Lecture Notes On Abstract Algebra (Week 3)

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

Contents

1 Lecture 5 (Sep 19, 2023): Homomorphisms of Rings

1.1 Homomorphisms of Rings

Definition 1.1. *Let R_1, R_2 be two rings (with identity). A map $f : R_1 \to R_2$ is called a* **homomorphism** (同态) *of rings if*

$$f(a+b) = f(a) + f(b),\ \ f(ab) = f(a)f(b) \tag{1}$$

for all $a, b \in R_1$. Furthermore, an injective homomorphism is called a **monomorphism** (单同态) *or* embedding (嵌入). *A surjective homomorphism is called an* **epimorphism** (满同态). *A bijective homomorphism is called an* **isomorphism** (同构).

Remark 1.1. We are mainly interested in rings with identity. It's reasonable to satisfy $f(1_{R_1}) = 1_{R_2}$ for a homomorphism $f : R_1 \to R_2$, unless otherwise specified.

If there is a monomorphism from R_1 to R_2, we say that R_1 can be *embedded* into R_2. An "embedding" is always denoted by a tailed arrow $\rightarrowtail$ or a hook arrow $\hookrightarrow$. For example, any subring R' of R can be embedded into R, denoted by $R' \hookrightarrow R$ or $R' \rightarrowtail R$. It's easy to see that $R_1 \hookrightarrow R_2$ if and only if R_1 is isomorphic to a subring of R_2. In other word, $R_1 \hookrightarrow R_2$ if and only if R_1 has the same structure with a subring of R_2.

"Epimorphism" are sometimes denoted by a two-headed rightwards arrow: $\twoheadrightarrow$.

As we discussed in group theory, the "isomorphism" between rings is an equivalence relation. If there is an isomorphism between R_1 and R_2, the two rings are said to be isomorphic or we say the two rings are isomorphic. This fact is denoted by $R_1 \cong R_2$. If two rings are isomorphic, they have the same ring structure. Actually, if $R_1 \cong R_2$, then

1. R_1 is finite if and only if R_2 is finite;
2. R_1 is commutative if and only if R_2 is commutative;
3. R_1 is a domain if and only if R_2 is a domain;
4. R_1 is a division ring if and only if R_2 is a division ring;
5. R_1 is a field if and only if R_2 is a field;
6. R_1 is a principal ideal ring if and only if R_2 is a principal ideal ring, etc.

Example 1.1. 1. Let $c \in [a, b]$. Define

$$\begin{aligned} \varphi_c : C[a,b] &\to \mathbb{R} \\ f &\mapsto f(c). \end{aligned}$$

Then φ_c is a homomorphism of rings. Note that φ_c depends on c, but not on $f \in C[a, b]$.

2. Let V be a vector space over a number field F and let $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$ be a fixed basis. Note that $\mathrm{End}(V)$ denotes the ring of linear transformations of V. Define

$$\begin{aligned} \tau : \mathrm{End}(V) &\to \mathrm{M}_n(F) \\ \mathbf{A} &\mapsto A, \end{aligned}$$

where A is the matrix of $\mathbf{A}$ with respect to the basis $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$. We know from linear algebra that τ is an isomorphism of rings. We write $\mathrm{End}(V) \cong \mathrm{M}_n(F)$. Eventually $\mathrm{End}(V)$ and $\mathrm{M}_n(F)$ have the same ring structure.

Proposition 1.1. *Let R be a ring and I an ideal. Then the natural map*

$$\begin{aligned} \tau : R &\to R/I \\ a &\mapsto \overline{a} = a + I \end{aligned}$$

is an epimorphism.

The **kernel** (核) of a homomorphism $f : R_1 \to R_2$ is defined by

$$\ker f = f^{-1}(0) = \{x \in R_1 \mid f(x) = 0\}.$$

It is an ideal of R_1. The kernel $\ker \varphi$ in Example 1 consists of all continuous functions f on $[a, b]$ with a zero at $x = c$.

Proposition 1.2. *Let $f : R_1 \to R_2$ be a homomorphism of rings.*

1. *The kernel* $\ker f$ *is an ideal of* R_1.
2. *The homomorphism f is monomorphic if and only if* $\ker f = 0$.

1.2 Fundamental Theorem of Homomorphisms

Let R_1, R_2 be two rings.

Theorem 1.1 (Fundamental Theorem of Homomorphisms of Rings)**.** *Let $f : R_1 \to R_2$ be a homomorphism of rings.*

1. *The kernel $\ker f = \{a \in R_1 \mid f(a) = 0\}$ is an ideal of R_1 and the image $f(R_1)$ is a subring of R_2.*
2. *The homomorphism f induces a natural isomorphism:*

$$\begin{aligned} \overline{f} : R_1/\ker f &\to f(R_1) \\ a + \ker f &\mapsto f(a). \end{aligned}$$

In particular, if f is an epimorphism, then $R_1/\ker f \cong R_2$.

Proof. First $\ker f$ is a abelian additive group since f is a homomorphism of additive groups. Secondly, if $a \in \ker f, r \in R_1$, then $f(ra) = f(r)f(a) = 0$. Hence $ra \in \ker f$. similarly $ar \in \ker f$. Therefore $\ker f$ is an ideal of R_1. It's routine to verify that $f(R_1)$ is a subring of R_2.

If $a + \ker f = b + \ker f$, then $a - b \in \ker f$. Thus $f(a - b) = 0$, yielding $f(a) = f(b)$. So the map $\overline{f}$ is well-defined. Since f is a homomorphism, we can easily show that $\overline{f}$ is also a homomorphism. Obviously $\overline{f}$ is surjective.

