近世代数基础读书笔记
Reading Notes on Algebra

李锡灏
Patrick X. Li [1] [2]

working in progress
2022 年 12 月 28 日

[1]This note is mainly based on the classical textbook of algebra by Prof. Zhang He Rui (张禾瑞, Ho-Jui Chang). He studied algebra in Universitaet Hamburg, under E. Artin, E. Witt, etc at 1930s. He returned to China in 1940s, first affiliated with Peking University and then Beijing Normal University, and became one of the founders of modern mathematics and education in the country.

[2]To my daughters Gaia and Sofia: Algebra is what we can find out from something like $1 + 1 = 2$.

目录

第一章　群论基础 (Basics of Group Theory)

1.1　群的定义 (Definition of Group)

定义 1.1.1. 一个非空集合 G 对于一个代数运算 (通常称为乘法) 是一个**群 (group)**, 如果满足以下条件:

I. G 对于这个代数运算来说是闭的;

II. 结合律成立:

$$a(bc) = (ab)c \tag{1.1}$$

对于 G 的任意三个元 a, b, c.

III. 对于 G 的任意两个元 a, b 来说, 下面的方程都在 G 里有解:

$$ax = b \text{ 和 } ya = b. \tag{1.2}$$

定义 1.1.2. 一个非空集合 G 对于一个代数运算 (通常称为乘法) 是一个**群 (group)**, 如果满足以下条件:

I. G 对于这个代数运算来说是闭的;

II. 结合律 (associative law of composition) 成立:

$$a(bc) = (ab)c \tag{1.3}$$

对于 G 的任意三个元 a, b, c.

IV. G 里至少存在一个左单元 e, 使得对于 G 的任意元 $a \in G$ 都有

$$ea = a. \tag{1.4}$$

V. 对于 G 的每一个元 a, 在 G 里至少存在一个左逆元 a^{-1}, 使得

$$a^{-1}a = e \tag{1.5}$$

备注 1.1.1. 第1.1.2 定义比第1.1.1 定义更加方便应用.

定义 1.1.3. 有限群: 一个群的元的个数是一个有限整数, 那么这个群称为有限群 (finite group). 一个有限群的元的个数叫做这个群的**阶 (order of the group)**.

定义 1.1.4. 一个群叫做**交换群 (Abelian group/commutative group)**, 如果对于 G 的任何两个元 a, b, 以下等式都成立:

$$ab = ba. \tag{1.6}$$

1.2 单位元, 逆元, 消去律 (Identity, Inverse, Cancellation Law)

定理 1.2.1. 一个群 G 有且只有一个元 e, 对于 G 的任意元 a, 以下等式都成立:

$$ea = ae = a. \tag{1.7}$$

证明. First we want to show $ae = a$: By definition 1.1.2 IV and V, there exists $ee = e$, $aa^{-1} = e$, $ea^{-1} = a^{-1}$.

$$\begin{aligned} & ea^{-1} = a^{-1} \implies aea^{-1} = aa^{-1} \\ \implies & aea^{-1}a = aa^{-1}a \implies aee = ea \\ \implies & ae = a \end{aligned}$$

Thus, we have $ea = ae = a$, $\forall a \in G$.

Next we want to show the uniqueness of e: Assume there exists another e' with $e'a = ae' = a$. Then, for e with $ea = ae = a$, choose $a = e'$, this leads to $ee' = e'e = e'$. For e' with $e'a = ae' = a$, choose $a = e$, this leads to $e'e = ee' = e$. Thus, $e' = e$.

□

备注 1.2.1. 一个群 G 里面存在这样唯一的一个 e, 我们称为 **单位元 (identity element, or identity in short)**.

定理 1.2.2. 对于一个群 G 的每一个元 a 来说, 在 G 里存在一个且只有一个元 a^{-1}, 使得

$$a^{-1}a = aa^{-1} = e. \tag{1.8}$$

证明. Assume there exists another inverse for $a \in G$, denoted as a' with $a'a = aa' = e$.

Then,

$$\begin{aligned} & a'aa^{-1} = ea^{-1} = a^{-1} \textbf{ and } a'aa^{-1} = a'e = a' \\ \implies & a^{-1} = a' \end{aligned}$$

□

备注 1.2.2. 给定一个群 G 中的任意元 a 而言, a^{-1} 称为 a 的 **逆元 (inverse)**.

定义 1.2.1. 对于一个群 G 的一个元 a, 能够使得等式

$$a^m = e \tag{1.9}$$

成立的最小的正整数 m 叫做 a 的**阶 (order of the element a in group G)**. 如果这样的一个 m 不存在, 我们称 a 是**无限阶**的.

定理 1.2.3. 一个群的代数运算 (通常称为乘法) 适合:

III' **消去律 (cancellation law)**: 如果 $ax = ax'$, 那么 $x = x'$; 如果 $ya = y'a$, 那么 $y = y'$.

证明.

$$ax = ax' \implies a^{-1}ax = a^{-1}ax' \implies ex = ex' \implies x = x'$$

With the same argument, we can show $ya = ya' \implies y = y'$.

□

推论 1.2.1. 在一个群里, 方程

$$ax = b, \quad ya = b \tag{1.10}$$

都有唯一的解.

1.3 有限群的另一定义 (Alternative Definition of Finite Group)

备注 1.3.1. 通常而言, 条件 I, II, III'(消去律) 不能构成群的定义, 有限群是特例. 例如:

$$G = \{\text{所有不等于零的整数}\} \tag{1.11}$$

这样的 G 适合 I, II, III': 消去律, 但是不适合 III: 对于任意的 a, b, 不一定 $ax = b$ 有解. (假设 $a = 2$, $b = 3$).

定理 1.3.1. 一个有乘法的有限集合 G 若是适合 I, II, III', 那么它也适合 III.

证明. 我们先证明 $ax = b$ 在 G 里面有解:

假定 G 有 n 个元, 表示为

$$a_1, a_2, \ldots, a_n. \tag{1.12}$$

用 a 左乘 G 中的所有元, 做成一个集合:

$$G' = \{aa_1, aa_2, \ldots, aa_n\} \tag{1.13}$$

由 I, 我们有 $G' \subseteq G$.

当 $i \neq j \iff a_i \neq a_j$ 的时候, 我们有 $aa_i \neq aa_j$. 否则, 由消去律, 我们得出 $aa_i = aa_j \Rightarrow a_i = a_j \iff i = j$, 与假定的 $i \neq j$ 不符. 因此 G' 有 n 个不同的元, 因而得出

$$G' = G \tag{1.14}$$

也就是说, 以上方程 $ax = b$ 的 $b \in G'$. 也就是说存在 a_k, 使得:

$$aa_k = b \tag{1.15}$$

那么 a_k 是以上方程的解. 同理可证: $ya = b$ 可解. □

定义 1.3.1. 有限群 (finite group) 的定义: 一个**有限**的非空集合 G 对于一个代数运算 (通常称为乘法) 是一个群, 如果满足以下条件:

I. G 对于这个代数运算来说是闭的;

II. 结合律成立: 对于 G 的任意三个元 a, b, c, 有

$$a(bc) = (ab)c \tag{1.16}$$

III' **消去律**: $ax = ax' \implies x = x'$; $ya = y'a \implies y = y'$.

1.4 群的同态 (Group Homomorphism)

定理 1.4.1. 群的同态: 假定 G 是一个群, $\overline{G}$ 是一个非空集合, 并有一个代数运算. 假定 G 与 $\overline{G}$ 对于他们的代数运算而言是 **同态 (满射)(surjective homomorphism/epimorphism)**, 那么 $\overline{G}$ 也是一个群.

证明. $\overline{G}$ 满足条件 I 和 II. 我们证明 $\overline{G}$ 也适合 IV, V 这两条.

- IV: G 有单位元 e, 在给定的同态满射之下, e 有象 $\overline{e}$:

$$e \longrightarrow \overline{e}. \tag{1.17}$$

假定任意一个元 $\overline{a} \in \overline{G}$, a 是 $\overline{a}$ 的一个逆象:

$$a \longrightarrow \overline{a}. \tag{1.18}$$

那么, 我们有

$$ea \longrightarrow \overline{ea}, \quad a \longrightarrow \overline{a} \tag{1.19}$$

$$\Rightarrow \quad ea = a \Rightarrow \overline{ea} = \overline{a} \tag{1.20}$$

$$\Rightarrow \quad \overline{e} \text{ 是 } \overline{G} \text{ 的一个单位元.} \tag{1.21}$$

- V: 假定任意元 $\overline{a} \in \overline{G}$, a 是 $\overline{a}$ 的逆象:

$$a \longrightarrow \overline{a}. \tag{1.22}$$

a 是群 G 的元, 它有逆元 $a^{-1} \in G$. a^{-1} 的象是 $\overline{a^{-1}} \in \overline{G}$. 那么,

$$a^{-1}a = e \longrightarrow \overline{a^{-1}}\overline{a} = \overline{e} \tag{1.23}$$

所以, $\overline{a^{-1}}$ 是 $\overline{a}$ 的逆元.

因此, $\overline{G}$ 满足群的条件 I, II, IV, V, 所以 $\overline{G}$ 是一个群.

□

由上述定理的证明过程, 我们得出以下:

定理 1.4.2. 假定两个群 G 和 $\overline{G}$. 在 G 到 $\overline{G}$ 的一个同态满射之下, G 的单位元 e 的象 $\overline{e}$ 是 $\overline{G}$ 的单位元. G 的元 a 的逆元 a^{-1} 的象 $\overline{a^{-1}}$ 是 a 的象 $\overline{a}$ 的逆元.

1.5 变换群 (Transformation Group)

定义 1.5.1. 假定一个集合 A, A 的一个**变换 (transformation)** 就是一个 A 到 A 自己的映射. 通常记为:

$$\tau : \quad a \longrightarrow a' = \tau(a) \tag{1.24}$$

或者:

$$\tau : a \longrightarrow a' = a^{\tau} \tag{1.25}$$

我们可以把给定的一个集合 A 的全体变换放在一起, 作成一个集合:

$$S = \{\tau, \lambda, \mu, \ldots\} \tag{1.26}$$

同时, 我们规定集合 S 的乘法运算:

$$\tau : a \longrightarrow a^{\tau}, \quad \lambda : a \longrightarrow a^{\lambda} \tag{1.27}$$

$$\tau\lambda : a \longrightarrow (a^{\tau})^{\lambda} = a^{\tau\lambda} \tag{1.28}$$

这个乘法顺序是**从左到右**, 有时候也记为: $\tau;\lambda$.[1]

那么, 对于这个乘法来说, S 有一个单位元, 就是 A 的**恒等变换 (identity, in short)**:

$$e : \quad a \longrightarrow a \tag{1.29}$$

备注 1.5.1. 一般而言, S 不作成一个群, 因为一个任意的变换 τ 不一定存在一个逆元.

[1] $\tau;\lambda$ 这样的记法在范畴论 (Category Theory) 里更为普遍.

虽然 S 本身一般不能作为一个群, 但它的一个子集 对于上述的乘法运算有可能作为一个群.

定理 1.5.1. 假定 G 是集合 A 的若干个变换所作成的集合, 并且 G 包含恒等变换 e. 如果 G 对于上述乘法运算作成一个群, 那么 G 只包含 A 的一一变换 (一一变换 (bijective) 既是单射 (injective) 也是满射 (surjective)).

证明. By assumption, G is a group. Given any element $\tau \in G$, there exists the inverse $\tau^{-1} \in G$ with

$$\tau^{-1}\tau = \tau\tau^{-1} = e.$$

We need to show τ is a bijective: given any element $a \in A$, then

$$\tau^{-1}\tau : a \longrightarrow a^{\tau^{-1}\tau} = a^e = a$$

So τ is surjective.

Now assume $\tau(a) = \tau(b) \iff a^\tau = b^\tau$. Then

$$a^\tau = b^\tau \implies \left(a^\tau\right)^{\tau^{-1}} = \left(b^\tau\right)^{\tau^{-1}} \implies a^e = b^e \implies a = b$$

So τ is injective, and therefore τ is bijective.

□

备注 1.5.2. 定理 1.5.1 给出 G 作成一个群的**必要条件**.

由此, 我们规定:

定义 1.5.2. 一个集合 A 的若干个一一变换 (bijection) 对于以上规定的代数运算作成的一个群叫做 A 的一个**变换群 (transformation group)**.

定理 1.5.1 不足以证明变换群是否存在. 变换群是否存在由以下的存在性定理得出:

定理 1.5.2. 一个集合 A 的所有一一变换作成一个变换群 (transformation group) G.

证明. We show G maintains the conditions I, II, IV, V in Definition 1.1.2.

I. If $\tau_1 : A \longrightarrow A$ and $\tau_2 : A \longrightarrow A$ are bijective, so is $\tau_1\tau_2 : A \longrightarrow A$. This means $\tau_1, \tau_2 \in G \implies \tau_1\tau_2 \in G$.

II. Associative law holds for bijectives: $\tau_1(\tau_2\tau_3) = (\tau_1\tau_2)\tau_3$.

IV. The identity $e : A \longrightarrow A$ is bijective, thus $e \in G$ as the identiy of G.

V. Given any bijective $\tau : A \longrightarrow A$, there exists the bijective $\tau^{-1} : A \longrightarrow A$ such that: If $\tau(b) = a$, then $\tau^{-1}(a) = b$, denoted b as $a^{\tau^{-1}}$. This implies that

$$\tau\big(\tau^{-1}(a)\big) = \big(a^{\tau^{-1}}\big)^{\tau} = a,$$

which shows $\tau^{-1}\tau = e$.

□

备注 1.5.3. 定理1.5.2 并不是说, 全体一一变换所作成的集合就是唯一的变换群.

备注 1.5.4. 变换群 (transformation group) 一般不是交换群 (commutative group).

定理 1.5.3. 任何一个群都同一个变换群 (transformation group) **同构**.

证明. Suppose a group G with elements $a, b, c, \ldots$. Consider an arbitrary element from G, denoted as $x \in G$, we can construct a transformation:

$$\tau_x : g \longrightarrow gx, \quad \text{denote } g^{\tau_x} := gx$$

Thus, we have for a transformation τ_x for each element in $x \in G$. Collect these transformations as a set

$$\overline{G} = \{\tau_a, \tau_b, \tau_c, \ldots\}$$

We have a mapping:

$$\phi : G \longrightarrow \overline{G}, \quad \phi(x) = \tau_x$$

By its construction, ϕ is surjective. Now we show ϕ is injective: Assume $x, y \in G$ with $x \neq y$, by (contrapositive) cancellation law shown in Theorem 1.2.3, $x \neq y \implies gx \neq gy$ for any $g \in G$. This means

$$x \neq y \implies \tau_x \neq \tau_y.$$

Thus, ϕ is injective, and thus ϕ is bijective.

Now we show ϕ is group homomorphism:

$$g^{\tau_{xy}} \tau_{xy}(g) = g(xy) = (gx)y = \tau_y\big(\tau_x(g)\big) = \big(g^{\tau_x}\big)^{\tau_y} = g^{\tau_x \tau_y}$$

This means $\tau_x \tau_y = \tau_{xy}$.

Therefore, by Theorem 1.4.1, $\overline{G}$ is also a group.

The last thing is to show $\overline{G}$ contains only bijectives. We need to show $\tau_e \in \overline{G}$ is identity of $\overline{G}$:

$$\tau_e(g) = ge = g$$

So τ_e is the identity in $\overline{G}$. By Theorem 1.5.1, $\overline{G}$ is a group and it contains identity τ_e, thus $\overline{G}$ is a transformation group.

In summary, we show that $\overline{G}$ is a transformation group and $G \cong \overline{G}$.

□

备注 1.5.5. 变换群在群论中很重要: 定理1.5.3 说明了, 任意一个抽象群都能够在变换群里找到一个实例.

1.6 置换群 (Permutation Group)

变换群 (transformation group) 的一个特例, 叫做置换群 (permutation group): permutation group $\subset$ transformation group.

定义 1.6.1. 一个 **有限集合**的一个一一变换叫做一个**置换 (permutation)**. 一个有限集合的若干个置换作成的一个群叫做一个**置换群 (permutation group)**.

备注 1.6.1. 假定一个有限集合 $A = \{a_1, a_2, \ldots, a_n\}$. 由定理1.5.2 可得出, A 的全体置换作成一个群 G.

定义 1.6.2. 一个包含 n 个元的集合的全体置换作成的群叫做 n 次**对称群 (symmetric group)**. 我们用 S_n 表示.

备注 1.6.2. 一定程度上而言, permutation group $\subset$ symmetric group.

n 个元的置换一共有 $n!$ 个. 因而, 我们有以下定理.

定理 1.6.1. n 次对称群 (symmetric group)S_n 的阶是 $n!$.

备注 1.6.3. 因为 S_n 是有限群, 因此它的元的个数称为群的阶. 定理 1.6.1 说明了 S_n 的元素个数为 $n!$.

备注 1.6.4. 以 S_4 为例, 置换可以表示为:

1. $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

   表示为 (1 2 3) 或者 (2 3 1) 或者 (3 1 2).

2. $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

   表示为 (1 2) (3 4).

基于以上的置换表达方式, 我们可以写出 S_4 中的 $4! = 4 \times 3 \times 2 \times 1 = 24$ 个置换:

(1);

(1 2), (3 4), (1 3), (2 4), (1 4), (2 3);

(1 2 3), (1 3 2), (1 3 4), (1 4 3), (1 2 4), (1 4 2), (2 3 4), (2 4 3);

(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2);

(1 2) (3 4), (1 3) (2 4), (1 4) (2 3).

定理 1.6.2. 每一个 n 个元的置换 π 都可以写成若干个互相没有共同数字 (不相连的) 循环置换的乘积.

证明. 略. 此处证明考虑使用归纳法. □

由定理 1.5.3, 我们得出以下:

定理 1.6.3. 每一个有限群 (finite group) 都与一个置换群 (permutation group) 同构.

也就是说, 每一个有限群都可以在置换群里找到例子. 所以我们用置换群来举有限群的例子是最合理的事.

1.7 循环群 (Cyclic Group)

备注 1.7.1. 如果我们能把定义1.5.2 中的变换群 (transformation group) 完全研究清楚, 那就等于把全体抽象群都研究清楚了. 同样, 如果能把定义1.6.1 中的置换群 (permutation group) 完全研究清楚, 也就等于把全体有限群都研究清楚了. 但是:

- 经验告诉我们, 研究变换群或者置换群并不比研究抽象群容易. 所以, 研究抽象群一般还是用直接方法.

- 研究群的最大目的: 找出所有的抽象群, 或者说, 看看一共有多少个互相不同构的群存在.
- 目前而言, 只有少数几类群已经完全弄清楚的. 例如: 循环群 (cyclic group).

例子 1.7.1. G 是所有整数的集合. G 对于普通加法作成一个群, 称为 **整数加群 (additive group of Z)**.

这个群的全体的元都是 1 的乘方. 假如我们把 G 的代数运算不用 + 而是用 $\circ$ 来表示, 那么 m 可以表示为:

$$m = \overbrace{1+1+...+1}^{m} = \overbrace{1\circ 1\circ ...\circ 1}^{m} = 1^m$$

定义 1.7.1. 若一个群 G 的每一个元都是 G 的某一个固定元 a 的乘方, 我们就把 G 叫做**循环群 (cyclic group)**. 我们也说, G 是由元 a 所生成的, 并且用符号表示为:

$$G = (a)$$

a 叫做 G 的一个**生成元 (generator of the group)**.

例子 1.7.2. G 包含模 n 的 n 个剩余类. 规定以下的代数运算 (加法):

$$[a] + [b] = [a + b]$$

那么, 对于这个代数运算而言, G 作成一个群. 这个群叫做模 n 的**剩余类加群 (additive group of $\mathbb{Z}/n\mathbb{Z}$)**.

剩余类加群 (additive group of $\mathbb{Z}/n\mathbb{Z}$) 是循环群 (cyclic group), 因为 [1] 是 G 的一个生成元 (generator): G 的每一个元 $[m]$ 可以写成:

$$[m] = \overbrace{[1]+[1]+...+[1]}^{m}$$

定理 1.7.1. 假定 G 是一个由元 a 所生成的循环群. 那么 G 的构造完全由 a 的阶来决定:

1. a 的阶若是无限, 那么 G 与整数加群 $\mathbb{Z}$ (additive group of $\mathbb{Z}$) 同构;
2. a 的阶若是一个有限整数 n, 那么 G 与模 n 的剩余类加群 $\mathbb{Z}/n\mathbb{Z}$ (additive group of $\mathbb{Z}/n\mathbb{Z}$) 同构.

备注 1.7.2. 对于定理 1.7.1中两种情况, 可以考虑以下一一映射:

1. $a^k \longrightarrow k$;
2. $a^k \longrightarrow [k]$.

证明. Consider two cases.

- The order of a is infinite. In this case, it has $h = k \implies a^h = a^k$. (Otherwise if $a^h = a^k$ but $h \neq k$, then suppose $h > k$, we can find $a^{h-k} = e$ which implies the order of a is $h - k$ not infinite, thus contradiction!)

  Thus, we have bijection:

  $$\phi : G \longrightarrow \mathbb{Z}, \quad \phi(a^k) = k$$

  Note that $\phi(a^h a^k) = \phi(a^{h+k}) = h + k = \phi(a^h) + \phi(a^k)$, thus ϕ is a group homomorphism. Therefore $G \cong \mathbb{Z}$.

- The order of a is finite. Suppose the order of a is n, which means $a^n = e$. This also means

  $$a^h = a^k \iff n|h-k \iff h - k = nq \text{ for } q \in \mathbb{Z}$$

  This implies the mapping

  $$\phi : G \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad \phi(a^k) = [k]$$

  is a bijection.

  ϕ is also a group homomorphism:

  $$\phi(a^h a^k) = \phi(a^{h+k}) = [h + k] = [h] + [k]$$

  Thus, ϕ is isomorphism, i.e. $G \cong \mathbb{Z}/n\mathbb{Z}$.

□

总而言之, 对于循环群, 一定有一个生成元, 这个元一定有一个固定的阶. 这个阶要么是无限大, 要么是一个正整数 n. 从群的同构的角度来看, 生成元的阶是无限大的循环群只有一个; 生成元的阶是给定的正整数 n 的循环群也只有一个.

由此得出, 我们对于循环群的**存在问题, 数量问题, 构造问题**都已能解答. 也就是说, 我们已经完全掌握了循环群. 这一节的研究方法是近世代数研究的一个典型示范.

1.8 子群 (Subgroup)

研究群的比较重要的一个方法就是利用一个群的子集来推测整个群的性质.

定义 1.8.1. 给定一个群 G. 如果 G 的一个子集 H 对于 G 的代数运算来说作成一个群, 那么 H 叫做 G 的一个**子群 (subgroup)**.

例子 1.8.1. 给定一个任意群 G, G 至少有两个子群:

1. G;
2. 只包含单位元 e 的子集: $\{e\}$.

一个子集作成一个子群的条件是什么?

定理 1.8.1. 一个群 G 的一个不空子集 H 作成 G 的一个子群的 *充分必要条件是*:

(i) $a, b \in H \Longrightarrow ab \in H$

(ii) $a \in H \Longrightarrow a^{-1} \in H$

证明. We use Definition 1.1.2 to show H with (i) and (ii) is a group:

I, by (i).

II. by (i) and associative law holds in G also holds in $H \subseteq G$.

IV. There exists at least one element $a \in H$, by (ii), $a^{-1} \in H$. By (i), $a^{-1}a = e \in H$, so $e \in H$.

V. by (ii).

On the other hand, if H is a subgroup, (i) holds. Assume its identity is $e' \in H$. Given an arbitrary element $a \in H$, we have $e'a = a$ in H. e' and a also in G. By definition of group G, $ya = a$ has a unique solution in G, which is $y = e$. This means $e' = e \in H$. Again by definition of group H, $ya = e$ has a unique solution in H, which is $y = a^{-1} \in H$. □

推论 1.8.1. 假定 H 是群 G 的一个子群. 那么 H 的单位元就是 G 的单位元, H 的任意元 a 在 H 里的逆元就是 a 在 G 里的逆元.

定理1.8.1中的两个条件也可以用一个条件来代替:

定理 1.8.2. 一个群 G 的一个不空子集 H 作成 G 的一个子群的充分必要条件是:

(iii) $a, b \in H \Longrightarrow ab^{-1} \in H$

证明. First, we show (i) and (ii) implies (iii): $a, b \in H$, by (ii), $b^{-1} \in H$. Then by (i) $ab^{-1} \in H$.

Next, we show (iii) implies (i) and (ii): Suppose $a \in H$, then $aa^{-1} = e \in H$. Thus $ea^{-1} = a^{-1} \in H$. Suppose $a, b \in H$, then $b^{-1} \in H$, thus $ab = a(b^{-1})^{-1} \in H$. □

假如所给子集 H 是一个**有限集合**, 那么 H 作成子群的条件更加简单:

定理 1.8.3. 一个群 G 的一个不空**有限子集** H 作成 G 的一个子群的充分必要条件是:

$$a, b \in H \Longrightarrow ab \in H$$

证明. By Definition 1.3.1, it is obvious. □

现在我们要认识一种构建一个子群的一般方法:

给定一个群 G, 我们任意取出一个不空子集 S . 利用 S 中的元素以及这些元素的逆元作各种乘积. 我们做一个集合 H , 让它包含所有这样的乘积. 这样作出来的 H 是包含 S 的最小的子群.

定义 1.8.2. 如上得到的 H 叫做**由 S 生成的子群**, 我们用符号 (S) 来表示它.

如果 S 只包含一个元素, $S = \{a\}$, 那么 (S) 可以记为

$$(S) = (a)$$

1.9 子群的陪集 (Coset of a Subgroup)

在这一节里, 我们利用群 G 的一个子群 H 做一个 G 的分类, 然后由这个分类我们可以推出几个重要的定理.

例子 1.9.1. 假定整数加群 $\mathbb{Z}$ (additive group of $\mathbb{Z}$), 记为 $\overline{G}$.

把包含所有 n 的倍数的集合叫做 $\overline{H}$:

$$\overline{H} = \{hn | h = \ldots, -2, -1, 0, 1, 2, \ldots\} \tag{1.30}$$

$\overline{H}$ 是 $\overline{G}$ 的一个子群.

我们把 $\overline{G}$ 分成剩余类时所利用的等价关系规定如下:

$$a \equiv b(n), \text{ 当且仅当} n|a-b \text{ 的时候} \tag{1.31}$$

但 $n|a-b \Longrightarrow a-b = kn \Longrightarrow a-b \in \overline{H}$. 反过来说, $a-b \in \overline{H} \Longrightarrow n|a-b$. 所以上述等价关系也可以规定为:

$$a \equiv b(n), \text{ 当且仅当} a-b \in \overline{H} \text{ 的时候} \tag{1.32}$$

这样, 我们也可以说 $\overline{G}$ 的剩余类是利用子群 $\overline{H}$ 来分的.

下面我们做一个推广: 利用一个子群 H 来把一个群 G 分类. 我们规定 G 中的一个二元关系 $\sim$ 为:

$$a \sim b, \text{ 当且仅当 } ab^{-1} \in H \tag{1.33}$$

这个关系 $\sim$ 是一个等价关系. 利用这个等价关系, 我们可以得到一个 G 的分类:

定义 1.9.1. 规定一个群 G 中的等价关系 $\sim$ 和 G 的一个子群 H:

$$a \sim b \iff ab^{-1} \in H.$$

由上面的等价关系 $\sim$ 所决定的类的叫做子群 H 的**右陪集 (right coset)**. 包含元 a 的右陪集用符号 Ha 表示.

备注 1.9.1. 用 Ha 表示包含元 a 的右陪集, 是因为: 如果我们用 a 右乘 H 的每一个元, 就得到包含 a 的类, 也就是说,

$$Ha = \{ha \,|\, \forall h \in H\}.$$

我们有以下的引理.

引理 1.9.1. 考虑在一个群 G 和它的子群 H. 给定两个元素 $a, b \in G$. 那么,

$$ab^{-1} \in H \iff Ha = Hb$$

其中

$$Ha = \{ha \,|\, \forall h \in H\}, \quad Hb = \{hb \,|\, \forall h \in H\}.$$

证明. Suppose $Ha = Hb$. Then,

$$\begin{aligned} & Ha = Hb \implies ea = a \in Ha = Hb \\ \implies & a = h_b b \text{ for some } h_b \in H \\ \implies & ab^{-1} = h_b b b^{-1} = h_b e = h_b \in H. \end{aligned}$$

So, we just show $Ha = Hb \implies ab^{-1} \in H$.

Suppose $ab^{-1} \in H$, then

$$\forall h_1 a \in Ha \implies h_1 a = h_1 ab^{-1} b \in Hb \text{ since } h_1 \in H,\ ab^{-1} \in H$$
$$\implies Ha \subseteq Hb$$

$ab^{-1} \in H \implies ba^{-1} = (ab^{-1}) \in H$. Similarly, $ba^{-1} \in H \implies Hb \subseteq Ha$. Therefore, $ab^{-1} \in H \implies Ha = Hb$.

□

例子 1.9.2. 考虑 $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$ 以及 $H = \{(1), (12)\} \subset G$. 那么, 我们有下面的右陪集:

$$\begin{aligned} H(1) &= \{(1), (12)\} \\ H(13) &= \{(13), (123)\} \\ H(23) &= \{(23), (132)\} \end{aligned}$$

注意 (132) 由以下得出:

$$(12)(23) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = 1 \to 3 \to 2 = (132).$$

这样, 子群 H 把整个群 G 分成了 $H(1), H(13), H(23)$ 三个不同 (两两不相交) 的右陪集. 而且 $H(1) \cup H(13) \cup H(23) = G$. 因此, $H(1), H(13), H(23)$ 是 G 的一个分类.

右陪集是从等价关系 $\sim$:

$$a \sim b, \text{ 当且仅当} ab^{-1} \in H \tag{1.34}$$

出发得到的. 假如我们规定一个关系 $\sim'$:

$$a \sim' b, \text{ 当且仅当} b^{-1}a \in H \tag{1.35}$$

这个关系 $\sim'$ 也同样是一个等价关系. 利用这个等价关系, 我们可以得到 G 的另一个分类:

定义 1.9.2. 规定一个群 G 中的等价关系 $\sim'$ 和 G 的一个子群 H:

$$a \sim' b \iff b^{-1}a \in H.$$

由上面的等价关系 $\sim'$ 所决定的类叫做子群 H 的**左陪集 (left coset)**. 包含元 a 的左陪集用符号 aH 来表示.

类似于引理 1.9.1, 我们有:

引理 1.9.2. 考虑在一个群 G 和它的子群 H. 给定两个元素 $a, b \in G$. 那么,

$$b^{-1}a \in H \iff aH = bH$$

其中

$$aH = \{ah \,|\, \forall h \in H\}, \quad bH = \{bh \,|\, \forall h \in H\}.$$

因为一个群的乘法不一定有交换律, 所以一般来说, $\sim$ 和 $\sim'$ 两个关系并不相同, 因此 H 的右陪集和左陪集也不相同.

但是, 一个子群的左右陪集有一个共同点:

定理 1.9.1. 一个子群 H 的右陪集的个数和左陪集的个数相等. 它们或者都是无限大, 或者都有限并且相等.

证明. Denote $S_r = \{Ha | \forall a \in G\}$ and $S_l = \{aH | \forall a \in G\}$. We construct a mapping

$$\phi : S_r \longrightarrow S_l, \quad \phi(Ha) = a^{-1}H.$$

We want to show ϕ is bijection.

1. ϕ is well-defined: By Lemma 1.9.1 and Lemma 1.9.2,

$$\begin{aligned} & Ha = Hb \iff ab^{-1} \in H \\ \Longrightarrow\ & (ab^{-1})^{-1} = ba^{-1} \in H \\ \Longleftrightarrow\ & a^{-1}H = b^{-1}H \end{aligned}$$

2. ϕ is surjective: Given any $aH \in S_l$, there always exists $Ha^{-1} \in S_r$.

3. ϕ is injective: Suppose $a^{-1}H = b^{-1}H$. Then again by Lemma 1.9.1 and Lemma 1.9.2,

$$\begin{aligned} & a^{-1}H = b^{-1}H \iff ba^{-1} \in H \\ \implies & ab^{-1} = (ba^{-1})^{-1} \in H \\ \iff & Ha = Hb. \end{aligned}$$

Thus, ϕ is bijective between S_r and S_l. So S_r and S_l have the same number of elements (they have the same cardinality).

□

定义 1.9.3. 一个群的一个子群 H 的右陪集 (或左陪集) 的个数叫做 H 在 G 里的**指数 (the index of H in G), 表示为** $[G : H]$.

下面的定理基于右陪集, 因为左陪集和右陪集的对称性, 同样适用于左陪集.

引理 1.9.3. 一个子群 H 与 H 的每一个右陪集 Ha 之间都存在一个一一映射.

证明. Construct a mapping from H to Ha

$$\phi : H \longrightarrow Ha, \quad \phi(h) = ha.$$

We show that

1. ϕ well-defined: $\forall h \in H$, there exists a unique ha and obviously $ha \in Ha$.

2. ϕ surjective: $\forall ha \in Ha$, the corresponding $h \in H$ gives $\phi(h) = ha$.

3. ϕ injective: if $h_1a = h_2a$, then $h_1 = h_2$ by cancellation law in group shown at Theorem 1.2.3.

□

由上述引理1.9.3, 我们得出以下两个重要定理:

定理 1.9.2. 假定 H 是一个**有限群** G 的一个子群. 那么 H 的阶 (order of H) n 和它在 G 里的指数 (index of H in G) j 都能整除 G 的阶 (order of G) N, 并且

$$N = nj \tag{1.36}$$

证明. The order of G is N, the order of H is n, and the index of H in G is j. They are all finite.

The N elements of G split into j right cosets. Each right coset has the same number of elements as H by Lemma 1.9.3, so each right coset has n elements. This means

$$N = nj \tag{1.37}$$

$$\iff |G| = |H| \cdot [G : H] \tag{1.38}$$

$$\iff \text{(order of } G) = \text{(order of } H) \text{ (number of cosets)} . \tag{1.39}$$

Here Equation 1.39 is the importatnt **Counting Formula**.

□

定理 1.9.3. 一个有限群 G 的任一个元 a 的阶 (order of a in G) n 都整除 G 的阶.

证明. The order of a in G is n. This means a generates a subgroup H with its order is $|H| = n$. By Theorem 1.9.2, n divides the order of G, which is $|G| = |H| \cdot [G : H] = n \cdot [G : H]$. □

同理, 上述定理 1.9.2 可得出以下:

定理 1.9.4 (Lagrange's Theorem)**.** 假定 H 是一个**有限群** G 的一个子群. 那么 H 的阶 (the order of H) 整除 G 的阶 (the order of G).

练习 1.9.1. 阶是素数的群一定是循环群.

证明. 假设群 G 的阶是素数 p. 在 G 中取一个不等于单位元的元 $a \neq e$, 那么 a 生成 G 的一个循环子群 (a). 假设 (a) 的阶是 n, 那么因为 a 不是单位元, 所以 $n \geq 2 \neq 1$. 而根据定理 1.9.2, n 可以整除 p, 但是 p 是素数, 所以我们有 $n = p$ 而 $G = (a)$ 是一个循环群. □

1.10 不变子群和商群 (Normal Subgroup and Quotient Group/Factor Group)

一般而言, 给定一个群 G, 一个子群 H, H 的一个右陪集 Ha 不一定等于 H 的左陪集 aH. 但是存在以下特殊情况:

定义 1.10.1. 一个群 G 的一个子群 N 叫做一个**不变子群 (Normal subgroup)**, 如果有:

$$Na = aN, \quad \forall a \in G$$

一个不变子群 N 的一个左 (或者右) 陪集叫做 N 的一个**陪集 (coset)**.

备注 1.10.1. 一个任意群 G 的子群 G 和 $\{e\}$ 总是不变子群.

不变子群还有另外一个定义:

定义 1.10.2. 群 G 的一个子群 N 如果有:

$$\forall a \in N, \forall g \in G \Rightarrow gag^{-1} \in N \tag{1.40}$$

那么这个子群 N 是一个不变子群.

如果 $a, b \in G$, 存在 $g \in G$ 使得 $b = gag^{-1}$, 那么 a 和 b **共轭 (conjugate)**.

根据这个定义, 我们有以下:

定理 1.10.1. 一个群之间的映射的核 (kernel) 是一个不变子群.

证明. 假定一个群之间的映射为: $\phi : G \to G'$, 它的核为

$$ker(\phi) = \{a \,|\, \phi(a) = 1_{G'}\} \subset G.$$

假设 $\forall a \in ker(\phi)$, $\forall g \in G$, 我们有:

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)1_{G'}\phi(g)^{-1} = 1_{G'}.$$

也就是说, $gag^{-1} \in ker(\phi)$. 所以, $ker(\phi)$ 是 G 的一个不变子群.

□

定义 1.10.3. 任意一个群 G, 它的**中心 (center)** 包含 G 的所有有以下性质的元 n:

$$Z = \{n \in G \,|\, na = an, \quad \forall a \in G\} \tag{1.41}$$

引理 1.10.1. 一个群 G 的中心 (center) Z 是 G 的不变子群 (normal subgroup).

证明. 首先, 因为 G 的单位元 e 符合条件 $ea = ae$, 因此 $e \in Z$, 也就是说, Z 是非空集合.

而且, Z 是 G 的子群:

- $n_1 \in Z, n_2 \in Z \Rightarrow n_1 n_2 \in Z$: $n_1 a = a n_1$, $n_2 a = a n_2 \Rightarrow n_1 n_2 a = n_1 a n_2 = a n_1 n_2$;
- $n \in Z \Rightarrow n^{-1} \in Z$: $na = an \Rightarrow n^{-1}a = n^{-1}ann^{-1} = n^{-1}nan^{-1} = an^{-1}$.

显然, $Za = aZ$, 因此, Z 是 G 的不变子群.

□

备注 1.10.2. 关于不变子群:

- 一个**交换群 (Abelian group)** 的每一个子群 H 都是不变子群.

- 所谓 $Na = aN$ 并不是说 a 可以同 N 中的每一个元交换, 而是说 Na 和 aN 这两个集合一样. 换而言之, 一个不变子群 (normal subgroup) 不一定是群的中心 (center).

定理 1.10.2. 一个群 G 的一个子群 N 是一个不变子群的充分必要条件是:

$$aNa^{-1} = N$$

对于 G 的任意一个元 a 都对.

这里,

$$aNa^{-1} = \{ana^{-1} \,|\, \forall n \in N, \forall a \in G\}$$

证明. 如果 N 是不变子群, 那么, $\forall a \in G$, $aNa^{-1} = (aN)a^{-1} = (Na)a^{-1} = N(aa^{-1}) = Ne = N$.

如果对于 $\forall a \in G$, 都有 $aNa^{-1} = N$, 那么, 任意的 $n \in N$ 都可以写成 an_1a^{-1} 的形式. 也就是说,

$$\begin{aligned} Na &= \{na | \forall n \in N, \forall a \in G\} \\ &= \{an_1a^{-1}a | \forall a \in G,\, n_1 \in N\} \\ &= (aNa^{-1})a. \end{aligned}$$

因此, 我们可以推出 $Na = (aNa^{-1})a = (aN)(a^{-1}a) = (aN)e = aN$. □

定理 1.10.3. 一个群 G 的一个子群 N 是一个不变子群的充分必要条件是:

$$\forall a \in G, \forall n \in N \Longrightarrow ana^{-1} \in N$$

证明. 定理 1.10.2 说明了这个条件是必要的. 我们来证明它是充分的: 假如这个条件成立, 那么, $aNa^{-1} \subseteq N$. 而且 $a^{-1} \in G$, 我们有 $a^{-1}Na \subseteq N \Longrightarrow a(a^{-1}Na)a^{-1} \subseteq aNa^{-1} \Longrightarrow N \subseteq aNa^{-1}$. 所以, 我们有 $aNa^{-1} = N$. □

备注 1.10.3. 证明一个子群是不是不变子群, 用定理 1.10.3 中的条件一般比较方便.

备注 1.10.4. 不变子群 (normal subgroup) 之所以重要, 是因为这个子群的陪集 (coset), 对于**某种与原来的群有密切关系的代数运算**来说, 也作成一个群.

考虑之前例子 1.9.1 讨论过的整数加群 $\mathbb{Z}$ (additive group of $\mathbb{Z}$), 记为 $\overline{G}$. 那么, 一个固定整数 n 的所有倍数作成一个子群 $\overline{N}$. 整数加群 $\overline{G}$ 是交换群 (Abelian group), 所以, 它的子群 $\overline{N}$ 是一个不变子群 (normal subgroup). 而 $\overline{N}$ 的陪集 (coset) 也就是模 n 的剩余类 (residue class), 对于代数运算

$$+ : [a] + [b] \mapsto [a + b]$$

作成一个群: **剩余类加群 (additive group of integers modulo n, $\mathbb{Z}/n\mathbb{Z}$)** (见例子 1.7.2).

接下来我们根据类似的思路, 在任意的一个不变子群的基础上构造出一个群: 不变子群 (normal subgroup) 的陪集 (coset), 称为 **商群 (quotient group)**.

给定一个群 G 和一个不变子群 (normal subgroup) N. 把 N 的所有陪集 (coset) 作成一个集合:

$$\overline{G} = \{aN, bN, cN, \ldots\}$$

考虑以下法则:

$$(xN)(yN) = (xy)N \tag{1.42}$$

是一个 $\overline{G}$ 的乘法.

定理 1.10.4. 一个不变子群 (normal subgroup) 的陪集 (cosets) 对于上面规定的乘法来说作成一个群.

具体而言, 给定一个群 G 和它的一个不变子群 N, N 的所有陪集做成一个集合 $\overline{G} = \{aN, bN, cN, \ldots\}$. 那么存在 $\overline{G}$ 的一个代数运算 (1.42) 使得 $\overline{G}$ 作成一个群.

证明. 我们证明群定义 1.1.2 的 I, II, IV, V:

- I: 乘法是闭的, 显然;

- II: 结合律成立: $(xNyN)zN = [(xy)N]zN = (xyz)N = xN[(yz)N] = xN(yNzN)$;
- IV: 这个群的单位元是 $eN = N$: $eNxN = (ex)N = xN$;
- V: aN 的逆元是 $a^{-1}N$: $aNa^{-1}N = (aa^{-1})N = eN$.

□

定义 1.10.4. 一个群 G 的一个不变子群 N 的陪集所作成的群叫做一个**商群 (quotient group/factor group)**. 这个群用符号 G/N 表示.

备注 1.10.5. 因为 N 的指数 (the index of N in G) 就是 N 的陪集的个数 (number of cosets), 因此, 我们有: 商群 G/N 的元的个数 (也就是商群 G/N 的阶 (order of G/N)) 就是 N 的指数 (index of N in G, or the number of cosets). 当 G 是有限群的时候, 由定理 1.9.2 可得出:

$$\frac{G\text{的阶}}{N\text{的阶}} = G/N\text{的阶} = N\text{的陪集的个数} = N\text{的指数}$$

或者说是,

$$\frac{\text{order of } G}{\text{order of } N} = \text{order of } G/N = \text{number of cosets of } N = \text{index of } N \text{ in } G$$

1.11 同态与不变子群 (Homomorphism and Normal Subgroup)

在不变子群 (normal subgroup), 商群 (quotient group) 和同态映射 (group homomorphism) 之间存在几个极端重要的关系.

定理 1.11.1. 一个群 G 和它的每一个商群 (quotient group) G/N 同态 (满射)(surjective homomorphism, or epimorphism).

证明. 考虑以下 G 到 G/N 的一个满射法则:

$$\phi : G \longrightarrow G/N, \quad \phi(a) = aN, \quad \forall a \in G$$

显然, 它是个满射: $\forall aN \in G/N$, 存在 $a \in G$ 使得 $\phi(a) = aN$.
同时, 它也是一个同态映射: 对于任意两个元 $\forall a \in G$, $\forall b \in G$,

$$\phi(ab) \longrightarrow abN = (aN)(bN) = \phi(a)\phi(b).$$

□

备注 1.11.1. 由群 G 的一个子群可以推测整个群 G 的性质. 假如 G 有一个不变子群 N, 那么我们有两个子群可以利用: N 和 G/N. 定理1.11.1 告诉我们, G 和 G/N 同态 (满射), 我们自然更加容易推测 G 的性质.

备注 1.11.2. 不变子群 (normal subgroup) 的重要性在于, 在某种意义上, 定理 1.11.1 的逆定理也是对的. 为此, 我们需要使用映射的核 (kernel) 的定义.

