n-1, \\ a(\lambda - a)^{n-1}, & \text{if } i = n-1. \end{cases}$$

It follows, with respect to the above basis, $\mathbb{T}$ has the matrix

$$J_n(a) = \begin{pmatrix} a & 0 & \ldots & 0 & 0 \\ 1 & a & \ldots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & a & 0 \\ 0 & 0 & \ldots & 1 & a \end{pmatrix} \in \mathrm{M}_n(k). \tag{2}$$

This is a *Jordan block* and it corresponds to the **Jordan canonical form** of $\mathbb{T}$. Rephrasing in terms of languages in vector spaces, there is an ordered k-basis $v, (\mathbb{T}-a\mathbb{I})v, (\mathbb{T}-a\mathbb{I})^2v, \ldots, (\mathbb{T}-a\mathbb{I})^{n-1}v$ such that the associated representing matrix of $\mathbb{T}$ is the Jordan block $J_n(a)$ as in (2), where $\mathbb{I}$ is the identity endomorphism.
(What kind of vectors v will achieve to form a basis of the form $v, (\mathbb{T}-a\mathbb{I})v, (\mathbb{T}-a\mathbb{I})^2v, \ldots, (\mathbb{T}-a\mathbb{I})^{n-1}v$ in the above discussion? A vector satisfying $(\mathbb{T}-a\mathbb{I})^{n-1}v$ will do! Why? Why such vectors do exist?)

Corollary 1.3. *Let k be an algebraically closed field k (for example, $k=\mathbb{C}$). Given a linear transformation $\mathbb{T}$ of a finite-dimensional vector space over k, there is a choice of basis such that the associated matrix is of the form*

$$\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_t \end{pmatrix},$$

where each J_i on the diagonal is a Jordan block, and all other entries are 0.

设 $\mathbb{T}$ 是 $\mathbb{C}$ 上 n 维向量空间 V 的一个线性变换, 则存在 V 的一组基, 使得 $\mathbb{T}$ 在这组基下的矩阵为对角形矩阵

$$J=\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_t \end{pmatrix},$$

其中每个 J_i 是Jordan块. 而且, 除开这些 J_i 的顺序, J 是由 $\mathbb{T}$ 唯一决定的, 称为 $\mathbb{T}$ 的**Jordan标准型**.

Remark 1.2. An *algebraically closed field* is a field that only polynomials of degree one are irreducible.

When k is not necessarily algebraically closed, there may be irreducibles in $k[\lambda]$ of higher degree. Let $k=\mathbb{R}, p(\lambda)=\lambda^2+1$, and consider the indecomposable $\mathbb{R}[\lambda]$-module

$$V=\mathbb{R}[\lambda]/\left((\lambda^2+1)^3\right).$$

According to the description just given, we take a basis

$$1, \lambda, \lambda^2+1, \lambda(\lambda^2+1), (\lambda^2+1)^2, \lambda(\lambda^2+1)^2.$$

Then the endomorphism τ_λ which is the multiplication by λ is, in terms of this basis,

$$\begin{aligned}
\tau_\lambda(1) &= \lambda \\
\tau_\lambda(\lambda) &= \lambda^2 = -1+(\lambda^2+1) \\
\tau_\lambda(\lambda^2+1) &= \lambda(\lambda^2+1) \\
\tau_\lambda(\lambda(\lambda^2+1)) &= \lambda^2(\lambda^2+1) = -(\lambda^2+1)+(\lambda^2+1)^2 \\
\tau_\lambda((\lambda^2+1)^2) &= \lambda(\lambda^2+1)^2 \\
\tau_\lambda(\lambda(\lambda^2+1)^2) &= \lambda^2(\lambda^2+1)^2 = -(\lambda^2+1)^2,
\end{aligned}$$

since $(\lambda^2+1)^3=0$ in the quotient. Hence the matrix of τ_λ with respect to this basis is

$$A = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Notice that there is no eigenvector or eigenvalue for the linear transformation τ_λ. But we still have a simple representing matrix for τ_λ.