Suppose $\overline{f}(a + \ker f) = 0$. That is, $f(a) = 0$. Then $a \in \ker f$. Hence $a + \ker f = 0$ in $R/\ker f$. This shows that $\overline{f}$ is a monomorphism. Therefore $\overline{f}$ is an isomorphism. □

Remark 1.2. The proof may be simplified with the help of fundamental theorem of homomorphism for groups. Because a homomorphism between rings is naturally a homomorphism between the underlying additive groups. Accordingly the above induced map has the same favor as those in group homomorphisms. This is also the same case for the following two theorems.

Remark 1.3. The The Fundamental Theorem shows that every homomorphism $f : R_1 \to R_2$ can be decomposed as the following parts:

$$\begin{array}{ccccccc} R_1 & \overset{\tau}{\twoheadrightarrow} & R_1/\ker f & \overset{\overline{f}}{\to} & \mathrm{im}(f) & \overset{\iota}{\hookrightarrow} & R_2 \\ a & \mapsto & \overline{a} & \mapsto & f(a) & \mapsto & f(a), \end{array}$$

where $\overline{f} : R_1/\ker f \to f(R_1)$ is an isomorphism.

In other words, we have

$$f = \iota \circ \overline{f} \circ \tau.$$

This can be described in the following commutative diagram:

$$\begin{array}{ccc} R_1 & \xrightarrow{f} & R_2 \\ \downarrow & & \uparrow \\ R_1/\ker f & \xrightarrow{\cong} & \mathrm{im}(f) \end{array}$$

This may be also simplified as the following commutative diagram:

$$\begin{array}{ccc} R_1 & \xrightarrow{f} & R_2 \\ & \searrow^{\tau} & \uparrow{\scriptstyle f'} \\ & & R_1/\ker(f) \end{array} \qquad f = f' \circ \tau, \text{ where } f' = \iota \circ \overline{f}, \text{ i.e. } f'(\overline{a}) = f(a)$$

Example 1.2. Let

$$f : \mathbb{Z}[x] \to \mathbb{F}_5[x]$$
$$\sum a_i x^i \mapsto \sum \overline{a}_i x^i.$$

Here $\mathbb{F}_5 = \mathbb{Z}/(5)$ is a finite field with 5 elements. One can see that f is an epimorphism of rings with kernel $\ker f = (5)$. Hence

$$\mathbb{Z}[x]/(5) \cong \mathbb{F}_5[x].$$

It follows that (5) is a prime ideal in $\mathbb{Z}[x]$.

Example 1.3. Let

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}[i]$$
$$\sum a_k x^k \mapsto \sum a_k i^k,$$

where $i = \sqrt{-1}$. It's clear that ϕ is an epimorphism of rings with kernel $\ker \phi = (x^2+1)$ and it induces an isomorphism

$$\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i].$$

So (x^2+1) is a prime ideal in $\mathbb{Z}[x]$. Is it a maximal ideal?

Theorem 1.2 (First Isomorphism Theorem for Rings)**.** *Let $f : R_1 \to R_2$ be an epimorphism of rings (i.e, $R_1 \twoheadrightarrow R_2$) and let I be an ideal of R_1 containing $\ker f$. Then $I' = f(I)$ is an ideal of R_2 and f induces a natural isomorphism η:*

$$R_1/I \cong R_2/I' = f(R_1)/f(I)$$
$$a + I \mapsto f(a) + I'.$$

$$\boxed{f : R_1 \twoheadrightarrow R_2 \Longrightarrow R_1/I \cong R_2/f(I), \text{ where } I \lhd R_1 \text{ and } I \supseteq \ker f.}$$

Proof. Obviously $f(I)$ is an additive subgroup of R_2. Let $r \in R_2$ and $f(a) \in I'$. Since f is surjective, then $r = f(x)$ for some $x \in R_1$. Hence $rf(a) = f(xa), f(a)r = f(ax)$. Consequently $rf(a), f(a)r \in I'$ and I' is an ideal of R_2.

If $a + I = b + I$, then $a - b \in I$, which implies $f(a) - f(b) \in I'$. Hence $f(a) + I' = f(b) + I'$. We then know that η is well-defined.

Since $\eta(1+I) = 1+I'$, $\eta((a+I)+(b+I)) = \eta(a+b+I) = f(a+b)+I' = (f(a)+I')+(f(b)+I') = \eta(a+I)+\eta(b+I)$ and similarly $\eta((a+I)(b+I)) = \eta(a+I)\eta(b+I)$, then η is a homomorphism of rings.

If $\eta(a+I) = 0$, then $f(a) \in I'$ and there is a $b \in I$ such that $f(a) = f(b)$. Hence $a - b \in \ker f \subseteq I$. So $a \in I$ and $a + I = 0$ in R_1/I. On the other hand, the surjectivity of f implies that η is surjective. Therefore η is an isomorphism. □

Noticing there is a canonic epimorphism from $R \to R/I$, we have

Corollary 1.1. *If I, J are two ideals of R, and $I \subseteq J$, then*

$$R/J \cong R/I \Big/ J/I.$$

This corollary can also be proved by considering the natural homomorphism: $R/I \to R/J$.