定义 1.11.1. 假定 ϕ 是一个群 G 到另一个群 $\overline{G}$ 的**同态满射 (surjective homomorphism, or epimorphism)**. $\overline{G}$ 的单位元 $\overline{e}$ 在 ϕ 之下的所有逆象所作成的 G 的子集叫做同态满射 ϕ 的**核 (kernel)**, 表示为 $ker(\phi)$.

$$ker(\phi) = \{a \in G \,|\, \phi(a) = \overline{e} \in \overline{G}\} \tag{1.43}$$

定理 1.11.2 (First Isomorphism Theorem)**.** 假定 G 和 G' 是两个群, 而且有 $\phi : G \longrightarrow G'$ 这样一个同态 (满射) (epimorphism). 这个同态满射的核 $N := ker(\phi)$ 是 G 的一个不变子群 (normal subgroup). 我们有 G 的商群 $\overline{G} := G/N$ 和 G' 同构

$$G/N = \overline{G} \cong G'.$$

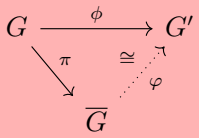
具体而言, 假定正则映射 (canonical map)

$$\pi : G \longrightarrow \overline{G}$$

那么, 存在一个同构映射

$$\varphi : G/N = \overline{G} \xrightarrow{\cong} G'$$

使得 $\phi = \varphi \cdot \pi$.



(1.44)

证明. 我们用 ϕ 表示给定的同态满射 (epimorphism). 由定理 1.10.1, 我们这个同态满射的核 $N := ker(\phi)$ 是 G 的一个不变子群.

考虑:

$$\varphi : G/N = \overline{G} \longrightarrow G', \quad \varphi(aN) = a' = \phi(a), \quad \forall a \in G.$$

我们要说明: 映射 φ 是一个 $G/N = \overline{G}$ 到 G' 的同构映射. 因为:

1. φ 存在 (well-defined): $aN = bN \Rightarrow b^{-1}a \in N \Rightarrow \phi(b^{-1}a) = e' \in G' \Rightarrow (b^{-1})'\, a' = e' \Rightarrow b'^{-1}\, a' = e' \Rightarrow a' = b'$.

2. φ 是 $G/N = \overline{G}$ 到 G' 的满射 (surjective): 给定任意一个元 $a' \in G'$, 在 G 里至少有一个元 a 满足 $\phi(a) = a'$, 也就是说至少有一个元 $\pi(a) = aN \in G/N$ 使得 $\varphi(aN) = a'$.

3. φ 是 $G/N = \overline{G}$ 到 G' 的单射 (injective): $aN \neq bN \Rightarrow b^{-1}a \notin N \Rightarrow \phi(b^{-1}a) \neq e' \in G' \Rightarrow (b^{-1})'\, a' \neq e' \Rightarrow b'^{-1}\, a' \neq e' \Rightarrow a' \neq b'$.

4. φ 是同态映射: $aNbN = abN \implies \varphi(aN)\varphi(bN) = a'b' = \phi(a)\phi(b) = \phi(ab) = (ab)' = \varphi(abN) \implies \varphi(aN)\varphi(bN) = \varphi(abN)$.

因此, $\varphi : \overline{G} \longrightarrow G'$ 是一个同构映射. □

备注 1.11.3. 定理1.11.1 告诉我们一个群 G 和它的商群 G/N 同态. 定理1.11.2 告诉我们, G (对于任意一个群 G' 与 G 同态, 那么 G' 与 G 的商群 G/N 同构) 只能和它的商群 G/N 同态. 某种意义上而言, 定理1.11.2 是定理1.11.1 的逆定理.

备注 1.11.4. 当群 G 和群 G' 同态的时候, G' 的性质并不和 G 的完全一样. 但是, 定理1.11.2 告诉我们, 一定能找到 G 的一个不变子群 N, 使得 G' 的性质和商群 G/N 的完全一样 (同构).

在一个同态满射之下, 一个群的若干性质是不变的, 若干性质是会变的.

定理 1.11.3. 假定 G 和 $\overline{G}$ 是两个群, 并且 G 和 $\overline{G}$ 同态满射 (epimorphism). 那么在这个同态满射之下:

1. G 的一个子群 (subgroup) H 的象 $\overline{H}$ 是 $\overline{G}$ 的一个子群;
2. G 的一个不变子群 (normal subgroup) N 的象 $\overline{N}$ 是 $\overline{G}$ 的一个不变子群.

定理 1.11.4. 假定 G 和 $\overline{G}$ 是两个群, 并且 G 和 $\overline{G}$ 同态满射 (epimorphism). 那么在这个同态满射之下:

1. $\overline{G}$ 的一个子群 (subgroup) $\overline{H}$ 的逆象 H 是 G 的一个子群;
2. $\overline{G}$ 的一个不变子群 (normal subgroup) $\overline{N}$ 的逆象 N 是 G 的一个不变子群.

备注 1.11.5. 也就是说, 一个群的一个子集是否一个**子群 (subgroup)** 以及是否一个**不变子群 (normal subgroup)** 这两个性质, 在一个**同态满射 (epimorphism)** 之下是不变的.

第二章　环与域 (Rings and Fields)

2.1　加群与环的定义 (Additive Group and Ring)

环 (ring) 的定义需要用到加群 (additive group) 的概念.

定义 2.1.1. 一个交换群 (Abelian group) 叫做一个**加群 (additive group)**. 我们可以把这个群的代数运算叫做**加法**, 并且用 + 来表示.

备注 2.1.1. 加群具有一些特有的记法 (notation):

1. 加法结合律 (associative law):

$$\sum_{i=1}^{n} a_i = a_1 + \ldots + a_n.$$

2. 单位元 (additive identity): 称为**零元 (zero identity, or zero)**. 有以下计算规则:

$$0 + a = a + 0 = a.$$

3. n 个元 a 的和 (n 为正整数) 表示为:

$$na = \overbrace{a + a + ... + a}^{n} \tag{2.1}$$

4. 有了以上 na 的记法, 我们有:

$$(-n)a = -(na), \quad 0a = \mathbf{0} \tag{2.2}$$

这里第一个零是整数 (integer), 第二个零是加群的**零元 (zero identity, or zero)**.

进一步而言, 对于任意整数 m, n, 和加群的任意元 a, b 来说, 都有

$$ma + na = (m+n)a \tag{2.3}$$

$$m \cdot na = mn \cdot a \tag{2.4}$$

$$n(a+b) = na + nb \tag{2.5}$$

需要注意, 这里的整数 m, n 一般不是加群的元.

5. 用新的加群符号记法, 加群的一个非空子集 S 作为一个子群的充分必要条件是:

   - $a, b \in S \Rightarrow a + b \in S$;
   - $a \in S \Rightarrow -a \in S$.

   或者是:

   - $a, b \in S \Rightarrow a - b \in S$.

下面我们给出环 (ring) 的定义.[1]

定义 2.1.2. 一个集合 R 叫做一个**环 (ring)**, 如果满足以下条件:

1. R 是一个加群 (additive group): R 对于一个叫做加法的代数运算来说作成一个交换群 (Abelian group);
2. R 对于另一个叫做乘法的代数运算来说是闭的;
3. 这个乘法适合结合律 (associative law of composition): 对于任意三个元 a, b, $c \in R$,

$$a(bc) = (ab)c \tag{2.6}$$

[1] 截止至目前为止 (2022 年), 关于是否在环的定义里面包括乘法的单位元仍在争论当中. 为了以示区分, 对于不包括乘法单位元的环的定义有时候也被称作 rng, 而把包括乘法单位元的环的定义成为 ring.

4. 两个分配律 (distributive laws) 都成立: 对于任意三个元 $a, b, c \in R$,

$$a(b+c) = ab + ac$$
$$(b+c)a = ba + ca$$

备注 2.1.2. 全体整数作成的集合对于普通的加法和乘法来说做成一个环 (ring of integers).

备注 2.1.3. 一个环 R 满足一般的计算规则: 给定 $a, b, c, 0 \in R$, 以及 $m, n \in \mathbb{Z}$,

1. $0 + a = a + 0 = a$.
2. $-a + a = a - a = 0$.
3. $-(-a) = a$.
4. $a + c = b \iff c = b - a$.
5. $-(a+b) = -a - b$; $-(a-b) = -a + b$.
6. $ma + na = (m+n)a$; $m \cdot na = mn \cdot a$; $n(a+b) = na + nb$.
7. $(a-b)c = ac - bc$; $c(a-b) = ca - cb$.
8. $0a = a0 = a$.
9. $(-a)b = a(-b) = -ab$.
10. $(-a)(-b) = ab$.
11. $a(b_1 + b_2 + \ldots + b_n) = ab_1 + ab_2 + \ldots + ab_n$; $(b_1 + b_2 + \ldots + b_n)a = b_1a + b_2a + \ldots + b_na$.
12. $(a_1 + \ldots + a_m)(b_1 + \ldots + b_n) = a_1b_1 + \ldots + a_1b_n + \ldots + a_mb_1 + \ldots + a_mb_n$.
13. $(na)b = a(nb) = a(ab)$.
14. $a^m a^n = a^{m+n}$; $(a^m)^n = a^m n$.

2.2 交换律, 单位元, 零因子, 整环 (Integral Domain)

在一般的环里面, 有一些普通的计算法则不成立. 它们要在有附加条件的环里才能成立. 下面, 我们讨论环的三种重要附加条件.

条件 2.2.1. 交换律 (commutative law): 环的定义没有要求乘法适合交换律 (commutative law), 所以在一个环里 ab 不一定等于 ba.

定义 2.2.1. 一个环 R 叫做一个 **交换环 (commutative ring)**, 假如对于任意两个元 $\forall a, b \in R$, 我们有:

$$ab = ba. \tag{2.7}$$

备注 2.2.1. 在一个交换环 (commutative ring) R 里, 对于任意正整数 n 和环的任意两个元 $a, b \in R$ 来说, 我们有:

$$a^n b^n = (ab)^n. \tag{2.8}$$

条件 2.2.2. 单位元 (multiplicative identity): 环的定义没有要求一个环要有一个对于乘法来说的单位元 (multiplicative identity).

定义 2.2.2. 一个环 R 的一个元 e 叫做一个**单位元 (multiplicative identity)**, 假如对于 R 的任意元来说, 都有

$$ea = ae = a. \tag{2.9}$$

备注 2.2.2. 一般来说, 一个环未必有一个单位元 (multiplicative identity). 例如:

$$R = \{\text{所有偶数}\}. \tag{2.10}$$

R 对于普通加法和乘法来说作成一个环, 但是它没有单位元 (multiplicative identity).

备注 2.2.3. 一个环如果有单位元 (multiplicative identity), 它只能有一个. 我们习惯把这个唯一的单位元表示为 1. 当然, 单位元的 1 一般不是普通整数意义上的 1.

备注 2.2.4. 对于有单位元的环, 我们规定一个元的零次方:

$$a^0 = 1 \tag{2.11}$$

定义 2.2.3. 一个有单位元 (multiplicative identity) 1 的环的一个元 b 叫做元 a 的一个 **(乘法) 逆元 (multiplicative inverse)**, 假如

$$ba = ab = 1 \tag{2.12}$$

如果一个元 a 有逆元 (multiplicative inverse), 那么这个元 a 称为环的 **单位 (unit)**.

由于历史的原因, 可逆的元被称为单位. 这个名称非常容易让人混淆. 因此, 在以下内容里面我们尽量使用 (乘法) 可逆元 (muliplicative invertible (element)) 的称呼来替代单位 (unit) .

备注 2.2.5. 一个元 a 最多只能有一个逆元, 我们一般表示为 a^{-1}, 并且规定:

$$a^{-n} = \left(a^{-1}\right)^n. \tag{2.13}$$

当然, 一个元 a 未必有逆元. 例如, 整数环 (ring of integers) $\mathbb{Z}$ 是一个有单位元 (multiplicative identity) 的环, 但是除了 ± 1 以外, 其他的整数都没有逆元 (multiplicative inverse): 如果 $a = 2$, 那么 a 的逆元 b 需要 $ab = 1$, 也就是说, 需要非整数 $b = \frac{1}{2}$. 很明显, $b = \frac{1}{2} \notin \mathbb{Z}$.

条件 2.2.3. 零因子 (zero divisor): 一个环的两个元 $a = 0$ 或者 $b = 0$, 那么 $ab = 0$. 反之则不一定成立. 也就是说:

$$ab = 0 \Rightarrow a = 0 \text{ 或者 } b = 0 \tag{2.14}$$

这一条件 2.14 一般而言在一个环里并不一定成立.

定义 2.2.4. 给定一个集合:

$$R = \{\text{所有模 } n \text{ 的剩余类}\}. \tag{2.15}$$

规定一种加法:

$$[a] + [b] = [a + b] \tag{2.16}$$

规定一种乘法:

$$[a][b] = [ab]. \tag{2.17}$$

我们得出 R 做成一个环, 称为 **模 n 的剩余类环 (ring of residue classes modulo n, or ring of integers modulo n)**.

备注 2.2.6. 如果 n 不是素数, 那么存在 $n = ab$. 在**模 n 的剩余类环**里,

$$[a] \neq [0],\ [b] \neq [0],\ \text{但是}\ [ab] = [n] = [0]. \tag{2.18}$$

而 $[0]$ 是 R 的零元. 也就是说, 零因子条件在**模 n 的剩余类环 (ring of integers modulo n)** 不成立.

定义 2.2.5. 在一个环里, 如果有

$$a \neq 0,\ b \neq 0\ \text{但是}/,\ ab = 0 \tag{2.19}$$

我们说, a 是这个环的一个**左零因子 (left zero divisor)**, b 是这个环的一个**右零因子 (right zero divisor)**.

备注 2.2.7. 一个环若是交换环 (commutative), 那么它的一个左零因子也是一个右零因子. 但是在非交换环中就未必.

一个环当然也可以没有零因子, 例如考虑整数环 (ring of integers $\mathbb{Z}$). 在而且只在 (if and only if) 一个没有零因子的环里条件 2.14 才会成立.

例子 2.2.1. 在一个域 (field) F 上的一切 $n \times n$ 矩阵, 对于矩阵的加法和乘法来说, 做成一个有单位元的环. 当 $n \geq 2$ 的时候, 这个环是非交换环, 并且

有零因子. 具体而言, 可以考虑:

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

备注 2.2.8. 零因子和消去律相互关联.

定理 2.2.1. 在一个没有零因子 (*no* zero divisor) 的环里, 两个消去律 (cancellation laws) 都成立:

$$a \neq 0,\ ab = ac \Rightarrow b = c$$
$$a \neq 0, ba = ca \Rightarrow b = c.$$

反之, 在一个环里如果有一个消去律 (cancellation law) 成立, 那么这个环没有零因子 (*no* zero divisor).

证明. 假定环 R 没有零因子, 那么,

$$ab = ac \Rightarrow a(b-c) = 0 \tag{2.20}$$

因此有:

$$a \neq 0,\ ab = ac \Rightarrow a \neq 0,\ a(b-c) = 0 \implies b - c = 0 \Rightarrow b = c. \tag{2.21}$$

同理可证 $a \neq 0, ba = ca \Rightarrow b = c$.

反过来, 假定环 R 的第一个消去律成立: $a \neq 0,\ ab = ac \Rightarrow b = c$.

那么有 $ab = 0 \Rightarrow ab = a0$. 由第一个消去律, 我们得出 $a \neq 0,\ ab = a0 = 0 \implies b = 0$. 也就是说, R 没有零因子.

同理可得, 在第二消去律成立的时候, R 没有零因子.

□

推论 2.2.1. 在一个环里, 如果有一个消去律成立, 那么另一个消去律也成立.

满足以上这三种附加条件的环特别重要.

定义 2.2.6. 一个环 R 叫做一个 **整环 (integral domain)**, 假如对于 R 的任意元 $a, b \in R$,

1. 乘法适合交换律 (commutative law in multiplication):

$$ab = ba \tag{2.22}$$

2. R 有乘法单位元 1 (has multiplicative identity 1):

$$1a = a1 = a \tag{2.23}$$

3. R 没有零因子 (has *no* zero divisor):

$$ab = 0 \Rightarrow a = 0, \text{ 或者 } b = 0 \tag{2.24}$$

备注 2.2.9. 整数环 (ring of integers $\mathbb{Z}$) 是一个整环 (integral domain).

练习 2.2.1. 假定一个环对于加法来说做成一个循环群 (cyclic group), 那么 R 是交换环 (commutative ring).

解答. 假设元 a 生成循环群, 那么任意两个元 $b, c \in R$ 有

$$b = ma, \quad c = na, \quad m, n \text{ 是整数} \tag{2.25}$$

我们有:

$$bc = (ma)(na) = (mn)aa = cb \tag{2.26}$$

因此, 交换律在 R 中成立. 所以, R 是交换环 (commutative ring).

练习 2.2.2. 对于有单位元 (multiplicative identity) 的环来说, 加法交换律可以由环定义 2.1.2 里的其他条件得出.

解答. 考虑

$$\begin{aligned}
&(a+b)(1+1) = a+b+a+b = a+a+b+b \\
\Rightarrow &-a+(a+b+a+b)-b = -a+(a+a+b+b)-b \\
\Rightarrow &b+a = a+b.
\end{aligned}$$

练习 2.2.3. 由所有实数 $a+b\sqrt{2}$ (a, b 是整数) 组成的集合对于普通加法和乘法来说是一个整环 (integral domain).

解答. 首先我们验证环的定义 2.1.2 里面的条件:

1. R 是一个加群 (Abelian group): $a,b,c,d\in\mathbb{Z}$ 为整数, 那么

   - R 对于加法是闭的, 而且加法适合交换律:

   $$\begin{aligned}&(a+b\sqrt{2})+(c+d\sqrt{2})\\=&(a+c)+(b+d)\sqrt{2}\\=&(c+a)+(d+b)\sqrt{2},\quad\text{(根据整数普通加法的交换律)}\\=&(c+d\sqrt{2})+(a+b\sqrt{2}).\end{aligned}$$

   - 对于任意元 $a+b\sqrt{2}\in R$, 有加法单元 $0+0\sqrt{2}=0\in R$
   - 对于任意元 $a+b\sqrt{2}\in R$, 有逆元 $-a-b\sqrt{2}\in R$ 使得

   $$(a+b\sqrt{2})+(-a-b\sqrt{2})=0\in R.$$

2. R 对于乘法而言是闭的 (closed in multiplication): $a,b,c,d\in\mathbb{Z}$ 为整数,

   $$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in R.$$

   其中 $(ac+2bd)$, $(ad+bc)\in\mathbb{Z}$ 为整数.

3. R 的乘法适合结合律 (associative law of composition): $a_1,a_2,b_1,b_2,c_1,c_2\in\mathbb{Z}$, 根据整数普通乘法的交换律, 我们可以验证

   $$\begin{aligned}&(a_1+a_2\sqrt{2})\big[(b_1+b_2\sqrt{2})(c_1+c_2\sqrt{2})\big]\\=&\big[(a_1+a_2\sqrt{2})(b_1+b_2\sqrt{2})\big](c_1+c_2\sqrt{2})\end{aligned}$$

接下来, 我们验证整环定义 2.2.6 里面的条件:

1. 乘法适合交换律 (commutative law in multiplication): 根据整数普通乘法的交换律, 我们可以验证

   $$\begin{aligned}&(a+b\sqrt{2})(c+d\sqrt{2})\\=&(ac+2bd)+(ad+bc)\sqrt{2}\\=&(ca+2db)+(cb+da)\sqrt{2}\\=&(c+d\sqrt{2})(a+b\sqrt{2})\end{aligned}$$

2. R 有乘法单位元 1 (has multiplicative identity 1):

$$1 + 0\sqrt{2} = 1 \in R$$

3. R 没有零因子 (has *no* zero divisor):

$$\begin{aligned} & a + b\sqrt{2} \neq 0,\, c + d\sqrt{2} \neq 0 \\ \Longrightarrow\ & (a \neq 0 \text{ OR } b \neq 0) \text{ AND } (c \neq 0 \text{ OR } d \neq 0) \\ \Longrightarrow\ & (ac + 2bd) + (ad + bc)\sqrt{2} \neq 0 \end{aligned}$$

所以, R 是整环 (integral domain).

2.3 除环和域 (Division Ring and Field)

一般而言, 环的一个任意元不一定有一个逆元. 在极特殊的情况下, 一个环里的每一个元都有一个逆元. 例如:

例子 2.3.1. R 只包括一个元 a, 加法和乘法是:

$$a + a = a, \quad , aa = a \tag{2.27}$$

R 是一个环, 而且这个环里的唯一的元 a 有一个逆元, 就是 a 本身. 有时候我们用 0 表示 a, 这样的一个环叫做 **零环 (zero ring)**.

- 对于至少有两个元的环, 至少有一个不等于零的元 a, 有 $0a = 0 \neq a$. 因此, 0 不是 R 的单位元 (multiplicative identity). 而此时, 0 没有逆元: 因为对于任何元 $b \in R$, 都有:

$$b0 = 0 \neq \text{单位元}.$$

- 我们进一步问, 除了零元以外, 其他的元会不会有一个乘法逆元 (multiplicative inverse)?

例子 2.3.2. $R = \{\text{全体有理数}\}$ 对于普通加法和乘法来说是一个环. 这个环的任意一个非零元的元 $a \neq 0$ 都有逆元 $\dfrac{1}{a} \in R$.

定义 2.3.1. 一个环 R 叫做一个**除环 (division ring)**, 假如:

1. R 至少包含一个不等于零的元;
2. R 有一个单位元 (multiplicative identity);
3. R 的每一个不等于零的元都有一个逆元 (multiplicative inverse).

定义 2.3.2. 一个 (乘法) 交换除环 (commutative division ring) 叫做一个**域 (field)**.

备注 2.3.1. 除环 (division ring) 的几个重要性质:

1. 一个除环没有零因子 (no zero divisor), 因为:

$$a \neq 0,\, ab = 0 \implies a^{-1}ab = b = a^{-1}0 = 0 \tag{2.28}$$

所以, 我们得出:

$$ab = 0 \Rightarrow a = 0, \text{ 或者} b = 0 \tag{2.29}$$

2. 一个除环的不等于零元的元对于乘法来说作成一个群 R^*, 这个群叫做除环 R 的**乘群 (multiplicative group of division ring, or unit group: every element in the unit group is multiplicative invertible (is unit))**.

3. 在一个除环 R 里, 方程

$$ax = b \quad \text{和} \quad ya = b, \quad (a, b \in R,\, a \neq 0) \tag{2.30}$$

各有一个唯一的解: $a^{-1}b$ 和 ba^{-1}.

一般而言, 在一个除环里, 这两个解不一定相等; 而在一个域里, 因为交换律 (multiplicative commutative law) 的成立, 我们有这两个解相等: $a^{-1}b = ba^{-1}$.

例子 2.3.3. 这是一个非交换除环 (non-commutative division ring):

$$R = \{\text{所有复数对}(\alpha, \beta)\}. \tag{2.31}$$

规定:

- $(\alpha_1, \beta_1) = (\alpha_2, \beta_2)$, 当且只当 $\alpha_1 = \alpha_2$ 和 $\beta_1 = \beta_2$.
- R 的加法:
$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2,\ \beta_1 + \beta_2) \tag{2.32}$$
- R 的乘法:
$$(\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1\alpha_2 - \beta_1\overline{\beta_2},\ \alpha_1\beta_2 + \beta_1\overline{\alpha_2}) \tag{2.33}$$

这里 $\overline{\alpha}$ 是 α 的共轭数 (complex conjugate):

$$\alpha = a + bi, \quad \overline{\alpha} = a - bi \tag{2.34}$$

那么 R 作成一个环.

R 有一个单位元 (multiplicative identity) $(1, 0)$: 对于任意元 (α, β)

$$\begin{aligned}
&(\alpha, \beta)(1, 0)\\
=&(\alpha \cdot 1 - \beta \cdot \overline{0},\ \alpha \cdot 0 + \beta \cdot \overline{1}) = (\alpha, \beta)\\
=&(1, 0)(\alpha, \beta)\\
=&(1 \cdot \alpha - 0 \cdot \overline{\beta},\ 1 \cdot \beta + 0 \cdot \overline{\alpha})
\end{aligned}$$

R 不是交换环: 例如,

$$(i, 0)(0, 1) = (0, i) \neq (0, -i) = (0, 1)(i, 0)$$

这个环叫做 **四元数除环 (Ring of quaternions (in Cayley–Dickson construction))**. [2]

总结一下我们目前已经讨论过的各种环的关系, 见图 2.1.

以下我们用的最多的是整环 (Integral domain) 和域 (Field).

[2] Cayley–Dickson construction 见 https://en.wikipedia.org/wiki/Cayley%E2%80%93Dickson_construction. 其中, 对于复数对 $(a, b) \in \mathbb{C}^2$ 的乘法运算如下:

$$(a, b)(c, d) = (ac - bd^*, b^* + da) \tag{2.35}$$

对于 $a = x + yi$, 我们有 a 的共轭数 (complex conjugate) 表示为 $a^* = x - yi$.

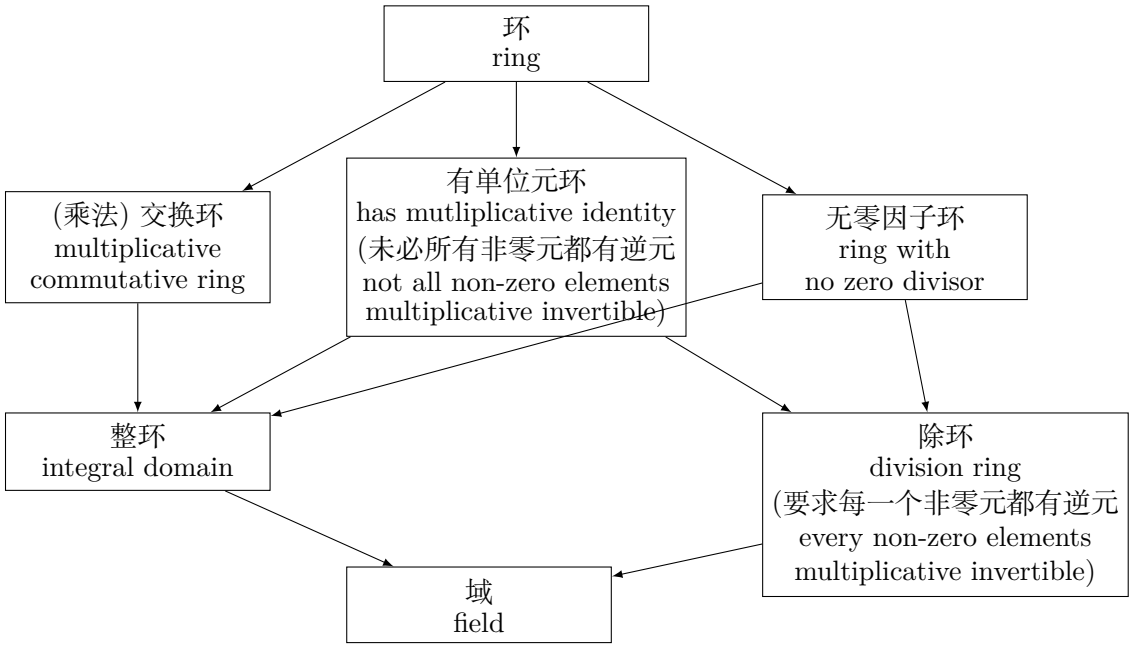


图 2.1: 环的隶属关系

练习 2.3.1. 证明: 一个至少有两个元而且没有零因子的有限环 R 是一个除环.

证明. 令 $R^* = \{R$ 的一切非零元$\}$. 因为 R 至少有两个元, 那么 R^* 非空.

- R 没有零因子, 所以 R^* 对于乘法来说是闭的.
- R 的元适合乘法结合律, 因此乘法结合律也同样适合 R^* 的元.
- R 没有零因子, 所以消去律对 R^* 的元成立.
- R^* 只有有限个元, 所以根据定义 1.3.1, R^* 做成一个乘群.
- 1 是 R^* 的单位元 (multiplicative identity). 对于不属于 R^* 但是属于 R 的零元而言, 我们有 $1 \cdot 0 = 0 \cdot 1 = 0$. 因此, 1 也是 R 的单位元.
- 而且 R^* 的元在乘群 R^* 中的逆元也是它在 R 中的逆元.

因此, R 是一个除环.

□

2.4 无零因子环的特征 (Characteristic of a Ring)

有一种普通运算规则在环 (ring) 甚至是域 (field) 里面也不一定能适用:

$$a \neq 0 \Rightarrow ma = \overbrace{a + a + ... + a}^{m} \neq 0 \tag{2.36}$$

例子 2.4.1. 考虑一个模 p (p 为素数) 的剩余类环 F (ring of residue classes modulo n, or ring of integers modulo n), 见定义 2.2.4. 证明 F 是一个域.

证明. 模 p (p 为素数) 的剩余类环 F 适合加法和乘法的交换律:

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$
$$[a][b] = [ab] = [ba] = [b][a].$$

我们只需要证明 F 的非零元作成一个乘群 F^* (这样的话, 可以对应于除环 (division ring) 的定义 2.3.1, F 中至少有一个不等于零的元, 有一个乘法单位元 (multiplicative identity), 而且每一个 F 中的非零元都有乘法逆元):

F^* 是一个有限集合, 根据定义 1.3.1, 它作成乘群的条件是: I. 对于乘法运算是闭的; II. 乘法适合结合律; III'. 消去律成立.

I. 乘法运算是闭的: 由于 p 是素数, 我们有

$$p \nmid a,\ p \nmid b \Rightarrow p \nmid ab \tag{2.37}$$

这里,$p \nmid a$ 表示 p 不能整除 a, 也就是说

$$p \nmid a \iff a \neq pn, \quad n = 0, 1, 2, \ldots \tag{2.38}$$

因此, 我们得出

$$[a] \neq 0,\ [b] \neq 0 \Rightarrow [a][b] = [ab] \neq 0; \tag{2.39}$$

也可以表示为:

$$[a] \in F^*,\ [b] \in F^* \Rightarrow [a][b] \in F^*. \tag{2.40}$$

II. 剩余类的乘法满足结合律.

$$\Big([a][b]\Big)[c] = [abc] = [a]\Big([b][c]\Big)$$

III'. 消去律成立: 给定

$$p \mid ax - ax',\ p \nmid a \Rightarrow p \mid x - x' \tag{2.41}$$

也就是说,

$$[ax] = [ax'],\ [a] \neq 0 \Rightarrow [x] = [x'] \tag{2.42}$$

也就是说,

$$[a][x] = [a][x'],\ [a] \in F^* \Rightarrow [x] = [x'] \tag{2.43}$$

所以, 我们有 F^* 是一个乘群. 因而, F 是一个域. □

备注 2.4.1. 在这个域里, 我们有

$$[a] \neq 0,\ \text{但是}\, p[a] = [pa] = 0. \tag{2.44}$$

由此, 我们看出条件 2.36 在这一剩余类环 F (也是一个域) 里面不成立.

备注 2.4.2. 条件 2.36 不一定能成立的原因分析:

假定 R 是一个环, 那么 R 的元对于加法来说作成一个加群. 根据这个加群里的元的阶 (order of the element) 的定义 1.2.1:

- 如果一个元 a 的阶是无穷大, 那么, 对于任意 m, 都有 $ma \neq 0$. 那么, 条件 2.36 成立.;
- 如果一个元 a 的阶是有限的, 那么, 条件 2.36 不成立.
- 另外, 可以出现一个环里, 某一个非零元对于加法的阶是无限, 而另一个非零元对于加法的阶是有限的情况. 见例 2.4.2.

例子 2.4.2. 假定两个循环群 $G_1 = (b)$, $G_2 = (c)$, b 的阶无限, c 的阶为 n. G_1 和 G_2 都是交换群, 代数运算是加法, 运算符号表示为 $+$. 我们有:

$$G_1 = \{hb \mid \text{任意整数}\, h\},$$
$$G_2 = \{kc \mid \text{任意整数}\, k\}.$$

G_1 中有 $hb = 0 \iff h = 0$, 而在 G_2 中有 $kc = 0 \iff n \mid k$.

我们作一个集合

$$R = \{(hb, kc) | hb \in G_1,\ kc \in G_2\} \tag{2.45}$$

规定 R 的加法:

$$(h_1 b, k_1 c) + (h_2 b, k_2 c) = (h_1 b + h_2 b, k_1 c + k_2 c) \tag{2.46}$$

R 对于这个加法作成一个加群.
规定 R 的乘法:

$$(h_1 b, k_1 c)(h_2 b, k_2 c) = (0, 0). \tag{2.47}$$

显然, R 对于这个乘法来说是闭的. 这个乘法适合结合律

$$a(bc) = (ab)c = (0, 0)$$

而且分配律成立:

$$a(b + c) = ab + bc = (0, 0), \quad (b + c)a = ba + ca = (0, 0).$$

因此, 由环的定义 2.1.2, R 做成一个环.

这个环的非零元 $(b, 0)$ 对于加法的阶是无穷大的, 但是非零元 $(0, c)$ 对于加法的阶是 n.

备注 2.4.3. 在一个一般的环里, 条件 2.36 可能对于某一个元来说成立, 对于另一个元来说则不成立.

在一个没有零因子的环里, 情况就不一样了.

定理 2.4.1. 在一个没有零因子 (*no* zero divisor) 的环里 R 里所有的非零元对于加法来说的阶都是一样的.

证明. 考虑以下两种情况:

1. R 的每一个非零元的阶都是无限大: 这个定理是对的.
2. R 的某一个非零元 a 的阶是有限整数 n, 而 b 是 R 的另一个非零元, 假定 b 的阶是 m.

由环的定义, 我们可以得出:

$$\overbrace{(a+\ldots+a)}^{n} \cdot b = \overbrace{(ab+\ldots ab)}^{n} = a \cdot \overbrace{(b+\ldots+b)}^{n} \tag{2.48}$$

也就是说,

$$(na)b = n(ab) = a(nb) \tag{2.49}$$

那么, 由于 a 的阶是 n, 我们有 $na = 0$, 因此:

$$(na)b = a(nb) = 0 \tag{2.50}$$

由于 R 无零因子, 因为 $a \neq 0$, 因此可得 $nb = 0$. 也就是说,

$$b \text{ 的阶} \leq n = a \text{ 的阶} \tag{2.51}$$

同理, 非零元 b 的阶是 m, 对于非零元 a 而言, 我们有:

$$(mb)a = b(ma) = 0 \Rightarrow ma = 0 \tag{2.52}$$

因此, 我们有

$$a \text{ 的阶} \leq m = b \text{ 的阶} \tag{2.53}$$

综上所述, 我们得出:

$$a \text{ 的阶} = b \text{ 的阶} \tag{2.54}$$

□

定义 2.4.1. 一个无零因子环 R 的非零元的 (对加法而言) 相同的阶 (order of element) 叫做环 R 的 **特征 (Characteristic of a ring)**.

备注 2.4.4. 如果一个无零因子 (*no* zero divisor) 的环 R 的特征是无限大, 那么计算规则 2.36 在这个 R 里成立. 如果 R 的特征是有限整数, 那计算规则 2.36 则在这个 R 里不成立.

定理 2.4.2. 如果无零因子环 R 的特征是有限整数, 那么 n 是一个素数.

证明. 如果 n 不是素数, 那么有:

$$n = n_1 n_2,\ n \nmid n_1,\ n \nmid n_2. \tag{2.55}$$

对于 R 的非零元 a 来说,

$$n_1 a \neq 0,\ n_2 a \neq 0,\ \ (n_1 a)(n_2 a) = (n_1 n_2) a \cdot a = 0 \tag{2.56}$$

这与 R 没有零因子的假定冲突. 反证完毕. □

推论 2.4.1. 整环, 除环, 以及域的特征是无限大, 或是一个素数 p.

备注 2.4.5. 在一个特征是 p 的交换环里, 我们有

$$(a+b)^p = a^p + b^p \tag{2.57}$$

这是因为

$$(a+b)^p = a^p + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1}b + \ldots + \begin{pmatrix} p \\ p-1 \end{pmatrix} ab^{p-1} + b^p \tag{2.58}$$

而二项式的系数 $\begin{pmatrix} p \\ i \end{pmatrix}$ 是 p 的一个倍数:

$$\begin{pmatrix} p \\ i \end{pmatrix} = \frac{p!}{i!(p-i)!} \tag{2.59}$$

练习 2.4.1. 如果 F 是一个有 4 个元的域. 我们有:

1. F 的特征是 2;
2. F 中不等于 0 或者 1 的两个元都适合方程 $x^2 = x + 1$.

解答. 1. F 的特征是 F 非零元的 (加法运算) 的阶, 并且是一个素数. F 作为加群的阶是 4, 因此 F 的非零元的阶只能是 1, 2, 4 (因为 3 不能整除 F 的阶, 由定理 1.9.3, 3 不是 F 的元的阶). 而只有 2 是素数, 所以 F 的特征只能是 2.

2. 乘群 F^* 的阶是 3, 根据 1.9.1, 它是一个循环群 (a), 而 F^* 的元可写作 $F^* = \{1, a, a^2\}$.

   这样, $F = \{0, 1, a, a^2\}$. F 是一个加群, 它与 Klein 四元群同构:

$$B_4 = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

   而且有:

$$a + 1 = a^2, \quad a^2 + 1 = a = (a^2)^2. \tag{2.60}$$

   因此, F 的不等于 0 或者 1 的元 a 和 a^2 都适合方程 $x^2 = x + 1$.

练习 2.4.2. 假定 $[a]$ 是模 n 的一个剩余类. 证明, 如果 a 同 n 互素, 那么所有 $[a]$ 的数都同 n 互素.

证明. 假设任意 b 属于模 n 的剩余类 $[a]$, 那么

$$n \mid a - b \Rightarrow a - b = ng \Rightarrow a = b + ng, \quad g = 0, 1, 2, \ldots \tag{2.61}$$

如果 $(b, n) \neq 1$, 那么 b 和 n 有公因子 $m > 1$. m 整除 $b + ng$, 也就是说 m 整除 a, 那么 $(a, n) = m \neq 1$. 这与我们的假设 a 和 n 互素: $(a, n) = 1$, 相矛盾.

由此, 我们证明了 $[a]$ 中任意的 b 与 n 互素.

□

练习 2.4.3. 所有和 n 互素的模 n 的剩余类对于剩余类的乘法来说作成一个群. (和 n 互素的剩余类的个数用 ϕ 函数 $\phi(n)$ 来表示, 叫做 Euler's totient function). [3]

证明. 考虑:

$$G = \{\text{所有和 } n \text{ 互素的模 } n \text{ 的剩余类}\}. \tag{2.62}$$

我们使用群的定义 1.1.2:

1. 如果整数 a 和 b 都和 n 互素, 那么 ab 也和 n 互素. 因此有, 如果 $[a] \in G$, $[b] \in G$, 那么 $[a][b] \in G$. 也就是说, G 对于剩余类的乘法是闭的.

[3] Euler's totient function 见 https://en.wikipedia.org/wiki/Euler%27s_totient_function

2. 剩余类的乘法适合结合律.

3. 由于 $(1,n)=1$, 我们有 $[1]\in G$, 也就是说 G 有单位元 $[1]$.

4. 给定任意的 $[a]\in G$, 那么我们有 $(a,n)=1$.

   根据 (a,b) 的性质: 存在整数 x 和 y, 使得 $(a,b)=ax+by$. [4]

   因此, 我们有: 对于 a 和 n, 存在整数 s 和 t, 使

$$as+nt=(a,n)=1. \tag{2.63}$$

   于是, 我们有:

$$[a][s]+[n][t]=[1], \tag{2.64}$$

   因为 $[n]=0$, 所以我们有 $[a][s]=1$.

   同时由于 $as+nt=1$, 根据最大公因数 (s,n) 的定义: 给定另外的整数 a 和 t, $as+nt$ 是 (s,n) 的倍数. 也就是说 $as+nt=1$ 是 (s,n) 的倍数. 所以, 我们有 $(s,n)=1$.

   也就是说, $[s]\in G$. 而 $[s]$ 是 $[a]$ 的逆, 因此, 我们得出: G 的任何元 $[a]$ 在 G 中有逆.

综上所述, G 作成一个群. □

练习 2.4.4 (Fermat's little theorem.[5])**.** 如果 $(a,n)=1$, 那么

$$a^{\phi(n)}\equiv 1(n), \tag{2.65}$$

其中 Euler's totient function $\phi(n)$ 表示的是和 n 互素的剩余类的个数.

证明. 根据上面的练习 2.4.3, 我们知道其中的群的阶是 $\phi(n)$.

考虑 $[a]\in G$, 因此我们有

$$[a]^{\phi(n)}=[a^{\phi(n)}]=[1] \quad \Rightarrow \quad a^{\phi(n)}\equiv 1(n). \tag{2.66}$$

□

[4] Bézout's identity: Let a and b be integers or polynomials with greatest common divisor $d=gcd(a,b)$. Then there exist integers or polynomials x and y such that $ax+by=d=gcd(a,b)$. Moreover, the integers or polynomials of the form $az+bt$ are exactly the multiples of d. It is proved based on extended Euclidean algorithm. See https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity.

[5] See https://en.wikipedia.org/wiki/Fermat%27s_little_theorem.

2.5 子环, 环的同态 (Subring and Ring Homomorphism)

定义 2.5.1. 一个环 R 的一个子集 S 叫做 R 的一个 **子环 (subring)**, 如果: S 本身对于 R 的代数运算来说作成一个环.

一个除环 (division ring) R 的一个子集 S 叫做 R 的一个 **子除环 (subring of division ring)**, 如果: S 本身对于 R 的代数运算来说作成一个除环.

一个整环 (integral domain) R 的一个子集 S 叫做 R 的一个 **子整环 (subring of integral domain)**, 如果: S 本身对于 R 的代数运算来说作成一个整环.

一个域 (field) R 的一个子集 S 叫做 R 的一个 **子域 (subfield)**, 如果: S 本身对于 R 的代数运算来说作成一个域.

备注 2.5.1. 一个环 R 的一个子集 S 作成一个**子环**的条件是:

$$a,\, b \in S \Longrightarrow a - b \in S,\, ab \in S \tag{2.67}$$

备注 2.5.2. 一个除环的一个子集 S 作成一个**子除环**的条件是:

1. S 有一个非零元;
2. $$a, b \in S \Longrightarrow a - b \in S$$ $$a, b \in S, b \neq 0 \Longrightarrow ab^{-1} \in S$$

例子 2.5.1. R 是一个环. 那么存在 R 和 $\{0\}$ 是 R 的子环.

定义 2.5.2. 一个环 R 的可以和每一个元交换的元做成一个子环. 这个子环叫做 R 的 **中心 (center)**.

$$Z(R) = \{x \in R | xa = ax, \forall a \in R\} \tag{2.68}$$

备注 2.5.3. 一个环的中心 (center of a ring) 是一个交换子环 (commutative subring).

备注 2.5.4. 一个除环的中心 (center of division ring) 是一个交换除环, 也就是一个域 (field).

以下我们假定:

假设 2.5.1. 一个非空集合 $\overline{R}$, 有两个代数运算, 一个叫做加法, 一个叫做乘法.

由同态满射保持结合律, 交换律, 第一和第二分配律, 以及群的同态定理 1.4.1, 我们得出以下定理:

定理 2.5.1. 如果存在一个环 R 到假设 2.5.1中的 $\overline{R}$ 的满射, 使得 R 和 $\overline{R}$ 对于加法和乘法来说都是同态, 那么 $\overline{R}$ 也是一个环.

备注 2.5.5. 我们说两个环 R 和 $\overline{R}$ 同态 (同构), 意思是存在一个 R 到 $\overline{R}$ 的满射 (一一映射), 使得 R 和 $\overline{R}$ 对于两个环的加法和乘法来说都是同态 (同构).

定理 2.5.2. 假定 R 和 $\overline{R}$ 是两个环, 并且 R 和 $\overline{R}$ 同态. 那么,

- R 的零元的象是 $\overline{R}$ 的零元;
- R 的元 a 的负元 (additive inverse) 的象是 a 的象的负元 (additive inverse);
- 如果 R 是交换环, 那么 $\overline{R}$ 也是交换环;
- 如果 R 有单位元 (multiplicative identity) 1, 那么 $\overline{R}$ 有单位元 (multiplicative identity) $\overline{1}$, 而且 $\overline{1}$ 是 1 的象.

备注 2.5.6. 环的同态满射不一定能保持一个环有没有零因子 (zero divisor) 这一性质. 见下面的例子 2.5.2 和 2.5.3.

例子 2.5.2. R 是整数环 (ring of integers), $\overline{R}$ 是模 n 的剩余类环 (ring of residue classes modulo n/ring of integers modulo n), 那么有

$$\phi : a \to [a] \tag{2.69}$$

是 R 到 $\overline{R}$ 的一个同态满射 (epimorphism). 我们知道, R 是没有零因子的, 而如果 n 不是素数的时候, $\overline{R}$ 有零因子.