Exercises Let k be a field and V a finite-dimensional k-vectorspace. Let S and T be two k-linear endomorphisms of V. We say S and T are conjugate if their representing matrices are similar.

1. Let V_S be V with the $k[\lambda]$-module structure in which λ acts on $v \in V$ by $xv = S(v)$, and let V_T be V with the $k[\lambda]$-module structure in which λ acts on $v \in V$ by $xv = T(v)$. Show that S and T are conjugate if and only if $V_S \cong V_T$ as $k[\lambda]$-modules.

2. Show that conjugacy classes of $\mathrm{End}_k(V)$ are in one-to-one correspondence with the choices of monic elementary divisors $d_1, \ldots d_r \in k[\lambda]$ in the isomorphism

$$V \cong k[\lambda]/(d_1) \oplus \cdots \oplus k[\lambda]/(d_r)$$

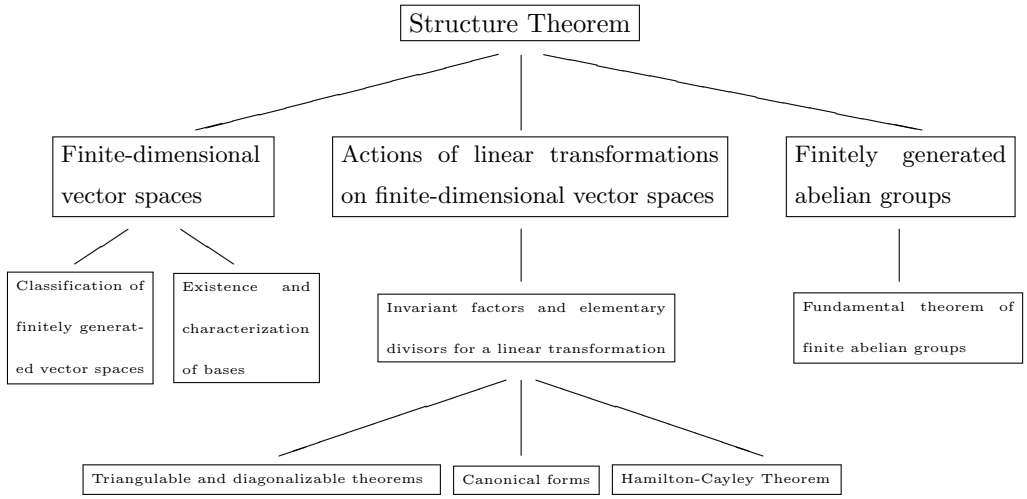
   as $k[\lambda]$-module.

3. Determine all conjugacy classes (i.e. similarity equivalence class) in $\mathrm{GL}_2(\mathbb{F}_3)$, the general linear group of size 2 over the finite field $\mathbb{F}_3$.

4. Show that $\mathrm{GL}_2(\mathbb{F}_2)$ is isomorphic to the permutation group S_3 on three letters.

1.3 Connections

The following schematic gives a picture of the interdependence and connections of many results we discussed above.



Exercises

1. Find the invariant factors and elementary divisors for the abelian group $G = C_2 \oplus C_2 \oplus C_4 \oplus C_3 \oplus C_9 \oplus C_9$.

2. Determine the number of elements of order p in an elementary abelian p-group.

3. Let n be a positive integer and $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ the prime decomposition. Describe the number of finite abelian groups of order n up to isomorphism.

4. Find the number of subgroups of order 4 in $C_2 \oplus C_2 \oplus C_4$.

5. Find the number of subgroups of order p^2 in an elementary abelian p-group.

6. Let G be a finite abelian group. Show that there exists a descending sequence of subgroups

$$G_0 = G \supset G_1 \supset \cdots \supset G_n = \{1\}$$

such that G_i/G_{i+1} is cyclic of prime order for $i = 0, 1, \ldots, n-1$.