Example 1.4. Let f be the epimorphism given in Example 1.2 and $I = (5, x^2+3)$. Then $f(I) = (x^2+\overline{3})$. By the First Isomorphism Theorem for Rings, we have

$$\mathbb{Z}[x]/(5, x^2+3) \cong \mathbb{F}_5[x]/(x^2+\overline{3}).$$

It's easy to see that $x^2+\overline{3}$ is irreducible in $\mathbb{F}_5[x]$. Thus $(x^2+\overline{3})$ is a prime ideal, hence maximal. This means that $\mathbb{F}_5[x]/(x^2+\overline{3})$ is a field. Consequently, $(5, x^2+3)$ is a maximal ideal of $\mathbb{Z}[x]$.

Theorem 1.3 (Second Isomorphism Theorem for Rings)**.** *Let S be a subring of R, $I \lhd R$.*

1. *Then $I \cap S \lhd S$, and $S+I = \{s+i \mid s \in S, i \in I\}$ is a subring of R containing I with $I \lhd S+I$.*
2. *The map*
$$\begin{aligned} \tau :\ & S/(S\cap I) \to (S+I)/I \\ & a + S\cap I \mapsto a+I, \quad a \in S \end{aligned}$$
is an isomorphism of rings. That is, $(S+I)/I \cong S/(S\cap I)$.

Proof. 1. Since $1 = 1+0$, we know $1 \in S+I$. Let $s+i, s'+i' \in S+I$, where $s, s' \in S, i, i' \in I'$. Then
$$(s+i)+(s'+i') = (s+s) = (i+i') \in S+I,$$
$$(s+i)(s'+i') = ss + (si' + is' + ii') \in S+I.$$
This shows that $S+I$ is a subring. If $a \in S\cap I, r \in S$, then $ar, ra \in S$ since S is a ring, and $ar, ra \in I$, since I is an ideal of R. Hence $ar, ra \in S\cap I$. This means $S\cap I$ is an ideal of S.

Since $I \lhd R$, it's obvious that $I \lhd S+I$.

2. Note that $(S+I)/I = \{s+I \mid s \in S\}$. If $a+I = b+I$ in $S+I/I$ with $a, b \in S$, then $a-b \in S\cap I$. Consequently $a+S\cap I = b = S\cap I$. Hence τ is well-defined. Clearly τ is a homomorphism of rings.

If $a+S\cap I = b+S\cap I$ for some $a, b \in S$, then $a-b \in I$. Hence $a+I = b+I$. So τ is a monomorphism. Obviously τ is surjective. Therefore τ is an isomorphism of rings.

□

Example 1.5. Let $R = \mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ be the Gaussian integers, $S = \mathbb{Z}, I = (1+3i)$. We have
$$S + I = \{a + (1+3i)b(i) \mid a \in \mathbb{Z}, b(i) \in \mathbb{Z}[i]\} = \mathbb{Z}[i],$$
since $i = 3 + i(1+3i) \in S+I$.

Notice $10 = (1+3i)(1-3i)$. If $n = (1+3i)(a+bi) \in \mathbb{Z}$ with $a, b \in \mathbb{Z}$, then $n = (a-3b) + (3a+b)i$. Consequently $b = -3a$ and $n = 10a$. Thus
$$S \cap I = \mathbb{Z} \cap (1+3i) = 10\mathbb{Z}.$$
By the Second Isomorphism Theorem for Rings,
$$\mathbb{Z}[i]/(1+3i) \cong \mathbb{Z}/10\mathbb{Z}.$$
This means that $\mathbb{Z}[i]/(1+3i)$ is a finite ring with 10 elements. It's not a domain. Therefore $(1+3i)$ is not a prime ideal in $\mathbb{Z}[i]$.

Exercises

1. Let $\eta : R \to R'$ be a homomorphism of rings and I' an ideal of R'. Show that $\eta^{-1}(I') = \{a \in R \mid \eta(a) \in I'\}$ is an ideal of R. If I is an ideal of R, is it true that $\eta(I)$ is an ideal of R'?
2. Let I be an ideal of R. Use the fundamental theorem on homomorphisms to prove that $\mathrm{M}_n(R)/\mathrm{M}_n(I) \cong \mathrm{M}_n(R/I)$, where $\mathrm{M}_n(I) = \left\{ (a_{ij})_{n\times n} \mid a_{ij} \in I \text{ for all } i, j \right\}$.

3. Assume $a+(m) \mapsto a+(n)$ is a homomorphism from the ring $\mathbb{Z}/(m)$ to $\mathbb{Z}/(n)$. What's the relation between m and n?

4. Show that R_1 can be embedded in a ring R_2 if and only if R_1 is isomorphic to a subring of R_2.

5. Let n be a positive integer. Is it possible to embed $\mathbb{Z}/(n)$ into $\mathbb{Z}$?

6. Let $f : R_1 \to R_2$ be an isomorphism and $a \in R_1$. Show that

   (1) a is a zero divisor if and only if $f(a)$ is a zero divisor in R_2;

   (2) a is a unit if and only if $f(a)$ is a unit in R_2.

7. Let $\eta : R \to R'$ be a homomorphism of rings and I an ideal of R'. Let

$$\eta^{-1}(I) = \{a \in R \mid \eta(a) \in I\}.$$

   (1) Show that $\eta^{-1}(I)$ is an ideal of R.

   (2) If I is a prime ideal of R', then $\eta^{-1}(I)$ is a prime.

   (3) If η is an epimorphism, then η induces a natural isomorphism

$$\begin{aligned} \overline{\eta} : R/\eta^{-1}(I) &\to R'/I \\ a+\eta^{-1}(I) &\mapsto \eta(a)+I. \end{aligned}$$

8. Show that $(2+3i)$ is a maximal ideal in $\mathbb{Z}[i]$.

9. Let p be a prime integer and let $f(x) \in \mathbb{Z}[x]$ be irreducible modulo p (i.e. $f(x) \bmod p$ is irreducible in $\mathbb{F}_p[x]$). Show that $(p, f(x))$ is a maximal ideal in $\mathbb{Z}[x]$.