由此, 我们可以看出, R 没有零因子的时候, 和 R 同态的 $\overline{R}$ 可以有.

例子 2.5.3. 假定

$$R = \{\text{所有整数对}(a, b)\} \tag{2.70}$$

定义代数运算:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$$

这样, R 作成一个环. R 的零元是 $(0, 0)$. 根据

$$(a, 0)(0, b) = (0, 0) \tag{2.71}$$

我们得出, R 有零因子.

我们用 $\overline{R}$ 表示整数环 (ring of integers), 那么我们有

$$\phi : (a, b) \longrightarrow a \tag{2.72}$$

这样一个 R 到 $\overline{R}$ 的同态满射 (epimorphism).

注意到整数环 $\overline{R}$ 没有零因子. 因此, 我们得出, 当 R 有零因子的时候, 与 R 同态的 $\overline{R}$ 可以没有零因子.

当然, 如果 R 和 $\overline{R}$ 之间存在的是同构映射的话, 这两个环的代数性质就没有区别了.

定理 2.5.3. 假定 R 和 $\overline{R}$ 是两个环, 并且 $R \cong \overline{R}$. 那么

- 如果 R 是整环, $\overline{R}$ 也是整环;
- 如果 R 是除环, $\overline{R}$ 也是除环;
- 如果 R 是域, $\overline{R}$ 也是域.

有时候我们需要作一个环, 使得它包含一个给定的环. 在这种情况下, 下面的定理 2.5.4 很重要.

引理 2.5.1. 假定在集合 A 和 $\overline{A}$ 之间存在一个一一映射 (bijection) ϕ, 并且 A 有加法和乘法. 那么我们可以在 $\overline{A}$ 中规定加法和乘法, 使得 A 和 $\overline{A}$ 对于加法和乘法来说都同构 (isomorphic).

证明. 在给定的一一映射 (bijection) ϕ 之下, $x \in A$ 对应 $\overline{x} \in \overline{A}$. 我们规定

$$a + b = c \xrightarrow{\phi} \overline{a} + \overline{b} = \overline{c}$$
$$ab = d \xrightarrow{\phi} \overline{a}\overline{b} = \overline{d}$$

通过这样, 我们就规定了 $\overline{A}$ 的加法和乘法: 因为 $\overline{a}$ 和 $\overline{b}$ 有唯一的 a 和 b, 在 A 里有唯一的 c 和 d, 由一一映射有唯一的 $\overline{c}$ 和 $\overline{d}$.

由此可得, ϕ 是对于加法和乘法的从 A 到 $\overline{A}$ 的同构映射 (isomorphism). □

定理 2.5.4 (ring cut and paste theorem)**.** 假设 S 是环 R 的一个子环, S 在 R 里的补集 $S^c \subset R$ 和另一个环 $\overline{S}$ 没有共同元, 并且 $S \cong \overline{S}$. 那么存在一个和 R 同构的环 $\overline{R}$, 而且 $\overline{S}$ 是 $\overline{R}$ 的子环.

证明. 假定

$$S = \{a_S, b_S, \ldots\}$$
$$\overline{S} = \{\overline{a}_S, \overline{b}_S, \ldots\}$$

而且 S 和 $\overline{S}$ 的同构映射是:

$$\phi : x_S \xrightarrow{\cong} \overline{x}_S$$

R 的不属于 S 的元用 $a, b, \ldots$ 来表示. 那么, S 在 R 里的补集是:

$$S^c = \{a, b, \ldots\} \subset R.$$

这样我们根据 R 构造 $\overline{R}$:

$$R = S \cup S^c, \quad S \cap S^c = \emptyset$$
$$\overline{R} = \overline{S} \cup S^c, \quad \overline{S} \cap S^c = \emptyset.$$

规定一个法则:

$$\psi : \begin{cases} x_S \longrightarrow \overline{x}_S, & x_S \in S, \overline{x}_S \in \overline{S} \\ x \longrightarrow x, & x \in S^c \end{cases} \tag{2.73}$$

那么 ψ 是一个从 R 到 $\overline{R}$ 的满射 (surjective).

下面我们证明 ψ 是一个单射 (injective):

- 对于 R 的任意两个元, 如果它们都属于 S, 或者都属于 S 的补集, 那么它们在 ψ 中的象显然不相同.
- 如果这两个元一个属于 S, 另一个属于 S 的补集, 那么在 S 的元在 ψ 之下的象属于 $\overline{S}$, 而在 S 的补集的元在 ψ 之下的象属于 S 的补集. 根据定理的假定: S 在 R 里的补集和 $\overline{S}$ 没有共同元, 这两个象也不相同.
- 因此, ψ 是一个单射.

因此, 我们得出 ψ 是 R 和 $\overline{R}$ 之间的一一映射 (bijective).

由引理 2.5.1 得出, 我们可以通过规定 $\overline{R}$ 的加法和乘法, 使得

$$R \cong \overline{R}.$$

由 $\overline{R}$ 的构成方法, 我们知道 $\overline{S} \subseteq \overline{R}$. 而且, 我们知道 $\overline{S}$ 原有的加法和乘法做成一个环. 下面我们需要说明的是 $\overline{S}$ 是 $\overline{R}$ 的子环:

$\overline{S}$ 是 $\overline{R}$ 子环的意思是 $\overline{S}$ 对于 $\overline{R}$ 的代数运算来说作成一个环. 把 $\overline{R}$ 的加法用 $\mp$ 来表示, $\overline{S}$ 和 S 的加法用 $+$ 来表示. 假定任意两个元 $\overline{x}_S, \overline{y}_S \in \overline{S}$. 根据 ψ, 它们在 S 中的对应元是 x_S 和 y_S, 而且在 S 中有:

$$x_S + y_S = z_S. \tag{2.74}$$

由 $\overline{R}$ 的加法来看, 我们有:

$$\overline{x}_S \mp \overline{y}_S = \overline{z}_S \tag{2.75}$$

由 S 和 $\overline{S}$ 同构来说, 我们有:

$$\overline{x}_S + \overline{y}_S = \overline{z}_S \tag{2.76}$$

由此可以看出, $\overline{R}$ 上的加法 $\pm$ 和 $\overline{S}$ 上的加法 $+$ 在作用到 $\overline{S}$ 上面没有任何区别.

同理, 我们可得到 $\overline{R}$ 的乘法和 $\overline{S}$ 原来的乘法在作用到 $\overline{S}$ 上面也没有任何区别.

所以, 我们可以得出 $\overline{S}$ 是 $\overline{R}$ 的子环. □

练习 2.5.1. 证明: 一个环的中心是一个交换子环.

证明. 这个由环的中心可以看出:

$$Z(R) = \{x \in R | xy = yx, \forall y \in R\} \tag{2.77}$$

对于任意 $y \in R$ 成立, 同样对于任意 $y \in Z(R)$ 也成立. □

练习 2.5.2. 证明: 一个除环 (division ring) (见定义 2.3.1) 的中心是一个域.

证明. 一个除环 D 的中心 Z 是一个交换子环 (commutative).

根据除环定义 2.3.1, 除环 D 有乘法单位元 (multiplicative identity) $1 \in D$. 我们知道 $1y = y1$, $\forall y \in R$, 所以 $1 \in Z$.

根据除环定义 2.3.1, 对于任何非零元 $z \in Z \subset D$, 存在其对应的乘法逆元 (multiplicative inverse) $z^{-1} \in D$. 因为 $z \in Z$, 我们有

$$az = za, \quad \forall a \in D$$

因此可得:

$$z^{-1}azz^{-1} = z^{-1}zaz^{-1} \Rightarrow z^{-1}a = az^{-1}, \quad \forall a \in D$$

因此, 有 $z^{-1} \in Z$.

□

练习 2.5.3. 证明: 有理数域 (field of rational numbers) Q 是所有复数 $a+bi$ (a 和 b 是有理数 (rational numbers)) 作成的域 (field) $Q(i)$ 的唯一的真子域 (proper subfield).

$$Q(i) = \{a + bi \,|\, a, b \in Q\}.$$

这里的复数形式 $a + bi$ 可以称为 Gaussian rational number, $Q(i)$ 称为 Gaussian rational field.

证明. 首先, $Q(i)$ 是一个域, 而 Q 是 $Q(i)$ 的一个真子域 (proper subfield). 我们需要证明其唯一性:

假设 F 是 $Q(i)$ 的任一子域, 那么 F 至少包含一个非零元 $a \neq 0$, 而且包含其逆元 a^{-1}, 使得 $a^{-1}a = 1$. $Q(i)$ 的加法应用到 F 上, 那么有 $1+1 = 2$, $2^{-1}2 = 1$, ... 由此可以得出, F 包含一切整数和一切有理数. 所以,

$$Q \subset F \subset Q(i) \tag{2.78}$$

如果 $F \neq Q$, 那么至少存在一个元

$$a + bi \in F, \quad a, b \in Q, \text{ 而且} b \neq 0 \tag{2.79}$$

可以得出

$$a + bi - a = bi \in F, \quad b^{-1}bi = i \in F \tag{2.80}$$

所以, F 包含一切 $a + bi$. 也就是说 $F = Q(i)$.

因而, 我们得出 Q 是 $Q(i)$ 的唯一的真子域.

□

练习 2.5.4. 证明: $Q(i)$ 只有两个自同构映射 (automorphism).

证明. 假设 ϕ 是 $Q(i)$ 的一个自同构. 那么必然有

$$\phi(0) = 0, \quad \phi(1) = 1, \quad \phi(\frac{p}{q}) = \frac{p}{q} \tag{2.81}$$

其中, $\frac{p}{q}$ 为有理数.

考虑 i 的象 $\phi(i)$:

$$-1 = \phi(-1) = \phi(i^2) = [\phi(i)]^2 \Longrightarrow \phi(i) = \pm i. \tag{2.82}$$

因此, $Q(i)$ 的自同构只能是:

$$\phi_1 : a + bi \longrightarrow a + bi$$
$$\phi_2 : a + bi \longrightarrow a - bi$$

因此, $Q(i)$ 只有两个自同构.

□

练习 2.5.5. J_3 表示模 3 的剩余类所作成的集合. 找出加群 (additive group) J_3 的所有自同构映射 (automorphism); 再找出域 (field) J_3 的所有自同构映射 (automorphism).

解答. 假设 ϕ 是加群 $J_3 = \{[0], [1], [2]\}$ 的一个自同构. 那么, 一定有 $\phi([0]) = [0]$. 因此加群 J_3 的自同构只能是:

$$\phi_1 : [0] \to [0],\ [1] \to [1],\ [2] \to [2]$$
$$\phi_2 : [0] \to [0],\ [1] \to [2],\ [2] \to [1]$$

显然, ϕ_1 和 ϕ_2 都是加群 J_3 的自同构.

假设 ϕ 是域 J_3 的一个自同构那么一定有

$$\phi([0]) = [0],\ \phi([1]) = [1] \tag{2.83}$$

因而, 必然有 $\phi([2]) = [2]$. 显然, 域 J_3 只有 ϕ 一个自同构.

练习 2.5.6. R 是四元数除环. R 的子集 $S = \{(a, 0)|\forall a \in \mathbb{R}\}$. S 和实数域 $\overline{S}$ 同构. 考虑 $\overline{R}$ 是把 R 中 S 换成 $\overline{S}$ 后所得的集合. 那么 $R \cong \overline{R}$.

分别用 $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ 表示 $\overline{R}$ 中的元 $(i, 0)$, $(0, 1)$, $(0, i)$. 那么 $\overline{R}$ 的元可以写成

$$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}, \quad \forall a, b, c, d \in \mathbb{R} \tag{2.84}$$

也就是, 对于四元数除环的任意元 $(a + bi, c + di)$, 可以写成:

$$\begin{aligned}(a + bi, c + di) &= (a, 0) + (b, 0)(i, 0) + (c, 0)(0, 1) + (d, 0)(0, i)\\ &= a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}\end{aligned}$$

验证以下等式成立:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$
$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k},\ \mathbf{jk} = -\mathbf{kj} = \mathbf{i},\ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$$

解答. 从例子 2.3.3 可得, 四元数除环 R 的乘法有:

$$(\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1\alpha_2 - \beta_1\overline{\beta_2},\ \alpha_1\beta_2 + \beta_1\overline{\alpha_2})$$

因为 $R \cong \overline{R}$, 我们可以用 R 中的乘法对应 $\overline{R}$ 中的乘法. 也就是说,

$\mathbf{i}^2 = \mathbf{ii}, \quad \mathbf{i} \in \overline{R} \longrightarrow (i, 0) \in R$

$=(i, 0)(i, 0) = (i \cdot i - 0 \cdot \overline{0}, i \cdot 0,\ 0 \cdot \overline{i}) = (i \cdot i, 0) = (-1, 0), \quad (i, 0) \in R$

$= -1, \quad -1 \in \overline{R}.$

也就是说, 我们验证了 $\mathbf{i}^2 = -1$. 同理, 可以验证别的等式.

2.6 多项式环 (Polynomial Ring)

假定 R_0 是一个环. R 是 R_0 的子环 $R \subseteq R_0$. 并且我们假定 R_0 有乘法单位元 (multiplicative identity) $1 \in R_0$, 而且 $1 \in R$.[6]

[6]在一些教材里面, 例如, Algebra by Artin, polynomial ring 基于 commutative ring with multiplicative identity. 这一做法的便利之处在于确保了多项式环 $R[\alpha]$ 的成立, 见下面的定理 **??**.

假设 R_0 中的一个元 $\alpha \in R_0$. 那么, 对于 $a_i \in R$, $i = 0, 1, \ldots, n$, 我们有 R_0 上的元, 可以写成以下形式:

$$a_0\alpha^0 + a_1\alpha^1 + a_2\alpha^2 + \ldots + a_n\alpha^n = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n \in R_0$$

定义 2.6.1. 一个形式为

$$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n \in R_0 \quad (a_i \in R,\, n \geq 0,\, n \in \mathbb{Z}) \tag{2.85}$$

的 R_0 的元叫做 R 上的 $\alpha \in R_0$ 的一个 **多项式 (polynomial)**. $a_i \in R$ 叫做多项式的 **系数 (coefficient)**.

我们把所有这样的 R 上的 $\alpha \in R_0$ 的多项式作成一个集合, 表示为 $R[\alpha] \subseteq R_0$.

备注 2.6.1. 多项式里面的**项 (单项式) (monomial)** α^i 相互独立. 对于 $m < n$, 我们有

$$\begin{aligned} &a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_m\alpha^m \\ =&a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_m\alpha^m + 0\,\alpha^{m+1} + \ldots + 0\,\alpha^n. \end{aligned}$$

那么, 给定两个多项式

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n \\ g(\alpha) &= b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_m\alpha^m, \end{aligned}$$

我们有:

$$f(\alpha) = g(\alpha) \iff a_i = b_i, \quad i = 0, 1, 2, \ldots$$

备注 2.6.2. $R[\alpha]$ 的加法和乘法如下:

$$\begin{aligned} (a_0 + \ldots + a_n\alpha^n) + (b_0 + \ldots + b_n\alpha^n) &= (a_0 + b_0) + \ldots (a_n + b_n)\alpha^n \\ (a_0 + \ldots + a_m\alpha^m)(b_0 + \ldots + b_n\alpha^n) &= c_0 + \ldots c_{m+n}\alpha^{m+n} \end{aligned}$$

这里

$$c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0 = \sum_{i+j=k} a_ib_j \tag{2.86}$$

$R[\alpha]$ 对于加法和乘法都是闭的. 同时, 我们有

$$-(a_0 + \ldots + a_n\alpha^n) = -a_0 - \ldots - a_n\alpha^n \in R[\alpha] \tag{2.87}$$

所以 $R[\alpha]$ 是一个环, 而且 R_0 **中包含** R **和** $\alpha \in R_0$ **的最小子环.**

定义 2.6.2. $R[\alpha]$ 叫做 R 上的 $\alpha \in R_0$ 的**多项式环**.

对于任意的 α, 可能存在 $1, \alpha, \alpha^2, \ldots, \alpha^n$ 线性相关. 也就是说, 存在非零的 $a_i \neq 0$, 但是有

$$a_0 + \ldots + a_n\alpha^n = 0$$

例如, 当 $\alpha \in R \subseteq R_0$ (在多项式定义里我们规定的是 $\alpha \in R_0$) 的时候, 有 $a_0 = \alpha$, $a_1 = -1$, 那么

$$a_0 + a_1\alpha = \alpha - \alpha = 0.$$

定义 2.6.3. $x \in R_0$ 叫做 R 上的一个 **未定元 (indeterminate)**, 假如: 在 R 里不存在非零元 $0 \neq a_i \in R$, 使得

$$a_0 + \ldots + a_n x^n = 0.$$

或者说 $\{1, x, x^2, \ldots, x^n\}$ 在 R 中线性无关 (linearly independent).

下面我们讨论未定元的多项式. 我们接受以下的前提条件: R 的一个未定元 $x \in R_0$ 的 **一元多项式 (polynomial in** 1 **indeterminate over** R**)**, 可以唯一的表示为

$$a_0 + \ldots + a_n x^n, \quad (a_i \in R).$$

定义 2.6.4. 给定环 R 上的一个一元多项式 (polynomial in 1 indeterminate over R)

$$f(x) = a_0 + \ldots + a_n x^n, \quad (a_i \in R),\ a_n \neq 0,$$

非负整数 n 叫做这个多项式的 **次数 (degree)**, 写为 $deg(f(x)) = n$. 最高项 x^n 对应的系数 $a_n \neq 0$ 称为 **最高项系数 (leading coefficient)**.

多项式的次数是对于非零多项式 (nonzero polynomial) 而言. 多项式次数为零的多项式 (polynomial of degree zero) 称为 **常数多项式 (constant polynomial)**. 常数多项式里面的一种特殊类型: **零多项式 (zero polynomial)**, 没有次数 (degree of zero polynomial is not defined).

对于给定的 R_0 而言, 未必有 R 上的未定元.

例子 2.6.1. R 是整数环, $R_0 \supset R$ 是包含所有 $a + bi$ (a, b 是整数) 的整环. 那么, 对于 $\forall x = a + bi \in R_0$, 都有:

$$(a^2 + b^2) + (-2a)x + x^2 = (a^2 + b^2) + (-2a^2 - 2abi) + (a^2 - b^2 + 2abi) = 0.$$

也就是说, 对于任意的 $x \in R_0$, 都有 $\{1, x, x^2\}$ 线性相关. 那么, R_0 中的任意元都不是 R 的未定元.

一个重要定理如下:

定理 2.6.1. 给定一个有乘法单位元 (multiplicative identity) 的交换环 (commutative ring) R, 一定有 R 上的未定元 (indeterminate) x 的存在, 因此有 R 上的多项式环 $R[x]$ 的存在.

证明. 证明分三步:

1. 用 R 作一个环 $\overline{P}$:

$$\overline{P} = \{(a_0, a_1, a_2, \ldots) | a_i \in R, \neg(\forall a_i \neq 0), \text{not all } a_i \text{ are zero}\}$$

规定 $\overline{P}$ 中两元素相等的条件为:

$$a_i = b_i, i = 0, 1, 2, \ldots \Longrightarrow (a_0, a_1, a_2, \ldots) = (b_0, b_1, b_2, \ldots)$$

规定 $\overline{P}$ 中的加法:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

$\overline{P}$ 对于这样的加法做成一个 (交换) 加群 (additive group/Abelian group), 这个加群的零元是 $(0, 0, \ldots)$.

规定 $\overline{P}$ 中的乘法:

$$(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

其中

$$c_k = \sum_{i+j=k} a_i b_j, \qquad (k = 0, 1, 2, \ldots)$$

显然, 这个也是 $\overline{P}$ 的代数运算, 而且这个乘法适合交换律 (commutative law).

我们下面验证 $\overline{P}$ 适合结合律 (associative law) 和分配律 (distributive law):

- 结合律 (associative law):

$$\begin{aligned}
&\big[(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots)\big](c_0, c_1, c_2, \ldots) \\
=&(a_0, a_1, a_2, \ldots)\big[(b_0, b_1, b_2, \ldots)(c_0, c_1, c_2, \ldots)\big] \\
=&(e_0, e_1, e_2, \ldots)
\end{aligned}$$

  其中

$$e_n = \sum_{m+k=n} \sum_{i+j=m} a_i b_j c_k = \sum_{i+j+k=n} a_i b_j c_k.$$

- 分配律 (distributive law):

$$\begin{aligned}
&(a_0, a_1, a_2, \ldots)\big[(b_0, b_1, b_2, \ldots) + (c_0, c_1, c_2, \ldots)\big] \\
=&(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) + (a_0, a_1, a_2, \ldots)(c_0, c_1, c_2, \ldots) \\
=&(d_0, d_1, d_2, \ldots)
\end{aligned}$$

  其中

$$d_k = \sum_{i+j=k} a_i (b_j + c_j)$$

因此, 根据环的定义 2.1.2 以及 $\overline{P}$ 的元素都适用于加法和乘法的交换律 (commutative law), 我们得出 $\overline{P}$ 作成一个交换环 (commutative ring).

$\overline{P}$ 有:

$$(a_0, 0, 0, \ldots)(b_0, b_1, \ldots) = (a_0 b_0, a_0 b_1, \ldots) \tag{2.88}$$

因而,

$$(1, 0, 0, \ldots)(b_0, b_1, \ldots) = (b_0, b_1, \ldots)$$

所以, $\overline{P}$ 的乘法单位元 (multiplicative identity) 是 $(1, 0, 0, \ldots)$.

2. 用 $\overline{P}$ 构造一个包含 R 的环 P.

首先考虑

$$\overline{R} = \{(a, 0, 0, \ldots) | a \in R\}$$

规定 $\overline{R}$ 的乘法和加法如下:

$$(a, 0, 0, \ldots)(b, 0, 0, \ldots) = (ab, 0, 0, \ldots)$$

$$(a, 0, 0, \ldots) + (b, 0, 0, \ldots) = (a + b, 0, 0, \ldots)$$

那么, $\overline{R}$ 是 $\overline{P}$ 的一个子环, 而且

$$\phi : \overline{R} \longleftrightarrow R, \quad \phi(a, 0, 0, \ldots) = a$$

是 $\overline{R}$ 和 R 之间的一个同构映射 (isomorphism), 也就是有 $R \cong \overline{R}$.

用 $\overline{R}^c$ 表示 $\overline{R}$ 在 $\overline{P}$ 上的补集. 因为 R 和 $\overline{P}$ 没有共同元, 根据定理 2.5.4, 可以用 R 代替 $\overline{R} \subset \overline{P}$, 从而构造一个包含 R 的环 $P = R \cup \overline{R}^c$, $R \cap \overline{R}^c = \emptyset$. 而且, $P \cong \overline{P}$.

由于 $\overline{P}$ 是有乘法单位元的交换环, 根据 $P \cong \overline{P}$, P 也是有乘法单位元的交换环, 而且 P 的乘法单位元也是 R 的乘法单位元 1.

3. 证明 P 包含 R 上的未定元:

我们规定

$$x = (0, 1, 0, 0, \ldots)$$

而且

$$x^k = (\overbrace{0, \ldots, 0}^{k}, 1, 0, \ldots). \tag{2.89}$$

首先考察这个等式 2.89 是否成立:

- 这个等式 2.89 在 $k=1$ 的时候成立.
- 假定 $k-1$ 的时候等式 2.89 也成立, 那么:

$$\begin{aligned} x^k &= (0,1,0,\ldots)(\overbrace{0,\ldots,0}^{k-1},1,0,\ldots) \\ &= \Big(\sum_{i+j=0} a_i b_j, \sum_{i+j=1} a_i b_j, \sum_{i+j=2} a_i b_j, \ldots\Big) \\ &= (\overbrace{0,0,\ldots,0}^{k},1,0,\ldots). \end{aligned}$$

上述最后的一个等号是因为只有 $a_1 = 1$ 和 $b_{k-1} = 1$, 而其他 $a_i = 0$, $b_j = 0$, 所以乘法的运算结果只有一个非零元:

$$\sum_{i+j=k} a_i b_j = a_1 b_{k-1} = 1 \times 1 = 1 \neq 0.$$

假定在 P 里, 有

$$a_0 + a_1 x + \ldots + x_n x^n = 0 \quad (a_i \in R)$$

那么在与 P 同构的 $\overline{P}$ 里, 有

$$\begin{aligned} &(a_0,0,\ldots) + (a_1,0,\ldots)x + \ldots (a_n,0,\ldots)x^n \\ &= (a_0,0,\ldots) + (a_1,0,\ldots)(0,1,0,\ldots) + (a_2,0,\ldots)(0,0,1,0,\ldots) + \ldots \\ &= (0,0,\ldots) \\ \Longrightarrow &(a_0,a_1,a_2,\ldots,a_n,0,\ldots) = (0,0,\ldots) \end{aligned}$$

因而,

$$a_0 = a_1 = a_2 = \ldots = a_n = 0.$$

也就是说, x 是 R 上的未定元.

□

从一元多项式 (polynomial in 1 indeterminate over R) 推广到多元多项式 (polynomial in n indeterminates over R): 从 R_0 中选出 n 个元 x_1, x_2, …, x_n, 我们作 R 在 x_1 上的多项式环 $R[x_1]$, 然后作 $R[x_1]$ 上的 x_2 的多项式环 $R[x_1][x_2]$. 如此类推, 我们得出多项式环 $R[x_1][x_2]\ldots[x_n]$. 具体而言, 我们有以下定义:

定义 2.6.5. 一个可以写成 2.90 的形式的元叫做 R 上的 x_1, x_2, ..., x_n 的一个 **多项式**. $a_{i_1\,i_2\,\ldots\,i_n}$ 叫做多项式的 **系数**.

这一多项式环的元可以写作:

$$y = \sum_{i_1\,i_2\,\ldots\,i_n} a_{i_1\,i_2\,\ldots\,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \in R[x_1][x_2]\ldots[x_n]; \tag{2.90}$$

$$a_{i_1\,i_2\,\ldots\,i_n} \in R, \quad \neg(\forall a_{i_1\,i_2\,\ldots\,i_n} = 0), \text{ not all } a_{i_1\,i_2\,\ldots\,i_n} \text{ are zero.}$$

环 $R[x_1][x_2]\ldots[x_n]$ 叫做 R **上的** x_1**,** x_2**,** ... **的多项式环**, 可以用符号 $\mathbf{R[x_1, x_2, \ldots, x_n]}$ 表示.

$R[x_1, x_2, \ldots, x_n]$ 的加法和乘法如下:

$$\sum_{i_1\,i_2\,\ldots\,i_n} a_{i_1\,i_2\,\ldots\,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} + \sum_{i_1\,i_2\,\ldots\,i_n} b_{i_1\,i_2\,\ldots\,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$
$$= \sum_{i_1\,i_2\,\ldots\,i_n} (a_{i_1\,i_2\,\ldots\,i_n} + b_{i_1\,i_2\,\ldots\,i_n}) x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

$$\Big(\sum_{i_1\,i_2\,\ldots\,i_n} a_{i_1\,i_2\,\ldots\,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}\Big)\Big(\sum_{j_1\,j_2\,\ldots\,j_n} b_{j_1\,j_2\,\ldots\,j_n} x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}\Big)$$
$$= \sum_{k_1\,k_2\,\ldots\,k_n} c_{k_1\,k_2\,\ldots\,k_n} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$$

这里

$$c_{k_1\,k_2\,\ldots\,k_n} = \sum_{\substack{i_1 + j_1 = k_1,\\ i_2 + j_2 = k_2,\\ \ldots\\ i_n + j_n = k_n}} a_{i_1\,i_2\,\ldots\,i_n} b_{j_1\,j_2\,\ldots\,j_n}$$

类似的, 我们有

定义 2.6.6. R_0 的 n 个元 x_1, x_2, ..., x_n 叫做 R 上的 **无关未定元 (indeterminate)**, 如果: 除非所有系数都为零, 否则不存在一个 R 上的 x_1, x_2, ..., x_n 的多项式为零.

定理 2.6.2. 给定一个有单位元的交换环 (commutative ring with multiplicative identity) R 和一个正整数 n, 一定存在 R 上的无关未定元 (indeterminate) x_1, x_2, ..., x_n, 因此也就存在有 R 上的多项式环 $R[x_1, x_2, \ldots, x_n]$.

证明. 用归纳法:

1. 根据定理 2.6.1, x_1 是 R 的无关未定元.

2. 假设 x_1, x_2, ..., x_{n-1} 是 R 上的无关未定元. 那么有

$$\sum_{i_1\, i_2 \ldots i_n} a_{i_1\, i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} = 0 \tag{2.91}$$
$$\Rightarrow \sum_{i_1\, i_2 \ldots i_n} \left(a_{i_1\, i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_{n-1}^{i_{n-1}}\right) x_n^{i_n} = 0$$
$$\Rightarrow \sum_{i_n} \Big(\sum_{i_1\, i_2 \ldots i_{n-1}} a_{i_1\, i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_{n-1}^{i_{n-1}} \Big) x_n^{i_n} = 0$$

   因为 x_n 是 $R[x_1, x_2, \ldots, x_{n-1}]$ 上的未定元, 如果 (2.91) 成立, 那么根据上面的推导, 一定有

$$\sum_{i_1\, i_2 \ldots i_{n-1}} a_{i_1\, i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_{n-1}^{i_{n-1}} = 0, \quad i_n = 0, 1, \ldots$$

   由于我们已经假设 x_1, x_2, ..., x_{n-1} 是 R 上的无关未定元, 因此, 我们得出所有的多项式的系数为零:

$$a_{i_1\, i_2 \ldots i_n} = 0 \tag{2.92}$$

   从而, 我们得出 x_1, x_2, ..., x_{n-1}, x_n 是 R 上的无关未定元.

□

n 个无关未定元的多项式简称为 n **元多项式 (polynomial in n indeterminates (over R))**.

定理 2.6.3 (Substitution Principle). 假定 $R[x_1, x_2, \ldots, x_n]$ 和 $R[a_1, a_2, \ldots, a_n]$ 都是有单位元的交换环 (commutative ring with multiplicative identity) R 上的多项式环, x_1, x_2, ..., x_n 是 R 上的无关未定元 (indeterminates), a_1, a_2, ..., a_n 是 R 上的任意元. 那么:

$R[x_1, x_2, \ldots, x_n]$ 与 $R[a_1, a_2, \ldots, a_n]$ 同态 (存在同态满射 (epimorphism))

证明. 我们用 $f(x_1, \ldots, x_n)$ 表示 $R[x_1, x_2, \ldots, x_n]$ 的元, $f(a_1, \ldots, a_n)$ 表示 $R[a_1, a_2, \ldots, a_n]$ 的元. 那么, 考虑以下的映射:

$$\phi : f(x_1, \ldots, x_n) \mapsto f(a_1, \ldots, a_n)$$

这是一个 $R[x_1, x_2, \ldots, x_n]$ 到 $R[a_1, a_2, \ldots, a_n]$ 的满射 (epimorphism): 因为 x_1, x_2, ..., x_n 是 R 上的无关未定元, 因此任何元 $y \in R[x_1, x_2, \ldots, x_n]$ 只能有唯一对应的多项式 $f(x_1, \ldots, x_n)$. 按照我们规定的 ϕ, y 只有一个象 $f(a_1, \ldots, a_n)$. 因此, ϕ 这个映射是存在的. 另一方面, 显然, 这个映射是一个满射 (ϕ 包括了所有在多项式环 $R[a_1, a_2, \ldots, a_n]$ 的元 $f(a_1, \ldots, a_n)$).

考虑到 $R[x_1, x_2, \ldots, x_n]$ 和 $R[a_1, a_2, \ldots, a_n]$ 中两个多项式的加法和乘法都适用同一规律, 因此这个映射 ϕ 是同态映射.

□

备注 2.6.3. 定理 2.6.3 说明了多项式环 $R[x_1, x_2, \ldots, x_n]$ 中若干个元通过加法和乘法得出的关系, 那么用一个包含 R 的有单位元的交换环 R_0 中任意 n 个元素 a_1, a_2, ..., a_n 去代替未定元 x_1, x_2, ..., x_n , 这些关系仍然存在. 这也就是说明了 (在多项式环 $R[x_1, x_2, \ldots, x_n]$ 中的) 多项式存在代入 (substitution) 的可能.

练习 2.6.1. 假定 R 是一个整环 (integral domain), 那么 R 上的一元多项式环 $R[x]$ 也是一个整环 (integral domain).

证明. 根据定义 2.2.6, 整环 R 是一个有乘法单位元 (multiplicative identity) 的交换环 (commutative ring). 因而, R 上的一元多项式环 $R[x]$ 也是一个有单位元的交换环. 要证明 $R[x]$ 是整环, 只要证明 $R[x]$ 没有零因子 (has *no* zero divisor):

假设 $f(x), g(x) \in R[x]$. $f(x) \neq 0$, $g(x) \neq 0$. 那么 $f(x)$ 和 $g(x)$ 可以写成以下形式:

$$f(x) = a_0 + a_1 x + \dots a_m x^m \quad (a_i \in R)$$
$$g(x) = b_0 + b_1 x + \dots b_n x^n \quad (b_i \in R)$$

至少有 $a_m \neq 0$, $b_n \neq 0$. 考虑

$$f(x)g(x) = c_0 + c_1 x + \dots a_m b_n x^{m+n}$$

因为 $a_m \in R$, $b_n \in R$, 而 R 没有零因子, 所以 $a_m b_n \neq 0$. 因而

$$f(x)g(x) \neq 0$$

所以我们得出 $R[x]$ 没有零因子. 从而, $R[x]$ 是一个整环.

□

练习 2.6.2. 假定 R 是模 7 的剩余类环. 在 $R[x]$ 里计算乘积

$$([3]x^3 + [5]x - [4])([4]x^2 - x + [3])$$

计算如下:

$$\begin{aligned}
&([3]x^3 + [5]x - [4])([4]x^2 - x + [3]) \\
=&[12]x^5 - [3]x^4 + [9]x^3 + [20]x^3 - [5]x^2 + [15]x - [16]x^2 + [4]x - [12] \\
=&[5]x^5 - [3]x^4 + [2]x^3 + [6]x^3 - [5]x^2 + [1]x - [2]x^2 + [4]x - [5] \\
=&[5]x^5 - [3]x^4 + [8]x^3 - [7]x^2 + [5]x - [5] \\
=&[5]x^5 - [3]x^4 + [1]x^3 - [0]x^2 + [5]x - [5] \\
=&[5]x^5 - [3]x^4 + x^3 + [5]x - [5]
\end{aligned}$$

练习 2.6.3. 证明:

1. $R[x_1, x_2] = R[x_2, x_1]$.
2. 如果 x_1, x_2, …, x_n 是 R 上的无关未定元, 那么每一个 x_i 都是 R 上的未定元.

证明. 证明:

1. 由 $R[x_1, x_2]$ 的定义, 以及 $x_1, x_2 \in R_0$ 而 R_0 是有单位元的交换环, 我们有 $x_1 x_2 = x_2 x_1$.

   假设 $f(x_1, x_2) \in R[x_1, x_2]$, 那么

   $$\begin{aligned} f(x_1, x_2) &= \sum_{i_1 i_2} a_{i_1 i_2} x_1^{i_1} x_2^{i_2} \\ &= \sum_{i_1 i_2} a_{i_1 i_2} x_2^{i_2} x_1^{i_1} \in R[x_2, x_1] \end{aligned}$$

   所以有: $R[x_1, x_2] \subseteq R[x_2, x_1]$.

   同理可得 $R[x_2, x_1] \subseteq R[x_1, x_2]$.

   结合起来, 得出 $R[x_1, x_2] = R[x_2, x_1]$.

2. 用反证法: 选择 x_1 不是 R 上的未定元. 那么有不完全为零的元 a_0, a_1, ..., $a_k \in R$, 使得

   $$a_0 + a_1 x_1 + \ldots + a_k x_1^k = 0 \tag{2.93}$$

   这个式子可以改写成

   $$a_0 + a_1 x_1 x_2^0 \ldots x_n^0 + \cdots + a_k x_1^k x_2^0 \ldots x_n^0 = 0 \tag{2.94}$$

   这和题目假设 x_1, x_2, ..., x_n 是 R 上的无关未定元矛盾.

   因而, 我们得出 x_1 是 R 上的未定元.

□

练习 2.6.4. 证明:

1. 如果 x_1, x_2, ..., x_n 和 y_1, y_2, ..., y_n 是 R 上的两组无关未定元, 那么

   $$R[x_1, x_2, \ldots, x_n] \cong R[y_1, y_2, \ldots, y_n] \tag{2.95}$$

2. R 上的一元多项式环 $R[x]$ 和它的一个真子环 (proper subring) 同构 (isomorphism).

证明. 1. 规定对于任意元 $f(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$, 有以下映射:

$$\phi : f(x_1, x_2, \ldots, x_n) \mapsto f(y_1, y_2, \ldots, y_n) \in R[y_1, y_2, \ldots, y_n]$$

首先, $R[x_1, x_2, \ldots, x_n]$ 里面的每一个元只能有唯一的方法写成 R 上的多项式 $f(x_1, x_2, \ldots, x_n)$, 所以 ϕ 这一映射成立.

同样, 由于 $R[y_1, y_2, \ldots, y_n]$ 里面的每一个元只能有唯一的方法写成 R 上的多项式 $f(y_1, y_2, \ldots, y_n)$, 所以, ϕ 是一个单射.

而且, 显然 ϕ 是满射. 因此, ϕ 是一个同构映射.

2. x^2 显然也是 R 上的一个未定元. 由上面的证明, 我们有

$$R[x^2] \cong R[x].$$

但是 $x \notin R[x^2]$, 因而 $R[x^2] \subset R[x]$. 所以, $R[x^2]$ 是 $R[x]$ 的一个真子集 (proper subset).

□

2.7 理想 (Ideal Subring)

我们讨论一种重要的子环, 叫理想子环 (ideal subring, or ideal in short). 这种子环在环论里的地位类似于不变子群 (normal subgroup) 在群论的地位.

定义 2.7.1. 环 R 的一个非空子集 I 叫做一个**理想子环 (ideal subring)**, 简称 **理想 (ideal)**, 假如:

1. $a, b \in I \Longrightarrow a - b \in I$;
2. $a \in I, r \in R \Longrightarrow ra, ar \in I$.

一个理想 (ideal) 一定是一个子环 (subring). 考虑定义 2.7.1 中的条件 2 不仅要求 I 的两个元的乘积在 I 里面, 而且还进一步要求, I 的任意元和 R 的任意元的乘积都必须要在 I 里. 因此, 理想适合的条件比一般子环要强一点.

我们考虑的第一个问题: 一个环是不是一定有理想? 答案是肯定的. 因为一个环 R 至少有两个理想:

1. 只有 R 的零元的集合 $\{0\}$, 这个理想叫做 R 的 **零理想 (zero ideal)**.

2. R 自己, 这个理想叫做 R 的 **单位理想 (unit ideal)**.

备注 2.7.1. 除环 (division ring) 除了零理想 (zero ideal) 和单位理想 (unit ideal) 之外没有别的理想.

定理 2.7.1. 一个除环 (division ring) R 只有两个理想, 那就是零理想 (zero ideal) 和单位理想 (unit ideal).

证明. 假设 I 是 R 的一个理想 (子环), 并且 I 不是零理想. 那么存在非零元 $a \in I$. 因为 R 是除环, 根据除环的定义 2.3.1, a 有乘法逆元 (multiplicative inverse) $a^{-1} \in R$. 那么由理想的定义 2.7.1 中的条件 2, 我们得出 $a^{-1}a = 1 \in I$. 因而, R 的任意元 $b = b \cdot 1 \in I$. 也就是说, $I = R$. □

备注 2.7.2. 由上述定理 2.7.1, 理想这个概念对于除环或者域 (交换除环) 没有多大意义.

备注 2.7.3. 定理的 2.7.1 的逆定理不成立. 考虑在一个有理数域 F 上的 2×2 的矩阵环 (matrix ring) $M_2(F)$. 根据例子 2.2.1, $M_2(F)$ 是一个有乘法单位元 (multiplicative identity) 的非交换环 (non-commutative ring). 在后面的例子 2.9.4, 我们发现:

- $M_2(F)$ 不是除环.
- $M_2(F)$ 只有零理想 (zero ideal) 和单位理想 (unit ideal).

一般来说, 一个环会有零理想 (zero ideal) 和单位理想 (unit ideal) 之外的其他理想.

例子 2.7.1. 考虑整数环 (ring of integers) R. (根据 2.2.9, 整数环是一个整环 (integral domain)) 那么一个固定整数 $n \neq 0$ 的所有倍数 rn, $r \in R$ 做成一个理想 (ideal).

例子 2.7.2. 考虑一个环 R 上的一元多项式环 (ring of polynomials in 1 indeterminate over R) $R[x]$. 那么, 所有没有常数的多项式

$$a_1x + a_2x^2 + \ldots + a_nx^n, \quad n \geq 1$$

作成 $R[x]$ 的一个理想 (ideal).

给定一个环 R, 我们可以有以下方法作出一些 R 的理想: 取任意元 $a \in R$. 利用 a 作一个集合:

$$I = \left\{(x_1 a y_1 + \ldots + x_m a y_m) + sa + at + na | \forall x_i, y_i, s, t \in R, \, n \text{ 是整数}\right\} \tag{2.96}$$

这个集合 I 是 R 的一个理想:

- 两个这样形式的元相减还是得出这样形式的元;
- 用 R 的一个元 r 左乘 I 中的任意一个元可得出这样形式的元:

$$\begin{aligned} &(rx_1 a y_1 + \ldots + rx_m a y_m) + rsa + rat + nra \\ =&[(rx_1)a y_1 + \ldots + (rx_m)a y_m + rat] + (rs + nr)a \\ =&[(rx_1)a y_1 + \ldots + (rx_m)a y_m + rat] + (rs + nr)a + a\,0 + 0a \end{aligned}$$

  同理, 从 r 右乘 I 的元也会得到这样形式的元.

- 这样构造出来的理想显然是包含 a 的最小的理想.

定义 2.7.2. 形式为 2.96 的 I 叫做有元 a 生成的 **主理想 (principle ideal generated by a)**, 用符号 (a) 表示.

以下我们考虑最多的理想就是主理想.

备注 2.7.4. 一个主理想 (a) 的元的形式可以作进一步简化:

1. R 是交换环 (commutative ring): (a) 的元可以写成:

$$ra + na, \quad r \in R, n \in \mathbb{Z}$$

2. R 有单位元 (has multiplicative identity): (a) 的元可以写成:

$$\sum x_i a y_i, \quad x_i, \, y_i \in R$$

   因为这时候有

$$sa = sa1, \, at = 1at, \, na = (n1)a1$$

3. R 是有单位元的交换环 (commutative ring with multiplicative identity [7]): (a) 的元可以写成:

$$ra, \quad r \in R$$

例 2.7.1 说明的就是由 n 生成的主理想 (principle ideal) (n).

主理想 (principle ideal) 的概念容易推广.

定义 2.7.3. 给定环 R 的 m 个元 $a_1, a_2, \ldots, a_m \in R$. 集合

$$I = \{s_1 + s_2 + \cdots + s_m \,|\, s_i \in (a_i),\ i = 1, 2, \ldots, m\} \tag{2.97}$$

称为 **由** $a_1, a_2, \ldots, a_m$ **生成的理想 (ideal generated by** $a_1, a_2, \ldots, a_m$**)**, 表示为符号 $(a_1, a_2, \ldots, a_m)$.

备注 2.7.5. (2.97) 定义的集合是 R 的一个理想:

- 任意的两个元 $a, a' \in I$,

$$\begin{aligned} a &= s_1 + s_2 + \ldots + s_m \quad (s_i \in (a_i)) \\ a' &= s_1' + s_2' + \ldots + s_m' \quad (s_i' \in (a_i)) \end{aligned}$$

那么, 由于 $s_i - s_i' \in (a_i)$, 所以有

$$a - a' = (s_1 - s_1') + (s_2 - s_2') + \ldots + (s_m - s_m') \in I$$

- 对于 R 的一个任意元 r 来说, $rs_i, s_i r \in (a_i)$, 所以有

$$\begin{aligned} ra &= rs_1 + rs_2 + \ldots + rs_m \in I \\ ar &= s_1 r + s_2 r + \ldots + s_m r \in I. \end{aligned}$$

备注 2.7.6. I 显然是包含 $a_1, a_2, \ldots, a_m$ 的最小理想.

[7] One example: Recall Theorem 2.6.1, the prerequisite of polynomial ring $R[x]$ over R with indeterminate x is that R is commutative ring with multiplicative identity.

例子 2.7.3. 假定 $R[x]$ 是整数环 R 上的一元多项式环. 考虑 $R[x]$ 的理想 $(2, x)$.