7. Let G be an abelian group of order n and m a divisor of n. Show that G has a subgroup of order m.

2 Lecture 16 (Nov 2, 2023): Extension of Fields

2.1 Brief History of Field and Galois Theory

The concept of *field* was used implicitly by Niels Henrik Abel and Évariste Galois in their work on the solvability of polynomial equations with rational coefficients of degree five or higher.

In 1857, Karl von Staudt published his *Algebra of Throws* which provided a geometric model satisfying the axioms of a field. This construction has been frequently recalled as a contribution to the foundations of mathematics.

In 1871, Richard Dedekind introduced, for a set of real or complex numbers which is closed under the four arithmetic operations, the German word *Körper*, which means "body" or "corpus" (to suggest an organically closed entity), hence the common use of the letter K to denote a field. He also defined rings (then called order or order-*modul*), but the term "a *ring*" (*Zahlring*) was invented by Hilbert. In 1893, Eliakim Hastings Moore called the concept "field" in English.

In 1881, Leopold Kronecker defined what he called a "domain of rationality", which is indeed a field of polynomials in modern terms. In 1893, Heinrich M. Weber gave the first clear definition of an abstract field. In 1910, Ernst Steinitz published the very influential paper *Algebraische Theorie der Körper* (Algebraic Theory of Fields). In this paper he axiomatically studies the properties of fields and defines many important field theoretic concepts like prime field, perfect field and the transcendence degree of a field extension.

Emil Artin developed the relationship between groups and fields in great detail from 1928 through 1942.

Galois theory grows originally out of attempts to solve polynomial equations. Galois (1811-1832) showed that solutions of a polynomial equation are governed by a group. Galois theory brings together the study of polynomial equations, the abstract study of fields and field extensions, and group theory. Let's have a brief history of this important problem.

- **Quadratic equations** Recall how one solves the quadratic equation

$$x^2 + bx + c = 0.$$

We "complete the square":

$$(x + \frac{b}{2})^2 + c - \frac{b^2}{4}$$

and solve for x:

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

This was known to the Babylonians (400 BC, algorithmic), to Euclid (300BC, geometric), and to Brahmagupta (6th century AD, allowing negative quantities, using letters for unknowns).

- **Cubic equations** We next consider a cubic equation

$$x^3 + bx^2 + cx + d = 0.$$

This was first solved (at least in special cases) by dal Ferro in 1515. He kept his methods secret for 11 years before passing his knowledge to his student Fior. By 1535 Tartaglia had a "general" solution, and defeated Fior in public competition. Cardano convinced Tartaglia to divulge his solution, and breaking an oath of secrecy, published it in his volume *Ars Magna*. The general equation above can be reduced to the case $y^3 + my - n = 0$ (by a translation). Then Cardano's formula is

$$y = \sqrt[3]{\sqrt{\frac{m^3}{27} + \frac{n^2}{4}} + \frac{n}{2}} - \sqrt[3]{\sqrt{\frac{m^3}{27} + \frac{n^2}{4}} - \frac{n}{2}}$$

Remarkably, negative numbers were not understood at the time; the formula "makes sense" when m and n are nonnegative, or generally the discriminant $4m^3 + 27n^2 \geq 0$.

- **Quartic equations** These were solved by Cardano's student Ferrari.

- **Quintic equations** Abel proved in 1824 that there is no general formula for x satisfying the equation

$$x^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

in terms of b, c, d, e, f combined using $+, -, \times, \div, \sqrt[n]{\ }$.

The birth of Galois theory was originally motivated by the following question, which is known as the Abel-Ruffini theorem:

> "*Why is there no formula for the roots of a fifth (or higher) degree polynomial equation in terms of the coefficients of the polynomial, using only the usual algebraic operations (addition, subtraction, multiplication, division) and application of radicals (square roots, cube roots, etc)?*"

Galois theory not only provides a beautiful answer to this question, it also explains in detail why it is possible to solve equations of degree four or lower in the above manner, and why their solutions take the form that they do.