2 Lecture 6 (Sep 21, 2023): Polynomial Rings and Algebraic Numbers

2.1 Characteristic of A Ring

Let R be an arbitrary ring with identity e. Then the natural map

$$\begin{aligned} \tau : \mathbb{Z} &\to R \\ n &\mapsto n \cdot e = e+e+\cdots+e \end{aligned} \tag{2}$$

is a homomorphism from $\mathbb{Z}$ to R. Note that the ideals of $\mathbb{Z}$ must be of the form (d) for some $d \geq 0$. Hence $\ker\tau = (d)$ for some $d \geq 0$. We call d the **characteristic** (特征) of R, denoted by $\underline{\mathrm{char}(R)}$. And the image of τ, $\mathrm{im}\tau$, is called the **prime ring** of R. By the fundamental theorem of homomorphism for rings (see next lecture note), we have

$$\mathbb{Z}/d\mathbb{Z} \simeq \mathrm{im}\tau.$$

Remark 2.1. If $\mathrm{char}(R) \neq 0$, then $\mathrm{char}(R)$ is just the smallest positive integer n such that $nx = 0$ for all x in R.

Example 2.1. 1. The characteristic of $\mathrm{M}_n(\mathbb{R})$ is 0 and $\mathbb{Z}$ is its prime ring.

2. For any $n \geq 0$, the residue class ring $\mathbb{Z}/n\mathbb{Z}$ has characteristic n. In particular, if p is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements and its characteristic is p.

3. Let p be a prime. we usually write $\mathbb{F}_p$ for the finite field $\mathbb{Z}/p\mathbb{Z}$. Then the matrix ring $\mathrm{M}_n(\mathbb{F}_p)$ is of characteristic p. Actually, we have

$$\begin{aligned} \mathbb{F}_p &\hookrightarrow \mathrm{M}_n(\mathbb{F}_p) \\ \overline{a} &\mapsto \mathrm{diag}(\overline{a}, \cdots, \overline{a}). \end{aligned}$$

Corollary 2.1. *The prime ring R' of a R is the smallest subring embedded in R. In other words, if $R'' \hookrightarrow R$, then $R' \hookrightarrow R''$.*

Corollary 2.2. *The prime ring of a ring is either isomorphic to $\mathbb{Z}$ or the ring $\mathbb{Z}/k\mathbb{Z}$ of residues modulo some $k > 0$.*

Prime rings: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ $(n \geq 1)$.

Corollary 2.3. *If R is an integral domain, then $\mathrm{char}\, R = 0$ or p. In particular, the characteristic of a field is either 0 or p with p a prime.*

For example, $\mathbb{Q}$, $\mathbb{R}$ have characteristic 0, while the finite field $\mathbb{F}_p$ has characteristic p. For a prime integer p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ can be embedded in every field of characteristic p. Consequently $\mathbb{F}_p$ is the smallest field with characteristic p. Similarly, $\mathbb{Q}$ is the smallest field with characteristic 0. So $\mathbb{F}_p$ and $\mathbb{Q}$ are called *prime fields*.

Prime fields: $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number.

Exercises

1. Let R be a ring with identity e and $N = \{t \in \mathbb{Z} \mid t > 0, te = 0\}$. Show that

   (a) $N = \{t \in \mathbb{Z} \mid t > 0, tx = 0 \text{ for all } x \in R\}$;

   (b) $\mathrm{char}(R) = 0$ if and only if $N = \emptyset$;

   (c) if $N \neq \emptyset$, then $\mathrm{char}(R) = \min\{t \mid t \in N\}$.

2. Let R be a ring. Show that the prime ring of R is the smallest subring of R.

3. Show that a prime ring is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$, where n is a positive integer.

4. Let p be a prime integer. Give an example of infinite field with characteristic p.

5. Show that the characteristic of an integral domain is 0 or prime.

6. Show that the only ring homomorphism from $\mathbb{Q}$ to $\mathbb{Q}$ is the identity.

7. Let $\alpha \in \mathbb{Z}[i]$ and $\alpha \neq 0$. Show that $\mathbb{Z}[i]/(\alpha)$ is a finite ring and compute the characteristics of $\mathbb{Z}[i]/(2+3i)$ and $\mathbb{Z}[i]/(3+4i)$.

8. Let R_1 and R_2 be rings with identity such that $\mathrm{char}(R_1) \neq \mathrm{char}(R_2)$. Prove that there exists no embedding from R_1 to R_2.

2.2 Polynomial Rings and Polynomial Functions

Assume R is a commutative ring with identity. Let x be an indeterminate. We introduce

$$R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \,\middle|\, a_i \in R, n \in \mathbb{Z}_{\geq 0} \right\} \tag{3}$$

Here $\mathbb{Z}_{\geq 0} = \{n \in \mathbb{Z} \mid n \geq 0\}$.

The set $R[x]$ may be described in another way:

$$R[x] = \left\{ \sum_{i=0}^{\infty} a_i x^i \,\middle|\, a_i \in R \text{ and } a_i = 0 \text{ for almost all } i \right\}.$$

For $\sum_{i=0}^{\infty} a_i x^i, \sum_{i=0}^{\infty} b_j x^j \in R[x]$, we define

$$\sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} b_j x^j \iff a_i = b_i \text{ for all } i.$$

For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$, all a_i are called the **coefficients** (系数) of $f(x)$. If $a_n \neq 0$, it is called the **leading coefficient** (首项系数) and n is defined to be the **degree** (次数) of $f(x)$. We write $\deg(f(x)) = n$. If $a_n = 1$, then $f(x)$ is called **monic** (首一).