因为 R 是整数环 (ring of integers), 根据 2.2.9, R 是整环 (integral domain), 根据练习 2.6.1, 那么 $R[x]$ 也是整环, 因而是有单位元的交换环. 因此, 由 2.7.4 中的 3, $(2, x)$ 可以写成

$$(2, x) = \{2p_1(x) + xp_2(x), \quad p_1(x), p_2(x) \in R[x]\} \tag{2.98}$$

或者说,

$$(2, x) = \{2a_0 + a_1x + \ldots + a_nx^n, \quad a_i \in R, n \geq 0\} \tag{2.99}$$

备注 2.7.7. $(2, x)$ 不是一个主理想.

证明. 用反证法. 假定 $(2, x)$ 是一个主理想, 可以写成 $(2, x) = (p(x))$. 那么 $2 \in (p(x))$, $x \in (p(x))$, 所以有

$$2 = q(x)p(x), \quad x = h(x)p(x).$$

由于 $2 = q(x)p(x)$, 我们可以得出 $p(x)$ 和 $q(x)$ 一定是常数, 假设 $p(x)$ 的常数为 a, 也就是

$$2 = q(x)p(x) \Longrightarrow p(x) = a$$

所以有

$$x = h(x)p(x) = h(x)a = ah(x)$$

假定 $h(x)$ 的形式为

$$h(x) = c_0 + c_1x + \ldots c_kx^k$$

那么,

$$\begin{aligned} & x = ah(x) = ac_0 + ac_1x + \ldots c_kx^k \\ \Longrightarrow & ac_1 = 1, \quad \text{implicitly by linearly independence of } 1, x, x^2, \ldots \\ \Longrightarrow & a = \pm 1 \quad \text{by } a, c_1 \in R, \text{ the ring of integers;} \\ \Longrightarrow & p(x) = a = \pm 1 \in (2, x). \end{aligned}$$

但是 ± 1 都不能写成 $2a_0 + a_1x + \ldots + a_nx^n$ 这样的形式, 也就是说 $\pm 1 \notin (2, x)$. 我们得出矛盾, 从而证明了 $(2, x)$ 不是一个主理想. □

练习 2.7.1. R 是偶数环. 证明: 所有整数 $4r$, $r \in R$ 是 R 的一个理想 I. 说明是否有 $I = (4)$.

证明. 考虑 $4r_1, 4r_2 \in I$. 由于偶数相减还是偶数, 我们有

$$4r_1 - 4r_2 = 4(r_1 - r_2) \in I$$

对于任意 $r \in R$, 由于偶数乘偶数还是偶数, 我们有

$$r(4r_1) = (4r_1)r = 4(r_1 r) \in I$$

因此, I 是 R 的一个理想.

由于 $4 \in (4)$, 但是 4 不能写成 $4r$, $r \in R$ 的形式, 所以有 $4 \notin I$. 也就是说 $I \neq (4)$.

□

练习 2.7.2. 假设 R 是整数环 (ring of integers). 证明 $(3, 7) = (1)$.

证明. $(3, 7)$ 是 R 的理想, 所以有 $3 \cdot 2 = 6 \in (3, 7)$, 而且 $7 - 6 = 1 \in (3, 7)$. 因此 $(1) \subseteq (3, 7)$.

另一方面, $(1) = R$, 所以有 $(3, 7) \subseteq (1)$.

因此, 我们得出

$$(3, 7) = (1)$$

□

练习 2.7.3. 假定例 2.7.3 中的 R 是有理数域. 证明: $(2, x)$ 是一个主理想.

证明. 如果 R 是有理数域, 那么 $\frac{1}{2} \in R \subseteq R[x]$. 因此, $(2, x)$ 包含有 $2p_1(x) = 2 \cdot \frac{1}{2} = 1 \in (2, x)$. 因此, $(2, x) = (1) = R$. □

备注 2.7.8. 两个理想的交集还是一个理想.

练习 2.7.4. 找出模 6 的剩余类环 R 的所有理想.

证明. $R = \{[0], [1], [2], [3], [4], [5]\}$. 如果 I 是 R 的一个理想, 那么 I 一定是剩余类加群 R 的一个子群. 剩余类加群是循环群, 因此, 它的子群也是循环群. 所以, 我们有:

$$\begin{aligned} G_1 &= ([0]) = \{[0]\} \\ G_2 &= ([1]) = ([5]) = R \\ G_3 &= ([2]) = ([4]) = \{[0], [2], [4]\} \\ G_4 &= ([3]) = \{[0], [3]\} \end{aligned}$$

G_1, G_2, G_3, G_4 都是 R 的理想, 也是 R 的所有理想. □

练习 2.7.5. 一个环 R 的一个非空集合 S 称为 R 的一个左理想 (left ideal), 如果:

1. $a, b \in S \Longrightarrow a - b \in S$;
2. $a \in S, r \in R \Longrightarrow ra \in S$.

在有理数域 F 上的 2×2 矩阵环 F_{22} 里找到一个不是理想的左理想.

证明. 考虑

$$S = \{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \quad a \in F, b \in F\}$$

容易验证:

$A, B \in S \Longrightarrow A - B \in S$

$$A \in S, L \in F_{22} \Longrightarrow LA = \begin{pmatrix} l_{11} & l_{12} \\ l_{21} & l_{22} \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} al_{11} + bl_{12} & 0 \\ al_{21} + bl_{22} & 0 \end{pmatrix} \in S$$

所以 S 是 F_{22} 的一个左理想.

S 不是 F_{22} 的理想: 考虑

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in S, \quad r = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in F_{22}$$

那么,

$$ar = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \notin S$$

所以, S 不满足 $a \in S, r \in F_{22} \Longrightarrow ar \in S$, 因此不是 F_{22} 的一个理想.

□

2.8 剩余类环, 同态与理想 (Quotient Ring/Residue Class Ring, Ring Homomorphism, and Ideal)

理想 (ideal) 在环论中的地位类似于不变子群 (normal subgroup) 在群论中的地位.

定义 2.8.1. 给定一个环 R 和 R 中的一个理想 I. 如果只考虑加法, 那么 R 做成一个加群 (additive group), I 做成 R 的一个不变子群 (normal subgroup). 那么, I 的陪集 (coset)

$$[a], [b], [c], \dots$$

做成一个 R 的分类. 这些类叫做 **模 I 的剩余类** (residue class of ideal I).

这个分类相当于 R 的元之间的一个等价关系 (equivalence relation), 表示为 (a 同余 b 模 I):

$$a \sim b \iff a \equiv b(I)$$

备注 2.8.1. 因为定义 2.8.1 中的 R 可以看作为加群, 类 $[a]$ 可以写成

$$[a] = \{a + u, \quad u \in I\}.$$

而且, 两个元 a 和 b 同余的条件是:

$$a \equiv b(I) \iff (a - b) \in I$$

定义 2.8.2. R 是一个环, I 是它的理想. 模 I 的所有剩余类 (residue class of I) 做成一个集合 $\overline{R}$

$$\overline{R} = \{[a], [b], [c], \dots\} \tag{2.100}$$

有以下的两个代数运算法则:

$$[a] + [b] = [a + b],$$
$$[a][b] = [ab].$$

那么, 如 2.100 中的模 I 的所有剩余类的集合 $\overline{R}$ 叫做环 R 的模 I 的**剩余类环 (quotient ring/residue class ring)**, 表示为 R/I.

备注 2.8.2. 环 R 可以看成一个加群 (additive group), 而模 I 可以看成一个不变子群 (normal subgroup). 因此, 模 I 的剩余类环 (quotient ring) R/I 可以看作一个加群 (additive group/Abelian group).

根据我们规定的代数运算法则: $[a]+[b]=[a+b]$ 和 $[a][b]=[ab]$, 容易验证 R/I 对于乘法来说是闭的, 而且适合结合律 (multiplicative associative law) $[a]([b][c])=([a][b])[c]=[abc]$.

分配律 (distributive law) 成立: $[a]([b]+[c])=[a][b]+[a][c]=[ab]+[ac]$, $([b]+[c])[a]=[b][a]+[c][a]=[ba]+[ca]$.

所以说, R/I 也是一个环 (ring).

定理 2.8.1. 假定 R 是一个环, I 是它的一个理想. R/I 是模 I 的剩余类环. 那么有, R 与 R/I 同态 (epimorphism/surjective homomorphism).

证明. 考虑映射

$$\phi : R \longrightarrow R/I, \quad a \mapsto [a] \tag{2.101}$$

这个映射是满射: $\forall [a] \in R/I$, 存在 $a \in R$ 使得 $\phi(a)=[a]$.

它是一个同态映射: $\forall a, b \in R$,

$$\phi(ab)=[ab]=[a][b]=\phi(a)\phi(b)$$

因此, R 和 R/I 同态.

□

定理 2.8.2. 假定 R 和 $\overline{R}$ 是两个环, 并且 R 和 $\overline{R}$ 同态. 那么, 这个同态映射 $\phi : R \mapsto \overline{R}$ 的核 $I=ker(\phi)$ 是 R 的一个理想 (ideal), 并且

$$R/I \cong \overline{R} \tag{2.102}$$

证明. 1. 先证明 $I=ker(\phi)$ 是 R 的一个理想 (ideal): 假定 $a \in I$, $b \in I$.

那么由于 I 是 ϕ 的核, 我们有

$$\phi(a)=\overline{0}, \phi(b)=\overline{0} \quad (\overline{0} \text{ 是 } \overline{R} \text{ 的零元})$$

也就是说

$$\phi(a-b)=\phi(a)-\phi(b)=\overline{0}-\overline{0}=\overline{0} \Longrightarrow a-b \in I$$

假设任意 $r \in R$, 我们有 $\phi(r) = \overline{r}$. 那么,

$$\phi(ra) = \phi(r)\phi(a) = \overline{r}\overline{0} = \overline{0} \Longrightarrow ra \in I$$
$$\phi(ar) = \phi(a)\phi(r) = \overline{0}\overline{r} = \overline{0} \Longrightarrow ar \in I$$

2. 证明 $R/I \cong \overline{R}$: 规定一个法则:

$$\psi : [a] \mapsto \overline{a} = \phi(a) \tag{2.103}$$

那么, 我们证明 ψ 是一个 R/I 和 $\overline{R}$ 之间的同构映射 (isomorphism):

- 映射 ψ 存在:

$$[a] = [b] \Longrightarrow a - b \in I \Longrightarrow \overline{a - b} = \overline{a} - \overline{b} = \overline{0} \Longrightarrow \overline{a} = \overline{b}$$

- ψ 是一个满射 (surjective): 任意的一个 $\overline{a} = \phi(a)$, 一定有对应的 $[a] \in R/I$.
- ψ 是一个单射 (injective):

$$[a] \neq [b] \Longrightarrow a - b \notin I \Longrightarrow \overline{a - b} = \overline{a} - \overline{b} \neq \overline{0} \Longrightarrow \overline{a} \neq \overline{b}$$

所以, ψ 是一个一一映射.

ψ 是同构, 因为:

$$[a] + [b] = [a + b] \Longrightarrow \overline{a + b} = \overline{a} + \overline{b}$$
$$[a][b] = [ab] \Longrightarrow \overline{ab} = \overline{a}\overline{b}$$

所以, ψ 是一个同构映射.

□

备注 2.8.3. 定理 2.8.1 对应定理 1.11.1. 定理 2.8.2 对应定理 1.11.2 (First Isomorphism Theorem).

由此, 我们可以看出理想和不变子群的平行地位.

例子 2.8.1. 给定一个整数 n, 考虑整数环 (ring of integers) R 的剩余类环 (quotient ring). 整数的剩余类环是利用这个整数 n 和整数环 R 的元之间的等价关系 (equivalence relation)

$$a \sim b \iff a \equiv b(n)$$

也就是条件

$$a \sim b \iff n \mid a-b.$$

同时, 这个等价关系和利用 R 的主理想 (n) 建立的等价关系是一样的:

$$a \sim b \iff a \equiv b((n))$$

也就是条件

$$a \sim b \iff a-b \in (n)$$

所以说, 模 n 的整数的剩余类环 (ring of integers modulo n) 就是 $R/(n)$. 而实际上, 一般的剩余类环是整数的剩余类环的推广.

定理 2.8.3. 在环 R 和 $\overline{R}$ 的一个同态映射之下,

1. R 的一个子环 (subring) S 的象 $\overline{S}$ 是 $\overline{R}$ 的一个子环 (subring);
2. R 的一个理想 (ideal) I 的象 $\overline{I}$ 是 $\overline{R}$ 的一个理想 (ideal);
3. $\overline{R}$ 的一个子环 (subring) $\overline{S}$ 的逆象 S 是 R 的一个子环 (subring);
4. $\overline{R}$ 的一个理想 (ideal) $\overline{I}$ 的逆象 I 是 R 的一个理想 (ideal).

备注 2.8.4. 定理 2.8.3 类比于群论里的定理 1.11.3 和定理 1.11.4.

练习 2.8.1. 假定一个环 R 有一个分类. S 是所有的类 $[a]$, $[b]$, $[c]$, ... 所作成的集合. 我们规定以下两个 S 的代数运算:

$$[x]+[y]=[x+y], \quad [x][y]=[xy]$$

证明 $[0]$ 是 R 的一个理想, 而且给定的类刚好是模 $[0]$ 的 R 剩余类 $R/[0]$.

证明. 证明分两步.

- 首先, 我们证明: $[0]$ 是 R 的一个理想.

考虑 $u, v \in [0]$, 我们有 $[u] = [v] = [0]$. 那么, 对于任意的 $r \in R$, 我们有:

$$\begin{aligned}[u - v] &= [u] - [v] = [0] - [0] = [0] \\ [ru] &= [r][u] = [r][0] = [r\,0] = [0] \\ [ur] &= [u][r] = [0][r] = [0\,r] = [0].\end{aligned}$$

因此, $u - v \in [0]$, $ru \in [0]$, $ur \in [0]$. 所以, $[0]$ 是 R 的一个理想.

- 下面, 我们证明: 给定的类刚好是模 $[0]$ 的 R 的剩余类.

  假设 $[u] = [v]$. 那么,

$$\begin{aligned}&[u] = [v] \\ \Longrightarrow &[u] - [v] = [0] = [u - v] \\ \Longrightarrow &u - v \in [0]\end{aligned}$$

  反过来, 假设 $u - v \in [0]$. 那么,

$$\begin{aligned}&u - v \in [0] \\ \Longrightarrow &[u] - [v] = [u - v] = [0] \\ \Longrightarrow &[u] = [v]\end{aligned}$$

  综上所述,

$$[u] = [v] \iff u - v \in [0].$$

  也就是说, 给定的类刚好是模 $[0]$ 的 R 的剩余类 $R/[0]$.

□

练习 2.8.2. 假定 ϕ 是环 R 到环 $\overline{R}$ 的一个同态满射 (epimorphism). 证明: ϕ 是环 R 到环 $\overline{R}$ 的同构映射 (isomorphism), 当且只当 (if and only if) ϕ 的核是 R 的零理想的时候 $ker(\phi) = \{0\}$.

证明. 假设同态满射是 $\phi(a) = \overline{a}$, $a \in R$, $\overline{a} \in \overline{R}$. 如果 ϕ 是一个同构映射, 那么 ϕ 是一个一一映射. 所以, 在 ϕ 之下, 只有 R 的零元 0 是 $\overline{R}$ 的零元 $\overline{0}$ 的逆象. 也就是说, ϕ 的核是 R 的零理想 $\{0\}$.

反过来假设 ϕ 的核是 R 的零理想 $\{0\}$. 那么, R 的任意非零元 $c \neq 0$, 它的象有 $\overline{c} \neq 0$.

因此,

$$\begin{aligned} & a \neq b,\, a, b \in R \\ \Longrightarrow & a - b \neq 0 \\ \Longrightarrow & \overline{a} - \overline{b} = \overline{a - b} \neq \overline{0} \\ \Longrightarrow & \overline{a} \neq \overline{b} \end{aligned}$$

所以, ϕ 是一个单射 (injective). 也就是说, ϕ 是一个同构映射 (isomorphism). □

练习 2.8.3. 假定 R 是所有复数 $a + bi$, a, b 是整数, 做成的环. 环 $R/(1+i)$ 有多少元?

证明. 首先, 我们看 R 的主理想 $(1+i)$ 包括哪些元:

如果 $a + bi \in (1+i)$, 那么 $a + bi$ 可以写成:

$$(a + bi) = (x + yi)(1 + i) = (x - y) + (x + y)i, \quad \forall x, y \in \mathbb{Z}.$$

$x - y$ 和 $x + y$ 为整数. 如果 x 和 y 同为奇数或者同为偶数, 那么 a 和 b 同为偶数; 如果 x 和 y 一奇一偶, 那么 a 和 b 同为奇数. 因此, 我们得出 a 和 b 必须有相同的奇偶性.

反过来看, 假设 a 和 b 有相同的奇偶性. 那么方程组

$$\begin{cases} x - y = a \\ x + y = b \end{cases}$$

有整数解:

$$x = \frac{a+b}{2}, \quad y = \frac{b-a}{2}$$

也就是说, $a + bi$ 可以写成 $(x + yi)(1 + i)$ 的形式, 其中 $x + yi \in R$. 所以有 $a + bi \in (1+i)$. 这时候, 我们有

$$[a + bi] = [0], \quad \text{或者说 } a + bi \equiv 0((1+i)).$$

下一步, 考虑 a 和 b 一奇一偶. 那么有

$$a + bi = 1 + (a - 1) + bi$$

这时候, $a-1$ 和 b 有相同的奇偶性. 也就是说, $(a-1)+bi \in (1+i)$. 所以有,

$$a+bi = 1+u, \quad u \in (1+i)$$

也就是有

$$[a+bi] = [1], \quad \text{或者说 } a+bi \equiv 1((1+i)).$$

综上所述, 环 $R/(1+i)$ 有两个元素 $[0]$ 和 $[1]$.

□

2.9 最大理想 (Maximal Ideal)

我们讨论两种由一个交换环得到域的重要方法. 第一种是利用最大理想 (maximal ideal) 的方法, 在本节讨论.

定义 2.9.1. 一个环 R 的一个不等于 R 的理想 I 叫做一个 **最大理想 (maximal ideal)**, 如果除了 R 和 I 之外, 没有包含 I 的理想.

备注 2.9.1. 可以这样去理解最大理想: 如果 I 是 R 的最大理想 (maximal ideal), 那么, 在 I 和 R 的中间就不存在另外一个理想 J:

$$\nexists J, \text{ s.t. } I \subset J \subset R$$

例子 2.9.1. 考虑整数环 (ring of integers) R. 由一个素数 p 生成的主理想 (principle ideal, 见定义 2.7.2) (p) 是一个最大理想 (maximal ideal, 见定义 2.9.1).

证明. 假定 J 是一个不等于 (p) 的 R 的理想, 并且 $(p) \subset J$. 那么, J 一定包含一个不能被 p 整除的整数 q. 由于 p 是素数, q 和 p 互素, 所以 $gcd(p,q) = 1$. 那么[8] 存在整数 s 和 t, 使得

$$sp + tq = gcd(p,q) = 1.$$

[8] 根据" 初等数论, 闵嗣鹤严士健第三版" 1.3 的推论 1.1: 任意两个不全为零的整数 a, b, 存在两个整数 s, t 使得 $as + bt = gcd(a,b)$.

因为 $p \in J$ 和 $q \in J$, 而且 J 是理想, 所以有

$$sp + tq \in J \Longrightarrow 1 \in J \Longrightarrow J = R.$$

□

我们可以利用最大理想 (maximal ideal), 从一个环 (ring) 构建一个域 (field).

引理 2.9.1. 如果 I 是环 R 的一个理想 (ideal), 那么剩余类环 (quotient ring) R/I 除了零理想 (zero ideal $\{0\}$) 和单位理想 (unit ideal, i.e., the ring itself) 之外没有别的理想, 当且仅当 (if and only if) I 是最大理想 (maximal ideal) 的时候.

备注 2.9.2. R/I 是一个除环 (division ring), 那么根据定理 2.7.1, R/I 除了零理想 (zero ideal $\{0\}$) 和单位理想 (unit ideal, i.e., the ring itself) 之外没有别的理想.

但是定理 2.7.1 的逆定理不成立: 如果 R/I 除了零理想 (zero ideal $\{0\}$) 和单位理想 (unit ideal, i.e., the ring itself) 之外没有别的理想, 那么 R/I 不一定是一个除环 (division ring), 见备注 2.7.3.

因此, 引理 2.9.1 可以表述为: 给定 I 是环 R 的一个理想 (ideal), 有剩余类环 (quotient ring) R/I:

1. 如果剩余类环 (quotient ring) R/I 是一个除环 (division ring), 那么, R/I 除了零理想 (zero ideal $\{0\}$) 和单位理想 (unit ideal, i.e., the ring itself) 之外没有别的理想, 从而得出, I 是最大理想 (maximal ideal).

2. 如果 I 是最大理想 (maximal ideal), 那么 R/I 除了零理想 (zero ideal $\{0\}$) 和单位理想 (unit ideal, i.e., the ring itself) 之外没有别的理想.

证明. 根据定理 2.8.1, 存在 R 到 $\overline{R} := R/I$ 的同态满射 (epimorphism) ϕ:

$$\phi : R \longrightarrow \overline{R} = R/I$$

R/I 中的零元 $[0] \in R/I$ 可以记为 $\overline{0} \in \overline{R}$.

- $\Longrightarrow$: 假设 I 是最大理想 (maximal ideal). 并且假设 $\overline{J} \neq \{\overline{0}\}$ 是 $\overline{R}$ 中的一个非零理想.

  那么, 由定理 2.8.3, $\overline{J}$ 在 ϕ 中的逆象 J 是 R 的理想.

我们知道 $\phi(I) = \{\overline{0}\}$. 因为 $\overline{J}$ 是 $\overline{R}$ 的理想, 我们得出零理想 (zero ideal) 包含在 $\overline{J}$ 里面: $\{\overline{0}\} \subset \overline{J}$. 所以有:

$$I = \phi^{-1}(\{\overline{0}\}) \subset \phi^{-1}(\overline{J}) = J \Longrightarrow I \subset J$$

根据假设 I 是 R 的最大理想 (maximal ideal), 因此有 $J = R$.

因为 ϕ 是 R 到 $\overline{R}$ 的满射, 我们有 $\overline{J} = \overline{R}$. 因此, $\overline{R}$ 中只有零理想 $\{\overline{0}\}$ 和单位理想 $\overline{R}$.

- $\Longleftarrow$: 我们证明其逆否命题 (contrapositive): 假设 I 不是最大理想 (maximal ideal), 我们要证明在 R/I 中存在不是零理想 (zero ideal) 也不是单位理想 (unit ideal) 的其他理想:

  如果 I 不是最大理想 (maximal ideal), 那么存在一个 R 的理想 J, 使得 $I \subset J \subset R$ 并且有 $J \neq R$. 根据定理 2.8.3, $\overline{J} = \phi(J)$ 是 $\overline{R}$ 的一个理想.

  1. 由于 I 是 J 的真子集, $I \subset J$, J 中一定包含一个不属于 I 的元. 我们知道 $\phi(I) = \{\overline{0}\}$, 那么因为 J 中包含不属于 I 的元, 所以有 $\overline{J} \supset \{\overline{0}\}$. 也就是说 $\overline{J}$ 不是 $\overline{R}$ 中的零理想.
  2. 我们还需要说明 $\overline{J} \neq \overline{R}$. 再次用反证法: 假设 $\overline{J} = \overline{R}$, 那么对于任意的 $r \in R$, 可以找到对应的元 $j \in J$ 使得

     $$\phi(r) = [r] \in \overline{R} = \overline{J} \ni [j] = \phi(j)$$

     也就是说

     $$[r] = [j] \Longrightarrow r - j \in I \subset J.$$

     由于 J 是 R 的理想, 加上 $j \in J$, 可以得出

     $$j + (r - j) \in J \Longleftarrow r \in J.$$

     所以说, 对于任意 $r \in R$, 有 $r \in J$, 也就是 $R \subseteq J$. 结合之前的假设 $J \subset R$, 可以得出 $R = J$. 但是这与我们之前的假定 $J \neq R$ 相矛盾. 因此, 我们证明了 $\overline{J} \neq \overline{R}$.

  综上所述, 我们证明了逆否命题: 如果 I 不是最大理想, 那么存在 $\overline{R}$ 上的一个理想 $\overline{J}$, $\overline{J}$ 既不是零理想也不是单位理想.

□

一个域只有零理想和单位理想. 反过来, 一个只有这两个理想的环不一定是域 (也不一定是除环). 因此, 我们需要进一步限定条件.

引理 2.9.2. 如果一个有单位元 (multiplicative identity) 的交换环 (commutative ring) R 除了零理想 (zero ideal) 和单位理想 (unit ideal) 以外没有其他的理想, 那么 R 一定是一个域 (field).

证明. 考虑 R 中的任意非零元 $a \neq 0$. a 生成的理想 (a) 显然不是零理想. 那么, 根据给定的条件, $(a) = R$. 因此, R 的单位元 $1 \in (a)$. (a) 中的元可以写成 ra $(r \in R)$ 的形式, 所以有

$$1 = a'a, \quad \exists a' \in R$$

也就是说, R 上的任意一个非零元 a 都有一个逆元 $a' \in R$. 因此可得, R 是一个域. □

一个域 (field) 一定是一个除环 (division ring). 因此, 引理 2.9.2 有以下的推论:

推论 2.9.1. 如果一个有单位元 (multiplicative identity) 的交换环 (commutative ring) R 除了零理想 (zero ideal) 和单位理想 (unit ideal) 以外没有其他的理想, 那么 R 一定是一个除环 (division ring).

由上述引理 2.9.1 和引理 2.9.2, 我们立刻得出:

定理 2.9.1. 假定 R 是一个有单位元 (multiplicative identity) 的交换环 (commutative ring), I 是 R 的一个理想 (ideal). 那么 R/I 是一个域 (field), 当且仅当 (if and only if) I 是一个最大理想 (maximal ideal) 的时候.

备注 2.9.3. 定理 2.9.1 说明了, 给定一个有单位元的交换环, 我们只要能找到 R 的一个最大理想 I, 我们就能构造出一个域 R/I.

例子 2.9.2. R 是整数环 (ring of integers). (p) 是由素数 p 生成的主理想. 那么由上面的例子 2.9.1, 我们知道 (p) 是 R 的一个最大理想 (maximal ideal). 因此 $R/(p)$ 是一个域 (field). 这个结果已经在上述例子 2.4.1 中说明过.

练习 2.9.1. 假定 R 是所有复数 $a+bi$ $(a,b\in\mathbb{Z})$ 做成的环. 证明, $R/(1+i)$ 是一个域.

证明. 只要证明 $(1+i)$ 是 R 的最大理想: 假设 I 是 R 的一个理想, 并且

$$(1+i)\subset I\subset R,\quad (1+i)\neq I$$

根据上述练习 2.8.3, 我们知道 $a+bi\in(1+i)$ 必须是 a, b 同奇偶. I 含有不在 $(1+i)$ 的元, 那么这个元一定是 a, b 一奇一偶, 这个元可以记为 $a+bi\in I$. 这也意味着 $a-1$ 和 b 同奇偶, 那么, 有 $a-1+bi\in(1+i)\subset I$. 因为 I 是理想, 而且有元 $a+bi\in I$ 和 $a-1+bi\in I$, 因此可得

$$a+bi-(a-1+bi)\in I\Longrightarrow 1\in I\Longrightarrow I=R.$$

因此, $(1+i)$ 是 R 的最大理想. 根据定理 2.9.1, $R/(1+i)$ 是一个域. □

证明. 另一种证明: 根据上述练习 2.8.3, 我们知道

$$R/(1+i)=\{[0],[1]\}$$

其中 $[0]=\{0+x|x\in(1+i)\}$, $[1]=\{1+x|x\in(1+i)\}$.

因此, $R/(1+i)$ 和模 2 的剩余类环同构. 由于 2 是素数, 根据例子 2.4.1 的讨论, 模 2 的剩余类环是一个域, 因此, $R/(1+i)$ 也是一个域. □

练习 2.9.2. 给定环 R 上的一个一元多项式环 $R[x]$. 当 R 是整数环 (ring of integers) 的时候, $R[x]$ 的主理想 (principle ideal) (x) 是不是一个最大理想 (maximal ideal)? 当 R 是有理数域 (field of rational numbers) 的时候呢?

证明. 考虑 $R[x]$ 的理想 $(2,x)$. $(2,x)$ 可以写成

$$(2,x)=\{2p_1(x)+xp_2(x)\,|\,p_1(x),\,p_2(x)\in R[x]\}$$

类似的, (x) 可以写成

$$(x)=\{xf(x)\,|\,f(x)\in R[x]\}.$$

显然有

$$(x)\subseteq(2,x),$$
$$2\in(2,x),\ 2\notin(x)\Longrightarrow(x)\subset(2,x)$$

也就说, (x) 是 $(2,x)$ 的真子集.

- 当 R 是整数环的时候, 有备注 2.7.7, 我们知道 $(2,x)$ 不是一个主理想 (principle ideal), 它不能写成 $(p(x))$ 的形式, $\forall p(x) \in R[x]$. 而 $1 \in R[x]$, 也就是说

$$(2,x) \neq (1) = R[x]$$

  综上所述, 我们证明了 $(x) \subset (2,x) \subset R[x]$. 所以, (x) 不是 $R[x]$ 的一个最大理想.

- 当 R 是有理数域的时候, 假设 I 是 $R[x]$ 的一个理想, 并且 $(x) \subset I$.

  那么, I 中有一个元素 $f(x) = a_0 + a_1x + \ldots + a_nx^n \in I$, $a_0 \neq 0$.

  我们知道 $a_1x + \ldots + a_nx^n = x(a_1 + \ldots + a_nx^{n-1}) \in (x) \subset I$. 因此有

$$\begin{aligned} & f(x) - x(a_1 + \ldots + a_nx^{n-1}) = a_0 \in I \\ \Longrightarrow & \frac{1}{a_0}a_0 = 1 \in I \\ \Longrightarrow & I = (1) = R \end{aligned}$$

  因此, 我们得出 (x) 是一个最大理想.

□

练习 2.9.3. 把所有偶数做成一个环 R. 证明: (4) 是 R 的最大理想 (maximal ideal), 但是 $R/(4)$ 不是一个域 (field).

证明. R 是交换环 (commutative ring), 没有单位元 (multiplicative identity). 所以, 它的主理想的元可以写成 $ra + na$, $r \in R$, $n \in \mathbb{Z}$ 的形式.

具体到 (4), 我们有

$$(4) = \{r4 + n4 | r \in R, n \in \mathbb{Z}\} = \{4n | n \in \mathbb{Z}\}$$

1. 证明 (4) 是 R 的最大理想:

   假设有 R 的一个理想 I, 并且 $(4) \subset I$, 我们要证明 $I = R$:

   因为 (4) 是 I 的真子集, 那么存在 $a \in I$, 并且 $a \notin (4)$: $a = 2m \neq 4n$, $m \in \mathbb{Z}$, $n \in \mathbb{Z}$. 因此, a 可以写成 $a = 4q + 2 \in I$, $q \in \mathbb{Z}$. 另一方面, $4q \in (4) \subset I$, 所以有

$$4q + 2 - 4q \in I \Longrightarrow 2 \in I \Longrightarrow I = (2) = R$$

   所以, (4) 是 R 的一个最大理想.

2. 证明 $R/(4)$ 不是一个域: 显然, $R/(4)$ 中有非零元 $[2] \neq [0]$. 而 $[2][2] = [4] = [0]$. 也就是说, $R/(4)$ 有零因子, 因此不是一个域.

□

练习 2.9.4. 考虑有理数域 F 上的所有的 2×2 矩阵所组成的环 $M_2(F)$.

证明: $M_2(F)$ 只有零理想 (zero ideal) 和单位理想 (unit ideal), 但不是一个除环 (division ring).

证明. 矩阵环 $M_2(F)$ 是非交换环 (non-commutative ring), 有单位元 (multiplicative identity).

假设 I 是 $M_2(F)$ 的一个非零理想, $I \neq \{0\}$. I 含有 2×2 的矩阵 $A \neq 0$.

- 如果 $rank(A) = 2$, 那么 A 有逆元 $A^{-1} \in M_2(F)$. 我们有

$$A^{-1}A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E \in I \Longrightarrow I = (E) = M_2(F).$$

- 如果 $rank(A) = 1$, 那么存在初等矩阵 $P, Q \in M_2(F)$, 使得

$$PAQ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I.$$

同时, 有

$$P_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(F), \quad Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(F),$$

使得

$$P_1 \cdot PAQ \cdot Q_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I$$

因此有

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E \in I \Longrightarrow I = (E) = M_2(F).$$

综上所述, $M_2(F)$ 只有零理想和单位理想.

我们知道

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

所以说, $M_2(F)$ 有零因子 (zero divisor), 因此不是一个除环 (division ring).

□

2.10 商域 (Field of Fractions)

下面讨论由一个环得出一个域的第二种方法.

备注 2.10.1. 考虑整数环 (ring of integers) 是由普通的整数做成的集合, 而有理数作成的集合做成一个有理数域 (field of rational numbers). 也就是说, 整数环 (ring of integers) 是有理数域 (field of rational numbers) 的一个子环 (subring).

从这个发现出发, 我们问: 给定一个环 R, 嫩股不能找到一个除环 (division ring) 或者是域 (field) 包含这个环 R?

在备注 2.3.1 中, 我们讨论了, 一个除环 (division ring) 或者是一个域 (field) 里面没有零因子 (has no zero divisors). 因此, 一个环 R 如果能被一个除环 (division ring) 或者一个域 (field) 包含, 那么 R 不能有零因子 (R has no zero divisor).

接下来, 我们问: 如果一个环 R 是非交换环 (non-commutative ring), 那么, 如果 R 没有零因子 (has no zero divisor), 是不是能推出 R 能包含在一个除环或者是一个域里面呢? 答案是: 不可以. 因为, 一个无零因子的非交换环不一定能被一个除环包含.

那么, 如果 R 是交换环 (commutative ring) 呢?

定理 2.10.1. 任意一个无零因子 (has no zero divisor) 的交换环 (commutative ring) R 都是一个域 (field) Q 的子环 (subring).

证明. 当 R 只有零元的时候, 定理成立.

下面, 我们考虑 R 至少有两个元的情况, $a, b, c, \ldots \in R$.

作一个集合

$$A = \{\frac{a}{b} \mid \forall a, b \in R, b \neq 0\}$$

规定 A 的一个关系 $\sim$:

$$\frac{a}{b} \sim \frac{a'}{b'} \iff ab' = a'b$$

我们验证以下条件:

1.
$$\frac{a}{b} \sim \frac{a}{b} \iff ab = ab.$$

2.
$$\frac{a}{b} \sim \frac{a'}{b'} \iff ab' = a'b \iff a'b = ab' \iff \frac{a'}{b'} \sim \frac{a}{b}.$$

3. 给定
$$\frac{a}{b} \sim \frac{a'}{b'}, \quad \frac{a'}{b'} \sim \frac{a''}{b''},$$

$$\begin{aligned}
&\frac{a}{b} \sim \frac{a'}{b'}, \quad \frac{a'}{b'} \sim \frac{a''}{b''} \\
\Longrightarrow &ab' = a'b, \quad a'b'' = a''b' \\
\Longrightarrow &(ab'')b' = ab'b'' = (ab')b'' = (a'b)b'' = a'b''b = (a'b'')b = (a''b')b = (a''b)b' \\
\Longrightarrow &ab'' = a''b, \quad \text{因为} b' \neq 0 \text{ 而且} R \text{ 无零因子 (has no zero divisor)} \\
\Longrightarrow &\frac{a}{b} \sim \frac{a''}{b''}
\end{aligned}$$

因此, 我们知道 $\sim$ 是一个等价关系. 这个等价关系把 A 分成了若干个类 $\left[\frac{a}{b}\right]$. 考虑以下的集合

$$Q_0 = \left\{ \left[\frac{a}{b}\right] \mid \forall a, b \in R,\, b \neq 0 \right\}$$

并且, 对于 Q_0 我们规定以下的加法和乘法:

$$\begin{aligned}
\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] &= \left[\frac{ad + bc}{bd}\right] \\
\left[\frac{a}{b}\right] \left[\frac{c}{d}\right] &= \left[\frac{ac}{bd}\right]
\end{aligned}$$

验证这样规定的加法和乘法是有效 (well-defined) 的:

1. 由于 R 没有零因子 (has no zero divisor), 因此,

$$b \neq 0,\, d \neq 0 \Longrightarrow bd \neq 0.$$

2.

$$\begin{aligned}
&\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right], \quad \left[\frac{c}{d}\right] = \left[\frac{c'}{d'}\right] \\
\Longrightarrow &ab' = a'b, \quad cd' = c'd \\
\Longrightarrow &ab'dd' = a'bdd', \quad cd'bb' = c'dbb' \\
\Longrightarrow &adb'd' + bcb'd' = a'd'bd + b'c'bd \Longrightarrow (ad+bc)b'd' = (a'd'+b'c')bd \\
\Longrightarrow &\left[\frac{ad+bc}{bd}\right] = \left[\frac{a'd'+b'c'}{b'd'}\right].
\end{aligned}$$

3.

$$\begin{aligned}
&\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right], \quad \left[\frac{c}{d}\right] = \left[\frac{c'}{d'}\right] \\
\Longrightarrow &ab' = a'b, \quad cd' = c'd \\
\Longrightarrow &ab'cd' = a'bc'd \Longrightarrow (ac)(b'd') = (a'c')(bd) \\
\Longrightarrow &\left[\frac{ac}{bd}\right] = \left[\frac{a'c'}{b'd'}\right]
\end{aligned}$$

接下来, 我们验证 Q_0 对于加法做成一个加群 (additive group):

1. 交换律:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right] = \left[\frac{cb+da}{db}\right] = \left[\frac{c}{d}\right] + \left[\frac{a}{b}\right].$$

2. 结合律:

$$\begin{aligned}
&\left[\frac{a}{b}\right] + \left(\left[\frac{c}{d}\right] + \left[\frac{e}{f}\right]\right) = \left[\frac{a}{b}\right] + \left[\frac{cf+de}{df}\right] = \left[\frac{adf+bcf+bde}{bdf}\right] \\
&\left(\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right]\right) + \left[\frac{e}{f}\right] = \left[\frac{ad+bc}{bd}\right] + \left[\frac{e}{f}\right] = \left[\frac{adf+bcf+bde}{bdf}\right] \\
\Longrightarrow &\left[\frac{a}{b}\right] + \left(\left[\frac{c}{d}\right] + \left[\frac{e}{f}\right]\right) = \left[\frac{adf+bcf+bde}{bdf}\right] = \left(\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right]\right) + \left[\frac{e}{f}\right].
\end{aligned}$$

3. 有单位元 (additive identity) $\left[\frac{0}{b}\right]$:

$$\left[\frac{0}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{bc}{bd}\right] = \left[\frac{c}{d}\right].$$

4. 有逆元 (additive inverse):

$$\left[\frac{a}{b}\right]+\left[\frac{-a}{b}\right]=\left[\frac{ab-ab}{bb}\right]=\left[\frac{(a-a)b}{bb}\right]=\left[\frac{a-a}{b}\right]=\left[\frac{0}{b}\right].$$

Q_0 的所有非零元做成的集合对于乘法来说做成一个交换群 (commutative group):

1. 交换律 (commutative law):

$$\left[\frac{a}{b}\right]\left[\frac{c}{d}\right]=\left[\frac{ac}{bd}\right]=\left[\frac{c}{d}\right]\left[\frac{a}{b}\right],\quad R \text{ commutative: } bd=db,\, b\in R, d\in R.$$

2. 结合律 (associative law):

$$\left[\frac{a}{b}\right]\left(\left[\frac{c}{d}\right]\left[\frac{e}{f}\right]\right)=\left[\frac{ace}{bdf}\right]=\left(\left[\frac{a}{b}\right]\left[\frac{c}{d}\right]\right)\left[\frac{e}{f}\right].$$

3. 有单位元 (multiplicative identity) $\left[\frac{a}{a}\right]$:

$$\left[\frac{a}{a}\right]\left[\frac{a}{b}\right]=\left[\frac{aa}{ab}\right]=\left[\frac{a}{b}\right].$$

4. 对于任意元 $\left[\frac{a}{b}\right]$, 有逆元 (multiplicative inverse) $\left[\frac{b}{a}\right]$:

$$\left[\frac{a}{b}\right]\left[\frac{b}{a}\right]=\left[\frac{ab}{ba}\right]=\left[\frac{a}{a}\right].$$

综上所述, Q_0 对于加法做成一个加群, 而且 Q_0 的所有非零元做成的集合对于乘法来说做成一个交换群, 因此, Q_0 是一个域.

我们选择一个固定的非零元 $0\neq q\in R$. 考虑以下形式的元的集合:

$$R_0=\left\{\left[\frac{qa}{q}\right]\in Q_0 \mid \forall a\in R\right\}$$

那么, 我们有一个 R 到 R_0 的映射:

$$\phi: R\longrightarrow R_0,\quad \phi(a)=\left[\frac{qa}{q}\right]$$

我们验证 ϕ 是一个一一映射:

1. ϕ 有效 (well-defined): 给定 $a = a'$,

$$\phi(a) = \left[\frac{qa}{q}\right], \phi(a') = \left[\frac{qa'}{q}\right]$$
$$a = a' \Longrightarrow qaq = qa'q \Longrightarrow \left[\frac{qa}{q}\right] = \left[\frac{qa'}{q}\right] \Longrightarrow \phi(a) = \phi(a')$$

2. 满射 (surjective): 任意一个在 $\left[\frac{qa}{q}\right] \in R_0$ 中的元都能找到一个元 $a \in R$ 对应于

$$\phi(a) = \left[\frac{qa}{q}\right].$$

3. 单射 (injective): 给定 $\phi(a) = \phi(a')$,

$$\phi(a) = \phi(a') \Longrightarrow \left[\frac{qa}{q}\right] = \left[\frac{qa'}{q}\right] \Longrightarrow qaq = qa'q$$
$$\Longrightarrow aqq = a'qq \Longrightarrow (a - a')qq = 0 \Longrightarrow a - a' = 0, \text{ 因为有} q \neq 0, qq \neq 0$$
$$\Longrightarrow a = a'$$

而且,

$$\phi(a) + \phi(b) = \left[\frac{qa}{q}\right] + \left[\frac{qb}{q}\right] = \left[\frac{q^2(a+b)}{q^2}\right] = \left[\frac{q(a+b)}{q}\right] = \phi(a+b)$$
$$\phi(a)\phi(b) = \left[\frac{qa}{q}\right]\left[\frac{qb}{q}\right] = \left[\frac{q^2ab}{q^2}\right] = \left[\frac{q(ab)}{q}\right] = \phi(ab)$$

所以, ϕ 是 R 和 R_0 的同构映射 (isomorphism):

$$R \cong R_0$$

根据定理 2.5.4: R_0 是 Q_0 的子环, R_0 在 Q_0 里的补集和 R 没有共同元, 并且 $R_0 \cong R$. 那么存在一个和 Q_0 同构的环 Q, 而且 R 是 Q 的子环.

进一步而言, 因为 Q 和 Q_0 同构, 而 Q_0 是一个域, 所以 Q 也是一个域. 因此, 我们找到了一个包含 R 的域 Q 的存在.

□

备注 2.10.2. 既然 Q 是包含 R 的域, 那么 R 里的任意非零元 $b \neq 0$ 在 Q 中有逆元 b^{-1}. 所以, 在 Q 中, 我们用符号 $\frac{a}{b}$ 表示以下:

$$ab^{-1} = b^{-1}a = \frac{a}{b} \quad (a, b \in R, b \neq 0)$$

定理 2.10.2. Q 刚好是由所有元 $\frac{a}{b}$, $a,b\in R$, $b\neq 0$ 所做成.

$$Q:=\left\{\frac{a}{b}\,|\,a,b\in R,\,b\neq 0\right\}.$$

这里规定

$$\frac{a}{b}=ab^{-1}=b^{-1}a\quad(a,b\in R,\,b\neq 0)$$

证明. 从上面定理 2.10.1, 我们有

$$\phi:R\longrightarrow R_0,\quad a\mapsto\phi(a)=\left[\frac{qa}{q}\right]$$

而且我们知道 $R\cong R_0$ 和 $Q\cong Q_0$.