Galois theory also gives a clear insight into questions concerning problems in compass and straightedge construction. It gives an elegant characterization of the ratios of lengths that can be constructed with this method. Using this, it becomes relatively easy to answer such classical problems of geometry as

> "*Which regular polygons are constructible polygons?*"
> "*Why is it not possible to trisect every angle?*"

2.2 Field Extensions, Algebraic Elements

Let F be a field. Then we have a natural homomorphism of rings:

$$\tau : \mathbb{Z} \to F.$$

Since every subring of F is a commutative domain, we have a monomorphism

$$\mathbb{Z}/\ker\tau \hookrightarrow F$$

with $\ker\tau = \{0\}$ or $\ker\tau = (p)$ for some prime integer p. If $\ker\tau = \{0\}$, then we call the **characteristic** (特征) of F to be 0. If $\ker\tau = (p)$, then the characteristic of F is defined to be p. For example, $\mathbb{Q}$, $\mathbb{R}$ have characteristic 0, while the finite field $\mathbb{F}_p$ has characteristic p.

Recall that a homomorphism between rings with identity must send the identity to identity. Because every field has only two ideals: (0) and (1), then every homomorphism between fields is monomorphism.

The *characteristic* of a field is 0 or p, a prime integer.

If a field F can be embedded into a field K, that is, there is a monomorphism $i : F \hookrightarrow K$, then we say F is a **subfield** (子域) of K and K is an **extension field** (扩域) of F, denoted by K/F. In other words, F is a subfield of K if and only if the field F can be viewed as a subring of K. For example, $\mathbb{R}$ is an extension field of $\mathbb{Q}$ and $\mathbb{R}$ is a subfield of $\mathbb{C}$. We denote this fact by $\mathbb{R}/\mathbb{Q}$ and $\mathbb{C}/\mathbb{R}$. But the finite field $\mathbb{F}_p$ can not be a subfield of $\mathbb{Q}$.

K/F: a field extension with $F \subseteq K$.

Proposition 2.1. *If K is an extension field of F, then F and K have the same characteristic.*

If $K \supseteq F$ is a field extension, and S is a subset of K, we write $F(S)$ for the intersection of all subfields of K containing containing F and S.

$F(S)$ is the smallest subfield of K containing F and S.

We say that $F(S)$ is the field obtained by adjoining S to F. The field $F(S)$ may be expressed as

$$F(S) = \left\{ \frac{\sum a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}}{\sum b_{j_1\cdots j_m}\beta_1^{j_1}\cdots\beta_m^{j_m}} \,\middle|\, a_{i_1\cdots i_n}, b_{j_1\cdots j_m} \in F, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in S \right\}, \tag{3}$$

where $i_1, \ldots, i_n, j_1, \ldots, j_m \geq 0$.

If $S = \{a_1, a_2, \ldots, a_n\}$, write $F(a_1, a_2, \ldots, a_n)$ for $F(S)$. A field extension K/F is *finitely generated* if there exist $\alpha_1, \ldots, \alpha_n \in K$ such that $K = F(\alpha_1, \ldots, \alpha_n)$. If $K = F(\alpha)$ for some $\alpha \in K$, then K/F is called a **simple extension** (单扩张).

Example 2.1. If $S \subseteq F$, then $F(S) = F$.

Example 2.2. 1. Consider $\mathbb{C} \supset \mathbb{R}$. Then

$$\mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{Q}\},$$

where $i = \sqrt{-1}$.

2. Consider $\mathbb{R} \supset \mathbb{Q}$ and $S = \{2023 + \sqrt{3}, 5 - 2\sqrt{3}\}$. It's easy to see that

$$\begin{aligned}\mathbb{Q}(S) &= \mathbb{Q}(2023 + \sqrt{3}, 5 - 2\sqrt{3}) \\ &= \mathbb{Q}(\sqrt{3}) \\ &= \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}.\end{aligned}$$

Hence $\mathbb{Q}(2023 + \sqrt{3}, 5 - 2\sqrt{3})/\mathbb{Q}$ is a simple extension.