Let $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$. Define

$$\begin{aligned} f(x) + g(x) &= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0) \\ f(x)g(x) &= a_n b_m x^{m+n} + (a_{n-1} b_m + a_n b_{m-1}) x^{m+n-1} + \cdots + a_0 b_0 \\ &= \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} a_i b_j \Big) x^k. \end{aligned}$$

Here we set $b_i = 0$ for $m < i \leq n$ if $m < n$.

With the operation above, one can see that $R[x]$ is a commutative ring, with zero element 0 and the unit 1. We call $R[x]$ the **polynomial ring over R in indeterminate x** (R上一元的多项式环), or simply a *polynomial ring in one variable over R*. An element in $R[x]$ is called a *polynomial in x with coefficients in R*. In later language, $R[x]$ is a free R-module with infinite rank.

Remark 2.2.

1. Let R be a subring of R'. Then $R[x]$ is a subring of $R'[x]$. That is, every polynomial over R is naturally a polynomial over R'.

2. Generally, R may not be commutative. For example, an $n \times n$ λ-matrix over $\mathbb{C}$ may be regarded as an element in the polynomial ring $R[\lambda]$, where $R = \mathrm{M}_n(\mathbb{C})$ is the matrix ring and is not commutative for $n \geq 2$.

   In our discussions, we always assume that R is commutative with identity.

3. In general, $(R[x])^\times \neq R^\times$. For example, $1 + 2x \in (\mathbb{Z}/4\mathbb{Z}[x])^\times$, but $1 + 2x \notin (\mathbb{Z}/4\mathbb{Z})^\times$.

For $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ and $\alpha \in R$, we can substitute x by α and get

$$f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \in R.$$

In such a way, we can regard $f(x) \in R[x]$ as a *polynomial function* from R to R. Accordingly we may also discuss the zeros (or roots) of a polynomial. If $f(c) = 0$, we say that c is a **root** (根) of $f(x)$. A root of a polynomial is also called a *zero* (零点) of the polynomial.

As we did in Linear Algebra on polynomial over a number field, some results are still works. For example, we can define the degree of a polynomial. But the relation $\deg(fg) = \deg(f) + \deg(g)$ does not always hold. For example, if R is not a domain, then $R[x]$ is neither a domain. The ring $\mathbb{Z}/4\mathbb{Z}[x]$ has zero divisors. The division algorithm still holds with a minor restriction.

Theorem 2.1 (Division Algorithm)**.** *Let $f(x), g(x) \in R[x]$ and assume that the leading coefficient of $g(x)$ is invertible. Then there exist unique $q(x), r(x) \in R[x]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

Corollary 2.4. *Let R is a subring of R' and $f(x) \in R[x]$. Then $c \in R'$ is a root of $f(x)$ if and only if $f(x) = (x - c)g(x)$ for some $g(x) \in R'[x]$.*

Corollary 2.5. *Let R be an integral domain and $f(x) \in R[x]$ with $\deg(f(x)) = n$. Then $f(x)$ has at most n distinct roots in R.*

Corollary 2.5 may be false if R is not a domain. For example, $x^2 - 1$ has 4 roots in $\mathbb{Z}/15\mathbb{Z}$.

When R is a field, successive use of division algorithm incorporated into the Euclidean algorithm which can be applied to compute the greatest common divisor of two given polynomials. We have the same results as the polynomial rings over number fields.

Theorem 2.2. *Let F be a field.*

1. *For two polynomials $f(x), g(x) \in F[x]$, the ideal $(f(x), g(x)) = (f(x)) + (g(x)) = (d(x))$, where $d(x)$ is the greatest common divisor of $f(x)$ and $g(x)$. Consequently, $F[x]$ is a principal ideal domain.*
2. *Let I be a nontrivial ideal of $F[x]$. Then the follow three are equivalent:*
   (a) *I is a prime ideal;*
   (b) *I is maximal;*
   (c) *there exists a monic irreducible polynomial $p(x) \in F[x]$ such that $I = (p(x))$.*

Note that $R[x]$ is still a commutative ring. For another indeterminate, we may accordingly define $R[x][y]$. It's conventional to write $R[x, y]$ for $R[x][y]$. More generally, if $x_1, x_2, \cdots, x_n$ are indeterminates, then

$$\begin{aligned} &R[x_1, x_2, \cdots, x_n] \\ =&\left\{ \sum a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \;\middle|\; i_1, i_2, \cdots, i_n \in \mathbb{Z}_{\geq 0} \text{ and } a_{i_1 i_2 \cdots i_n} \in R \text{ are almost all } 0 \right\} \end{aligned}$$

is called the *ring of polynomials over R in indeterminates $x_1, x_2, \cdots, x_n$*.

Remark 2.3. For general ring R, even domain, the polynomial ring $R[x]$ is not necessarily a principal ring. For example, $\mathbb{Z}[x]$ is not principal, and the nonzero ideal $(2), (x)$ are prime, but not maximal.

Basic Facts on The Polynomial Ring over A Field

Let F be a field.