我们知道在 Q_0 中的逆元可以写成:

$$\left[\frac{qb}{q}\right]^{-1}=\left[\frac{q}{qb}\right],$$

因此, 对于任意的 $\left[\frac{a}{b}\right]\in Q_0$, 有

$$\left[\frac{a}{b}\right]=\left[\frac{q^2a}{q^2b}\right]=\left[\frac{qa}{q}\right]\left[\frac{q}{qb}\right]=\left[\frac{qa}{q}\right]\left[\frac{qb}{q}\right]^{-1}=\frac{\left[\frac{qa}{q}\right]}{\left[\frac{qb}{q}\right]}$$

根据 $Q\cong Q_0$ 以及 ϕ 是两者之间的一个一一映射, 我们可以得出

$$\left[\frac{a}{b}\right]=\frac{\left[\frac{qa}{q}\right]}{\left[\frac{qb}{q}\right]}=\left[\frac{qa}{q}\right]\left[\frac{qb}{q}\right]^{-1}=\phi(a)\phi(b)^{-1}=\frac{\phi(a)}{\phi(b)}=\phi(\frac{a}{b});$$

也就对应了在 Q 中的任意元可以写成 $\frac{a}{b}$ 的形式. 因此有, 每一个元 $\frac{a}{b}\in Q$.

由于 $Q\cong Q_0$, Q 也只能有可以写成 $\frac{a}{b}$ 的元.

□

备注 2.10.3. Q 的元可以写成 $\frac{a}{b}$ 的形式. 那么有以下性质:

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

定义 2.10.1. 一个域 Q 叫做环 R 的一个**商域 (field of fractions)**, 假如 $R \subseteq Q$, 并且 Q 刚好是由所有元组成的:

$$Q := \{\frac{a}{b} \in Q \,|\, a, b \in R,\, b \neq 0\}$$

定理 2.10.3. 同构的环的商域也同构 (isomrophism). 抽象来说, 一个环 (ring) 最多只有一个商域 (field of fractions).

证明. 假设环同构 $R \cong R'$, 我们要证明其对应的商域也同构 $F \cong F'$.

假定 $\phi : R \longrightarrow R'$ 是一一映射, 我们规定

$$f(\frac{a}{b}) = \frac{\phi(a)}{\phi(b)} \in F',\ \frac{a}{b} \in F$$

可以说明 f 是一个映射, 而且这个映射是满射 (surjective), 也是单射 (injective). 因此, 我们可以得出域同构 $F \cong F'$.

□

定理 2.10.4. 假定 R 是一个有两个以上的元的环, F 是一个包含 R 的域. 那么 F 包含 R 的一个商域. 也就是说, R 的商域是包含 R 的最小的域.

证明. 域 F 包含环 R, 因此, R 一定是无零因子的交换环.

考虑 F 里, 有

$$ab^{-1} = b^{-1}a = \frac{a}{b}, \quad \forall a, b \in R,\, b \neq 0$$

作 F 的子集

$$\overline{Q} = \{\frac{a}{b} \,|\, \forall a, b \in R,\, b \neq 0\}$$

我们知道 $\overline{Q}$ 是 R 的商域: 根据备注 2.5.2, $\overline{Q}$ 是 F 的一个子除环 (而且交换), 验证如下:

1. $\overline{Q}$ 的加法和乘法和 F 一致 (可交换):

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

2. $\overline{Q}$ 包含一个不等于零的元 $\frac{a}{a} = 1 \in \overline{Q}$.

3.

$$\frac{a}{b}, \frac{c}{d} \in \overline{Q} \Longrightarrow \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \in \overline{Q}$$

4.

$$\frac{a}{b}, \frac{c}{d} \in \overline{Q}, \frac{c}{d} \neq 0 \Longrightarrow \frac{a}{b}\left(\frac{c}{d}\right)^{-1} = \frac{a}{b}\frac{d}{c} = \frac{ad}{bc} \in \overline{Q}$$

□

练习 2.10.1. 证明一个域 F 是它自己的商域.

证明. F 可以看成是一个环, F 的商域 Q 包含 F: $F \subseteq Q$.

而 F 作为一个域, 它包含商域 Q: $Q \subseteq F$.

因此, 我们得出 $Q = F$. □

第三章　Factoring in Integral Domain (整环里的因子分解)

Recall: By Memo 2.2.9, the ring of integers R is an integral domain as Definition 2.2.6. By Exercise 2.6.1, $R[x]$ is also an integral domain.

In the **ring of integers**, we have **Fundamental Theorem of Arithmetic**, also called the **unique factorization theorem** or **prime factorization theorem**.

定理 3.0.1. Every integer $a \geq 1$ can be represented uniquely as a product of prime numbers, up to the order of the factors.

$$a = p_1 \cdots p_k, \quad p_i \text{ are positive prime integers, } k > 0$$

We want to extend this idea to see if unique factorization theorem holds for any arbitrary ring R.

3.1　Prime Number, Unique Factorization (素元, 唯一分解)

In this section we generalize the concepts of division and prime number to integral domain.

Recall the definition of integral domain:

定义 3.1.1. A ring R is an **integral domain (整环)**, if for $\forall a, b \in R$,

1. Multiplication is **commutative**:

$$ab = ba \tag{3.1}$$

2. R has a **multiplicative identity**, denoted by 1:

$$1a = a1 = a \tag{3.2}$$

3. R has **no nonzero zero divisors**

$$ab = 0 \Rightarrow a = 0, \text{ or } b = 0 \tag{3.3}$$

An integral domain is a *nonzero commutative ring with no nonzero zero divisors.*

定义 3.1.2. An element $e \in I$ is a **unit**, or **multiplicative invertible**, if e has a multiplicative inverse:

$$1 = ee^{-1}.$$

In other words, the unit, or the multiplicative invertible element, divides the multiplicative identity 1.

定义 3.1.3. Given an integral domain I, An element $b \in I$ **divides** $a \in I$, if there exists $c \in I$ such that

$$a = bc$$

If a is **divisible** by b (b **divides** a), we say b is a **factor (or divisor)**

of a, denoted by

$$b \mid a,$$

reading as b divides a.

If b can *not* divide a, we denote it by

$$b \nmid a.$$

定义 3.1.4. b is an **associate (associated element)** of a, if:

$$b = ea$$

where e is a unit, or multiplicative invertible element.

This also means that a is an associate of b, since $a = e^{-1}b$ by e multiplicative invertible.

备注 3.1.1. Some examples of multiplicative invertible elements or units, in rings:

- The ring of integers has two multiplicative invertible elements or units, 1 and -1.
- The ring of Gauss integers

  $$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

  has multiplicative invertible elements or units, ± 1 and $\pm i$.
- The ring $\mathbb{R}[x]$ of real polynomials has multiplicative invertible elements or units: nonzero constant polynomials.
- An integral domain has at least two units, 1 and -1. General speaking, an integral domain has more than two units, see Exercise 3.1.2.
- Fields are rings in which $0 \neq 1$ and in which every nonzero element is multiplicative invertible or is a unit.

定理 3.1.1. In an integral domain, the product of units is also a unit; the multiplicative inverse of a unit is also a unit.

(**Equivalent statement:** In an integral domain, the product of multiplicative invertible elements is also multiplicative invertible; the multiplicative inverse of a multiplicative invertible element is also multiplicative invertible.)

备注 3.1.2. Given an integral domain I, consider any element $a \in I$ and any multiplicative invertible element or unit, $e \in I$. We have:

$$a = ee^{-1}a = e(e^{-1}a) = e^{-1}(ea).$$

This implies that for any element $a \in I$,

- any multiplicative invertible element e divides a, and
- any associative of a, ea or $e^{-1}a$, divides a.

定义 3.1.5. Consider an integral domain I. For any $a \in I$, the **trivial divisor** of $a \in I$ are:

- multiplicative invertible elements (units), and
- the associates of a.

The other divisors of a, if exists, are called **proper divisors of** a.

定义 3.1.6. An **irreducible element** in I is:

- a non-zero element;
- not an multiplicative invertible element (unit);
- with **no proper divisor** - its only divisors are trivial divisors.

备注 3.1.3. Given a prime number p in an integral domain I, ± 1 and $\pm p$ divide p. And there is no other divisor than ± 1 and $\pm p$. In other words, prime number p has only trivial divisors.

Of course, a prime number $p \neq 0$, $p \neq \pm 1$.

定义 3.1.7. In an integral domain I, an element $p \in I$ is a **prime element**, if:

- p is a non-zero element,
- p is not an multiplicative invertible element (unit),
- **if** $p|bc$**, then** $p|b$**, or** $p|c$**.**

命题 3.1.1. In an integral domain I, prime element is irreducible element.

证明. Assume a is a prime element in I. Consider b is a factor of a, then there exists $c \in I$ such that

$$a = bc.$$

This means $a|bc$. a is a prime element, by definition, we have either $a|b$, or $a|c$.

- When $a|b$, that is b is a factor of a. It has $b = ax$ for some $x \in I$. So $a = bc = axc$, so $a(xc - 1) = 0$. Since $a \neq 0$, $xc - 1 = 0$, which means $xc = 1$. So c is multiplicative invertible element. Thus, by $a = bc \implies b = ac^{-1}$. This implies that b is the associate of a.
- When $a|c$, that is c is a factor of a. It has $c = ad$ for some $d \in I$. Thus, $a = bc = bad \implies a(bd-1) = 0$. Since $a \neq 0$, $bd-1 = 0$, which means $bd = 1$, so b is multiplicative invertible element (unit).
- Therefore, b is the factor of a. And b is either the associate of a, or the multiplicative invertible element (unit) in I. This means a has only trivial divisors, so a is irreducible element by Definition 3.1.6.

□

命题 3.1.2. In an integral domain, irreducible element is not necessarily prime element.

证明. We prove by showing a counterexample of integral domain with irreducible element but not prime.

Consider the integral domain

$$I = \{a + b\sqrt{-3} \,|\, a, b \in \mathbb{Z}\} = \{a + bi\sqrt{3} \,|\, a, b \in \mathbb{Z}\}$$

Elements in I are complex numbers. From properties of complex numbers, we have the following:

1. $e \in I$ is multiplicative invertible (or unit) iff $|e|^2 = 1$.

   - Assume $e = a + b\sqrt{-3}$ is multiplicative invertible, then e has an inverse e'. By property of complex number $|ee'|^2 = |e|^2|e'|^2$, we have:

   $$\begin{aligned} & 1 = ee' \\ \Longrightarrow & |1|^2 = |ee'|^2 = |e|^2|e'|^2 \\ \Longrightarrow & 1 = |e|^2|e'|^2 \end{aligned}$$

   $|e|^2 = a^2 + 3b^2$ is a positive integer, so is $|e'|^2$ a positive integer, thus, to make $1 = |e|^2|e'|^2$, there must be $|e|^2 = 1$.

   - Assume $|e|^2 = a^2 + 3b^2 = 1$. Then it must be $b = 0$ (if $b \neq 0 \Longrightarrow 3b^2 \geq 3 \Longrightarrow |e|^2 \geq 3$ since $a^2 \geq 0$), this implies that $a = \pm 1$. This means $e = \pm 1$. Thus, e is multiplicative invertible.
   - Remark: $e \in I$ is multiplicative iff $|e|^2 = 1$ means I has only two multiplicative invertible elements (or units) ± 1.

2. Element $\alpha = a + b\sqrt{-3} \in I$ such that $|\alpha|^2 = 4$ is irreducible.

- Since $|\alpha|^2 = 4$, $\alpha \neq 0$. Then by previous argument 1, α is not multiplicative invertible (because α to be multiplicative invertible, it has to be $|\alpha|^2 = 1$).
- $\alpha \neq 0$, and α is not multiplicative invertible. From the definition of irreducible element at 3.1.6, we need to verify that α has **no** proper divisor.

  Assume $\beta = c + d\sqrt{-3}$ is the divisor of α:

  $$\begin{aligned} &\alpha = \beta\gamma \\ \Longrightarrow &|\alpha|^2 = |\beta|^2|\gamma|^2 \\ \Longrightarrow &4 = |\beta|^2|\gamma|^2 \quad \text{, by } |\alpha|^2 = 4 \end{aligned}$$

  Since $\beta = c + d\sqrt{-3}$ is for any arbitrary integers c and d, it is obvious that $|\beta|^2 = c^2 + 3d^2 \neq 2$ and we have

  $$|\beta|^2 = 1, \text{ or } |\beta|^2 = 4.$$

  - If $|\beta|^2 = 1$, then by previous argument, β is multiplicative invertible. So β is not a proper divisor of a.
  - If $|\beta|^2 = 4$, then

    $$\begin{aligned} &|\alpha|^2 = |\beta|^2|\gamma|^2 \\ \Longrightarrow &4 = |\beta|^2|\gamma|^2 \\ \Longrightarrow &4 = 4|\gamma|^2 \\ \Longrightarrow &|\gamma|^2 = 1 \\ \Longrightarrow &\gamma \text{ is multiplicative invertible} \end{aligned}$$

    By $\alpha = \beta\gamma$ and γ is multiplicative invertible (γ is multiplicative invertible and γ^{-1} is also multiplicative invertible), we have $\beta = \gamma^{-1}\alpha$. So β is an associate of α, not a proper divisor of α.
  - Thus, α has only trivial divisors, so α is an irreducible element.

3. Consider the element $4 \in I$:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}) \tag{3.4}$$

We know

$$|2|^2 = 4, \quad |1+\sqrt{-3}|^2 = 4, \quad |1-\sqrt{-3}|^2 = 4.$$

By argument 2, $1+\sqrt{-3}$ is irreducible element of I.

Equation 3.4 implies $1+\sqrt{-3} | 2\cdot 2$. We need to show $1+\sqrt{-3} \nmid 2$:

By contradiction, if $1+\sqrt{-3} | 2$, then it must be

$$\begin{aligned} 2 &= (1+\sqrt{-3})(a+b\sqrt{-3}) \quad \text{for some } a+b\sqrt{-3} \in I \\ &= a-3b+(a+b)\sqrt{-3} \\ \Longrightarrow\ & a-3b=2, \quad a+b=0 \\ \Longrightarrow\ & -4b=2 \end{aligned}$$

No integer b can have $-4b=2$. Therefore, $1+\sqrt{-3} \nmid 2$. By Definition 3.1.7, this means $1+\sqrt{-3}$ is *not* prime.

In summary, we just show $1+\sqrt{-3} \in I$ is irreducible but *not* prime.

□

备注 3.1.4. Consider the set of integers $\mathbb{Z}$, as we will see later on, it is UFD. UFD has the proper that prime is equivalent to irreducible. This keeps the consistency with which in number theory the definition of prime number is by the definition of irreducible element.

定理 3.1.2. Let I be an integral domain, the product between a multiplicative invertible element (unit) e and an irreducible element p, ep is also an irreducible element.

证明. We show in the following steps:

1. Since $e \neq 0$, $p \neq 0$, and integral domain has no non-zero zero divisor, so $ep \neq 0$.

2. ep is not a multiplicative invertible element (unit): By contradiction. Assume ep is multiplicative invertible (unit), then it has an inverse,

denoted as e'. We have the following:

$$1 = e'(ep) = (e'e)p$$

This means p has a multiplicative inverse $e'e$, so p is multiplicative invertible (unit), this is contradictory to the presumption that p is an irreducible element and an irreducible element is not multiplicative invertible (unit). Thus, ep has to be multiplicative invertible.

3. Assume b is the factor of ep, which is $ep = bc$ for some $c \in I$. Assume b is not multiplicative invertible (unit), we want to show b is the associate of ep, by this we can conclude ep is prime element:

   - Since b is not multiplicative invertible (unit), then

   $$\begin{aligned} & ep = bc \\ \Longrightarrow & p = e^{-1}bc = b(e^{-1}c) \\ \Longrightarrow & b \mid p, \quad \text{that is } b \text{ divides } p \end{aligned}$$

   Since p is an irreducible element, b is not multiplicative invertible (unit), thus b has to be the associate of p.

   - Since b has to be the associate of p, by Definition 3.1.4: we have for some multiplicative invertible (unit) e'' such that

   $$b = e''p = e''e^{-1}ep = (e''e^{-1})(ep).$$

   By Theorem 3.1.1, the product of multiplicative invertible (units) and the inverse of multiplicative invertible (unit) are multiplicative invertible (units), so $e''e^{-1}$ is a multiplicative invertible (unit). Thus, b is the associate of ep.

□

定理 3.1.3. Given an integral domain I, a nonzero element $a \in I$ has proper divisor if and only if

$$a = bc,$$

where b and c are not multiplicative invertible (unit).

证明. If a has a proper divisor b, then we can write

$$a = bc.$$

- Since b is the proper divisor of a, b is not multiplicative invertible (unit) by Definition 3.1.5.
- We show that c is not multiplicaitve invertible (unit): By contradiction, assume c is multiplicative invertible (unit). Then

  $$a = bc \Longrightarrow ac^{-1} = bcc^{-1} = b \Longleftrightarrow b = ac^{-1}$$

  c is multiplicative invertible (unit), so c^{-1} is also a multiplicative invertible (unit) by Theorem 3.1.1. $b = ac^{-1}$ means that b is the associate of a. This contradicts to the presumption that b is the proper divisor of a. Thus, c is not a multiplicative invertible (unit).

For the opposite direction, assume

$$a = bc,$$

where b and c are not multiplicative invertible (units). We show b is not the associate of a by contradiction: Assume b is the associate of a, then we can write for some multiplicative invertible (unit) e such that

$$\begin{aligned} & b = ea \\ \Longrightarrow & a = bc = eac = aec \\ \Longrightarrow & 1 = ec \text{ by cancellation law in integral domain .} \end{aligned}$$

(Here we know integral domain has no nonzero zero divisors, and thus cancellation law holds in integral domain.)

$1 = ec$ implies that c is a multiplicative invertible (unit). This contradicts to the presumption that c is not a multiplicative invertible (unit). Therefore, we just show that b is not the associate of a by contradiction.

In summary, b is not a multiplicative invertible (unit), and b is not the associate of a. Thus, b is the proper divisor of a. □

推论 3.1.1. In an integral domain, assume a non-zero element $a \neq 0$ has proper divisor b with $a = bc$, then c is also a proper divisor of a.

证明. From the first half in the proof of Theorem 3.1.3, we have shown that c is not a multiplicative invertible (unit).

From the second half in the proof of Theorem 3.1.3, we can show that c is not an associate and thus is a proper divisor of a: By contradiction, assume c is an associate of a. Then we have some multiplicative invertible (unit) e such that

$$\begin{aligned} & c = ea \\ \Longrightarrow & a = bc = bea \\ \Longrightarrow & 1 = be \text{ by cancellation law in integral domain} \end{aligned}$$

$1 = be$ implies that b is a multiplicative invertible (unit). This contradicts to the presumption that b is not a multiplicative invertible (unit) since b by assumption is a proper divisor of a.

Thus, we just show c is also a proper divisor of a. □

We want to know which condition can ensure that an element can be uniquely factorized as a product of a finite number of prime elements.

定义 3.1.8. Let I be an integral domain. An element $a \in I$ has **unique factorization**, if the following conditions are satisfied:

1. $a = p_1 p_2 \cdots p_r$ (p_i is irreducible element in I);
2. If there exists $a = q_1 q_2 \cdots q_s$ (q_i is irreducible element in I), then

$$r = s$$

and by suitable rearrangement, q_i is an associate of p_i for each i, i.e.

$$q_i = e_i p_i \quad (e_i \in I \text{ is a multiplicative invertible (unit) }).$$

备注 3.1.5. By definition 3.1.8, zero and multiplicative invertible (units) in an integral domain do not have unique factorization:

1. If we write

$$0 = a_1 a_2 \cdots a_n$$

   Then since I is integral domain, it has no nonzero zero divisors, thus there must be some $a_i = 0$. But 0 is not an irreducible element, so a_i is not an irreducible element, and thus 0 can not be uniquely factorized.

2. If we write a multiplicative invertible (unit) e, with its multiplicative inverse as e', by:

$$\begin{aligned} & e = a_1 a_2 \cdots a_n \\ \Longrightarrow & e^{-1} e = e^{-1} a_1 a_2 \cdots a_n \\ \Longrightarrow & 1 = a_1 (e^{-1} a_2 \cdots a_n) \end{aligned}$$

   Thus, a_1 has an inverse. This means a_1 is a multiplicative invertible (unit), not an irreducible element. Therefore, e can not be uniquely factorized.

With this reason, we exclude zero and multiplicative invertible (units) when we study unique factorization.

例子 3.1.1. Not all non-zero non-multiplicative-invertible elements in an integral domain have unique factorization.

Consider again the integral domain in Proposition 3.1.2:

$$I = \{a + b\sqrt{-3} \,|\, a, b \in \mathbb{Z}\}$$

Check again the element $4 \in I$:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}). \tag{3.5}$$

- We know

$$|2|^2 = 4, \quad |1 + \sqrt{-3}|^2 = 4, \quad |1 - \sqrt{-3}|^2 = 4.$$

  By argument 2, 2, $1 + \sqrt{-3}$, and $1 - \sqrt{-3}$ are all irreducible elements of I. Equation 3.5 means 4 has two ways of factorization in I.

- I has only two multiplicative invertible (units) $e = \pm 1$. This means $2 \neq (1+\sqrt{-3})e$ and $2 \neq (1-\sqrt{-3})e$. So $1+\sqrt{-3}$ and $1-\sqrt{-3}$ are not associates of 2.
- By definition of unique factorization, the factorization $4 = 2 \cdot 2$ is different from the factorization $4 = (1+\sqrt{-3})(1-\sqrt{-3})$. Thus, 4 does not have unique factorization in I.

练习 3.1.1. Prove that 0 is not a proper factor for any element a in an integral domain I.

证明. Given a multiplicative invertible (unit) $e \in I$, we have $0 = e \cdot 0$, which means 0 is the associate of 0 itself.

Given any element a in an integral domain I, consider

$$a = a \cdot 0 \Longrightarrow a = 0$$

By 0 is the associate of 0, we know 0 is the associate of $a = 0$. Thus, 0 is not a proper factor of $a = 0$.

□

练习 3.1.2. Consider the following integral domain I:

$$I = \{\frac{m}{2^n} \,|\, m,\, n \in \mathbb{Z}, n \geq 0\}$$

What are the multiplicative invertible (units) of I? What are the irreducible elements of I?

证明. Elements in I can be rewritten as

$$\frac{m}{2^n} \iff 2^i u, \quad i \in \mathbb{Z},\ u \text{ is an odd number.} \tag{3.6}$$

Remark: It is obvious that

$$\{2^i ui \in \mathbb{Z},\ u \text{ is an odd number}\} \subseteq \{\frac{m}{2^n} \,|\, m,\, n \in \mathbb{Z}, n \geq 0\}.$$

For any $\frac{m}{2^n}$, m is either even number or odd number. If m is odd number, it can be written as the form of $2^i u$; if m is even number, it can be written as the form of $2^i \cdot 1$ with $u = 1$. Therefore, Equation 3.6 holds with $\frac{m}{2^n} \iff 2^i u$.

1. We show multiplicative invertible (units) of I are $\pm 2^i$, $i \in \mathbb{Z}$.

   - If $e = 2^i u$ is a multiplicative invertible (unit) of I, then there exists a multiplicative inverse e^{-1} with $e^{-1}2^i u = 1$. This means

     $$e^{-1} = 2^{-i}u^{-1}$$

     e^{-1} must follow the format in Equation 3.6:

     $e^{-1} = 2^{-i}u^{-1} = 2^{i'}u', \quad -i =: i' \in \mathbb{Z}, \; u^{-1} =: u'$ is an odd number

     This means u and $u' := u^{-1}$ are odd number, which implies that $u = \pm 1$. So we have

     $$e = 2^i u = \pm 2^i.$$

   - Suppose an element $e = \pm 2^i$ ($i \in \mathbb{Z}$). Then it has multiplicative inverse $\pm 2^{-i} \in I$, so e is a multiplicative invertible unit of I.
   - Summing up, we have shown the multiplicative invertible unit of I has the form of $\pm 2^i$.

2. We show $2^i u$ is irreducible element of I: By Theorem 3.1.2 and 2^i is unit of I, to show $2^i u$ is irreducible element of I is to show its associate u is irreducible element of I.

   In particular, we want to show the odd number u is an irreducible number (in the ring of integers $\mathbb{Z}$) iff u is an irreducible element in I.

   - First, we show if the odd number u is an irreducible element of I, then u is an irreducible number. It is done by contrapositive: to show if the odd number u is not irreducible, then u is not an irreducible element of I:

     If u as the odd number is not an irreducible number in $\mathbb{Z}$, then there is factorization $u = u_1 u_2$ where u_1 and u_2 are odd number and with $u_1, u_2 \neq \pm 1$.

     u_1 and u_2 can not be written as the form of $\pm 2^i$ ($i \in \mathbb{Z}$), they are <u>not</u> multiplicative invertible units of I.

     By Theorem 3.1.3, this means u has proper divisor, and thus u is not an irreducible element of I.

- Next, we show if the odd number u is an irreducible number in $\mathbb{Z}$, then u is an irreducible element of I:

  Assume the odd number u is an irreducible number and assume u has a factorization in I:

  $$u = (2^{i_1}u_1)(2^{i_2}u_2) = 2^{i_1+i_2}u_1u_2$$

  where $2^{i_1}u_1 \in I$ and $2^{i_2}u_2 \in I$, so u_1 and u_2 are odd numbers.

  u is an odd number, so $i_1 + i_2 = 0$. This means

  $$u = 2^0u_1u_2 = u_1u_2.$$

  Since u is irreducible, this means $u_1 = \pm 1$ or $u_2 = \pm 1$, which means $2^{i_1}u_1 = \pm 2^{i_1} \in I$ or $2^{i_2}u_2 = \pm 2^{i_2} \in I$. So at least one of $2^{i_1}u_1$ and $2^{i_2}u_2$ is the multiplicative invertible unit of I, while another one is the associate of u in I. So u is nonzero element in I, is not a multiplicative invertible unit, has only multiplicative invertible unit and associate as divisors. u is thus an irreducible element of I.

- Summing up, we have shown that the odd number u is an irreducible number (in the ring of integers $\mathbb{Z}$) iff u is an irreducible element in I.

  By Theorem 3.1.2, irreducible element in I has the form 2^iu where u is irreducible number in $\mathbb{Z}$.

□

练习 3.1.3. Consider an integral domain

$$I = \{a + bi | a, b \in \mathbb{Z}\}.$$

Prove 5 is not irreducible element of I. Does 5 have unique factorization?

证明. Similar to Example 3.1.1, we can prove:

1. $e \in I$ is multiplicative invertible (unit) iff $|e|^2 = 1$.

- Assume $e = a + bi$ is multiplicative invertible , then e has a multiplicative inverse e'. By property of complex number $|ee'|^2 = |e|^2|e'|^2$, we have:

$$\begin{aligned} & 1 = ee' \\ \Longrightarrow & |1|^2 = |ee'|^2 = |e|^2|e'|^2 \\ \Longrightarrow & 1 = |e|^2|e'|^2 \end{aligned}$$

  $|e|^2 = a^2 + b^2$ is a positive integer, so is $|e'|^2$ a positive integer, thus, to make $1 = |e|^2|e'|^2$, there must be $|e|^2 = 1$.

- Assume $|e|^2 = a^2 + b^2 = 1$. Then it must be either $a = 0$ or $b = 0$, this implies that $e = \pm 1$ or $e = \pm i$.

  $e = \pm 1$ is multiplicative invertible in I.

  For $e = \pm i$, we know $i \cdot -i = 1$, so i and $-i$ are mutually inverse, thus $e = \pm i$ is multiplicative invertible in I as well.

- Summing up, we have just shown that $e \in I$ is multiplicative invertible (unit) iff $|e|^2 = 1$.

- Remark: $e \in I$ is multiplicative invertible (unit) iff $|e|^2 = 1$ means I has only 4 multiplicative invertible (units): ± 1 and $\pm i$.

2. $\alpha \in I$ with $|\alpha|^2 = 5$ is irreducible in I.

   - Since $|\alpha|^2 = 5$, $\alpha \neq 0$. Then by argument aforementioned, α is not multiplicative invertible (for α to be multiplicative invertible, it has to be $|\alpha|^2 = 1$).

   - $\alpha \neq 0$, and α is not multiplicative invertible. From the definition of irreducible element at Definition 3.1.6, we need to check α has **no** proper factor.

     Assume β is the factor of α:

$$\begin{aligned} & \beta = c + di, \quad \alpha = \beta\gamma \\ \Longrightarrow & |\alpha|^2 = |\beta|^2|\gamma|^2 \\ \Longrightarrow & 5 = |\beta|^2|\gamma|^2, \quad \text{by } |\alpha|^2 = 5 \end{aligned}$$

Since $5 = |\beta|^2|\gamma|^2$, $|\beta|^2$ and $|\gamma|^2$ are both integers, we have

$$|\beta|^2 = 1, \text{ or } |\beta|^2 = 5.$$

- If $|\beta|^2 = 1$, then by previous argument, β is multiplicative invertible. So β is not a proper factor of a.
- If $|\beta|^2 = 5$, then

$$\begin{aligned} & 5 = |\beta|^2|\gamma|^2 \\ \Longrightarrow & 5 = 5|\gamma|^2 \\ \Longrightarrow & |\gamma|^2 = 1 \\ \Longrightarrow & \gamma \text{ is mulitplicative invertible (unit)} \end{aligned}$$

  By $\alpha = \beta\gamma$ and γ is a multiplicative invertible (γ is multiplicative invertible and γ^{-1} is also multiplicative invertible), we have $\beta = \gamma^{-1}\alpha$. So β is an associate of α, not a proper factor of α.
- Thus, α has only trivial factors, so α is an irreducible element.

Now we need to prove:

3. 5 is not an irreducible element of I, but 5 has unique factorization.

   - First, 5 is not an irreducible element of I: We can write

   $$5 = (1 + 2i)(1 - 2i).$$

   Here $|1 + 2i|^2 = |1 - 2i|^2 = 5$. By aforementioned argument that $|\alpha|^2 = 5$ is irreducible in I, $1 + 2i$ and $1 - 2i$ are irreducible elements of I. So, 5 is <u>not</u> an irreducible element of I.

   - Assume a factorization of 5 by irreducible elements has the form:

   $$5 = \alpha_1\alpha_2 \ldots \alpha_m,$$

   where α_i is irreducible element of I, $i = 1, \ldots, m$.

   Since 5 is not an irreducible element, we have $m \geq 2$.

   On the other hand, we know

   $$25 = |5|^2 = |\alpha_1|^2|\alpha_2|^2 \ldots |\alpha_m|^2,$$

where $|\alpha_i|^2 = 5$ by α_i irreducible element of I. So we have $m = 2$. Assume then

$$5 = \alpha_1\alpha_2 \dots \alpha_m \Longrightarrow 5 = \alpha\beta$$

with $|\alpha|^2 = |\beta|^2 = 5$.

We see 4 types of factorization for 5:

$$\begin{aligned}
5 &= (1+2i)(1-2i) \\
5 &= (-1-2i)(-1+2i) = [-1(1+2i)][-1(1-2i)] \\
5 &= (2+i)(2-i) = [i(1-2i)][-i(1+2i)] \\
5 &= (-2-i)(-2+i) = [-i(1-2i)][i(1+2i)]
\end{aligned}$$

Since ± 1 and $\pm i$ are multiplicative invertible (units) in I, so these 4 types of factorization are actually equivalent. Thus, 5 has a unique factorization.

□

3.2 Unique Factorization Domain (唯一分解整环)

From previous discussion, Unique Factorization Theorem (UFT) does not necessarily hold in integral domain. We also know Unique Factorization Theorem holds in some integral domain such as rings of integers $\mathbb{Z}$. We want to classify those integral domains that maintain the UFT.

定义 3.2.1. An integral domain I is called a **Unique Factorization Domain (UFD)**, if every nonzero and non-unit element in I has unique factorization.

First, we study what import property a unique factorization domain (UFD) has.

定理 3.2.1. A UFD has the following property:

3. If a prime element $p \in I$ can divides ab, then p can divide a or b.

证明. Assume p divide ab:

$$ab = pc$$

- Assume a and b are not zero element, not units.
  - By $a \neq 0$ and $b \neq 0$, we know $ab \neq 0$, so $c \in I$ is nonzero.
  - We want to argue c is not unit. By contradiction: Assume c is a unit. Then

    $$ab = pe \quad (e = c \text{ is a unit of } I)$$

    By Theorem 3.1.2, pe is prime element since p is prime element and e is unit.

    But then $pe = ab$ with a and b not units, thus pe has proper factors, contradict to pe is prime element of I.
  - Now that c is non-zero, and not unit, by definition of unique factorization domain,

    $$c = p_1 p_2 \cdots p_n \quad (p_i \text{ is prime element}),\ i = 1, 2, \ldots n$$

    On the other hand, since $a \in I$ and $b \in I$, we have:

    $$a = q_1 q_2 \ldots q_r, \quad b = q_1' q_2' \ldots q_s', \quad (q_i, q_i' \text{ are prime element})$$

    This means

    $$ab = pc \Longrightarrow q_1 q_2 \ldots q_r q_1' q_2' \ldots q_s' = p p_1 p_2 \cdots p_n$$

    By definition of unique factorization, p is the associate of some q_i or q_i'.

If p is the associate of q_i, then

$$pe'' = q_i \quad (e'' \text{ is unit})$$

So, we have

$$\begin{aligned} & a = q_1 q_2 q_{i-1} p e'' q_{i+1} \dots q_r \\ \Longrightarrow & a = p(q_1 q_2 q_{i-1} e'' q_{i+1} \dots q_r) \\ \Longrightarrow & p|a \end{aligned}$$

Similarly, if p is the associate of q_i', $p|b$.

Therefore, p divides either a or b.

- Assume one of a and b is zero element or unit.
  - If $a = 0$, $a = 0 = 0 \cdot b = ab = pc$, so $p|a$.
  - If a is unit, i.e. $a = e$. Then $ab = pc \Longrightarrow eb = pc \Longrightarrow b = p(ce^{-1})$. So $p|b$.

□

定理 3.2.2. If an integral domain I has the following properties:

1. Every non-zero non-unit element $a \in I$ has a prime factorization

$$a = p_1 p_2 \cdots p_2 \quad (p_i \text{ prime element of } I)$$

2. If a prime element $p \in I$ divides ab, then p divides either a or b.

Then I is a *unique factorization domain.*

证明. Assume a non-zero and non-unit element $a \in I$. By Property 1, we have a prime factorization

$$a = p_1 p_2 \dots p_r \quad (p_i \text{ is prime element })$$

We need to prove a has unique factorization: Assume a has another prime factorization

$$a = q_1 q_2 \dots q_s \quad (q_i \text{ is prime element })$$

then $r = s$, and by suitable rearrangement, q_i is the associate of p_i. We prove it by induction.

- When $r = 1$,

  $$a = p_1 = q_1 q_2 \dots q_s$$

  By contradiction, assume $s \neq 1$. Then we have

  $$p_1 = q_1(q_2 \dots q_s)$$

  where q_1 is not a unit, and $q_2 \dots q_s$ is product of prime elements so is not unit. That means the prime element p_1 has factorization as a product of two non-units elements.

  By Theorem 3.1.3, if $a = bc$ where b and c are not unit, then a has proper divisor, and thus a is not prime element. Here $p_1 = q_1(q_2 \dots q_s)$ where q_1 and $(q_2 \dots q_s)$ are not units, so p_1 has proper divisor and thus not prime element of I. We observe contradiction.

  This implies that $s = 1 = r$. That is

  $$a = p_1 = q_1$$

  This shows a has unique factorization.

- Assume the element a that can be written as product of $r - 1$ number of prime elements has unique factorization. Then consider two types of prime factorization for a:

  $$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

  By Property 2, p_1 divides $a = q_1 q_2 \dots q_s$, so p_1 divides some q_i with $p_1 | q_i$. After rearrangement, we can have $p_1 | q_1$ with

  $$q_1 = p_1 c \quad \text{for some } c \in I$$

Since q_1 is prime element, p_1 is not unit, so c has to be a unit, denoted by e. That is

$$q_1 = p_1 c \Longrightarrow q_1 = p_1 e^{-1} \Longrightarrow p_1 = e q_1$$

where e and e^{-1} are units.

This means

$$\begin{aligned} & e q_1 p_2 \dots p_r = q_1 q_2 \dots q_s \\ \Longrightarrow & b = (e p_2) \dots p_r = q_2 q_3 \dots q_s \end{aligned}$$

Here b is written as product of $r-1$ number of prime elements. By our hypothesis in induction, we have

$$r - 1 = s - 1$$

and by suitable rearrangement,

$$q_2 = e_2'(e p_2),\ q_2 = e_3' p_3, \dots, q_r = e_r' p_r \quad (e_i' \text{ is unit of } I)$$

This means we have

$$r = s$$

with

$$q_1 = e^{-1} p_1,\ q_2 = e_2'(e p_2),\ q_2 = e_3' p_3, \dots, q_r = e_r' p_r$$

□

备注 3.2.1. From Theorem 3.2.2, Property 1 and 2 can be used as the definition of unique factorization domain.

备注 3.2.2. Another important property of unique factorization domain is the existence of the **greatest common divisor (GCD)**.

定义 3.2.2. An element e is called the **common divisor** of elements a_1, a_2, a_3, ... a_n, if c divides simultaneously a_1, a_2, a_3, ... a_n. (b divides a (b is factor of a) iff $a = bc$, denoted by $b|a$.)

A common divisor d of elements a_1, a_2, a_3, ... a_n is called the **greatest common divisor (GCD)** of a_1, a_2, a_3, ... a_n, if every common divisor c of a_1, a_2, a_3, ... a_n divides d (every common divisor c is factor of d).

定理 3.2.3. There exists greatest common divisor for any two elements a and b in a unique factorization domain I. Any two greatest common divisors of a and b, denoted as d and d', has difference up to one unit, with

$$d' = ed \quad (e \text{ is unit of } I)$$

证明. Consider difference cases:

1. If either a or b is zero, say $a = 0$. Then,

$$\begin{aligned} & b = b \cdot 1, \quad a = 0 = b \cdot 0 = b \cdot a \\ \Longrightarrow & b|b, \quad b|a \\ \Longrightarrow & gcd(a, b) = b \end{aligned}$$

2. If either a or b is unit, say $a = e$ where e is a unit of I. Then,

$$\begin{aligned} & a = e = e \cdot e = a \cdot a, \quad b = b \cdot e = b \cdot a \\ \Longrightarrow & a|a, \quad a|b \\ \Longrightarrow & gcd(a, b) = a \end{aligned}$$

3. If a and b are non-zero, not unit. We can write

$$a = q_1 q_2 \dots q_r, \quad b = q_1' q_2' \dots q_s', \quad (q_i, q_i' \text{ are prime elements})$$

It is possible that there exists some q_i and q_i' are associates with each other:

$$q_i = q_i' e \quad (e \text{ is unit})$$

Let us assume among these $r+s$ elements, there are n elements p_1, p_2, ..., p_n **not** associates among each other, while other elements are associates of one of these n elements. By this we can rewrite:

$$a = e_a p_1^{h_1} p_2^{h_2} \cdots p_n^{h_n} \quad (e_a \text{ is unit}, h_i \geq 0)$$
$$b = e_b p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} \quad (e_b \text{ is unit}, k_i \geq 0)$$

Denote

$$l_i = \min(h_i, k_i),\ i = 1, \ldots, n$$

We construct a common divisor of a and b

$$d = p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n},$$

with $d|a$ and $d|b$.

Assume c is another common divisor of a and b.

- If c is unit (invertible), then c divides d since $d = cc^{-1}d = c(c^{-1}d)$.
- If c is not a unit, then we can write

  $$c = p_1' p_2' \cdots p_t' \quad (p_i' \text{ is prime element})$$

  Since $p_i'|c$ and $c|a$, we have $p_i'|a$. By Property 2, p_i' divides some p_j in the product of $a = p_j(p_1 \ldots p_{j-1} p_{j+1} \ldots p_n)$. Thus, p_i' is an associate of p_j (since p_j is prime element, so it has only trivial factors, while p_i' is also a prime element not a unit). Therefore, we have

  $$c = e_c p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n} \quad (e_c \text{ is unit }, m_i \geq 0)$$

  Since $c|a$, any p_i and p_j are not associates with each other, this implies $m_i \leq h_i$.

  Analogously, $c|b$ implies that $m_i \leq k_i$. This implies that $m_i \leq l_i$, thus $c|d$.

  Summing up, we have proved d is the greatest common factor of a and b.

- Here we show the greatest common factors have difference up to a unit. Assume another greatest common factor of a and b, denoted by d'. Since $d|d'$ and $d'|d$,

$$d' = ud,\ d = vd',\ d = uvd$$

  - If $d = 0$, then $d' = 0$. That is $d = d' = 0$.
  - If $d \neq 0$, by $d = uvd$, we have $1 = uv$. Thus, u is a unit:

$$d' = ud \Longrightarrow d' = ed.$$

□

推论 3.2.1. There exists greatest common divisor for any n elements a_1, a_2, ..., a_n in a unique factorization domain I. Any two greatest common divisors of a_1, a_2, ..., a_n, denoted as d and d', has difference up to one unit, with

$$d' = ed \quad (e \text{ is unit of } I)$$

We can use the concept of greatest common divisor to interpret the concept of co-prime in unique factorization domain.

定义 3.2.3. Elements a_1, a_2, ..., a_n in an unique factorization domain I are **co-prime**, if they have unit as their greatest common divisor.

练习 3.2.1. In a unique factorization domain, suppose we have:

$$a_1 = db_1,\ a_2 = db_2,\ \ldots, a_n = db_n$$

where not all $a_i = 0$.

Prove: b_1, b_2, ..., b_n are co-prime if and only if d is the greatest common divisor of a_1, a_2, ..., a_n.

证明. 1. We prove: if b_1, b_2, ..., b_n are co-prime, then d is a gcd of a_1, a_2, ..., a_n.

- By contradition: Assume d is not a gcd of a_1, a_2, ..., a_n. Further assume c is a gcd of a_1, a_2, ..., a_n.
- Since d is a common divisor of a_1, a_2, ..., a_n, we have $d|c$ such that $c = dh$, where h is not a unit (otherwise d is also a gcd.) Thus, for $i = 1, 2, \ldots, n$, we have

$$a_i = ck_i = dhk_i = db_i,$$

  Not all $a_i = 0$, this implies $d \neq 0$. By cancellation law, we have

$$b_i = hk_i, \quad i = 1, 2, \ldots, n$$

- This means h is a non-unit common divisor of b_1, b_2, ..., b_n. So, b_1, b_2, ..., b_n are not co-prime.

2. We prove: if d is a gcd of a_1, a_2, ..., a_n, then b_1, b_2, ..., b_n are co-prime.

- Assume d is a gcd of a_1, a_2, ..., a_n. Let t is a common divisor of b_1, b_2, ..., b_n. So, dt is a common divisor of a_1, a_2, ..., a_n.
- On the other hand, d is a gcd of a_1, a_2, ..., a_n. So we know $dt|d$, which is $d = dth$ for some h. As $d \neq 0$, this leads to $1 = th$ by cancellation law. This means t is a unit (invertible).
- Therefore, b_1, b_2, ..., b_n has unit as common divisor. This shows b_1, b_2, ..., b_n are co-prime.

□

练习 3.2.2. Suppose (a) and (b) are two principle ideals of an integral domain I.

Prove: $(a) = (b)$ if and only if b is the associate of a.

证明. An integral domain I has multiplicative identity and is commutative. According to 2.7.4, a principle ideal (a) in I has the format

$$ra, \quad r \in I$$

1. We prove: if $(a) = (b)$, then b is the associate of a (that is $b = ae$ where e is a unit (invertible element) in I).

   Assume $(a) = (b)$, then $a \in (b)$, so $a = sb$, for some $s \in I$. Also, $b \in (a)$, so $b = ta$, for some $t \in I$. This means $a = sta$.

   If $a = 0$, then $bta = t \cdot 0 = 0 = 0 \cdot e$. So b is the associate of a.

   If $a \neq 0$, then $a = sta$ implies $1 = st$. t is a unit (invertible element). So b is the associate of a by $b = ta$ where t is a unit (invertible element).

2. Assume b is the associate of a, we prove $(a) = (b)$: Since b is the associate of a, we can write $b = ta$, where t is a unit (invertible element) of I. Thus, for any element rb in (b), we have $rb = rta \in (a)$, which means $(b) \subseteq (a)$.

   On the other hand, t is a unit (invertible), so $a = t^{-1}b$, with the similar logic, we have $(a) \subseteq (b)$.

   Therefore, we have proved $(a) = (b)$.

□

3.3 Principal Ideal Domain (主理想环)

It is not easy to identify if an integral domain is **unique factorization domain** or not. However, there exists certain special integral domain as unique factorization domain.

定义 3.3.1. An integral domain in which every ideal is principal (ideal) is called a **Principal Ideal Domain (主理想环)**.

We want to prove a principal ideal domain is a unique factorization domain. Before that, we need the following two lemmas.