Notice that $F[S]$ is the ring obtained by adjoining S to F, a subring of K, hence is a domain. By formula (3), we have

Proposition 2.2. *Let $K \supseteq F$ be a field extension and S a subset of K. Then $F(S)$ is a field of fractions of the ring $F[S]$.*

$$\boxed{F(S) \text{ is a fraction field of } F[S].}$$

In virtue of this proposition, we define $F(x)$ to be the field of fractions of the polynomial ring $F[x]$, where x is an indeterminate. Thus

$$F(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in F[x], g(x) \neq 0 \right\}. \tag{4}$$

The field $F(x)$ is called the **field of rational functions** (有理函数域). It's the field of fractions of the polynomial ring $F[x]$.

Let K_1, K_2 be two subfields of K. The field $K_1(K_2)$ is a the subfield of K obtained by adjoining all elements of K_2 to K_1. This field is called the **compositum** (复合域) of K_1 and K_2, denoted simply by K_1K_2. It's clear that $K_1(K_2) = K_2(K_1)$, hence $K_1K_2 = K_2K_1$. For example, the compositum of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-5})$ is just the field $\mathbb{Q}(\sqrt{2}, \sqrt{-5})$.

More generally,

$$\boxed{K_i = F(\alpha_i),\ 1 \leq i \leq n \Longrightarrow K_1K_2\cdots K_n = F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n)}$$

Let K/F be a field extension and $\alpha \in K$. There is a canonical epimorphism

$$\begin{aligned}\tau : F[x] &\to F[\alpha] \\ f(x) &\mapsto f(\alpha) \\ \sum_{i=0}^{n} a_i x^i &\mapsto \sum_{i=0}^{n} a_i \alpha^i.\end{aligned} \tag{5}$$

Recall that $F[x]$ is a PID and that every prime ideal of a PID is maximal. So we have

$$F[x]/\ker\tau \cong K[\alpha] \tag{6}$$

with $\ker\tau = (0)$ or $\ker\tau = (p(x))$ for some monic irreducible polynomial $p(x)$ (why irreducible?). If $\ker\tau = (0)$, we say that α is **transcendental** (超越的) over F. Otherwise, α is called an **algebraic element** (代数元) over F. If $\ker\tau = (p(x))$ with $\deg p(x) = n$, then α is said to be an algebraic element of **degree** n over F and the monic irreducible polynomial $p(x)$ is called the **minimal polynomial** (极小多项式) (or irreducible polynomial) of α over F.

An algebraic element over $\mathbb{Q}$ is called an **algebraic number** (代数数).

Notice $\tau(f(x)) = f(\alpha)$. Then $f(\alpha) = 0 \Longleftrightarrow f(x) \in \ker\tau \Longleftrightarrow p(x) \mid f(x)$. Hence we have

Proposition 2.3. *Let K/F be an extension of fields and $\alpha \in K$.*

1. *Then α is algebraic over F if and only if there is a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$.*
2. *Let $f(x) \in F[x]$ and assume that $\alpha \in K$ is an algebraic element whose minimal polynomial over F is $m(x)$. Then $f(\alpha) = 0$ if and only if $m(x) \mid f(x)$.*

The minimal polynomial of an algebraic element α over F is the monic polynomial $f(x) \in F[x]$ with smallest degree such that $f(\alpha) = 0$.

Example 2.3. 1. Every element of F is algebraic of degree one over F. Actually, for $\alpha \in F$, $x - \alpha$ is the minimal polynomial over F of α.

2. The number $\omega = e^{\frac{2\pi}{3}i} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, since $f(\omega) = 0$ for $f(x) = x^3 - 1$. But $f(x) = x^3 - 1$ is not the minimal polynomial of ω. The minimal polynomial of ω is $x^2 + x + 1$. And ω is algebraic of degree 2 over $\mathbb{Q}$. But ω is an algebraic number of degree 1 over $\mathbb{Q}(\omega)$.