- The polynomial ring $F[x]$ is a domain. Actually, if R is a domain, so is $R[x]$.
- Every ideal in $F[x]$ is principal. Actually, the ideals of $F[x]$ are of the form

$$(f(x)) = f(x)F[x]$$

  and $F[x]$ is a principal ideal domain (PID).
- For nonzero polynomial $f(x), g(x)$ in $F[x]$, $(f(x)) \subseteq (g(x))$ if and only if $g(x) \mid f(x)$. In particular, $(f(x)) = (g(x))$ if and only if $f(x)$ differs from $g(x)$ by a nonzero constant (an element in F^*).
- The ideal $(f(x))$ is prime if and only if $f(x) = 0$ or $f(x)$ is irreducible over F.
- The ideal $(f(x))$ is maximal if and only if $f(x)$ is irreducible over F. Hence every nonzero prime ideal in $F[x]$ is maximal.
- We have $(f(x)) + (g(x)) = (\gcd(f, g))$, $(f(x)) \cap (g(x)) = (\operatorname{lcm}(f, g))$, $(f(x)) \cdot (g(x)) = (f(x)g(x))$.
- For $f(x) \in F[x]$ with $\deg f(x) = n \geq 1$, $f(x)$ has at most n roots in F.
- Every monic polynomial in $F[x]$ of degree ≥ 1 may be uniquely written in a product of monic irreducible polynomials ($F(x)$ is a UFD).

2.3 The Structure of the Ring $R[u]$ and Algebraic Numbers

Let R be a subring of a commutative ring R' and U a subset of R'. Then

$$R[U] = \left\{ \sum a_{i_1 i_2 \cdots i_n} u_1^{i_1} u_2^{i_2} \cdots u_n^{i_n} \,\middle|\, i_1, i_2, \cdots, i_n \in \mathbb{Z}_{\geq 0} \text{ and } a_{i_1 i_2 \cdots i_n} \in R \text{ are almost all } 0 \right\} \tag{4}$$

is a subring containing R and U. One can see that

$$R[U] = \bigcap_{\substack{T \supseteq R \text{ and } T \supseteq U \\ T \text{ is a subring of } R'}} T.$$

Hence $R[U]$ is the smallest subring of R' which contains R and U. We call $R[U]$ the *ring generated by adjoining U to R* (将U添加到R上生成的环).

If $U = \{u\}$ has one element, then we write

$$\begin{aligned} R[u] &= \left\{ \sum a_i u^i \,\middle|\, a_i \in R \text{ and } a_i = 0 \text{ for almost all } i \right\} \\ &= \left\{ \sum_{i=0}^{n} a_i u^i \,\middle|\, n \geq 0, a_i \in R, 0 \leq i \leq n \right\} \end{aligned}$$

and $R[u]$ is the ring obtained by *adjoining u to R*.

$$\boxed{R[u] = \{f(u) \mid f(x) \text{ is a polynomial over } R\}}$$

If $U = \{u, v\}$, then

$$R[u,v] = \left\{ \sum a_{ij} u^i v^j \,\middle|\, a_{ij} \in R \text{ and } a_{ij} = 0 \text{ for almost all } i,j \right\}$$

is the ring obtained by adjoining u, v to R. One can see that

$$R[u,v] = (R[u])\,[v].$$

This fact is simply described as

$$R[u,v] = R[u][v].$$

Hence $R[u][v] = R[v][u]$.

Example 2.2. Let $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$. Then $\omega^3 = 1$ and $\omega^2 = -\omega - 1$. Consequently $\omega^{3n} = 1, \omega^{3n+1} = \omega, \omega^{3n+2} = \omega^2 = -\omega - 1$. Hence we have

$$\begin{aligned}
\mathbb{Z}[\omega] =& \left\{ \sum a_i \omega^i \,\middle|\, a_i \in \mathbb{Z} \text{ and } a_i = 0 \text{ for almost all } i \right\} = \{a + b\omega \mid a, b \in \mathbb{Z}\}, \\
\mathbb{Z}[\frac{1}{2}] =& \left\{ \frac{n}{2^m} \mid m, n \in Z, m \geq 0 \right\}, \\
\mathbb{R}[\omega] =& \{a + b\omega \mid a, b \in \mathbb{R}\}, \\
\mathbb{C}[\omega] =& \mathbb{C}.
\end{aligned}$$

Example 2.3. Suppose $u \in \mathbb{C}$ is a zero of the polynomial $x^5 - 2x + 2$. Then we have $u^5 = 2u - 2$. Consequently $u^6 = 2u^2 - 2u, u^7 = 2u^3 - 2u^2, u^8 = 2u^4 - 2u^3, u^9 = -2u^4 + 4u - 4, u^{10} = 4u^2 - 4u + 4, \cdots$. Inductively, if $n \geq 0$, there exist $a_{n0}, a_{n1}, a_{n2}, a_{n3}, a_{n4} \in \mathbb{Z}$ such that $u^n = a_{n0} + a_{n1}u + a_{n2}u^2 + a_{n3}u^3 + a_{n4}u^4$. Therefore

$$\mathbb{Z}[u] = \{a_0 + a_1 u + a_2 u^2 + a_4 u^3 + a_4 u^4 \mid a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}\}.$$

One can similarly see that $\mathbb{Q}[u] = \{a_0 + a_1 u + a_2 u^2 + a_4 u^3 + a_4 u^4 \mid a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}\}$.