引理 3.3.1. Suppose I is a principal ideal domain. If a sequence

$$a_1, a_2, a_3, \ldots \quad (a_i \in I)$$

has a_{i+1} is a proper divisor of a_i for every $i = 1, 2, \ldots$, then this sequence is finite.

证明. We construct the principal ideals for each element a_i:

$$(a_1), (a_2), (a_3), \ldots$$

Since a_{i+1} is the proper divisor of a_i, we write $a_i = a_{i+1}r$ for some $r \in I$. This means

$$(a_i) \subseteq (a_{i+1}), \quad \forall i = 1, 2, \ldots$$

Thus, we have

$$(a_1) \subseteq (a_2) \subseteq (a_3) \ldots$$

Consider the union of all these ideals

$$U = \cup_i (a_i) \tag{3.7}$$

Suppose $a \in U$, $b \in U$. Then $a \in (a_i)$, $b \in (a_j)$ for some (a_i), (a_j). Assume $i \leq j$. Then $a \in (a_i) \subseteq (a_j)$. Thus, $a \in (a_j)$ and $b \in (a_j)$. So we have

$$a - b, ra \in (a_j) \subseteq U, \quad \forall r \in I$$

By Definition 2.7.1 of ideal, we know U is an ideal in I, with

1. If $a \in U$, $b \in U$, then $a - b \in U$;
2. If $a \in U$, $r \in I$, then $ra = ar \in U$

Since I is a principal ideal domain, U must be a principal ideal, with $U = (d)$ for some $d \in I$. Thus, d is in some (a_n), with $d \in (a_n)$.

We want to argue a_n is the last one in the sequence a_1, a_2, a_3, ...:

By contradiction, assume a_n is not the last one in the sequence. Then there is an element a_{n+1}. We know

$$\begin{aligned}
& d \in (a_n),\ a_{n+1} \in U = (d) \\
\Longrightarrow & d = a_n r,\ a_{n+1} = ds, \quad \text{for some } r \in I,\ s \in I \\
\Longrightarrow & a_n | d,\ d | a_{n+1} \\
\Longrightarrow & a_n | a_{n+1} \\
\Longrightarrow & a_{n+1} = a_n c, \quad \text{for some } c \in I
\end{aligned}$$

But we also know

$$a_n = a_{n+1}c', \quad \text{for some } c' \in I$$

In combination, we have

$$a_{n+1} = a_n c = a_{n+1}c'c \Longrightarrow 1 = c'c$$

This means c is a unit (invertible element) in I. By $a_{n+1} = a_n c$, a_{n+1} is an associate of a_n. This contradicts to the presumption that a_{n+1} is a proper divisor of a_n.

Therefore, we just prove a_n is the last one in the sequence a_1, a_2, a_3, ... This means the sequence a_1, a_2, a_3, ... stops at a_n and thus is finite.

□

引理 3.3.2. An ideal generated by a prime element p in a principal ideal domain I is a maximal ideal.

证明. Assume An ideal U contains (p) as a proper subset. Since I is a principal ideal domain, we have

$$\begin{aligned}(p) \subset U = (a), &\quad \text{for some } a \in I \\ \Longrightarrow p = rs &\quad (\text{for some } r \in I)\end{aligned}$$

This means a is a factor of p. But p is a prime element, so a is either the associate of p or a unit (invertible).

- If a is the associate of p: $a = ep$ for some unit $e \in I$. Then

  $$a \in (p) \Longrightarrow U = (a) \subseteq (p)$$

  This contradicts with the assumption that (p) is a proper subset of U. So a is not the associate of p.

- So a has to be a unit (invertible): $aa^{-1} = 1$.

  $$1 = aa^{-1} \Longrightarrow 1 \in (a) = U \Longrightarrow I = U$$

  Thus, (p) is a maximal ideal of I.

□

定理 3.3.1. A principal ideal domain I is a unique factorization domain.

证明. We use Theorem 3.2.2.

1. Suppose a non-zero and non-unit element $a \in I$. By contradiction: assume a can not be written as the product of finite number of prime elements. Then a is not a prime element. (Because if a is a prime element, then we can write $a = a$ as a product of one number of prime element itself.) This means a has proper divisor b such that $a = bc$. Then, by Corollary 3.1.1, c is also a proper divisor of a.

   At least one of b and c can not be written as the product of finite number of prime elements. (Otherwise, a would be written as the product of finite number of prime elements.)

   Therefore, if a has no format of the product of finite number of prime elements, then one of its proper divisor a_1 has the same property that a_1 can not be written as the product of finite number of prime elements.

   This means we obtain a infinite sequence

   $$a_1, a_2, a_3, \ldots$$

   where a_{i+1} is the proper divisor of a_i. But according to Lemma 3.3.1, it is impossible. We obtain contradiction here. This proves that a can be written as the product of finite number of prime elements.

2. Assume the prime element $p \in I$ can divides ab. Then

   $$\begin{aligned} & ab = rp \quad \text{for some } r \in I \\ \Longrightarrow & ab \in (p) \\ \Longrightarrow & ab \equiv 0((p)) \end{aligned}$$

This means in the quotient ring $I/(p)$, ab represents the class of $[0]$, with $[ab] = [0]$. We have

$$[ab] = [0] = [a][b]$$

By Lemma 3.3.2, (p) is the maximal ideal. According to Theorem 2.9.1 [I is a commutative ring R with multiplicative identity, then R/I is a field if and only if I is a maximal ideal], $I/(p)$ is a field. And a field has no non-zero zero divisor. Thus,

$$\begin{aligned}
&[ab] = [0] = [a][b] \\
\Longrightarrow &[a] = [0], \text{ or } [b] = [0] \\
\Longrightarrow &a \equiv 0((p)), \text{ or } b \equiv 0((p)) \\
\Longrightarrow &a - 0 \in (p), \text{ or } b - 0 \in (p) \\
\Longrightarrow &a \in (p), \text{ or } b \in (p) \\
\Longrightarrow &p|a, \text{ or } p|b
\end{aligned}$$

□

练习 3.3.1. I is a principal ideal domain, with $(a, b) = (d)$. Prove: d is a greatest common divisor of a and b, any greatest common divisor of a and b, denoted as d', has the following format:

$$d' = sa + tb \quad (s, t \in I)$$

证明. since $(a, b) = (d)$, we have

$$d|a, \quad d|b$$

So d is a common divisor of a and b.

Also, $d \in (a, b)$ implies that

$$d = s'a + t'b$$

Suppose c is any common divisor of a and b. Then

$$c|a,\ c|b \Longrightarrow c|s'a + t'b \Longrightarrow c|d$$

So, d is a gcd of a and b.

A PID is a UFD, by Theorem 3.3.1. By Theorem 3.2.3, any gcd d' of a and b is the associate of d:

$$\begin{aligned} & d' = ed \quad (e \text{ is unit(invertible) of } I) \\ \Longrightarrow & d' = es'a + et'b \\ \Longrightarrow & d' = sa + tb, \quad (s = es' \in I,\, t = et' \in I) \end{aligned}$$

Thus, any d' as the gcd of a and b has the format

$$d' = sa + tb, \quad (s, t \in I)$$

□

练习 3.3.2. Every non-zero maximal ideal of a principal ideal domain is generated by a prime element.

证明. Since it is under a principal ideal domain, every maximal ideal is (a) for some element $a \in I$. Suppose (a) is a non-zero maximal ideal of I. Then, $(a) \neq I$. So a is not a unit(invertible).

(a) is non-zero, so $a \neq 0$.

Assume a is not a prime element. Then we can write $a = bc$, where b is a proper divisor of a. This means

$$(a) \subseteq (b).$$

b is a proper divisor of a, this means b is not unit, so $(b) \neq I$.

b is not a associate of a, which is $b \neq ea$ for some unit e. So (b) exists some element not in (a)

□

练习 3.3.3. Suppose two principal ideal domains (PIDs) I and I_0, with I_0 is a subring of I. If a, $b \in I_0$ and d is the greatest common divisor of a and b in I_0, then d is also the greatest common divisor of a and b in I.

证明. I and I_0 are PIDs, so it ensures the existence of gcd of a and b in I_0 and in I.

1. Prove d is common divisor of a and b in I:

   d is the gcd of a and b in I_0. This means we can write

   $$d|a,\ d|b \Longrightarrow a = da_1,\ b = db_1, \quad a_1,\ b_1 \in I_0.$$

   Notice I_0 is a subring of I. So a, b, d, a_1, b_1 are also in I. This means d is a common divisor of a and b in I as well.

2. Prove d is the gcd of a and b in I:

   By Exercise 3.3.1, the greatest common divisor d of a and b in I_0 has the format:

   $$d = sa + tb$$

   Notice a, b, s, t are also in I. So this equation holds in I as well.

   Suppose any common divisor c of a and b in I.

   $$c|a,\ c|b \Longrightarrow c|sa + tb \Longleftrightarrow c|d$$

   So, d is the gcd of a and b in I.

□

3.4 Euclidean Domain (欧氏环)

备注 3.4.1. A comparison between integral domain and field:

ID	Field
$ab = ba$	$ab = ba$
$1a = a1 = a$	$1a = a1 = a$
$ab = 0 \Longrightarrow a = 0,$ or $b = 0$	$ab = 0 \Longrightarrow a = 0,$ or $b = 0$
	$\forall a, \exists a^{-1}$

定义 3.4.1. An integral domain I is called a Euclidean Domain (ED) if

1. there is a **size function** ϕ from the set of all non-zero elements of I to the set of non-zero integers denoted by $\mathbb{N}_+ = \{n \in \mathbb{N} | n > 0\}$;

2. Given a non-zero element $a \in I$, any element b has the form of

$$b = qa + r \quad (q, r \in I)$$

where $r = 0$, or $\phi(r) < \phi(a)$.

例子 3.4.1. The ring of integer numbers is an ED.

证明. This is because:

1. we can have the size function

$$\phi(a) = |a| \quad (|a| \text{ is the absolute value of integer } a)$$

2. Given non-zero integer $a \neq 0$, any integer b can be written as

$$b = qa + r$$

where $r = 0$, or $\phi(r) = |r| < |a| = \phi(a)$.

□

定理 3.4.1. Any Euclidean Domain I is a Principal Ideal Domain (PID), is a Unique Factorization Domain (UFD).

证明. Consider an ideal U in I.

1. If $0 \in U$, then $U = (0)$.

2. If U has non-zero element. By definition of ED, there is a size function ϕ such that every non-zero element $x \in U$ has an integer $\phi(x) > 0$. Then there exists a minimum integer among these integers $\phi(x)$, denote it as $\phi(a)$ such that for every non-zero element $x \in U$ with

$$\phi(a) \leq \phi(x), \quad x \neq 0,\ x \in U$$

By Definition of ED, for any element $b \in U \subset I$, it has the form

$$b = qa + r$$

where

$$r = 0, \text{ or } \phi(r) < \phi(a)$$

Since $a, b \in U$, $r = b - qa \in U$.

If $r \neq 0$, then $r \in U$ with $\phi(r) < \phi(a)$, which contradicts with the presumption of $\phi(a) \leq \phi(x)$, for any non-zero element $x \in U$.

Thus, it should be

$$r = 0 \Longrightarrow b = qa \Longrightarrow U = (a)$$

□

备注 3.4.2. By Theorem 3.4.1 and the previous example that shows the ring of integer numbers is a ED, we know the ring of integer numbers is a UFD.

备注 3.4.3. A common example of ED is a polynomial ring on a field.

引理 3.4.1. Suppose $I[x]$ is a polynomial ring over an integral domain. The leading coefficient of an element of $g(x) \in I[x]$ with

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

is denoted by a_n. Suppose a_n is an invertible element (unit) of I. Then, any element $f(x) \in I[x]$ has the form

$$f(x) = q(x)g(x) + r(x), \quad (q(x),\, r(x) \in I[x])$$

where

$$r(x) = 0, \text{ or } deg(r(x)) < deg(g(x)) = n$$

证明. 1. If $f(x) = 0$ or $deg(f(x)) < n$, then use

$$q(x) = 0,\, r(x) = f(x) \Longrightarrow q(x)g(x) + r(x) = 0g(x) + f(x) = f(x).$$

2. Now assume $deg(f(x)) \geq n$ with

$$f(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0 \quad (m \geq n)$$

Since a_n is invertible, we use

$$q_1(x) = a_n^{-1} b_m x^{m-n}.$$

Then,

$$\begin{aligned}
&f(x) - q_1(x)g(x) \\
=&(b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0) \\
&- (a_n^{-1} b_m x^{m-n} a_n x^n + a_n^{-1} b_m x^{m-n} a_{n-1} x^{n-1} + \ldots) \\
=&b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0 - (b_m x^m + a_n^{-1} b_m x^{m-n} a_{n-1} x^{n-1} + \ldots) \\
=&f_1(x)
\end{aligned}$$

where $f_1(x) = 0$ or $deg(f_1(x)) < m = deg(f(x))$.

If $f_1(x) = 0$ or $deg(f_1(x)) < n$, then let $q(x) = q_1(x)$, we have $f(x) = q(x)g(x) + r(x) = q_1(x)g(x) + f_1(x)$.

If $deg(f_1(x)) \geq n$, proceed the same step on $f_1(x)$:

$$f_1(x) - q_2(x)g(x) = f(x) - [q_1(x) + q_2(x)]g(x) = f_2(x)$$

and so on, until we have $f_i(x) = 0$ or $deg(f_i(x)) < n$, with

$$f(x) = [q_1(x) + q_2(x) + \ldots + q_i(x)]g(x) + f_i(x)$$

□

Lemma 3.4.1 leads to the following theorem:

定理 3.4.2. A polynomial ring $F[x]$ over a field F is an ED.

证明. By definition of ED, we need to show:

1. We can construct the size function by mapping the polynomial to its degree:

$$\phi(f(x)) = deg(f(x)), \quad f(x) \in F[x]$$

2. Assume a non-zero element $g(x) \in F[x]$. Let the leading coefficient of $g(x)$ denoted by $a_n \neq 0$. $a_n \in F$, by definition of field, any non-zero element in a field has its inverse. So a_n is invertible in F. Then by Lemma 3.4.1, any element $f(x) \in F[x]$ has the form

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

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

□

备注 3.4.4. We have shown ED is a PID, and a PID is a UFD. The inverse is not necessarily true.

$$ED \subset PID \subset UFD.$$

By Theorem 3.4.2, $F[x]$ over a field F is ED, is also PID, is also UFD.

练习 3.4.1. Prove that a field is a ED.

证明. Suppose a field F. It is a ED, since

1. Consider the size function

$$\phi : a \in F \longrightarrow 1 \in N, \quad a \in F, a \neq 0$$

It is a mapping from the set of non-zero elements of F to N.

2. Given any non-zero element $a \in F$, we can write for any element $b \in F$ as

$$b = ba^{-1}a + 0$$

here we admit $q = ba^{-1}$ and $r = 0$.

So a field F is an ED. □

练习 3.4.2. Consider a field of rational numbers F. $F[x]$ is the polynomial ring over F. What is the equivalent principal ideal of the ideal

$$(x^2+1, x^5+x^3+1)?$$

解答. From

$$\begin{aligned}&(x^5+x^3+1)-x^3(x^2+1)=1\\ \Longrightarrow &1\in(x^2+1,x^5+x^3+1)\\ \Longrightarrow &(1)=(x^2+1,x^5+x^3+1)\end{aligned}$$

练习 3.4.3. Prove a ring

$$R=\{a+bi|a,b\in\mathbb{Z}\}$$

is an ED, by setting the size function

$$\phi(a)=|a|^2$$

证明. Denote the set of non-zero elements in R as

$$R^*=R/\{0\}$$

1. Consider the function

   $$\phi:\alpha=a+bi\in R^*\longrightarrow|\alpha|^2=a^2+b^2\in N$$

   which is a mapping from R^* to N. So ϕ is a size function.

2. Suppose any element $\alpha=a+bi\in R^*$. Then in the *field of complex numbers*, there is an inverse

   $$\alpha^{-1}=\frac{a-bi}{\phi(\alpha)}=\frac{a-bi}{a^2+b^2}$$

   such that

   $$\alpha^{-1}\alpha=\frac{(a-bi)(a+bi)}{a^2+b^2}=\frac{a^2+b^2}{a^2+b^2}=1$$

   Consider any element $\beta=c+di\in R$. Then

   $$\beta=\beta\alpha^{-1}\alpha$$

Let

$$\begin{aligned}\lambda' &= \beta\alpha^{-1} \\ &= (c+di)\frac{a-bi}{a^2+b^2} \\ &= k'+l'i\end{aligned}$$

with k' and l' rational numbers, since $k'+l'i$ is in the field of complex numbers.

Notice that $k'+l'i$ is not necessarily in R.

For the next step, we find integers k and l such that

$$|k'-k| \le \frac{1}{2}, \quad |l'-l| \le \frac{1}{2}$$

with

$$|k'-k|^2 \le \frac{1}{4}, \quad |l'-l|^2 \le \frac{1}{4}$$

Let $\lambda = k+li$, so

$$\begin{aligned}\beta &= \lambda'\alpha = \lambda\alpha + (\lambda'-\lambda)\alpha \\ &= \lambda\alpha + \rho\end{aligned}$$

with $\rho = (\lambda'-\lambda)\alpha = \beta - \lambda\alpha$.

By our assumption, $\beta \in R$.

Note that $\lambda\alpha = (k+li)\alpha$. $\alpha \in R^* \subset R$. k and l are integers, so $k+li \in R$. This implies that $\lambda\alpha \in R$. Thus, $\rho = \beta - \lambda\alpha \in R$.

Here we have either $\rho = 0$, or

$$\begin{aligned}|\rho|^2 = |\beta-\lambda\alpha|^2 &= |(\lambda'-\lambda)\alpha|^2 \\ &= |\Big(k'+l'i-(k+li)\Big)\alpha|^2 \\ &= |\Big((k'-k)+(l'-l)i\Big)\alpha|^2 \\ &= \Big((k'-k)^2+(l'-l)^2\Big)|\alpha|^2 \\ &\le \Big(\frac{1}{4}+\frac{1}{4}\Big)|\alpha|^2 = \frac{1}{2}|\alpha|^2 < |\alpha|^2\end{aligned}$$

This means $\phi(\rho) < \phi(\alpha)$.

Thus, R is ED.

□

3.5 Factorization in Polynomial Ring(多项式环上的分解)

备注 3.5.1. We know: F is a field, then $F[x]$ is UFD (By Theorem 3.4.2, $F[x]$ over a field F is ED, is also PID, is also UFD.)

We want to relax the condition of a field, in this section we want to show: if I is UFD, then $I[x]$ is also UFD.

$$\text{Field} \subset ED \subset PID \subset UFD \subset ID \subset \text{commutative ring} \subset \text{ring}.$$

定义 3.5.1. A polynomial is **irreducible**, if it is prime polynomial. A polynomial is **reducible**, if it has proper divisor.

备注 3.5.2. Some useful facts show in the following:

1. **Irreducible element** in a **domain** (a nonzero ring with $ab = 0 \Longrightarrow a = 0, \text{ or } b = 0$):
   - NOT zero
   - NOT invertible, which is NOT unit
   - NOT product of 2 non-invertible elements
2. **Prime element** a in commutative ring: $a|bc \Longrightarrow a|b, \text{ or } a|c$.
3. In ID:
   - Prime element $\Longrightarrow$ irreducible element.
   - Irreducible element $\not\Longrightarrow$ prime element.
4. In UFD:

- Prime element $\Longleftrightarrow$ irreducible element.

From now on, we focus on $I[x]$ over UFD I.

引理 3.5.1. Fact (A): The only invertible elements in $I[x]$ are invertible elements of I.

证明. Invertible elements of I is also invertible elements of $I[x]$.

On the other hand, by contradiction, assume $f(x)$ is invertible in $I[x]$. Then there is

$$f(x)g(x) = 1, \quad (g(x) \in I[x])$$

So, by $deg(1) = 0$,

$$deg(f(x)) = deg(g(x)) = 0$$

This implies $f(x) \in I$ and $g(x) \in I$.

□

定义 3.5.2. Consider an element $f(x) \in I[x]$ as:

$$f(x) = a_0 + a_1x + \ldots + a_nx^n. \tag{3.8}$$

Since I is UFD (by our presumption in this section), and $a_0, a_1, \ldots, a_n \in I$, there exists a $gcd(a_0, a_1, \ldots, a_n)$.

An element $f(x) \in I[x]$ is a **Primitive Polynomial (PP)**, if the gcd of its coefficients $gcd(a_0, a_1, \ldots, a_n)$ is invertible (unit).

备注 3.5.3. PP has the following properties:

1. PP is non-zero: since if a polynomial is zero, then $gcd(0, 0, \ldots, 0)$ does not exist, it can be any number in I.

2. If a PP $f(x)$ is reducible, then

$$f(x) = g(x)h(x) \tag{3.9}$$

with

$$0 < deg(g(x)) < deg(f(x)),$$
$$0 < deg(h(x)) < deg(f(x)).$$

证明. First note that: For $f(x) = g(x)h(x)$, we have:

$$deg(f(x)) = deg(g(x)) + deg(h(x)).$$

It suffices to show $deg(g(x)) > 0$: By contradiction. Assume $f(x) = ah(x)$ by setting $g(x) = a$ for some constant $a \in I$, which implies $deg(g(x)) = 0$.

Since $f(x)$ is PP, so the gcd of its coefficients is invertible.

$$gcd(\text{coefficients of } f(x)) = a \times gcd(\text{coefficients of } h(x))$$
$$\Longrightarrow a \text{ is invertible, by Theorem 3.1.3.}$$

This means $g(x) = a$ is invertible, so $g(x) = a$ is not a proper divisor, thus $f(x)$ is not reducible, which contradicts to our presumption that $f(x)$ is reducible.

So, we we have shown that $deg(g(x)) > 0$, which means $0 < deg(g(x)) < deg(f(x))$ and $0 < deg(h(x)) < deg(f(x))$ since $deg(f(x)) = deg(g(x)) + deg(h(x))$.

□

例子 3.5.1. Consider $I = \mathbb{Z}$ the ring of integers ($\mathbb{Z}$ is ED and thus is UFD). Take one element

$$f(x) = 2 + 2x = 2(1 + x)$$

The gcd of its coefficients $gcd(2, 2) = 2$ is not invertible in $I = \mathbb{Z}$. So, $f(x)$ is not PP in $I[x]$.

$f(x)$ is reducible though, with

$$f(x) = 2(1 + x)$$

where by taking $g(x) = 2$ and $h(x) = 1 + x$: $g(x) = 2$ is not invertible in I, and $h(x) = 1 + x \notin I$ is thus also not invertible. So $g(x) = 2$ and $h(x) = 1 + x$ are proper divisors of $f(x)$.

But it is obvious to see

$$deg(g(x)) = 0$$
$$0 < deg(h(x)) = 1 = deg(f(x)).$$

引理 3.5.2. Given $f(x) = g(x)h(x)$, $f(x)$ is PP iff $g(x)$ and $h(x)$ are PP.

证明. Assume

$$g(x) = a_n x^n + \ldots + a_1 x + a_0$$
$$h(x) = b_m x^m + \ldots + b_1 x + b_0$$

and

$$\begin{aligned} f(x) &= g(x)h(x) \\ &= c_{m+n} x^{m+n} + \ldots + c_1 x + c_0 \end{aligned}$$

where

$$c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0.$$

We prove this lemma in two parts:

1. $f(x)$ is PP $\Longrightarrow$ $g(x)$ and $h(x)$ are PP.

   By contradiction: assume $g(x)$ is not PP. This implies that $gcd(a_n, \ldots, a_1, a_0) = a$ is not invertible.

   On the other hand, we know

   $$a|a_0,\ a|a_1, \ldots, a|a_n \Longrightarrow a|c_i,\ \forall i$$

   This means the coefficients of $f(x)$ has common divisor a.

   Statement: *If a as the common divisor of the coefficients of $f(x)$ is not invertible, then the gcd of the coefficients of $f(x)$ is not invertible*: Because by contradiction: let $c = gcd(c_{m+n}, \ldots, c_1, a_0)$, and c is

invertible. Since c is the gcd, $a|c$, this means $c = ax$ for some x. Since c is invertible, we have $cc^{-1} = 1$. Thus, $cc^{-1} = axc^{-1} = a(xc^{-1} = 1$, this means a is invertible, contradiction to our presumption that c is not invertible.

By this statement, we know the gcd of coefficients of $f(x)$ is not invertible. So $f(x)$ is not PP, by Definition 3.5.2. We observe contradiction to the presumption that $f(x)$ is PP. So we have proved the argument: $f(x)$ is PP $\Longrightarrow$ $g(x)$ and $h(x)$ are PP.

2. $g(x)$ and $h(x)$ are PP $\Longrightarrow$ $f(x)$ is PP.

   This is to find $c = gcd(c_{m+n}, \ldots, c_1, c_0)$ is invertible. Again, by contradiction: assume c is not invertible.

   Not that $c \in I$, c is not invertible and $c \neq 0$. Since I is UFD, we have unique factorization of c, denoted by

   $$c = pp_1 \ldots p_k$$

   where p, p_1, ..., p_k are prime elements of I. p divides c and thus divides all c_i.

   Statement: *If a common divisor p of a_0, a_1, ..., a_n is not invertible, then $a = gcd(a_0, a_1, \ldots, a_n)$ is not invertible:* Because if a is invertible, then $a^{-1}a = 1$. a is the gcd, so $p|a$, which means $a = xp$ for some x. Together we have $1 = a^{-1}a = a^{-1}xp = (a^{-1}x)p$ that means p is invertible, contradiction!

   By this statement, since p is prime element, p is not invertible. Thus, p can not be the common divisor of coefficients of $g(x)$ or $h(x)$ that are PP by assumption which means the gcd of their coefficients a and b are invertible.

   Let a_r be the first coefficient of $g(x)$ that p does not divide. Let b_s be the first coefficient of $h(x)$ that p does not divide.

Consider the coefficient c_{r+s} of $f(x)$:

$$\begin{aligned} c_{r+s} =& a_r b_s + a_{r+1} b_{s-1} + b_{r+2} b_{s-2} + \dots \\ &+ a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \dots \end{aligned}$$

p divides c_{r+s}, and p divides all elements on the right hand side that include $a_r b_s$. This means either p divides a_r or p divides b_s, but this contradicts to what we presume that a_r and b_s are elements that p does not divide.

Thus, we have just shown by contradiction that $g(x)$ and $h(x)$ are PP $\Longrightarrow$ $f(x)$ is PP.

□

备注 3.5.4. Consider field of fraction Q of I. Obviously,

$$I[x] \subseteq Q[x]$$

By Theorem 3.4.2, a polynomial ring $F[x]$ over a field F is an ED, thus is PID, thus is UFD. Q is a field, so $Q[x]$ is ED, PID, UFD. We want to use this to derive $I[x]$ is also UFD.

引理 3.5.3. Every non-zero polynomial $f(x) \in Q[x]$ has the form

$$f(x) = \frac{b}{a} f_0(x) \tag{3.10}$$

where $0 \neq a \in I$, $b \in I$, $f_0(x)$ is a PP in $I[x]$.

If there exists $g_0(x)$ with

$$f(x) = \frac{b'}{\prime} g_0(x),$$

then

$$g_0(x) = e f_0(x) \quad (e \in I \text{ is invertible.}$$

证明. By definition of field of fraction at 2.10.1, Q is a field of fraction of I means that Q has element in the format of $\frac{b}{a}$ where $b, a \in I$ and $a \neq 0$. This implies

$$f(x) = \frac{b_0}{a_0} + \frac{b_1}{a_1} x + \dots + \frac{b_n}{a_n} x^n \quad (a_i,\, b_i \in I)$$

Denote $a = a_0 a_1 \dots a_n$, then

$$f(x) = \frac{1}{a}(b_0 a_1 \dots a_n + b_1 a_0 a_2 \dots a_n x + \dots + a_0 \dots a_{n-1} b_n x^n)$$

Denote

$$\begin{aligned} c_0 &= b_0 a_1 \dots a_n \\ c_1 &= b_1 a_0 a_2 \dots a_n \\ &\dots \\ c_n &= a_0 \dots a_{n-1} b_n, \end{aligned}$$

then

$$f(x) = \frac{1}{a}(c_0 + c_1 x + \dots + c_n x^n)$$

Let $b = gcd(c_0, c_1, \dots, c_n)$, then

$$\begin{aligned} f(x) &= \frac{b}{a}(\frac{c_0}{b} + \frac{c_1}{b}x + \dots + \frac{c_n}{b}x^n) \\ &= \frac{b}{a} f_0(x) \end{aligned}$$

Here we denote

$$f_0(x) = \frac{c_0}{b} + \frac{c_1}{b}x + \dots + \frac{c_n}{b}x^n.$$

To show $f_0(x)$ is PP is to show $gcd(\frac{c_0}{b}, \frac{c_1}{b}, \dots, \frac{c_n}{b})$ is invertible.
By Exercise 3.2.1:
[in an UFD,

$$a_1 = db_1,\ a_2 = db_2, \dots, a_n = db_n$$

$d = gcd(a_1, a_2, \dots a_n)$ iff b_1, b_2, ..., b_n are coprime, which is $gcd(b_1, b_2, \dots, b_n)$ is invertible.]

Here we have

$$c_0 = b\frac{c_0}{b},\ c_1 = b\frac{c_1}{b},\ \dots, c_n\ b\frac{c_n}{b}$$

with $b = gcd(c_0, c_1, \dots, c_n)$. Thus, this implies that $\frac{c_0}{b}$, $\frac{c_1}{b}$, ..., $\frac{c_n}{b}$ coprime, which is $gcd(\frac{c_0}{b}, \frac{c_1}{b}, \dots, \frac{c_n}{d})$ is invertible. This means $f_0(x)$ is PP.

Next, let us assume $f(x) = \frac{d}{c}g_0(x)$, $0 \neq c, d \in I$, and $g_0(x)$ is PP in $I[x]$ with

$$g_0(x) = g_0 + g_1x + \ldots + g_nx^n$$

$$\begin{aligned} bcf_0(x) &= ac(\frac{b}{a}f_0(x)) = acf(x) \\ &= ac\frac{d}{c}g_0(x) = adg_0(x) \end{aligned}$$

Denote $h(x) = adg_0(x) = h_0 + h_1x + \ldots + h_nx^n$.

If we see

$$h_0 = bc\frac{c_0}{b},\ h_1 = bc\frac{c_1}{b},\ \ldots, h_n = bc\frac{c_n}{b}$$

$f_0(x)$ is PP implies that $gcd(\frac{c_0}{b}, \frac{c_1}{b}, \ldots, \frac{c_n}{d})$ is invertible, which implies that

$$bc = gcd(h_0, h_1, \ldots, h_n)$$

If we see

$$h_0 = adg_0,\ h_1 = adg_1,\ \ldots, h_n = adg_n.$$

$g_0(x)$ is PP implies that

$$ad = gcd(h_0, h_1, \ldots, h_n).$$

This means both bc and ad are gcd of coefficients of $h(x)$. We thus have

$$bc = ead, \quad e \in I \text{ is invertible .}$$

This leads to

$$bcf_0(x) = adg_0(x) \Longrightarrow eadf_0(x) = adg_0(x) \Longrightarrow ef_0(x) = g_0(x).$$

□

引理 3.5.4. Suppose $f_0(x) \in I[x]$ is PP, $f_0(x)$ is reducible in $I[x]$ iff $f_0(x)$ is reducible in $Q[x]$.

证明. We prove this lemma by two parts.

1. To prove $f_0(x)$ is reducible in $Q[x] \Longrightarrow f_0(x)$ is reducible in $I[x]$.

   Assume $f_0(x)$ is reducible in $Q[x]$. Then, $f_0(x)$ has proper divisors. $f_0(x)$ is PP in $I[x] \subseteq Q[x]$. By property 2 in Memo 3.5.3,

   $$f_0(x) = g(x)h(x)$$

   with $g(x)$, $h(x) \in Q[x]$, and

   $$0 < deg(g(x)),\ deg(h(x)) < deg(f_0(x)).$$

   $g(x) \in Q[x]$ and $h(x) \in Q[x]$, by Lemma 3.5.3, there are

   $$g(x) = \frac{b}{a}g_0(x)$$
   $$h(x) = \frac{b'}{a'}h_0(x)$$

   where a, b, a', $b' \in I$ with $g_0(x) \in I[x]$ and $h_0(x) \in I[x]$ are PP.

   So,

   $$f_0(x) = g(x)h(x) = \frac{b}{a}\frac{b'}{a'}g_0(x)h_0(x) = \frac{bb'}{aa'}g_0(x)h_0(x)$$

   with $bb' \in I$, $aa' \in I$, and $g_0(x)h_0(x) \in I[x]$ are PP by Lemma 3.5.2.

   Note that $f_0(x) = 1 \cdot f_0(x)$, with $1 \in I$. By Lemma 3.5.3 again,

   $$f_0(x) = f_0(x),\ f_0(x) = \frac{bb'}{aa'}g_0(x)h_0(x)$$
   $$\Longrightarrow f_0(x) = eg_0(x)h_0(x), \quad (e \in I \text{ is invertible (unit)}.$$

   Obviously, $eg_0(x) \in I[x]$ and $h_0(x) \in I[x]$.

   But from $g(x) = \frac{b}{a}g_0(x)$, $deg(g(x)) = deg(g_0(x)) = deg(eg_0(x))$. From $h(x) = \frac{b'}{a'}h_0(x)$, $deg(h(x)) = deg(h_0(x))$. By $deg(g(x)) > 0$ and $deg(h(x)) > 0$, we know $deg(eg_0(x)) > 0$ and $deg(h_0(x)) > 0$. This means $eg_0(x) \notin I$ and $h_0(x) \notin I$, so they are not invertible elements in $I[x]$ according to Lemma 3.5.1.

   By Theorem 3.1.3: In an ID I, $a \neq 0 \in I$ has proper divisor iff $a = bc$ where b and c are not unit(invertible), since $eg_0(x)$ and $h_0(x)$ are not

invertible, $f_0(x) = eg_0(x)h_0(x)$ has proper divisor in $I[x]$. This means $f_0(x)$ is reducible in $I[x]$.

2. To prove $f_0(x)$ is reducible in $I[x] \Longrightarrow f_0(x)$ is reducible in $Q[x]$: If $f_0(x)$ is PP and reducible in $I[x]$, then by Property 2 in Memo 3.5.3, we can write

$$f_0(x) = g(x)h(x)$$

with $0 < deg(g(x)), deg(h(x)) < deg(f_0(x))$, $g(x) \in I[x] \subseteq Q[x]$, and $h(x) \in I[x] \subseteq Q[x]$.

By Lemma 3.5.1, invertible elements of $Q[x]$ are only those invertible elements of Q. Since $deg(g(x)) > 0$ and $deg(h(x)) > 0$, $g(x) \notin Q$ and $h(x) \notin Q$, this means $g(x)$ and $h(x)$ are not invertible in $Q[x]$. By Theorem 3.1.3 again, this implies $f_0(x) = g(x)h(x)$ has proper divisor in $Q[x]$. This implies $f_0(x)$ is reducible in $Q[x]$.

□

引理 3.5.5. $f_0(x) \in I[x]$ is PP, $deg(f_0(x)) > 0$. Then $f_0(x)$ has unique factorization in $I[x]$.

证明. To show $f_0(x)$ has unique factorization in $I[x]$ is to show $f_0(x)$ is a finite product of irreducible polynomials in $I[x]$. We consider the following cases:

1. If $f_0(x)$ is irreducible, then it is trivial: let $f_0(x) = f_0(x)$.

2. If $f_0(x)$ is reducible, then by Property 2 in Memo 3.5.3 , we can write

$$f_0(x) = g_0(x)h_0(x)$$

with $0 < deg(g(x)), deg(h(x)) < deg(f_0(x))$, $g(x) \in I[x]$, and $h(x) \in I[x]$.

By Lemma 3.5.2, $f_0(x)$ is PP in $I[x]$ implies that $g_0(x)$ and $h_0(x)$ are PP in $I[x]$.

If $g_0(x)$ and $h_0(x)$ are reducible, proceed further to write $g_0(x) = g_1(x)h_1(x)$ and $h_0(x) = g_2(x)h_2(x)$, and so on.

Since $deg(f_0(x))$ is finite, this procedure will stop finitely, with

$$f_0(x) = p_0^{(1)}(x)p_0^{(2)}(x)\dots p_0^{(r)}(x),$$

with $p_0^{(i)}(x)$ irreducible in $I[x]$, for $i = 1, \dots, r$.

Next, assume another factorization of $f_0(x)$ with

$$f_0(x) = q_0^{(1)}(x)q_0^{(2)}(x)\dots q_0^{(s)}(x),$$

with $q_0^{(i)}(x)$ irreducible in $I[x]$, for $i = 1, \dots, s$.

Since $f_0(x)$ is PP in $I[x]$, by Lemma 3.5.2, $q_0^{(i)}(x)$ is also PP in $I[x]$, for $i = 1, \dots s$.

On the other hand, since $p_0^{(i)}(x)$ are irreducible in $I[x]$, by Lemma 3.5.4, $p_0^{(i)}(x)$ are irreducible in $Q[x]$, for $i = 1, \dots, r$. Analogously, $q_0^{(i)}(x)$ are irreducible in $Q[x]$, for $i = 1, \dots, s$

$Q[x]$ is UFD, and $f_0(x)$ has two factorizations in $Q[x]$:

$$f_0(x) = p_0^{(1)}(x)p_0^{(2)}(x)\dots p_0^{(r)}(x),$$
$$f_0(x) = q_0^{(1)}(x)q_0^{(2)}(x)\dots q_0^{(s)}(x).$$

Recall that $p_0^{(i)}(x)$ and $q_0^{(i)}(x)$ are irreducible in $Q[x]$. By UFD Definition 3.1.8, this implies $r = s$ and after suitable rearrangement

$$q_0^{(i)}(x) = \frac{b_i}{a_i} p_0^{(i)}(x)$$

where $\frac{b_i}{a_i} \in Q$ is invertible element of Q, since Q is a field and every non-zero element in Q is invertible.

Note that $q_0^{(i)}(x) = q_0^{(i)}(x) \in I[x]$, $q_0^{(i)}(x) = \frac{b_i}{a_i} p_0^{(i)}(x)$ with $p_0^{(i)}(x) \in I[x]$, and $a_i, b_i \in I$. By Lemma 3.5.3, we have:

$$q_0^{(i)}(x) = e p_0^{(i)}(x)$$

where $e \in I$ is invertible.

This implies that $f_0(x)$ has unique factorization in $I[x]$.

□

We are now ready to prove the main theorem.

定理 3.5.1. If I is UFD, then $I[x]$ is also UFD.

证明. Let $f(x) \in I[x]$, with

$$f(x) = c_0 + c_1x + \ldots + c_nx^n$$

where c_0, c_1, ..., $c_n \in I$.

We have the following cases:

1. If $f(x) \in I$, then $f(x)$ has unique factorization since I is UFD.
2. If $f(x) \in I[x]$ is PP, then by Lemma 3.5.5, $f(x)$ has unique factorization in $I[x]$.
3. If $f(x)$ is not PP in $I[x]$, which is the gcd of coefficients of $f(x)$ is not invertible (unit).

   - Write

     $$f(x) = df_0(x)$$

     where $d = gcd(c_0, c_1, \ldots, c_n)$ and d is not invertible in I.
     Specifically,

     $$\begin{aligned} f(x) &= c_0 + c_1x + \ldots + c_nx^n \\ &= d(\frac{c_0}{d} + \frac{c_1}{d}x + \ldots + \frac{c_n}{d}x^n) \\ &= df_0(x) \end{aligned}$$

     where $f_0(x) = \frac{c_0}{d} + \frac{c_1}{d}x + \ldots + \frac{c_n}{d}x^n$.
     Note that

     $$c_0 = d \cdot (\frac{c_0}{d}),\ c_1 = d \cdot (\frac{c_1}{d}),\ \ldots, c_n = d \cdot (\frac{c_n}{d})$$

     By Exercise 3.2.1:

[in an UFD,

$$a_1 = db_1,\ a_2 = db_2, \ldots, a_n = db_n$$

$d = gcd(a_1, a_2, \ldots a_n)$ iff b_1, b_2, ..., b_n are coprime, which is $gcd(b_1, b_2, \ldots, b_n)$ is invertible.]

Here we have

$$\begin{aligned} & c_0 = d \cdot (\frac{c_0}{d}),\ c_1 = d \cdot (\frac{c_1}{d}), \ldots, c_n = d \cdot (\frac{c_n}{d}), \\ & d = gcd(c_0, c_1, \ldots, c_n) \\ \iff & \frac{c_0}{d}, \frac{c_1}{d}, \ldots, \frac{c_n}{d} \text{ coprime} \\ \Longrightarrow & f_0(x) = \frac{c_0}{d} + \frac{c_1}{d}x + \ldots + \frac{c_n}{d}x^n \text{ is PP .} \end{aligned}$$

- Since $d \in I$, d is not invertible and $d \neq 0$, by I is UFD, d has unique factorization:

$$d = p_1 p_2 \ldots p_m$$

where p_i is prime element of I, $i = 1, \ldots, m$.

- Since $f_0(x)$ is PP in $I[x]$, from Lemma 3.5.5, $f_0(x)$ has unique factorization:

$$f_0(x) = p_0^{(1)}(x) p_0^{(2)}(x) \ldots p_0^{(r)}(x)$$

where $p_0^{(i)}(x)$ is irreducible and is also PP by Lemma 3.5.2, for $i = 1, \ldots, r$.

- So, $f(x)$ has factorization in $I[x]$:

$$f(x) = p_1 p_2 \ldots p_m p_0^{(1)}(x) p_0^{(2)}(x) \ldots p_0^{(r)}(x)$$

- Next, assume $f(x)$ has another factorization in $I[x]$:

$$f(x) = q_1 q_2 \ldots q_n q_0^{(1)}(x) q_0^{(2)}(x) \ldots q_0^{(t)}(x)$$

where $q_i \in I$, $q_0^{(j)}(x) \in I[x] \notin I$, and they are irreducible in $I[x]$, for $i = 1, \ldots, n$ and $j = 1, \ldots, t$.

We know that:

- q_i is prime element in I: Because otherwise, if q_i is not prime element, then q_i is reducible in UFD I, and thus reducible in $I[x]$.
- $q_0^{(j)}(x)$ is PP in $I[x]$: Because otherwise, if $q_0^{(j)}(x)$ is not PP in $I[x]$, then its gcd of coefficients of $q_0^{(j)}(x)$, denoted by gcd_q, is not invertible. We can write a factorization of $q_0^{(j)}(x)$ as:

$$q_0^{(j)}(x) = gcd_q \cdot q_1^{(j)}(x)$$

where gcd_q is not invertible (unit), so is a proper divisor of $q_0^{(j)}(x)$. Thus, this means $q_0^{(j)}(x)$ is reducible, contradiction!

Since $q_0^{(j)}(x)$ is PP in $I[x]$ for $j = 1, \ldots, t$, by Lemma 3.5.2, $q_0^{(1)}(x)q_0^{(2)}(x)\ldots q_0^{(t)}(x)$ is PP in $I[x]$.

Recall

$$f(x) = \underbrace{p_1p_2\ldots p_m}_{\in I}\underbrace{p_0^{(1)}(x)p_0^{(2)}(x)\ldots p_0^{(r)}(x)}_{\text{PP in } I[x]}$$
$$f(x) = \underbrace{q_1q_2\ldots q_n}_{\in I}\underbrace{q_0^{(1)}(x)q_0^{(2)}(x)\ldots q_0^{(t)}(x)}_{\text{PP in } I[x]}$$

By Lemma 3.5.3, we have

$$\begin{aligned} f_0(x) &= p_0^{(1)}(x)p_0^{(2)}(x)\ldots p_0^{(r)}(x) \\ &= e\Big(q_0^{(1)}(x)q_0^{(2)}(x)\ldots q_0^{(t)}(x)\Big) \\ &= [eq_0^{(1)}(x)]q_0^{(2)}(x)\ldots q_0^{(t)}(x) \end{aligned} \tag{3.11}$$

where e is invertible in I.

So,

$$\begin{aligned} f(x) &= p_1p_2\ldots p_m f_0(x) \\ &= p_1p_2\ldots p_m e\Big(q_0^{(1)}(x)q_0^{(2)}(x)\ldots q_0^{(t)}(x)\Big) \\ &= q_1q_2\ldots q_n q_0^{(1)}(x)q_0^{(2)}(x)\ldots q_0^{(t)}(x) \\ \Longrightarrow & p_1p_2\ldots p_m e = q_1q_2\ldots q_n \\ \Longrightarrow & d = p_1p_2\ldots p_m = [e^{-1}q_1]q_2\ldots q_n \end{aligned} \tag{3.12}$$

Equation 3.11 shows two factorizations of $f_0(x)$ that is PP in $I[x]$. By Lemma 3.5.2, this factorization is unique, so

$$r = t,$$

and by proper rearrangement,

$$q_0^{(i)}(x) = e_i p_0^{(i)}(x),$$

where e_i is invertible in I, for $i = 1, \ldots, t = r$.