Example 2.4. Let n be a positive integer. The n-th root of unity $\zeta_n = e^{\frac{2\pi}{n}i}$ is algebraic over $\mathbb{Q}$, because ζ_n is a root of $x^n - 1$. But $x^n - 1$ is reducible over $\mathbb{Q}$. The irreducible polynomial $\Phi_n(x)$ of ζ_n (over $\mathbb{Q}$) is called the n-th *cyclotomotic polynomial* (分圆多项式). If p is a prime, then one can prove that $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$ (please do not forget Eisenstein Criterion!). Hence $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is the irreducible polynomial of ζ_p over $\mathbb{Q}$. For general n, it's not so easy to write out $\Phi_n(x)$ explicitly. It is known that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})},$$

where $\mu(n)$ is the Mobius function given by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n \text{ is not square-free}, \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ different primes}. \end{cases}$$

Hence ζ_n is an algebraic number of degree $\varphi(n)$, where $\varphi(n)$ is the Euler totient function. The number field $\mathbb{Q}(\zeta_n)$ is called the *n-th cyclotomic field*. The discussion on the cyclotomic fields have a strong background with Fermat's Last Theorem.

Theorem 2.1. *If α is transcendental over F, then $F(\alpha) \cong F(x)$, where x is an indeterminate.*

This is because $F[\alpha] \cong F[x]$ as rings and $F(\alpha), F(x)$ are the field of fractions of $F[\alpha], F[x]$ respectively.

Theorem 2.2. *If α is algebraic of degree n over F, then*

$$F(\alpha) = F[\alpha] = \left\{ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F \right\}.$$

Proof. Let $m(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ be the minimal polynomial of α over F. Then $m(x)$ is irreducible. It follows that $(m(x))$ is a prime ideal of $F[x]$, hence is maximal. So $F[x]/(m(x))$ is a field. Note that

$$F[\alpha] \cong F[x]/(m(x)).$$

Thus $F[\alpha]$ is a field containing F and α. Therefore $F[\alpha] = F(\alpha)$ by the definition of $F(\alpha)$. On the other hand, by division algorithm in $F[x]$, we have

$$F[x]/(m(x)) = \left\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + (m(x)) \mid a_0, a_1, \ldots, a_{n-1} \in F\right\}.$$

Recall the epimorphism τ given in (5). We know that $g(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}$ for every polynomial $g(x)$ in the coset $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + (m(x))$. So the induced isomorphism $F[x]/(x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0) \cong F[\alpha]$ implies that

$$F[\alpha] = \left\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\right\}.$$

□

Example 2.5. Obviously $\alpha = \sqrt[3]{2}$ is an algebraic number of degree 3, with minimal polynomial $m(x) = x^3 - 2$. Hence

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

You may wonder how to express $\frac{1}{1+\alpha}$ in the form of $a + b\alpha + c\alpha^2$.

Let $\omega = e^{\frac{2\pi}{3}}$ be the third root of unity. Then $\omega^2 + \omega = -1$ and we have the decomposition $x^3 - 2 = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$. Substituting $x = -1$, we get

$$3 = (1 + \alpha)(1 + \omega\alpha)(1 + \omega^2\alpha).$$

So

$$\frac{1}{1+\alpha} = \frac{(1+\omega\alpha)(1+\omega^2\alpha)}{(1+\alpha)(1+\omega\alpha)(1+\omega^2\alpha)} = \frac{1 + (\omega^2+\omega)\alpha + \omega^3\alpha^2}{3} = \frac{1}{3} - \frac{1}{3}\alpha - \frac{1}{3}\alpha^2.$$

This shows that the inverse of $1 + \alpha$ is actually in $\mathbb{Q}[\alpha]$.