Theorem 2.3. *Let R be a subring of a commutative R' and $u \in R'$. Define a natural map from $R[x]$ to $R[u]$ given by*

$$\begin{aligned}
\tau_u : R[x] &\to R[u] \\
f(x) &\mapsto f(u).
\end{aligned}$$

In particular, $\tau_u(x) = u$ and $\tau_u(a) = a$ for all $a \in R$. Then τ_u is an epimorphism of rings. Furthermore, $R[x]/I_u \cong R[u]$ and $I_u \cap R = \{0\}$, where

$$I_u = \ker \tau_u = \{f(x) \in R[x] \mid f(u) = 0\}.$$

Consequently $R[u]$ is a homomorphic image of the polynomial ring $R[x]$.

Proof. By the definition of polynomial ring and the construction of the subring $R[u]$ of R', we know that τ_u is an epimorphism of rings. If $a \in I_u \cap R$, then $\tau_u(a) = a$ by the definition of τ_u. But $a \in I_u = \ker \tau_u$ means $\tau_u(a) = 0$. So $a = 0$. Therefore $R[x]/I_u \cong R[u]$ and $I_u \cap R = \{0\}$. □

Let's reconsider the above two examples. It's easy to verify that $\mathbb{Z}[\omega] \cong \mathbb{Z}[x]/(x^2 + x + 1)$ in example (2.2). In the same way, $\mathbb{Z}[u] \cong \mathbb{Z}[x]/(x^5 - 2x + 2)$ and $\mathbb{Q}[u] \cong \mathbb{Q}[x]/(x^5 - 2x + 2)$ in example (2.3).

How do we understand the complex field $\mathbb{C}$ from algebraic point of view? First we know now that $\mathbb{C} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\}$. This shows that $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$, since $\sqrt{-1}$ is a root of $x^2 + 1 = 0$. By Theorem

2.3, we always know that $\mathbb{C}$ is a quotient ring of $\mathbb{R}[x]$, i.e., $\mathbb{C} = \mathbb{R}[x]/I$ for some ideal of $\mathbb{R}[x]$. Note that $I = \{f(x) \in R[x] \mid f(\sqrt{-1}) = 0\}$. If $f(x) \in \mathbb{R}[x]$, then

$$\begin{aligned} f(\sqrt{-1}) = 0 &\Leftrightarrow x - \sqrt{-1} \mid f(x) \\ &\Leftrightarrow x + \sqrt{-1} \mid f(x) \\ &\Leftrightarrow x^2 + 1 \mid f(x). \end{aligned}$$

So $I = (x^2 + 1)$ and we have

$$\boxed{\mathbb{C} = \mathbb{R}[\sqrt{-1}] \cong \mathbb{R}[x]/(x^2+1).}$$

This is an algebraic explanation of $\mathbb{C}$. It's really a piece of cake to understand the complex numbers algebraically.

Definition 2.1. *Let the notations be as in Theorem 2.3. If*

$$I_u = \{f(x) \in R[x] \mid f(u) = 0\} \neq 0,$$

then u is called an **algebraic element** (代数元) *over R. Otherwise, u is called an* **transcendental element** (超越元) *over R. An algebraic element over $\mathbb{Q}$ is called an* **algebraic number** (代数数)*, and a transcendental element over $\mathbb{Q}$ is called an* **transcendental number** (超越数)*.*

More precisely, for $\alpha \in \mathbb{C}$, by Theorem 2.3, we have

$$\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/I_\alpha,$$

where $I_\alpha = \{f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0\}$ is an ideal of $\mathbb{Q}[x]$. Then α is an algebraic number if and only if $I_\alpha \neq (0)$. And α is a transcendental number if and only if $I_\alpha = (0)$. It's clear to see that α is an algebraic number if and only if α is a zero to some nonzero polynomial over $\mathbb{Q}$. For example, the n-th root of unity $\zeta_n = e^{\frac{2\pi i}{n}}$ is an algebraic number, since it's a zero of the polynomial $x^n - 1$. The number $\alpha = \frac{\sqrt{3}-1}{2}$ is an algebraic number, since it's a root of $2x^2 + 2x - 1 = 0$.

Notice that every ideal of $\mathbb{Q}[x]$ is principal. Hence, for an algebraic number α,

$$I_\alpha = (\varphi_\alpha(x))$$

for some monic polynomial $\varphi_\alpha(x) \in \mathbb{Q}[x]$. On the other hand, as a subring of $\mathbb{C}$, $\mathbb{Q}[\alpha]$ is a domain. It follows that such $\varphi_\alpha(x)$ must be irreducible over $\mathbb{Q}$. Furthermore, such $\varphi_\alpha(x)$ is unique (why?). We call $\varphi_\alpha(x)$ the **minimal polynomial** (极小多项式) of α. Since $(\varphi_\alpha(x))$ is a maximal ideal of $\mathbb{Q}[x]$, $\mathbb{Q}[x]/(\varphi_\alpha(x))$ is a field. By Theorem 2.3, $\mathbb{Q}[\alpha]$ is essentially a field, called an **algebraic number field**, or simply a **number field**. If $\deg \varphi_\alpha(x) = n$, then α is called a algebraic number of **degree** n.

For example, if p is an odd prime integer, then $\zeta_p = e^{\frac{2\pi i}{p}}$ is an algebraic number of degree $p - 1$. Actually, $x^{p-1} + x^{p-2} + \cdots + x + 1$ is the minimal polynomial of ζ_p. And $\frac{\sqrt{3}-1}{2}$ is an algebraic number of degree 2, whose minimal polynomial is $x^2 + x - \frac{1}{2}$.

Proposition 2.1. *Let $\alpha \in \mathbb{C}$.*

1. *The following three are equivalent:*

   (1) α is an algebraic number;

   (2) there is a nonzero polynomial $m(x) \in \mathbb{Q}[x]$ such that $m(\alpha) = 0$;

(3) there is a monic irreducible polynomial $m(x) \in \mathbb{Q}[x]$ such that $m(\alpha) = 0$.