Equation 3.12 shows two factorization of $d \in I$. Since I is UFD, this factorization is unique, so

$$m = n,$$

and by proper rearrangement,

$$q_i = e_i' p_i,$$

where e_i' is invertible in I, for $i = 1, \ldots, n = m$.

Thus,

$$\begin{aligned} f(x) &= p_1 p_2 \ldots p_m p_0^{(1)}(x) p_0^{(2)}(x) \ldots p_0^{(r)}(x) \\ &= q_1 q_2 \ldots q_n q_0^{(1)}(x) q_0^{(2)}(x) \ldots q_0^{(t)}(x) \end{aligned}$$

with $q_i = e_i' p_i$, $q_0^{(i)}(x) = e_i p_0^{(i)}(x)$.

This means $f(x)$ has unique factorization in $I[x]$.

4. By the above cases, we have proved that $I[x]$ is UFD.

□

定理 3.5.2. If I is UFD, then $I[x_1, x_2, \ldots, x_n]$ is also UFD.

证明. Apply Theorem 3.5.1 under mathematical induction. □

备注 3.5.5. If I is ring of integers, it is UFD, thus $I[x]$ is UFD. But by Exercise 2.7.3 and the following Memo 2.7.7, $I[x]$ is not PID, since the principle $(2, x) \in I[x]$ is not the principal ideal:

证明. By contradiction: if $(2, x)$ is principal ideal, then it writes

$$\begin{aligned}
&(2, x) = (p(x)) \\
\Longrightarrow &2 \in (p(x)),\ x \in (p(x)) \\
\Longrightarrow &2 = q(x)p(x),\ x = h(x)p(x), \quad q(x),\ h(x) \in I[x] \\
\Longrightarrow &2 = q(x)p(x) \Longrightarrow p(x) = a \quad a \text{ is constant} \\
\Longrightarrow &x = h(x) \cdot a \Longrightarrow a = \pm 1 \\
\Longrightarrow &\ p(x) = \pm 1
\end{aligned}$$

But this contradicts to $p(x) \in (2, x)$ with the format

$$p(x) = 2a_0 + a_1 x + \ldots + a_n x^n, \quad a_i \in I, n \geq 0.$$

□

This gives a counter-example to show: $PID \Longrightarrow UFD$, but it is **not** necessary to have $UFD \Longrightarrow PID$.

练习 3.5.1. Suppose I is UFD. Q is field of fraction of I. Prove that if a polynomial $f(x) \in I[x]$ is reducible in $Q[x]$, then $f(x)$ is reducible in $I[x]$.

证明. Let $f(x) \in I[x]$ reducible in $Q[x]$. Then, by Lemma 3.5.3,

$$f(x) = \frac{b}{a} f_0(x)$$

where $f_0(x)$ is a PP in $I[x]$, with $0 \neq a, b \in I$.

Note that $0 \neq d = \dfrac{b}{a} \in Q$ and Q is a field, so $d \in Q \subset Q[x]$ is invertible.

We have the following argument: $f(x)$ is reducible in $Q[x] \implies f_0(x)$ is reducible in $Q[x]$. Because: $f(x)$ is reducible in $Q[x]$, then we can write

$$f(x) = g(x)h(x) \implies f_0(x) = d^{-1}f(x) = d^{-1}g(x)h(x), \quad g(x),\ h(x) \in Q[x]$$

So, $f_0(x)$ is reducible in $Q[x]$.

Since $f_0(x)$ is reducible in $Q[x]$, and is PP in $I[x]$, by Lemma 3.5.4, $f_0(x)$ is reducible in $I[x]$. □

练习 3.5.2. Let I be an Integral Domain. $I[x]$ is polynomial ring. $f(x) \in I[x]$, and $f(x) \notin I$. The leading coefficient of $f(x)$ is invertible in I. Prove: $f(x)$ has factorization in $I[x]$.

证明. Use the fact:

- a, $b \in I$. If $ab = e$, e is invertible in I, then a, b also invertible in I, because:

$$ab = e \implies abe^{-1} = ee^{-1} = 1 \implies a(be^{-1}) = 1 \implies a \text{ invertible}$$
$$ab = e \implies e^{-1}ab = e^{-1}e = 1 \implies (e^{-1}a)b = 1 \implies b \text{ invertible}$$

We want to show $f(x)$ has factorization as a product of finitely many irreducible polynomials.

1. If $f(x)$ is irreducible, then trivial by considering the factorization $f(x) = f(x)$.

2. If $f(x)$ is reducible in $I[x]$, then write

$$f(x) = g(x)h(x)$$

Here $g(x)$ and $h(x)$ are proper divisors of $f(x)$ in $I[x]$. ($g(x)$ and $h(x)$ are proper divisors of $f(x)$ means neither $g(x)$ nor $h(x)$ is invertible)

We want to show $g(x)$ and $h(x)$ not in I: By contradiction: If $g(x) = a \in I$, then $f(x) = ah(x)$. a times the leading coefficient of $h(x)$ is equal to the leading coefficient of $f(x)$ that is invertible. By the fact listed above, a is invertible and the leading coefficient of $h(x)$ is also invertible. Thus, $g(x) = a$ is invertible. However, this contradicts to our presumption that $g(x)$ and $h(x)$ are proper divisors of $f(x)$ in $I[x]$. So we have shown by contradiction that $g(x) \notin I$, which is $deg(g(x)) > 0$. Analogous argument can show $h(x) \notin I$, which is $deg(h(x)) > 0$.

In other words, we have shown

$$0 < deg(g(x)),\ deg(h(x)) < deg(f(x))$$

and the leading coefficient of $g(x)$ and $h(x)$ are invertible.

We can apply the same argument to $g(x)$ and $h(x)$. Since $deg(f(x))$ is finite, this chain of argument is finite and it ends with

$$f(x) = g(x)h(x) = g_0(x)g_1(x)\cdots g_n(x)h_0(x)h_1(x)\cdots h_m(x)$$

as a product of finitely many irreducible polynomials.

□

3.6 Root of Polynomial(多项式的根)

Consider polynomial ring $I[x]$ over an integral domain I.

定义 3.6.1. An element $a \in I$ is a root of the polynomial $f(x) \in I[x]$, if

$$f(a) = 0$$

定理 3.6.1. a is a root of $f(x) \in I[x]$ iff $x - a$ divides $f(x)$.

证明. We prove it by two parts.

1. $x - a$ divides $f(x) \implies a$ is a root of $f(x)$:

   Assume $x - a$ divides $f(x)$, then

   $$f(x) = (x - a)g(x).$$

   By polynomial substitution Theorem 2.6.3, we substitute x by a:

   $$f(a) = (a - a)g(a) = 0$$

   So, a is a root of $f(x)$.

2. a is a root of $f(x) \implies x - a$ divides $f(x)$:

   Assume a is a root of $f(x)$. Note $x - a$ has leading coefficient of 1 that is invertible in I, by Lemma 3.4.1, we have

   $$\begin{aligned}
   & f(x) = q(x)g(x) + r(x), \quad r(x) = 0, \text{ or } deg(r(x)) < deg(g(x)) \\
   \implies & f(x) = q(x)(x - a) + r, \quad r \in I \\
   \implies & f(a) = q(a)(a - a) + r \quad \text{(substitue } x \text{ by } a\text{)} \\
   \implies & 0 = r \quad \text{(by } a \text{ is a root of } f(x) \text{ with } f(a) = 0\text{)} \\
   \implies & f(x) = q(x)(x - a)
   \end{aligned}$$

Thus, $x - a$ divides $f(x)$.

□

定理 3.6.2. k distinct elements a_1, a_2, ..., a_k are roots of $f(x)$ iff $(x - a_1)(x - a_2)\dots(x - a_k)$ divides $f(x)$.

证明. Prove by two parts.

1. Assume $(x - a_1)(x - a_2)\dots(x - a_k)$ divides $f(x)$. This implies $x - a_1$ divides $f(x)$, $x - a_2$ divides $f(x)$, and so on. By Theorem 3.6.1, a_1, a_2, ..., a_k are roots of $f(x)$.

2. Assume a_1, a_2, ..., a_k are roots of $f(x)$. By Theorem 3.6.1, with a_1 is root of $f(x)$ implying $x - a_1$ divides $f(x)$,

$$\begin{aligned} & f(x) = (x - a_1)f_1(x) \\ \implies & 0 = f(a_2) = (a_2 - a_1)f_1(a_2) \quad \text{(substitute } x \text{ by } a_2 \text{ the root of } f(x)\text{)} \\ \implies & f_1(a_2) = 0 \quad \text{(by } a_2 - a_1 \neq 0 \text{ and } I \text{ is ID with no non-zero divisor)} \end{aligned}$$

So, a_2 is a root of $f_1(x)$. This means

$$\begin{aligned} f_1(x) &= (x - a_2)f_2(x), \\ f(x) &= (x - a_1)(x - a_2)f_2(x) \end{aligned}$$

Proceed with the process to exhaust all distinct roots of $f(x)$ for a_1, a_2, ..., a_k, we obtain

$$f(x) = (x - a_1)(x - a_2)\dots(x - a_k)f_k(x)$$

This means $(x - a_1)(x - a_2)\dots(x - a_k)$ divides $f(x)$.

□

推论 3.6.1. If $f(x)$ has degree of n, then $f(x)$ has at most n roots in I.

定义 3.6.2. $a \in I$ is a multiple root of $f(x)$, if $(x-a)^k$ divides $f(x)$ for an integer $k > 1$.

定义 3.6.3. Suppose a polynomial $f(x)$ with the format

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

It has a uniquely determined polynomial

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1,$$

called the **derivative** of $f(x)$.

Derivative of $f(x)$ applies the normal rules of derivative in mathematical analysis:

$$\begin{aligned}
&[f(x) + g(x)]' = f'(x) + g'(x) \\
&[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x) \\
&[f(x)^t]' = tf(x)^{t-1}f'(x)
\end{aligned}$$

定理 3.6.3. Given a root of $f(x)$ a, it is a multiple root iff $x - a$ divides $f'(x)$.

证明. Prove by two parts:

1. Assume a is multiple root of $f(x)$.

$$\begin{aligned}
&f(x) = (x-a)^k g(x) \quad (\text{integer } k > 1) \\
\Longrightarrow\ &f'(x) = (x-a)^k g'(x) + k(x-a)^{k-1}g(x) \\
\Longrightarrow\ &f'(x) = (x-a)^{k-1}[(x-a)g'(x) + kg(x)]
\end{aligned}$$

Thus, $x - a$ divides $f'(x)$

2. By contrapositive. Assume a is not a multiple root of $f(x)$. But since a is a root of $f(x)$, we have

$$\begin{aligned} & f(x) = (x-a)g(x), \quad x-a \text{ does not divide } g(x) \\ \Longrightarrow\ & f'(x) = (x-a)g'(x) + g(x) \\ \Longrightarrow\ & f'(a) = (a-a)g'(a) + g(a) = g(a) \neq 0 \end{aligned}$$

   So, a is not a root of $f'(x)$. By Theorem 3.6.1, $x-a$ does not divide $f'(x)$.

□

推论 3.6.2. Given an integral domain I, $a \in I$ is a multiple root of $f(x)$ iff $x-a$ divides the gcd of $f(x)$ and $f'(x)$.

练习 3.6.1. R is a quotient ring (residue-class ring) with modulo 16. How many roots for polynomial $x^2 \in R[x]$?

解答. x^2 has 4 roots: $x_1 = [0]$, $x_2 = [4]$, $x_3 = [8]$, $x_4 = [12]$ ($12^2 \, mod \, 16 = 144 \, mod \, 16 = 0$) .

练习 3.6.2. F is a quotient ring with modulo 3. Suppose a polynomial $f(x) \in F[x]$ with

$$f(x) = x^3 - x$$

Prove that $f(a) = 0$ for a is any element in $F = \{[0], [1], [2]\}$.

解答. Compute for each element $a \in F = \{[0], [1], [2]\}$. For example, $a = [2]$, then $f([2]) = (2^3 - 2) \, mod \, 3 = [2] - [2] = [0]$.

第四章　Field Extension (扩域)

4.1　Field Extension, Prime Field (域的扩张, 素域)

定义 4.1.1. Given a field F and E, if $F \subseteq E$, then E is a field extension of F.

备注 4.1.1. A field F has no non-zero divisor, has characteristic of either inf or prime number p.

$$charF = \text{inf}, \quad \text{or } charF = p.$$

We also denote

$$charF = \text{inf} \iff charF = 0.$$

定理 4.1.1. E is a field. Then,

1. If $charE = \text{inf}$, then $\mathbb{Q} \cong$ subfield of E, where $\mathbb{Q}$ is the field of rational numbers;
2. If $charE = p$, then $R/(p) \cong$ subfield of E, where R is the ring of integers and (p) is the principle ideal generated by p.

证明. E is a field, thus it has multiplicative identity e. This means E contains all elements of ne where $n \in R$.

Consider a map

$$\phi : R \longrightarrow R' = \{ne \,|\, \forall n \in R\}, \quad \phi(n) = ne$$

ϕ is a surjective homomorphism:

$$\phi(m+n) = (m+n)e = me + ne = \phi(m) + \phi(n)$$
$$\phi(mn) = (mn)e = mene = \phi(m)\phi(n)$$

1. $charE = \inf$ (or $charE = 0$).

   In this case,

   $$(m_1 - n_1)e = 0 \implies m_1 - n_1 = 0 \implies m_1 = n_1$$

   So, ϕ is isomorphism in this case. This implies $R \cong R'$. By Theorem 2.10.3, the field of fraction of R is isomorphic to the field of fraction of R'.

   E contains R', by Theorem 2.10.4, E contains the field of fraction of R'. On the other hand, the field of fraction of R is isomorphic to $\mathbb{Q}$ the field of rational numbers. Therefore, we just show $\mathbb{Q} \cong$ subfield of E.

2. $charE = p$ where p is prime.

   In this case, by Theorem 2.8.2, the kernel of ϕ, denoted by $\mathfrak{A} = ker(\phi)$, is an ideal of R, and $R/\mathfrak{A} \cong R'$. Here again $R' = \{ne \,|\, \forall n \in R\}$.

   In the next, we will show $\mathfrak{A} = (p)$:

   Because $p \longrightarrow pe = 0$, we have $p \in \mathfrak{A}$. This means $(p) \subseteq \mathfrak{A}$.

   By Lemma 3.3.2, R is a PID, then the prime element $p \in R$ generates a maximal ideal (p).

   Since $1 \longrightarrow e \neq 0$, this means $R \ni 1 \notin \mathfrak{A}$. This is $\mathfrak{A} \neq R$. This implies $\mathfrak{A} = (p)$ since (p) is a maximal ideal in R and $\mathfrak{A}$ is an ideal that contains (p).

   Therefore, we have $R/\mathfrak{A} \cong R' \implies R/(p) \cong R'$.

□

定义 4.1.2. If a field F has no proper subfield, then it is a **prime field**.

Using this concept of prime field at Definition 4.1.2, what Theorem 4.1.1 says is:

1. when $charE = \inf$, a prime field $\cong \mathbb{Q}$
2. when $charE = p$, a prime field $\cong R/(p) =: \mathbb{Z}_p$, where p is a prime number.

So, we have the following equivalent theorem.

定理 4.1.2. E is a field. Then,

1. If $charE = \inf$, then E has a subfield that is a prime field $\cong \mathbb{Q}$, where $\mathbb{Q}$ is the field of rational numbers;
2. If $charE = p$, then E has a subfield that is a prime field $\cong R/(p) =: \mathbb{Z}_p$, where R is the ring of integers and (p) is the principle ideal generated by p.

From Theorem 4.1.2, every field is a field extension of a prime field.

Look at the structure of a field extension. Suppose E is a field extension of F. Assume $S \subseteq E$. Denote $F(S)$ as a minimum subfield of E that contains F and S.

The existence of $F(S)$ is ensured: E contains F and S. Taking intersection on every subfield of E that contains F and S gives us the minimum subfield of E that contains F and S.

Example: if $E = F$ and $S \subseteq F$, then $F(S) = F = E$. Another example: take $S = E$, then $F(S) = E$.

备注 4.1.2. $F(S)$ can be constructed as:

$$X = \{\frac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)} \,|\, \forall \alpha_1, \alpha_2, \ldots, \alpha_n \in S\},$$

where f and $g \neq 0$ are polynomials of $\alpha_1, \alpha_2, \ldots, \alpha_n$ on F.

证明. By taking $g(\ldots) = 1$ and $\forall f \in F$, we know $F \subseteq X$.

By taking $f(\ldots) = \alpha_i \ \forall \alpha_i \in S$ and $g(\ldots) = 1$, we know $S \subseteq X$.

$f(\ldots) \in X$, $g(\ldots) \in X$, so $\dfrac{f(\ldots)}{g(\ldots)} \in X$. Obviously, X is a field.

Thus, $F(S) \subseteq X$.

On the other hand, $F(S)$ contains F and S, so $f(\ldots) \in F(S)$ and $g(\ldots) \in F(S)$. This means $\dfrac{f(\ldots)}{g(\ldots)} \in F(S)$. This implies $X \subseteq F(S)$.

Therefore, we have $X = F(S)$.

□

Consider the following:

- if $S = E$, then $F(S) = E$, trivial.
- if $S \subset E$ where S can be infinitely many, then $F(S)$ is the union of sets that are constructed by adding finite subset of S to F.

So we focus on the case of S as a finite set:

$$S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

In this situation, we can write

$$F(S) = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

denoting this field extension is by adding elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ to F.

Example: the field of complex numbers is the field extension of the field of real numbers by adding i: $\mathbb{C} = \mathbb{R}(i)$.

定理 4.1.3. E is a field extension of F. $S_1, S_2 \subseteq E$. Then

$$F(S_1)(S_2) = F(S_1 \cup S_2) = F(S_2)(S_1)$$

证明. It is sufficient to show $F(S_1)(S_2) = F(S_1 \cup S_2)$.

1. To show $F(S_1 \cup S_2) \subseteq F(S_1)(S_2)$.

$$
\begin{aligned}
& F, S_1 \subseteq F(S_1) \\
\Longrightarrow\ & F, S_1, S2 \subseteq F(S_1)(S_2); \\
& F, S_1 \cup S_2 \subseteq F(S_1 \cup S_2), \text{ i.e.} \\
& F(S_1 \cup S_2) \text{ is minimum subfield that contains } F \text{ and } S_1 \cup S_2 \\
\Longrightarrow\ & F(S_1 \cup S_2) \subseteq F(S_1)(S_2).
\end{aligned}
$$

2. To show $F(S_1)(S_2) \subseteq F(S_1 \cup S_2)$.

$$
\begin{aligned}
& F, S_1 \cup S_2 \subseteq F(S_1 \cup S_2) \\
\Longrightarrow\ & F, S_1, S_2 \subseteq F(S_1 \cup S_2) \\
\Longrightarrow\ & F(S_1), S_2 \subseteq F(S_1 \cup S_2); \\
& F(S_1), S_2 \subseteq F(S_1)(S_2), \text{ i.e.} \\
& F(S_1)(S_2) \text{ is minimum subfield that contains } F(S_1) \text{ and } S_2 \\
\Longrightarrow\ & F(S_1)(S_2) \subseteq F(S_1 \cup S_2).
\end{aligned}
$$

□

By Theorem 4.1.3, we can write

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1)(\alpha_2)\ldots(\alpha_n)$$

定义 4.1.3. The field extension by one element α, denoted by $F(\alpha)$, is called a **simple field extension** of F, in short **simple extension**.

练习 4.1.1. E is a field extension of F. $S \subseteq E$. Prove that the union of subfield constructed by adding finite subset of S to F, denoted by $\overline{F}$, is a field.

解答. Assume any element $\alpha \in F(S)$. By definition, there must be

$$\alpha = \frac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)}$$

where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} =: S_\alpha \subset S$, f and $g \neq 0$ are polynomials of $\alpha_1, \alpha_2, \ldots, \alpha_n$ on F.

Since S_α is a finite subset of S, $\alpha \in F(S_\alpha \subset \overline{F}$.

Therefore, we just show $F(S) \subset \overline{F}$.

Obviously, any subfield that extends F by any finite subset of S is a subset of $F(S)$, so the union of these subfields $\overline{F} \subset F(S)$.

Therefore, $\overline{F} = F(S)$. So, $\overline{F}$ is a field.

4.2 Simple Field Extension (单扩域)

E is a field extension of F. Suppose an arbitrary element $\alpha \in E$. There are two types of elements in E.

定义 4.2.1. Given $\alpha \in E$. If there exists $a_0, a_1, \ldots a_n \in F$, not all zeros, such that

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$$

then α is **algebraic element** over F.

Otherwise, α is **transcendental element** over F.

备注 4.2.1. α is **algebraic element** over F implies that there exists a nonzero polynomial $f \in F[x]$ such that $f(\alpha) = 0$, which means that α is a root of f.

定义 4.2.2. If α is an algebraic element over F, then $F(\alpha)$ is called a **simple algebraic extension** of F.

If α is a transcendental element over F, then $F(\alpha)$ is called a **simple transcendental extension** of F.

定义 4.2.3. A **monic polynomial** is a single-variable polynomial (that is, a univariate polynomial) in which the **leading coefficient** (the nonzero coefficient of highest degree) is equal to 1.

定理 4.2.1. If $\alpha \in E$ is transcendental over F, then

$$F(\alpha) \cong \text{ quotient field of } F[x]$$

If $\alpha \in E$ is algebraic over F, then

$$F(\alpha) \cong F[x]/(p(x))$$

where $p(x) \in F[x]$ is a unique irreducible monic polynomial at Definition 4.2.3 such that $p(\alpha) = 0$.

证明. $F(\alpha)$ is the minimal field that contains F and α.

By Memo 4.1.2, $F(\alpha)$ contains all polynomials of α over F:

$$F[\alpha] = \{\sum a_k \alpha^k \,|\, \forall a_k \in F\}$$

That is: $F[\alpha] \subseteq F(\alpha)$.

Consider a surjective homomorphism from $F[x]$ to $F[\alpha]$:

$$\phi : F[x] \longrightarrow F[\alpha], \quad \sum a_k x^k \mapsto \sum a_k \alpha^k$$

1. α is transcendental over F.

   To show ϕ is injective: By contradiction. Assume ϕ is NOT injective, then there exists

   $$\sum a_k x^k \neq \sum b_k x^k, \text{ and } \phi(\sum a_k x^k) = \phi(\sum b_k x^k) = \sum c_k \alpha^k$$

   Take

   $$\phi(\sum a_k x^k - \sum b_k x^k) = \phi(\sum a_k x^k) - \phi(\sum b_k x^k) = \sum c_k \alpha^k - \sum c_k \alpha^k = 0$$

   $$\phi(\sum a_k x^k - \sum b_k x^k) = \phi(\sum (a_k - b_k) x^k) = \sum (a_k - b_k) \alpha^k$$

   $$\implies \sum (a_k - b_k) \alpha^k = 0$$

Since by assumption,

$$\sum a_k x^k \neq \sum b_k x^k \implies \exists k, \text{ such that } a_k \neq b_k \implies a_k - b_k \neq 0$$

$\implies \alpha$ is algebraic

$\implies \alpha$ is NOT transcendental $\implies$ contradiction!

$\implies \phi$ is injective

Thus, $F[\alpha] \cong F[x]$ since ϕ is injective, surjective, homomorphism.

By Theorem 2.10.3, isomorphic rings have isomorphic quotient field, thus,

$$\text{Quotient field of } F[\alpha] \cong \text{Quotient field of } F[x]$$

Next, we will show:

$$\text{Quotient field of } F[\alpha] = F(\alpha)$$

(a) $F \subset$ Quotient field of $F[\alpha]$, $\alpha \in$ Quotient field of $F[\alpha]$. $F(\alpha)$ is the minimal field that contains F and α. This implies

$$F(\alpha) \subseteq \text{Quotient field of } F[\alpha].$$

(b) By Theorem 2.10.4,the field $F(\alpha)$ contains the ring $F[\alpha]$, thus $F(\alpha)$ contains the quotient field of $F[\alpha]$. This means

$$\text{Quotient field of } F[\alpha] \subseteq F(\alpha).$$

(c) In summary,

$$F(\alpha) = \text{Quotient field of } F[\alpha].$$

2. α is algebraic over F.

ϕ is not injective: Since α is algebraic, there exists some $f(x) = a_0 + a_1 x + \ldots a_n x^n \neq 0$ such that $\phi(f(x)) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. By this we have $f(x) \neq 0$ with $\phi(f(x)) = \phi(0) = 0$.

By Theorem 2.8.2, $F[x]$ and $F[\alpha]$ are rings, with $\phi : F[x] \longrightarrow F[\alpha]$ a surjective homomorphism, then $\mathfrak{A} = ker(\phi)$ is an ideal of $F[x]$ and $F[x]/\mathfrak{A} \cong F[\alpha]$.

F is a field, so $F[x]$ is ED, PID (and UFD). $\mathfrak{A}$ is an ideal of $F[x]$, thus, $\mathfrak{A}$ is a principle ideal generated by some polynomial $p(x)$, which is $\mathfrak{A} = (p(x))$. This means any element $q(x) \in \mathfrak{A}$ can be written as

$$q(x) = p(x)f(x), \quad f(x) \in \mathfrak{A}$$

Here we claim: if $\mathfrak{A} = (q(x))$ generated by some other $q(x) \in \mathfrak{A}$, then by Exercise 3.2.2, since $F[x]$ is Integral Domain, two principle ideals $(p(x)) = \mathfrak{A} = (q(x))$ implies $p(x)$ is the associate of $q(x)$. So we can write

$$p(x) = q(x)\epsilon, \quad \epsilon \text{ is unit (invertiable)}$$

ϵ is invertible means that $\epsilon \in F$.

If we choose $p(x)$ to be monic, with leading coefficient $= 1$, then

$$p(x) = q(x)\epsilon \implies x^n = x^n \cdot \epsilon \implies \epsilon = 1$$

Therefore, $p(x)$ as monic polynomial is uniquely determined.

To show $p(\alpha) = 0$: Since $p(x) \in \mathfrak{A}$, so $\phi(p(x)) = 0$, which means $\phi(p(x)) = p(\alpha) = 0$.

$p(x) \neq 0$. Otherwise, $\mathfrak{A} = (p(x)) = (0) = \{0\}$, which contradicts to $\mathfrak{A}$ has non-zero element since α is algebraic.

$deg(p(x)) \geq 1$. Otherwise, $p(x) = a_0 \neq 0$ for some $0 \neq a_0 \in F$. This means $p(\alpha) = a_0 \neq 0$, contradiction to α is algebraic with $p(\alpha) = 0$.

Now that $p(x) \neq 0$ and $deg(p(x)) \geq 1$, we show next that $p(x)$ is irreducible. By contradiction, assume $p(x)$ is reducible, then

$$p(x) = g(x)h(x), \quad deg(p(x)) > deg(g(x)), deg(h(x)) \geq 1$$

$$
\begin{aligned}
& p(\alpha) = g(\alpha)h(\alpha) = 0 \\
\Longrightarrow\ & g(\alpha) = 0, \text{ or } h(\alpha) = 0 \text{ since } F(\alpha) \text{ is a field, has no non-zero divisor} \\
\Longrightarrow\ & \phi(g(x)) = g(\alpha) = 0, \text{ or } \phi(h(x)) = h(\alpha) = 0 \\
\Longrightarrow\ & g(x) \in \mathfrak{A}, \text{ or } h(x) \in \mathfrak{A} \\
\Longrightarrow\ & g(x) = p(x)r(x), \text{ or } h(x) = p(x)s(x) \\
\Longrightarrow\ & deg(g(x)) \geq deg(p(x)), \text{ or } deg(h(x)) \geq deg(p(x)) \\
\Longrightarrow\ & \text{contradicts to } deg(p(x)) > deg(g(x)), deg(h(x)), \text{ by } p(x) \text{ reducible} \\
\Longrightarrow\ & p(x) \text{ is irreducible}
\end{aligned}
$$

Again since F is a field, $F[x]$ is PID. For a UFD, irreducible element $\cong$ prime element. PID implicitly is UFD. Thus, $p(x)$ is irreducible in $F[x]$ means that $p(x)$ is prime in $F[x]$.

By Lemma 3.3.2, an ideal generated by a prime element in a PID is a maximal ideal, $(p(x))$ is a maximal ideal in $F[x]$. So $\mathfrak{A} = (p(x))$ is a maximal ideal.

By Theorem 2.9.1, $F[x]$ is Integral Domain (ID), and $\mathfrak{A} = p(x)$ is a maximal ideal, thus $F[x]/\mathfrak{A}$ is a field. So $F[\alpha] \cong F[x]/\mathfrak{A} = F[x]/(p(x))$ is a field.

Note that $F \subseteq F[\alpha]$ and $\alpha \in F[\alpha]$, $F(\alpha)$ is the minimal field that contains F and α. Thus, $F(\alpha) \subseteq F[\alpha]$.

We know from the beginning of this proof that $F(\alpha)$ contains all polynomials of α over F. Thus, $F[\alpha] \subseteq F(\alpha)$.

Therefore, $F[\alpha] = F(\alpha)$.

By this, we know

$$F(\alpha) = F[\alpha] \cong F[x]/\mathfrak{A} = F[x]/(p(x))$$

□

From Theorem 4.2.1, when α is algebraic in F, we know its field extension $F(\alpha) = F[\alpha]$. We can have more explicit description on $F(\alpha)$.

定理 4.2.2. If α is algebraic over F, with

$$F(\alpha) = F[\alpha] \cong F[x]/\mathfrak{A} = F[x]/(p(x)).$$

Then every element in $F(\alpha)$ has the unique form

$$\sum_{i=1}^{n-1} a_i \alpha^i, \quad a_i \in F$$

where n is the degree of $p(x)$.

For any element $f(\alpha)$ and $g(\alpha)$ in $F(\alpha)$, addition is by adding coefficients of corresponding term α^i. multiplication is by taking modulus $p(x)$:

$$f(\alpha)g(\alpha) = r(\alpha)$$

where

$$r(x) = f(x)g(x) \mod p(x).$$

证明. Note that $F(\alpha) = F[\alpha]$. Any element $\beta \in F(\alpha)$ is $\beta \in F[\alpha]$ has the form

$$\beta := h(\alpha) = \sum b_i \alpha^i, \quad b_i \in F$$

$h(\alpha)$ has the corresponding element $h(x) \in F[x]/(p(x))$ with

$$h(x) = p(x)q(x) + r(x)$$

where $r(x) = 0$ or $deg(r(x)) < deg(p(x)) = n$.

By isomorphism $F[\alpha] \cong F[x]/(p(x))$, this means

$$h(\alpha) = p(\alpha)q(\alpha) + r(\alpha) \implies h(\alpha) = r(\alpha), \text{ since } p(\alpha) = 0.$$

Thus, we just show

$$\beta = h(\alpha) = r(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i$$

To show uniqueness, suppose $\beta = r_1(\alpha) = r_2(\alpha)$, and $deg(r_1(x)), deg(r_2(x)) < deg(p(x)) = n$. Then, we need to show $r_1(x) = r_2(x)$, by the following:

$$\begin{aligned}
& r_1(\alpha) - r_2(\alpha) = 0 \implies \phi(r_1(x) - r_2(x)) = 0 \\
\implies & r_1(x) - r_2(x) \in ker(\phi) =: \mathfrak{A} \\
\implies & r_1(x) - r_2(x) = p(x)s(x), \quad \text{for some } s(x) \in F[x]/(p(x)) \\
\implies & s(x) = 0 \text{ since } deg(r_1(x)),\ deg(r_2(x)) < deg(p(x)) = n \\
\implies & r_1(x) - r_2(x) = 0 \implies r_1(x) = r_2(x)
\end{aligned}$$

□

$p(x)$ in Theorem 4.2.2 has important role.

定义 4.2.4. The monic polynomial $p(x) \in F(x)$

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0, \quad a_i \in F$$

with $deg(p(x)) = n$ and $p(\alpha) = 0$, is called the **minimal polynomial** for α over F. The degree of $p(x)$ is called the **degree of α over F**.

Next we want to answer the question: Does the simple extension of a field F, $E = F(\alpha)$, exists?

There are two scenarios:

1. When α is transcendental over F: F is a field, so by Theorem 2.6.1, its polynomial ring $F[x]$ exists. The quotient field of $F[x]$ exists by Theorem 2.10.1. Thus $F(\alpha)$ exists, since by Theorem 4.2.1, $F(\alpha) \cong$ Quotient field of$F[x]$.
2. When α is algebraic over F? See Theorem 4.2.3 for a positive answer.

定理 4.2.3. Consider a field F, $F[x]$ is its monic polynomial ring. Given an irreducible polynomial $p(x) \in F[x]$ with

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0,$$

then there exists simple algebraic extension $F(\alpha)$ of F, where the minimal polynomial for α over F is $p(x)$.

证明. F is a field, so by Theorem 2.6.1, there exists its polynomial ring $F[x]$. Since F is a field, by Theorem 3.4.2, $F[x]$ is an ED. Thus, $F[x]$ is implicitly an PID. Now that $p(x) \in F[x]$ is irreducible, by Lemma 3.3.2, the principle ideal $(p(x))$ is thus maximal ideal.

By Theorem 2.9.1, $K' := F[x]/(p(x))$ is a field since $F[x]$ is commutative ring with multiplicative identity and $(p(x))$ is a maximal ideal of $F[x]$.

Consider a mapping:

$$\phi : F[x] \longrightarrow F[x]/(p(x)) =: K' \quad , \phi(f(x)) = \overline{f(x)}$$

where $\overline{f(x)}$ is the equivalent class of $f(x)$ in $K' = F[x]/(p(x))$.

Note that ϕ is a surjective homomorphism:

1. ϕ is well-defined: $\forall f(x) \in F[x]$, there exists $\overline{f(x)}$ uniquely determined.

2. ϕ is surjective: $\overline{f(x)}$ is equivalent class, covers $F[x]/(p(x))$.

3. ϕ is homomorphism: By operation of equivalent class

$$\phi(f(x) + g(x) = \overline{f(x) + g(x)} = \overline{f(x)} + \overline{g(x)} = \phi(f(x)) + \phi(g(x))$$
$$\phi(f(x)g(x) = \overline{f(x)g(x)} = \overline{f(x)g(x)} = \phi(f(x))\phi(g(x))$$

Thus, ϕ is surjective homomorphism.

Consider F under ϕ has the image $\overline{F}$:

$$\phi(F) = \overline{F} \subseteq K' = F[x]/(p(x))$$

$\phi_F : F \longrightarrow \overline{F}$ is surjective homomorphism. Furthermore, let $a \neq b$,

$a, b \in F$. Then

$$\begin{aligned} & a \neq b \implies a - b \neq 0 \\ & deg(a-b) = 0 \neq 1 \leq deg(p(x) \implies p(x) \not| a - b \\ \implies & \overline{a-b} \neq \overline{0} \\ \implies & \overline{a} - \overline{b} \neq \overline{0} \\ \implies & \overline{a} \neq \overline{b} \end{aligned}$$

So, ϕ_F is injective. Thus, $\phi_F : F \longrightarrow \overline{F}$ is isomorphism. This is $F \cong \overline{F}$ by ϕ.

Note that $\overline{F} \subseteq K' = F[x]/(p(x))$. Replace $\overline{F}$ by F to get K. Notice that $K' - \overline{F}$ and F don't intersect, which is $K' - \overline{F} \cap F = \emptyset$. By Theorem 2.5.4, $K \cong K'$. So, K is a field since K' is a field. Obviously, $F \subseteq K$.

- Now we need to find algebraic element $\alpha \in K$ over F such that $p(\alpha) = 0$:

  Note that

  $$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \equiv 0 \mod p(x).$$

  So, $\phi(p(x)) = \overline{0} \in K'$, and

  $$\phi(p(x)) = \overline{x}^n + \overline{a_{n-1}}\overline{x}^{n-1} + \ldots + \overline{a_0} = \overline{0} \in K' = F[x]/(p(x)),$$

  where $\overline{0}$, $\overline{a_0}$, ..., $\overline{a_{n-1}} \in \overline{F}$.

  So, correspondingly in F we have

  $$0, a_0, \ldots, a_{n-1} \in F \subseteq K$$

  Thus, correspondingly in K we have from $\phi(p(x) = \overline{0}$ that

  $$\overline{x}^n + a_{n-1}\overline{x}^{n-1} + \ldots + a_0 = 0.$$

  Take $\alpha = \overline{x} \in K$, then we find α is algebraic over F, with:

  $$p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$$

- To prove $p(x)$ is minimal polynomial for α over F:

- By assumption, $p(x)$ is irreducible.
- By construction, $p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$
- Need to show $p(x)$ has the minimal degree. By contradiction, assume $p_1(x)$ is the minimal polynomial. So $p_1(\alpha) = 0$, with

$$deg(p_1(x)) < deg(p(x))$$

Consider the set

$$U = \{f(x) \in F[x] | f(\alpha) = 0\}.$$

U is an ideal of $F[x]$:

$$f(\alpha) = 0, g(\alpha) = 0 \implies f(\alpha) - g(\alpha) = 0 \implies f(x) - g(x) \in U$$
$$f(\alpha)r(\alpha) = 0, \forall r(x) \in F[x] \implies f(x)r(x) \in U$$

Since $F[x]$ is PID, U is an ideal in $F[x]$ implies U is a principle ideal, so $U = (p_1(x))$.

Note that $p(\alpha) = 0$, so $p(x) \in U$. Thus, $p(x) = ap_1(x)$ since $p(x)$ is irreducible.

By assumption, $p(x) \in F[x]$ and $p_1(x) \in F[x]$ are monic polynomial, they have leading coefficient $= 1$. This implies that $a = 1$. So $p(x) = ap_1(x) = p_1(x)$.

- Therefore, $p(x)$ is the minimal polynomial.

□

练习 4.2.1. Use $F[\alpha] = F(\alpha)$, prove $F(\alpha) = K$, as in Theorem 4.2.3.

证明. K is a field, F is a field. K contains F. So, K is a field extension of F. Note that $\alpha \in K$. $F(\alpha)$ is the minimum field that contains F and α. So $F(\alpha) \subseteq K$.

Consider any element $\beta \in K$. Consider

$$\phi : K \longrightarrow F[x]/(p(x)) =: K'$$

Here $\phi(\beta) = \overline{\beta} \in K'$. Thus, we can write

$$\overline{\beta} = \overline{b_m}\overline{x}^m + \overline{b_{m-1}}\overline{x}^{m-1} + \ldots + \overline{b_0}$$

By ϕ isomorphism, we find correspondingly

$$\overline{\beta} \leftrightarrow \beta,\ \overline{x} \leftrightarrow \alpha,\ \overline{b_i} \leftrightarrow b_i,\ i = 1, \ldots, m$$

So,

$$\beta = b_m\alpha^m + b_{m-1}\alpha^{m-1} + \ldots + b_0.$$

Obviously, $\beta \in F[\alpha] = F(\alpha)$.
Thus, we just show $K \subseteq F(\alpha)$.
Therefore, $K = F(\alpha)$.

□

定理 4.2.4. $F(\alpha)$ and $F(\beta)$ are simple algebraic extension of F. α and β have the same minimal polynomial over F, denoted as $p(x)$. Then,

$$F(\alpha) \cong F(\beta)$$

证明. Let $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, with the degree of $p(x)$ is n. Write $F(\alpha)$ and $F(\beta)$ as:

$$F(\alpha) = \{\sum_{i=0}^{n-1} b_i\alpha^i \,|\, b_i \in F\}$$
$$F(\beta) = \{\sum_{i=0}^{n-1} c_i\beta^i \,|\, c_i \in F\}$$

Construct a mapping

$$\phi : F(\alpha) \longrightarrow F(\beta), \quad \phi\Big(\sum_{i=0}^{n-1} b_i\alpha^i\Big) = \sum_{i=0}^{n-1} b_i\beta^i$$

- ϕ is well-defined: $\sum_{i=0}^{n-1} b_i\alpha^i$ is unique in $F(\alpha)$.
- ϕ is surjective: $\forall f(\beta) \in F(\beta)$ has the form $\sum_{i=0}^{n-1} b_i\beta^i$.

- ϕ is injective: If $\gamma_1 = \gamma_2 \in F(\beta)$. Since F is a field, $F(\beta)$ is UFD, so γ_1 and γ_2 have unique form:

$$\gamma_1 = \gamma_2 = \sum_{i=0}^{n-1} b_i \beta^i$$

Its pre-image is unique

$$\phi^{-1}(\gamma_1) = \phi^{-1}(\gamma_2) = \sum_{i=1}^{n-1} b_i \alpha^i$$

- ϕ is homomorphism: For addition:

$$\sum_{i=0}^{n-1} b_i \alpha^i + \sum_{i=0}^{n-1} c_i \alpha^i = \sum_{i=0}^{n-1} (b_i + c_i)\alpha^i$$

$$\Longrightarrow \phi(\sum_{i=0}^{n-1} b_i \alpha^i + \sum_{i=0}^{n-1} c_i \alpha^i) = \phi(\sum_{i=0}^{n-1} b_i \alpha^i) + \phi(\sum_{i=0}^{n-1} c_i \alpha^i) = \sum_{i=0}^{n-1} b_i \beta^i + \sum_{i=0}^{n-1} c_i \beta^i$$

$$\phi(\sum_{i=0}^{n-1} (b_i + c_i)\alpha^i) = \sum_{i=0}^{n-1} (b_i + c_i)\beta^i = \sum_{i=0}^{n-1} b_i \beta^i + \sum_{i=0}^{n-1} c_i \beta^i$$

$$\Longrightarrow \phi(\sum_{i=0}^{n-1} b_i \alpha^i + \sum_{i=0}^{n-1} c_i \alpha^i) = \phi(\sum_{i=0}^{n-1} (b_i + c_i)\alpha^i)$$

For multiplication:

$$\Big(\sum_{i=0}^{n-1} b_i \alpha^i\Big)\Big(\sum_{i=0}^{n-1} c_i \alpha^i\Big) = \sum_{i=0}^{2n-2} d_i \alpha^i = r(\alpha)$$

where

$$f(x) = \sum_{i=0}^{2n-2} d_i x^i = p(x)q(x) + r(x).$$

So,

$$\phi\Big(\Big(\sum_{i=0}^{n-1} b_i \alpha^i\Big)\Big(\sum_{i=0}^{n-1} c_i \alpha^i\Big)\Big) = \phi(\sum_{i=0}^{2n-2} d_i \alpha^i) = \sum_{i=0}^{2n-2} d_i \beta^i = r(\beta).$$

On the other hand,

$$\phi\Big(\Big(\sum_{i=0}^{n-1} b_i \alpha^i\Big)\Big)\phi\Big(\Big(\sum_{i=0}^{n-1} c_i \alpha^i\Big)\Big) = \Big(\sum_{i=0}^{n-1} b_i \beta^i\Big)\Big(\sum_{i=0}^{n-1} c_i \beta^i\Big)$$

$$= \sum_{i=0}^{2n-2} d_i \beta^i = r(\beta)$$

where using the same form of

$$f(x) = \sum_{i=0}^{2n-2} d_i x^i = p(x)q(x) + r(x).$$

Therefore, ϕ is isomorphism, which is $F(\alpha) \cong F(\beta)$.

□

Theorem 4.2.5 summarizes what we find in this section:

定理 4.2.5. For a field F, there exists one simple algebraic extension $F(\alpha)$, with the minimal polynomial $p(x) \in F[x$ of α over F. $p(x)$ is irreducible and monic with leading coefficient $= 1$.

练习 4.2.2. E is a field extension of F. $a \in F$. Prove: α is algebraic over F, and $F(\alpha) = F$.

证明. Consider $f(x) = x - \alpha$. It is a non-zero polynomial of $F[x]$, and $f(\alpha) = 0$. So α is algebraic over F.

$F(\alpha)$ contains F and α, so $F \subseteq F(\alpha)$.

F is a field. It contains F and α. $F(\alpha)$ is the minimum field that contains F and α. So $F(\alpha) \subseteq F$.

Therefore, $F = F(\alpha)$. □

练习 4.2.3. F is a field of rational numbers. What are the minimal polynomial of i and $\frac{2i+1}{i-1}$? $F(i)$ and $F(\frac{2i+1}{i-1})$ are isomorphic?

解答. Obviously, $\frac{2i+1}{i-1} \in F(i)$, so $F(\frac{2i+1}{i-1}) \subseteq F(i)$.