The following corollary is an immediate consequence from the proof of Theorem 2.2.

Corollary 2.1. *Let K/F be a field extension and let $\alpha \in K$ be algebraic over F with minimal polynomial $m(x)$. Then*

$$F(\alpha) = F[\alpha] \cong F[x]/(m(x)).$$

$$\boxed{\alpha \text{ is algebraic over } F \iff f(\alpha) = F[\alpha]}$$

Example 2.6. Let ζ be a primitive 5th-root of unity. We know that $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ is the minimal polynomial of ζ. Hence

$$\mathbb{Q}(\zeta) = \mathbb{Q}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 \mid a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}\}.$$

Exercises

1. Let F be a field and $f(x), g(x) \in F[x]$. Show that $(f(x)) = (g(x))$ if and only if $f(x) = cg(x)$ for some $c \in F^*$.
2. Show that $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and $\mathbb{F}_2[x]/(x^3 + x + 1)$ is a finite field with 8 elements. Write out all elements of $\mathbb{F}_2[x]/(x^3 + x + 1)$.
3. Let F be a field with characteristic p. Show that $(a + b)^p = a^p + b^p$ for all $a, b \in F$.
4. Let α be a root of $f(x) = x^{2023} - 3x^{211} + 2x^7 - x^2 + 2000 \in \mathbb{Q}[x]$. Prove directly that $\alpha^{-2} \in \mathbb{Q}[\alpha]$.

5. Let α be a root of $f(x) = x^3 + 2x + 1$. Compute the minimal polynomials of $\alpha - 1$ and $\alpha^2 + 3$.

6. Show that $\mathbb{Q}(\sqrt{3} + 2) = \mathbb{Q}(\sqrt{3})$.

7. Show that $\mathbb{Q}(\sqrt{\frac{5}{6} - 7}) = \mathbb{Q}(\sqrt{30})$.

8. Let K/F be a field extension and let $\alpha \in K$ be a root of $f(x) \in F[x]$. So we can write $f(x) = (x - \alpha)g(x)$ for some $g(x) \in K[x]$. Show that actually $g(x) \in F(\alpha)[x]$.

9. Let $\alpha \in K$ and $F(\alpha) = F[\alpha]$. Show that α is algebraic over F.

10. Let K/F be a field extension and $\alpha \in K$. Show that α is algebraic over F if and only if $F(\alpha)$ is a finite dimensional vector space over F.

11. A *quadratic extension* of $\mathbb{Q}$ is an extension field of $\mathbb{Q}$ which is a free module of rank 2 over $\mathbb{Q}$. Show that quadratic extensions of $\mathbb{Q}$ must be of the form $\mathbb{Q}(\sqrt{m})$, where m is a square-free integer (i.e m has no divisors of the form d^2 for some positive integer).

12. Let d_1, d_2 be two square-free integers. Show that $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ are isomorphic as rings if and only if $d_1 = d_2$.

13. Let d_1, d_2 be two square-free integers and $d_1 \neq 1 \neq d_2$. Let $\alpha \in \mathbb{Q}(\sqrt{d_1})\backslash\mathbb{Q}, \beta \in \mathbb{Q}(\sqrt{d_2})\backslash\mathbb{Q}$. Suppose that $\alpha + \beta$ lies in a quadratic extension field over $\mathbb{Q}$. Show that $d_1 = d_2$.

14. Let K/F be a field extension and let $\alpha, \beta \in K$ be algebraic over F with the same minimal polynomial. Show that $F(\alpha) \cong F(\beta)$ as rings. Is it necessarily true that $F(\alpha) = F(\beta)$?

15. Show that a finite multiplication group of a field is cyclic.

16. Let K_1, K_2 be two intermediate field of the field extension $F \subseteq K$. Show that $K_1 \subseteq K_2$ if and only if $K_1 K_2 = K_2$.

Homework Exercise 15, 16, 21 on page 210. Exercise 3, 6 on page 242.