2. *If α is an algebraic number of degree n, then*

$$\mathbb{Q}[\alpha] = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i \mid a_0, a_1, \cdots a_{n-1} \in \mathbb{Q} \right\}$$

is a field. Furthermore, $\mathbb{Q}[\alpha]$ is a vector space over $\mathbb{Q}$ with dimension n.

3. *If α is a transcendental number, then*

$$\mathbb{Q}[\alpha] \cong \mathbb{Q}[x].$$

In particular, $\mathbb{Q}[\alpha]$ is a vector space over $\mathbb{Q}$ with infinite dimension n.

If the minimal polynomial $\varphi_\alpha(x) \in \mathbb{Z}[x]$ (i.e, the coefficients of the minimal polynomial are all integers), then α is called an **algebraic integer** (代数整数).

For example, $\sqrt{-1}$ is an algebraic integer with minimal polynomial $\varphi(x) = x^2 + 1$. And $\frac{1+\sqrt{-3}}{2}$ is an algebraic integer with minimal polynomial $\varphi(x) = x^2 - x + 1$. The number $\sqrt{2} + \sqrt{-3}$ is an algebraic integer with minimal polynomial $\varphi(x) = x^4 + 2x^2 + 25$. Actually, every root of unity is an algebraic integer. The number $\frac{\sqrt{3}-1}{2}$ is not an algebraic integer, since its minimal polynomial $x^2 + x - \frac{1}{2} \notin \mathbb{Z}[x]$.

Remark 2.4. 1. If α is an algebraic integer of degree n, then

$$\begin{aligned} \mathbb{Z}[\alpha] &= \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \cdots, a_{n-1} \in \mathbb{Z}\} \\ &= \{f(\alpha) \mid f(x) \in \mathbb{Z}[x], \deg f(x) < n.\} \end{aligned}$$

2. All algebraic numbers form an subfield of $\mathbb{C}$. It's just the *algebraic closure* of $\mathbb{Q}$ in $\mathbb{C}$.

3. All algebraic integers form a subring of $\mathbb{C}$. In particular, for a number field K, all algebraic integers in K form a subring of K, called the *ring of integers of* K, denoted by $\mathcal{O}_K$.

Exercises

1. Describe explicitly the elements of the integral domain $\mathbb{Z}[1 + \sqrt{2}]$.
2. Show that $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \left\{ \frac{a+b\sqrt{-3}}{2} \mid a, b \in \mathbb{Z}, a \equiv b (\mathrm{mod}\ 2) \right\} \neq \mathbb{Z}[\sqrt{-3}]$.
3. Show that the matrix ring $\mathrm{M}_n(R[\lambda]) \cong \mathrm{M}_n(R)[\lambda]$, where R is a commutative ring and λ is an indeterminate in both cases.
4. Show that $(x^2 + 1)$ is a maximal ideal of $\mathbb{R}[x]$.
5. Find the minimal polynomial and degree for $\alpha = \sqrt[3]{-2} + 1$.
6. Determine the ideal I so that $\mathbb{Q}[x]/I \cong \mathbb{Q}[1 + \sqrt{2}]$.
7. (a) Show that a number $\alpha \in \mathbb{C}$ is algebraic if and only if the ideal

$$I(\alpha) = \{f(x) \in \mathbb{Q}[x] \mid f(\alpha) = 0\}$$

is not $\{0\}$.

(b) Show that the non-zero monic polynomial with the least degree in $I(\alpha)$ is just the minimal polynomial of α.

8. Let n be a positive integer and set $\zeta_n = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, where $i = \sqrt{-1}$. Show that ζ_n is an algebraic number. If p is a prime number, determine the minimal polynomial and degree of ζ_p.

9. Let α be an algebraic integer of degree n. Show that

$$\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(\varphi(x)),$$

where $\varphi(x)$ is the minimal polynomial of α.

10. Express the elements in $\mathbb{Z}[x]/(2x)$ in a simplest form.

11. Let α be an algebraic number of degree n.

    (a) Show that there exists an integer $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.

    (b) Is it true that $\mathbb{Z}[\alpha] = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i \;\middle|\; a_0, a_1, \cdots, a_{n-1} \in \mathbb{Z} \right\}$?

12. Show that $\sqrt{2} \notin \mathbb{Q}[\sqrt{3}]$ and that the real numbers $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent over $\mathbb{Q}$. Show that $u = \sqrt{2} + \sqrt{3}$ is an algebraic number and determine an ideal I such that $\mathbb{Q}[x]/I \cong \mathbb{Q}[u]$.

13. Show that $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

14. Let F be a field.

    (a) Show that there is a unique smallest subfield of F. We call such subfield the *prime field* of F.

    (b) Show that the prime field of F is either isomorphic to $\mathbb{Q}$ or a finite field $\mathbb{F}_p$ with p elements for some prime integer p. If $\mathbb{Q}$ can be embedded in F, then F is of characteristic 0. If $\mathbb{F}_p$ can be embedded in F for some prime integer p, then F is of characteristic p.

15. Lindemann-Weierstrass Theorem says that if $\alpha_1, \ldots, \alpha_n$ are distinct algebraic numbers over $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are linearly independent over $\mathbb{Q}$. In virtue of this theorem, prove that π is a transcendental number.

Homework Exercise 33, 35, 36, 37, 41, 43, 44, 51 on page 134.