On the other hand,

$$(\frac{2i+1}{i-1})^2 = \frac{4i-3}{-2i} = -2 + \frac{3}{2i} \in F(\frac{2i+1}{i-1})$$

Obviously,

$$\frac{\frac{3}{2}}{(\frac{2i+1}{i-1})^2 + 2} = \frac{\frac{3}{2}}{-2 + \frac{3}{2i} + 2} = i \in F(\frac{2i+1}{i-1})$$

This means $F(i) \subseteq F(\frac{2i+1}{i-1})$.

Therefore, $F(i) = F(\frac{2i+1}{i-1})$, which is $F(i) \cong F(\frac{2i+1}{i-1})$.

Any linear polynomial in $F[x]$ can not have $f(i) = 0$, since element in F is rational number.

Consider $f(x) = x^2 + 1 \in F[x]$. It has $f(i) = 0$. So the minimal polynomial of i over F is

$$f(x) = x^2 + 1.$$

For the same reason, the minimal polynomial of $\frac{2i+1}{i-1}$ over F can not be linear.

Note that $(\frac{2i+1}{i-1})^2 = -2 + \frac{3}{2i} = -2 + \frac{3i}{2i^2} = -2 - \frac{3i}{2}$. Also

$$\frac{2i+1}{i-1} = \frac{(2i+1)(i+1)}{(i-1)(i+1)} = \frac{2i^2+3i+1}{-2} = \frac{1}{2} - \frac{3i}{2}$$

This implies that

$$(\frac{2i+1}{i-1})^2 - \frac{2i+1}{i-1} = -2 - \frac{3i}{2} - \frac{1}{2} + \frac{3i}{2} = -\frac{5}{2}$$

Thus, the minimal polynomial of $\frac{2i+1}{i-1}$ over F is:

$$g(x) = x^2 - x + \frac{5}{2}.$$

4.3 Algebraic Extension (代数扩域)

备注 4.3.1. Consider the following as a fact:

If E is a field extension over F, E contains transcendental element over F, then there exists a subfield T such that

$$F \subset T \subset E$$

Here T is obtained by $F(\alpha_1, \alpha_2, \ldots)$ where $\alpha_1, \alpha_2, \ldots$ are transcendental over F.

E contains only algebraic elements over T.

This is to say: a field extension has two parts:

1. one transcendental part of field extension,
2. one algebraic part of field extension.

We focus on algebraic field extension (algebraic extension in short).

定义 4.3.1. E is a field extension of F. If any element of E is algebraic over F, then E is an **algebraic field exstension** of F, or E is an **algebraic extension** of F.

In this section we want to answer the question: If $E = F(S)$ and any element in S is algebraic over F, then is any element in E is algebraic over F?

To answer this question, we consider E the field extension of F as a vector space V over the field F, here $V = E$.

V as vector space has dimension, correspondingly, E as field extension has degree.

定义 4.3.2. If E the field extension of F as a vector space has dimension of n, then we call n **the degree of** E as field extension of F, denoted by

$$(E : F).$$

If $(E : F) = n$ is finite, then we call E a **finite field extension** of F.

If $(E : F) = n$ is infinite, then we call E a **infinite field extension** of F.

定理 4.3.1. I is finite field extension of F, E is finite field extension of I. Then E is finite field extension of F, and

$$(E : F) = (E : I)(I : F)$$

证明. Let $(I : F) = r$, $(E : I) = s$.

The basis of I over F is: $\alpha_1, \alpha_2, \ldots, \alpha_r \in I$.

The basis of E over I is: $\beta_1, \beta_2, \ldots, \beta_s \in E$.

Obviously,

$$\alpha_i\beta_j \in E, \text{ for } i = 1, \ldots, r; j = 1, \ldots, s, \text{ since } \alpha_i \in I, \beta_j \in E.$$

We want to show $\alpha_i\beta_j$, $i = 1, \ldots, r$, $j = 1, \ldots, s$, is a basis of E over F:

- To show linearly independence: Consider

$$\sum_{i,j} a_{ij}\alpha_i\beta_j = 0, \quad a_{ij} \in F$$

Then,

$$\sum_{i,j} a_{ij}\alpha_i\beta_j = \sum_j \left(\sum_i a_{ij}\alpha_i \right) \beta_j = 0$$

Here $a_{ij} \in F$, $\alpha_i \in I$. This implies that $\sum_i a_{ij}\alpha_i \in I$.

Since $\beta_j \in E$ is basis of E over I,

$$\sum_j \left(\sum_i a_{ij}\alpha_i \right) \beta_j = 0 \implies \sum_i a_{ij}\alpha_i = 0, \quad \forall i, j$$

And since α_i is basis of I over F,

$$\sum_i a_{ij}\alpha_i = 0 \implies a_{ij} = 0, \quad \forall i, j$$

This means $\alpha_i\beta_j$, for $i = 1, \ldots, r$, $j = 1, \ldots, s$, is linearly independent.

- To show any element $\omega \in E$ can be represented as linear combination:

Since β_j is basis of E over I, we can write

$$\omega = \sum_j \theta_j\beta_j, \quad \theta_j \in I, \, j = 1, \ldots, s$$

Since α_i is basis of I over F, we can write

$$\theta_j = \sum_i c_{ij}\alpha_i, \quad c_{ij} \in F.$$

Thus, we can write

$$\omega = \sum_j \theta_j \beta_j = \sum_{ij} c_{ij} \alpha_i \beta_j, \quad c_{ij} \in F,\ \alpha_i \beta_j \in E$$

- Therefore, $\alpha_i \beta_j$ for $i = 1, \ldots, r$, $j = 1, \ldots, s$, is basis of E over F.

□

推论 4.3.1. F_1, F_2, ..., F_t are fields. F_i is a finite field extension of F_{i-1}, for $i = 2, \ldots, t$.

Then,

$$(F_t : F_1) = (F_t : F_{t-1})(F_{t-1} : F_{t-2}) \cdots (F_2 : F_1)$$

定理 4.3.2. $E = F(\alpha)$ is a simple algebraic field extension. Then, E is an algebraic field extension.

证明. α is algebraic over F. It has a minimal polynomial

$$p(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

with not all $a_i = 0$ and $p(\alpha) = 0$. So, we have

$$a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1} = -\alpha^n \neq 0.$$

This means $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ are linearly independent.

Also, by Theorem 4.2.2, any element in $F(\alpha) = F[\alpha]$ can be written as the form

$$\sum_{i=0}^{n-1} a_i \alpha^i, \quad a_i \in F$$

Thus, $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis of $E = F(\alpha)$. So, $(E : F) = n$.

Take any element $\beta \in E$. Note that $\{1, \beta, \beta^2, \ldots, \beta^n\}$ with $n + 1$ elements are linearly dependent. This means

$$b_0 + b_1 \beta + b_2 \beta^2 + \ldots + b_n \beta^n = 0$$

with not all $b_i = 0$.

So, by definition, β is algebraic over F. Therefore, $E = F(\alpha)$ is algebraic field extension.

□

From the proof of Theorem 4.3.2, we notice the following corollaries.

推论 4.3.2. $F(\alpha)$ is a simple field extension of F. The degree of α is n. Then, $F(\alpha)$ is a n degree finite field extension.

推论 4.3.3. E is a finite field extension of F. Then E is an algebraic field extension of F.

定理 4.3.3. $E = F(\alpha_1, \alpha_2, \ldots, \alpha_t)$, where α_i is algebraic over F, for $i = 1, \ldots, t$.

Then, E is finite field extension of F, and thus is algebraic field extension of F.

证明. By induction.

- $t = 1$: $E = F(\alpha_1)$. By Theorem 4.3.2 or Corollary 4.3.3, E is finite field extension, and thus is algebraic field extension of F.
- Assume for $t-1$, $E = F(\alpha_1, \alpha_2, \ldots, \alpha_{t-1})$ is finite field extension.

  Denote $E = F(\alpha_1, \alpha_2, \ldots, \alpha_t)$, and $I = F(\alpha_1, \alpha_2, \ldots, \alpha_{t-1})$.

  $$\begin{aligned} & F(\alpha_1, \alpha_2, \ldots, \alpha_t) = F(\alpha_1, \alpha_2, \ldots, \alpha_{t-1})(\alpha_t) \\ \iff & E = I(\alpha_t) \end{aligned}$$

  α_t is algebraic over F, so it is algebraic over I:

  $$\alpha_t^n + a_{n-1}\alpha_t^{n-1} + \ldots + a_1\alpha_t + a_0 = 0, \quad a_i \in F$$

  for not all $a_i = 0$.

  Obviously, $a_i \in F \subseteq I \implies a_i \in I$, so α_t is algebraic over I.

This means E is simple algebraic extension of I, and by assumption in induction $I = F(\alpha_1, \alpha_2, \ldots, \alpha_{t-1}$ is finite field extension, by Corollary 4.3.2, E is finite field extension of I. By Theorem 4.3.1, E is finite field extension of F, with

$$(E : F) = (E : I)(I : F).$$

□

推论 4.3.4. Algebraic elements over a field F are closed at the operation of $+, -, \times, \div$.

证明. Consider α and β algebraic over a field F. Then $E = F(\alpha, \beta)$ is finite field extension of F. $\alpha \in E$ and $\beta \in E$. So $\alpha+\beta \in E$, $\alpha-\beta \in E$, $\alpha\times\beta \in E$, and $\alpha \div \beta \in E$.

By Theorem 4.3.3, $E = F(\alpha, \beta)$ with α and β algebraic over F is algebraic field extension, any element in E is algebraic, so is $\alpha + \beta \in E$, $\alpha - \beta \in E$, $\alpha \times \beta \in E$, and $\alpha \div \beta \in E$. □

定理 4.3.4. $E = F(S)$, for $S = \{\alpha_i \,|\, \alpha_i \text{ algebraic over } F\}$.
Then E is algebraic field extension of F.

证明. Given any element $\beta \in E$, we can write explicitly as

$$\beta = \frac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)}$$

This implies $\beta \in F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. By Theorem 4.3.3, β is algebraic over F.

□

备注 4.3.2. This section goes along the line:

1. $F(\alpha)$ is finite field extension $\implies$ $F(\alpha)$ is algebraic field extension.
2. $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is finite field extension $\implies$ $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is algebraic field extension.

3. $F(S)$ where S can be infinite set:

$$\begin{aligned} & \beta \in F(S) \\ \Longrightarrow\ & \beta \in F(\alpha_1, \alpha_2, \ldots, \alpha_n) \text{ for some finite set } \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \\ \Longrightarrow\ & \beta \text{ algebraic over } F \end{aligned}$$

练习 4.3.1. E is an algebraic field extension of F. α is algebraic over E. Prove that α is algebraic over F.

证明. α is algebraic over E, this implies there exists a polynomial of $0 \neq f(x) \in E[x]$ with

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0, \quad a_i \in E.$$

E is algebraic field extension of F, so element in E is algebraic over F. Thus, $a_i \in E$ are algebraic over F.

Construct a subfield of E by

$$E' = F(1, a_0, a_1, \ldots, a_{n-1}).$$

E' is a finite field extension over F, and thus by Corollary 4.3.3, E' is a algebraic field extension over F.

By $f(\alpha) = 0$ stated above, we note that α is algebraic over E'. So $E'(\alpha)$ is a simple extension of E' and thus is finite field extension of E' by Corollary 4.3.2.

By Theorem 4.3.1, $E'(\alpha) = F(1, a_0, a_1, \ldots, a_{n-1})(\alpha)$ is a finite field extension of F, and thus by Corollary 4.3.3 again, $E'(\alpha)$ is algebraic field extension of F. Thus the element $\alpha \in E'(\alpha)$ is algebraic over F.

□

练习 4.3.2. F, I, E are fields, with $E \supset I \supset F$.

Assume

$$(I : F) = m,$$

and the degree of $\alpha \in E$ over F is n. Assume further $(m, n) = 1$.

Prove that the degree of $\alpha \in E$ over I is n.

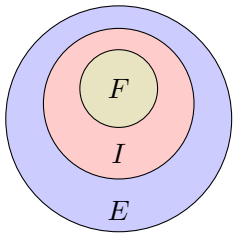


图 4.1: Field extensions $E \supset I \supset F$.

证明. The field extensions has the following relations.

Since $\alpha \in E$ has degree of n over F, the minimal polynomial $p(x)$ of α over F has degree of n.

Assume the minimal polynomial of α over I is $p_1(x)$, it has degree of s. $p(x)$ is also a polynomial over $I \supset F$ with $p(\alpha) = 0$, but since $p_1(x)$ is minimal polynomial of α over I, this implies $s \leq n$.

Assume the degree of $I(\alpha)$ over $F(\alpha)$ is t. Then

$$(I(\alpha) : F) = (I(\alpha) : F(\alpha))(F(\alpha) : F) = tn$$
$$(I(\alpha) : F) = (I(\alpha) : I)(I : F) = sm$$

This implies that $tn = sm$, thus $n|sm$. Note that $(n, m) = 1$, so $n|s$. From $s \leq n$, this gives $s = n$. Thus, α has degree of n over I.

□

练习 4.3.3. Suppose a field with $char(F) \neq 2$. E is a field extension of F, with

$$(E : F) = 4.$$

Prove that there exists a 2-degree field extension I of F, with $F \subseteq I \subseteq E$ iff $E = F(\alpha)$ with the minimal polynomial of α over F is

$$p(x) = x^4 + ax^2 + b$$

证明. • Assume $E = F(\alpha)$ with the minimal polynomial of α over F is

$$p(x) = x^4 + ax^2 + b$$

Consider $I = F(\alpha^2)$. Obviously, $F \subseteq I \subseteq E$.

? : $p(x) = x^4 + ax^2 + b$ is irreducible over F, so $x^2 + ax + b$ is also irreducible over F.

But then

$$(\alpha^2)^2 + a(\alpha^2) + b = \alpha^4 + a\alpha^2 + b = 0, \quad \text{by } p(\alpha) = 0$$

So x^2+ax+b is the minimal polynomial of α^2 over F. Thus, $I = F(\alpha^2)$ is the 2-degree field extension of F.

- On the other direction, assume

$$F \subseteq I \subseteq E, \quad (I : F) = 2, \quad (E : F) = 4.$$

1. Obviously, $(I : F) = 2$ and $(E : F) = 4$ imply that $(E : I) = 2$. We can find $\theta \in E$ and $\theta \notin I$. θ has degree of 2 over I, with its minimal polynomial over I having the form:

$$x^2 + \beta x + \gamma, \quad \theta^2 + \beta\theta + \gamma = 0, \quad \beta, \gamma \in I$$

Since $char(F) \neq 2$, we can write $\frac{\beta}{2}$.

$$(\theta + \frac{\beta}{2})^2 = \theta^2 + \beta\theta + \frac{\beta^2}{4} + \gamma - \gamma = \frac{\beta^2}{4} - \gamma.$$

Denote $\omega = \theta + \frac{\beta}{2}$ and $\delta = \frac{\beta^2}{4} - \gamma$. Then $E = E(\omega)$ and ω has minimal polynomial over I as

$$x^2 - \delta, \quad \delta \in I$$

2. If $\delta \in I$ but $\delta \notin F$, then by $(I : F) = 2$, δ has minimal polynomial over F

$$x^2 + ax + b, \quad a, b \in F.$$

Since $(\theta + \frac{\beta}{2})^2 = \frac{\beta^2}{4} - \gamma$, which is
$omega^2 = \delta$, the minimal polynomial of δ over F shows $\omega^4 + a\omega^2 + b = 0$.

Notice $I = F(\delta)$ (by δ degree of 2 over F?), so $E = I(\omega) = F(\delta, \omega) = F(\omega)$ (since δ is a polynomial of ω, $\delta = \omega^2$?).

By assumption, $(E : F) = 4$, so ω has minimal polynomial over F with degree of 4, which is

$$x^4 + ax^2 + b$$

3. If $\delta \in F \subseteq I$, then since $(I : F) = 2$, we can find $\lambda \in I$ and $\lambda \notin F$. Take

$$\omega' = \omega(1 + \lambda)$$

Then,

$$\omega'^2 = \omega^2(1 + 2\lambda + \lambda^2)$$

Since $\lambda \notin F$, $(1 + 2\lambda + \lambda^2) \notin F$, with $\omega^2 = \delta \in F$, we derive $\omega' \notin F$. Denote $\delta' := \omega'^2 \notin F$. So δ' has minimal polynomial over F as

$$x^2 + ax + b$$

Apply the same argument as in Step 2, we have $E = F(\omega')$ and ω' has minimal polynomial over F as

$$x^4 + ax^2 + b.$$

□

练习 4.3.4. E is a finite field extension of F. There exists finite number of elements $\alpha_1, \alpha_2, \ldots, \alpha_m \in E$ such that

$$E = F(\alpha_1, \alpha_2, \ldots, \alpha_m).$$

解答. Assume $(E : F) = m$, and consider E as a vector space over F. Then there exists basis of E as $\alpha_1, \alpha_2, \ldots, \alpha_m$. Obviously,

$$E = F(\alpha_1, \alpha_2, \ldots, \alpha_m).$$

练习 4.3.5. F is a field of rational numbers. Add complex number for field extension:

$$E_1 = F(2^{\frac{1}{3}}, 2^{\frac{1}{3}}i)$$
$$E_2 = F(2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega i), \quad \omega = \frac{-1+\sqrt{3}i}{2}, \text{ with } \omega^3 = 1.$$

Prove that

$$(E_1, F(2^{\frac{1}{3}})) = 2, \quad (E_1, F) = 6$$
$$(E_2, F(2^{\frac{1}{3}})) = 4, \quad (E_2, F) = 12$$

证明. $F \subseteq F(2^{\frac{1}{3}}) \subseteq F(2^{\frac{1}{3}}, i) = F(2^{\frac{1}{3}}, 2^{\frac{1}{3}}i) = E_1$.

$i \notin F(2^{\frac{1}{3}})$. i is a root of x^2+1, so $(E_1 : F(2^{\frac{1}{3}}) = 2$.

$2^{\frac{1}{3}} \notin F$, $2^{\frac{1}{3}}$ is a root of the irreducible polynomial $x^3 - 2$ over F, so $(F(2^{\frac{1}{3}}) : F) = 3$.

Thus,

$$(E_1 : F) = \big(E_1 : F(2^{\frac{1}{3}})\big)\big(F(2^{\frac{1}{3}}) : F\big) = 2 \times 3 = 6.$$

On the other hand, $E_2 = F(2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega i)$. So $\omega i \in E_2$, and $-(\omega i)^3 = -1i^3 = i \in E_2$. Then again by $\omega i = \frac{-1}{2}i - \sqrt{3}2 \in E_2$, this implies $\sqrt{3} \in E_2$.

Therefore,

$$E_2 = F(2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega i) = F(2^{\frac{1}{3}}, \sqrt{3}, i) \supseteq F(2^{\frac{1}{3}}, \sqrt{3}) \supseteq F(2^{\frac{1}{3}}) \supseteq F$$

$\big(E_2 : F(2^{\frac{1}{3}}, \sqrt{3})\big) = \big(F(2^{\frac{1}{3}}, \sqrt{3}, i) : F(2^{\frac{1}{3}}, \sqrt{3})\big) = 2$.

$\sqrt{3} \notin F(2^{\frac{1}{3}})$, otherwise $F(2^{\frac{1}{3}}) \supseteq F(\sqrt{3})$ makes contradiction with $\big(F(2^{\frac{1}{3}}) : F\big) = 3$ and $\big(F(\sqrt{3}) : F\big) = 2$ by Theorem 4.3.1.

Thus, $\big(F(2^{\frac{1}{3}}, \sqrt{3}) : F(2^{\frac{1}{3}})\big) = 2$.

With $\big(F(2^{\frac{1}{3}}) : F\big) = 3$, we know

$$\big(E_2 : F\big) = \big(E_2 : F(2^{\frac{1}{3}}, \sqrt{3})\big)\big(F(2^{\frac{1}{3}}, \sqrt{3}) : F(2^{\frac{1}{3}})\big)\big(F(2^{\frac{1}{3}}) : F\big)$$
$$= 2 \times 2 \times 3 = 12$$

□

4.4 Splitting Field (分裂域)

定理 4.4.1. Every n degree polynomial in $\mathbb{C}[x]$ over complex number field $\mathbb{C}$ has n roots.

In other words, any polynomial in $\mathbb{C}[x]$ has roots.

定义 4.4.1. Given a field E and its polynomial ring $E[x]$ over E. If every polynomial $f(x) \in E[x]$ factors as a product of linear factor $(x + a_i)$, then E has no further algebraic field extension. We call E **algebraic closed**.

We can have alternative definition for algebraic closure.

定义 4.4.2. Given a field F, and its field extension E, we define **algebraic closure of F in E** as a field with all elements in E are algebraic over F.

That is, a field F is **algebraically closed** if every non-constant polynomial in $F[x]$ has a root.

定理 4.4.2. A field F is algebraically closed iff every non-constant polynomial in $F[x]$ factors into linear factors over $F[x]$.

证明. Assume F is algebraically closed. Then, for any non-constant polynomial $p(x) \in F[x]$ has $p(\alpha) = 0$, for some $\alpha \in F$.

Assume the form of $p(x)$ with $p(\alpha)$ as

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$
$$p(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_1 \alpha + a_0 = 0$$

Obviously, $p(x) = p(x) - p(\alpha)$, which gives

$$\begin{aligned} p(x) &= a_n(x^n - \alpha^n) + a_{n-1}(x^{n-1} - \alpha^{n-1}) + \ldots + a_1(x - \alpha) \\ &= (x - \alpha)(\ldots) \end{aligned}$$

That is $(x - \alpha)$ is a linear factor of $p(x)$. We can write

$$p(x) = (x - \alpha)q_1(x)$$

with $deg(q_1(x)) < deg(p(x))$.

Since $deg(p(x))$ is finite, this process will stop after finite steps with

$$p(x) = (x - \alpha)(x - \beta)\ldots$$

Thus, we have $p(x)$ as a product of linear factors.

Conversely, assume for any non-constant polynomial $p(x) \in F[x]$, $p(x)$ can be factored as the product of linear factors, such as

$$p(x) = (x - \alpha)\ldots, \quad \alpha \in F$$

Obviously, $p(\alpha) = 0$. Thus, $\alpha \in F$ is a root of $p(x)$. So by Definition 4.4.2 of a field being algebraically closed, F is algebraically closed.

□

推论 4.4.1. An algebraically closed field F has no proper algebraic extension E.

证明. Suppose E is field extension of F. Then $F \subseteq E$.

Take any element $\alpha \in E$. The minimal polynomial of α over F is $p(x) \in F[x]$. $p(x)$ factors into linear factors by Theorem 4.4.2 since F is algebraically closed.

Note that minimal polynomial is irreducible, this implies that $p(x) \in F[x]$ is linear, with the form

$$p(x) = x - \alpha.$$

Since $p(x) \in F[x]$, $\alpha \in F$.

This means $\forall \alpha \in E \implies \alpha \in F$. This is $E \subseteq F$.

Therefore, we show $E = F$. □

We have the Fundamental Theorem of Algebra in different form.

定理 4.4.3. The field of complex numbers is algebraically closed.

We use the concept of splitting field for a weaker version of Fundamental Theorem of Algebra.

定义 4.4.3. Suppose a field F with its field extension E. Give a n-degree polynomial $f(x) \in F[x]$, E is **a splitting field of** $f(x)$ **over** F if:

1. $f(x)$ factors into product of linear factors in $E[x]$ with
$$f(x) = a_n(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n), \quad \alpha_i \in E;$$
2. In a field I with $F \subseteq I \subseteq E$, $f(x)$ can not factor into product of linear factors in $I[x]$.

备注 4.4.1. E is a minimal field that $f(x)$ factors into product of linear factors.

Splitting field is a weaker concept in the sense that it goes from $\forall f(x)$ in Fundamental Theorem of Algebra to $\exists f(x)$.

定理 4.4.4. If E is a splitting field of $f(x) \in F[x]$ over F, with
$$f(x) = a_n(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n), \quad \alpha_i \in E;$$
then,
$$E = F(\alpha_1, \alpha_2, \dots, \alpha_n).$$

证明. E is field extension of F, $F \subseteq E$, and $\alpha_i \in E$. So,
$$F(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq E$$

On the other hand, $f(x)$ in $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ has roots α_1, α_2, ..., α_n, since $f(\alpha_i) = 0$ with $\alpha_i \in F(\alpha_1, \alpha_2, \ldots, \alpha_n)$

Then,

$$f(x) = f(x) - f(\alpha_1) = (x - \alpha_1)q_1(x)$$

$$\begin{aligned} & f(\alpha_2) = (\alpha_2 - \alpha_1)q_1(\alpha_2) = 0 \\ \Longrightarrow\ & q_1(\alpha_2) = 0, \text{ since } (\alpha_2 \neq \alpha_1 \iff \alpha_2 - \alpha_1 \neq 0) \end{aligned}$$

So,

$$\begin{aligned} & q_1(x) = q_1(x) - q_1(\alpha_2) = (x - \alpha_2)q_2(x) \\ \Longrightarrow\ & f(x) = (x - \alpha_1)(x - \alpha_2)q_2(x) \end{aligned}$$

and

$$\begin{aligned} & f(\alpha_3) = 0 \implies q_2(\alpha_3) = 0, \text{ with} \\ & q_2(x) = q_2(x) - q_2(\alpha_3) = (x - \alpha_3)q_3(x) \\ \Longrightarrow\ & f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)q_3(x) \end{aligned}$$

and so on.

Since $f(x)$ has finite degree, the process above stops after finite steps and we have

$$f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n).$$

This means $f(x)$ factors as product of linear factors in $F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

By definition of splitting field, E is the minimal field that $f(x)$ factors as product of linear factors. This implies $E \subseteq F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Therefore, in summary, it shows $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

□

The following theorem tells the existence of a splitting field.

定理 4.4.5. Given a n-degree polynomial $f(x) \in F[x]$ over a field F, there exists a splitting field E of $f(x)$ over F.

证明. Note that F is a field, so $F[x]$ is a UFD. Thus, $f(x) \in F[x]$ has unique factorization. We can write as

$$f(x) = f_1(x)g_1(x), \quad f_1(x),\, g_1(x) \in F[x]$$

where $f_1(x)$ is an irreducible monic polynomial (with leading coefficient $= 1$). By Theorem 4.2.3, $f_1(x)$ has simple algebraic extension $E_1 = F(\alpha_1)$ of F, where the minimal polynomial of α_1 is $f_1(x) \in F[x]$.

This implies that $f(\alpha_1) = 0$ in E_1, thus we have in $F[x]$ that

$$(x - \alpha_1) | f(x).$$

Thus, we can write in $E_1[x] \supseteq F[x]$

$$f(x) = (x - \alpha_1)f_2(x)g_2(x), \quad f_2(x), g_2(x) \in E_1[x]$$

where $f_2(x)$ is an irreducible monic polynomial in $E_1[x]$.

Apply again Theorem 4.2.3 for $f_2(x)$, $f_2(x)$ has simple algebraic extension $E_2 = E_1(\alpha_2) = F(\alpha_1)(\alpha_2) = F(\alpha_1, \alpha_2)$ where the minimal polynomial of α_2 is $f_2(x) \in E_1[x]$ with $f_2(\alpha_2) = 0$.

Then, in $E_2[x]$ we can write

$$f(x) = (x - \alpha_2)(x - \alpha_2)f_3(x)g_3(x), \quad f_3(x), g_3(x) \in E_2[x]$$

where $f_3(x)$ is an irreducible monic polynomial in $E_2[x]$.

Apply again Theorem 4.2.3 for $f_3(x)$, $f_3(x)$ has simple algebraic extension $E_3 = E_2(\alpha_3) = F(\alpha_1, \alpha_2, \alpha_3)$ where the minimal polynomial of α_3 is $f_3(x) \in E_2[x]$ with $f_3(\alpha_3) = 0$.

This process continues after finite step, up to:

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

in $E[x]$ with

$$E = F(\alpha_1, \alpha_2, \dots, \alpha_n).$$

□

Now we investigate the question: Given a polynomial $f(x)$, its splitting field is isomorphic or not?

引理 4.4.1. Suppose L and $\overline{L}$ are fields, $L \cong \overline{L}$. Then

$$L[x] \cong \overline{L}[x].$$

证明. Consider the isomorphic mapping

$$a \in L \cong \overline{a} \in \overline{L}.$$

From there, we construct

$$\phi : L[x] \mapsto \overline{L}[x], \quad \phi(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \overline{a_i} x^i$$

We want to show ϕ is isomorphism between $L[x]$ and $\overline{L}[x]$:

1. ϕ is well-defined: every element $\sum_{i=0}^{n} a_i x^i \in L[x]$ maps to one element $\sum_{i=0}^{n} \overline{a_i} x^i \in \overline{L}[x]$.

2. ϕ is surjective: every element $\sum_{i=0}^{n} \overline{a_i} x^i \in \overline{L}[x]$ has one corresponding element $\sum_{i=0}^{n} a_i x^i \in L[x]$;

3. ϕ is injective: Suppose $\overline{f}(x) = \overline{g}(x)$ for $\overline{f}(x)$, $\overline{g}(x) \in \overline{L}[x]$, this implies their coefficients $\overline{a_i} = \overline{b_i}$ where $\overline{a_i}$ are coefficients of $\overline{f}(x)$ and $\overline{b_i}$ are coefficients of $\overline{g}(x)$. By isomorphism between L and $\overline{L}$, we have $a_i = b_i$, and thus $f(x) = g(x)$ for $f(x)$ is the preimage of $\overline{f}(x)$ in $L[x]$ and $g(x)$ is the preimage of $\overline{g}(x)$ in $L[x]$.

4. ϕ is homomorphism: Suppose

$$f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \overline{f}(x) = \sum_{i=0}^{n} \overline{a} x^i$$
$$g(x) = \sum_{i=0}^{n} b_i x^i \mapsto \overline{g}(x) = \sum_{i=0}^{n} \overline{b} x^i$$

$$\begin{aligned}
\phi\big(f(x)+g(x)\big) &= \phi\big(\sum_{i=0}^{n}(a_i+b_i)x^i\big) \\
&= \sum_{i=0}^{n}\big(\overline{a_i+b_i}\big)x^i \\
&= \sum_{i=0}^{n}\big(\overline{a}_i+\overline{b}_i\big)x^i, \qquad \text{by additio on } \overline{L} \\
&= \sum_{i=0}^{n}\overline{a}x^i+\sum_{i=0}^{n}\overline{b}x^i \\
&= \overline{f}(x)+\overline{g}(x)
\end{aligned}$$

$$\begin{aligned}
\phi\big(f(x)g(x)\big) &= \phi\big(\sum_{k}\big(\sum_{i+j=k}a_ib_j\big)x^k\big) \\
&= \sum_{k}\big(\sum_{i+j=k}\overline{a_ib_j}\big)x^k \\
&= \sum_{k}\big(\sum_{i+j=k}\overline{a}_i\overline{b}_j\big)x^k \\
&= \overline{f}(x)\overline{g}(x)
\end{aligned}$$

5. Summing up, ϕ is isomorphic between $L[x]$ and $\overline{L}[x]$.

Therefore, we just show $L[x] \cong \overline{L}[x]$.

□

引理 4.4.2. Suppose L and $\overline{L}$ are fields, $L \cong \overline{L}$. $p(x) \in L[x]$ is irreducible monic polynomial. $p(x)$ has corresponding irreducible polynomial $\overline{p}(x) \in \overline{L}[x]$.

Assume $L(\alpha)$ is simple algebraic field extension of α of L, where the minimal polynomial of α over L is $p(x) \in L[x]$ with $p(\alpha) = 0$.

Assume $\overline{L}(\overline{\alpha})$ is simple algebraic field extension of $\overline{\alpha}$ of $\overline{L}$, where the minimal polynomial of $\overline{\alpha}$ over $\overline{L}$ is $\overline{p}(x) \in \overline{L}[x]$ with $\overline{p}(\overline{\alpha}) = 0$.

Then, there exists isomorphism between $L(\alpha)$ and $\overline{L}(\overline{\alpha})$. This isomorphism keeps the isomorphism between $L \subset L(\alpha)$ and $\overline{L} \subset \overline{L}(\overline{\alpha})$.

证明. Suppose the isomorphism between L and $\overline{L}$ with

$$\forall a \in L \iff \overline{a} \in \overline{L}.$$

Assume the degree of $p(x)$ is n, thus $deg(\overline{p}(x)) = n$..

Construct a mapping

$$\phi : L(\alpha) \longrightarrow \overline{L}(\overline{\alpha}), \quad \sum_{i=0}^{n-1} a_i\alpha^i \in L(\alpha) \mapsto \sum_{i=0}^{n-1} \overline{a}_i\overline{\alpha}^i \in \overline{L}(\overline{\alpha}).$$

We want to show ϕ is isomorphism. Analogous to the reasoning in the proof of Lemma 4.4.1, we have

1. ϕ is well-defined, and $\phi : a \mapsto \overline{a}$;
2. ϕ is surjective;
3. ϕ is injective.

We are left to show ϕ is homomorphism: Suppose

$$f(\alpha) = \sum_{i=0}^{n-1} a_i\alpha^i \mapsto \overline{f}(\overline{\alpha}) = \sum_{i=0}^{n-1} \overline{a}_i\,\overline{\alpha}^i$$
$$g(\alpha) = \sum_{i=0}^{n-1} b_i\alpha^i \mapsto \overline{g}(\overline{\alpha}) = \sum_{i=0}^{n-1} \overline{b}_i\,\overline{\alpha}^i$$

$$\begin{aligned}
\phi\big(f(\alpha) + g(\alpha)\big) &= \phi\big(\sum_{i=0}^{n-1}(a_i + b_i)\alpha^i\big) \\
&= \sum_{i=0}^{n-1} \big(\overline{a_i + b_i}\big)\overline{\alpha}^i \\
&= \sum_{i=0}^{n-1} \big(\overline{a}_i + \overline{b}_i\big)\overline{\alpha}^i \\
&= \sum_{i=0}^{n-1} \overline{a}_i\overline{\alpha}^i + \sum_{i=0}^{n-1} \overline{b}_i\overline{\alpha}^i \\
&= \overline{f}(\overline{\alpha}) + \overline{g}(\overline{\alpha})
\end{aligned}$$

On the other hand, $f(x)g(x) \in L[x]$. This implies

$$f(\alpha)g(\alpha) = r(\alpha).$$

where

$$f(x)g(x) = p(x)q(x) + r(x), \quad deg(r(x)) = 0, \text{ or } deg(r(x)) < deg(p(x)).$$

By Lemma 4.4.1,

$$\begin{aligned} & f(x)g(x) = p(x)q(x) + r(x) \\ \implies & \overline{f}(x)\overline{g}(x) = \overline{p}(x)\overline{q}(x) + \overline{r}(x) \\ \implies & \overline{f}(\overline{\alpha})\overline{g}(\overline{\alpha}) = \overline{p}(\overline{\alpha})\overline{q}(\overline{\alpha}) + \overline{r}(\overline{\alpha}) = \overline{r}(\overline{\alpha}), \quad \text{since } \overline{p}(\overline{\alpha}) = 0 \end{aligned}$$

This means

$$f(\alpha)g(\alpha) = r(\alpha) \implies \overline{f}(\overline{\alpha})\overline{g}(\overline{\alpha}) = \overline{r}(\overline{\alpha})$$

Thus, we just show ϕ is a homomorphism, and therefore ϕ is isomorphic between $L(\alpha)$ and $\overline{L}(\overline{\alpha})$. Moreover, ϕ reserves the isomorphism between L and $\overline{L}$.

□

Now we prove the uniqueness of the splitting field.

定理 4.4.6. Suppose fields F and $\overline{F}$, with $F \cong \overline{F}$. The n-degree polynomial $f(x) \in F[x]$ has the corresponding polynomial $\overline{f}(x) \in \overline{F}[x]$ in the sense of Lemma 4.4.1.

Further assume

- $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a splitting field of $f(x)$ over F;
- $\overline{E} = \overline{F}(\beta_1, \beta_2, \ldots, \beta_n)$ is a splitting field of $\overline{f}(x)$ over $\overline{F}$.

Then, there exists a isomorphism

$$\phi : E \iff \overline{E}$$

where

- ϕ keeps isomorphism $F \cong \overline{F}$;
- After proper rearrangement,

$$\alpha_i \iff \beta_i.$$

证明. Prove by mathematical induction:

Note that by $F \cong \overline{F}$, there exists $a \in F \iff \overline{a} \in \overline{F}$.

1. If $k = 0$, then $E = F$ and $\overline{E} = \overline{F}$. So $F \cong \overline{F} \implies E \cong \overline{E}$.

2. Suppose if $k < n$, there exists

$$L := F(\alpha_1, \alpha_2, \ldots, \alpha_k) \cong \overline{L} := \overline{F}(\beta_1, \beta_2, \ldots, \beta_k), \quad \alpha_i \iff \beta_i$$

by proper rearrangement of β_1, β_2, ..., β_k.

Then, L and $\overline{L}$ are fields. So we can consider $L[x]$ and $\overline{L}[x]$. Suppose $f(x) \in L[x]$, we can factor $f(x)$ as

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_k) p_k(x) q_k(x)$$

where $p_k(x)$ is irreducible monic polynomial of $L[x]$.

By Lemma 4.4.1, there exists the corresponding polynomial $\overline{f}(x) \in \overline{L}[x]$ such that

$$\overline{f}(x) = (x - \beta_1)(x - \beta_2) \ldots (x - \beta_k) \overline{p_k}(x) \overline{q_k}(x)$$

where $\overline{p_k}(x)$ is irreducible monic polynomial of $\overline{L}[x]$.

Consider in the field extensions $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\overline{F}(\beta_1, \beta_2, \ldots, \beta_n$, we can factor

$$p_k(x) q_k(x) = (x - \alpha_{k+1}) \ldots (x - \alpha_n)$$
$$\overline{p_k}(x) \overline{q_k}(x) = (x - \beta_{k+1}) \ldots (x - \beta_n).$$

After rearragement of α_{k+1}, ..., α_n and β_{k+1}, ..., β_n, we can have

$$p_k(\alpha_{k+1}) = 0, \quad \overline{p_k}(\beta_{k+1}) = 0.$$

Apply Lemma 4.4.2, there exists isomorphism between $L(\alpha_{k+1}$ and $\overline{L}(\beta_{k+1}$, which is

$$L(\alpha_{k+1}) = F(\alpha_1, \alpha_2, \ldots, \alpha_{k+1}) \cong \overline{L}(\beta_{k+1}) = \overline{F}(\beta_1, \beta_2, \ldots, \beta_{k+1}),$$

with $\alpha_i \iff \beta_i$, $i = 1, \ldots, k+1$.

□

备注 4.4.2. By Corollary 3.6.1, n-degree polynomial over some field has at most n roots.

Theorem 4.4.5 tells there exists some field extension where $f(x)$ has n roots.

Theorem 4.4.6 tells $f(x)$ via different field extension has the same n roots in the sense of isomorphism.

So, this means that given any polynomial $f(x)$ over any field F, the roots of $f(x)$ is 'fixed'.

In some sense, if given the polynomial $f(x)$, we can use splitting field extension to replace the Fundamental Theorem of Algebra.

Here below shows an important property of splitting field.

定理 4.4.7. Suppose E is a splitting field of some polynomial $f(x) \in F[x]$ over F.

Given any element $\beta \in E$, then the minimal polynomial of β over F factors into a product of linear factors in E.

证明. Let the splitting field of $f(x)$ over F is

$$E = F(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

where $f(\alpha_i) = 0$. (Obviously, α_i is algebraic over F.)

Prove by contradiction: Assume β has the minimal polynomial $g(x)$ over F, with $g(\beta) = 0$. Further assume $g(x)$ can not be factored as product of linear factors. Thus, we can write

$$g(x) = (x - \beta)p(x)g_1(x), \quad p(x), g_1(x) \in F[x] \subseteq E[x].$$

where $p(x)$ is irreducible monic polynomial.

By our assumption, $deg(p(x)) = m > 1$.

Let $p(x)$ be the minimal polynomial of β' over E, with $p(\beta') = 0$.

Note that

$$g(\beta') = (\beta' - \beta)p(\beta')g_1(\beta') = 0, \quad \text{by } p(\beta') = 0.$$

By Theorem 4.2.4, $F(\beta)$ and $F(\beta')$ are simple algebraic extension of F. β and β' has the same minimal polynomial over F, $p(x)$, then we have

$$F(\beta) \cong F(\beta').$$

By Lemma 4.4.1, $F(\beta) \cong F(\beta')$ implies $F(\beta)[x] \cong F(\beta')[x]$.

Also, this isomorphism keeps $f(x) \longleftrightarrow f(x)$.

By Theorem 4.4.6, the splitting field of $f(x)$ over $F(\beta)$ is isomorphic to the splitting field of $f(x)$ over $F(\beta')$.

Note that $F(\beta, \alpha_1, \alpha_2, \ldots, \alpha_n)$ is the splitting field of $f(x)$ over $F(\beta)$, while $F(\beta', \alpha_1, \alpha_2, \ldots, \alpha_n)$ is the splitting field of $f(x)$ over $F(\beta')$. Thus,

$$\begin{aligned} & F(\beta, \alpha_1, \alpha_2, \ldots, \alpha_n) \cong F(\beta', \alpha_1, \alpha_2, \ldots, \alpha_n) \\ \Longrightarrow\ & \big(F(\beta, \alpha_1, \alpha_2, \ldots, \alpha_n) : F\big) = \big(F(\beta', \alpha_1, \alpha_2, \ldots, \alpha_n) : F\big). \end{aligned}$$

Obviously, we have

$$\big(F(\beta', \alpha_1, \alpha_2, \ldots, \alpha_n) : F\big) = \big(E(\beta') : E\big)\big(E : F\big) = m\big(E : F\big)$$

Since $\beta \in E$, we have

$$\big(F(\beta, \alpha_1, \alpha_2, \ldots, \alpha_n) : F\big) = \big(F(\beta, \alpha_1, \alpha_2, \ldots, \alpha_n) : E\big)\big(E : F\big) = \big(E : F\big)$$

Because $deg(p(x)) = m > 1$ from our assumption, we obtain contradiction.

□

练习 4.4.1. Prove that in the field of rational numbers, the splitting field of the polynomial $x^4 + 1$ is a simple field extension $F(\alpha)$, where a is one of the roots of $x^4 + 1$.

证明. Consider the field of complex numbers $\mathbb{C}$ where polynomial has roots. The polynomial $x^4 + 1$ in $\mathbb{C}$ has 4 roots:

$$\alpha_1 = \frac{sqrt2}{2}(1 + i), \quad \alpha_2 = \frac{sqrt2}{2}(1 - i),$$
$$\alpha_3 = -\alpha_1, \quad \alpha_4 = -\alpha_2.$$

Note that $\alpha_2 = -\alpha_1^3$, which implies

$$F(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = F(\alpha_1).$$

This simple field extension $F(\alpha_1)$ is the splitting field of the polynomial $x^4 + 1$ over F. □

练习 4.4.2. Suppose F is a field of rational numbers. the irreducible polynomial $x^3 - a$ over F, with α is one of the roots of $x^3 - a$. Prove that $F(\alpha)$ is not the splitting field of the polynomial $x^3 - a$ over F.

证明. $x^3 - a$ has 3 roots:

$$a^{\frac{1}{3}}, \quad a^{\frac{1}{3}}\omega, \quad a^{\frac{1}{3}}\omega^2,$$

where

$$\omega = \frac{-1 + \sqrt{3}i}{2}, \quad \omega^3 = 1.$$

The splitting field of $x^3 - a$ over F is

$$E := F\big(a^{\frac{1}{3}}, a^{\frac{1}{3}}\omega, a^{\frac{1}{3}}\omega^2\big) = F\big(a^{\frac{1}{3}}, \omega\big)$$

Thus, we have

$$F\big(a^{\frac{1}{3}}, \omega\big) \supseteq F\big(a^{\frac{1}{3}}\big) \supseteq F.$$

Note that $\omega \notin F\big(a^{\frac{1}{3}}\big)$, and ω is the root of the polynomial $x^2 + x + 1$ over $F\big(a^{\frac{1}{3}}\big)$, thus,

$$\big(F\big(a^{\frac{1}{3}}, \omega\big) : F\big(a^{\frac{1}{3}}\big)\big) = 2.$$

Note that $a^{\frac{1}{3}}$ is the root of irreducible polynomial $x^3 - a$ over F. Thus,

$$\big(F\big(a^{\frac{1}{3}}\big) : F\big) = 3.$$

Therefore,

$$\begin{aligned}
&\big(E : F\big) \\
=&\big(F\big(a^{\frac{1}{3}}, \omega\big) : F\big) \\
=&\big(F\big(a^{\frac{1}{3}}, \omega\big) : F\big(a^{\frac{1}{3}}\big)\big)\big(F\big(a^{\frac{1}{3}}\big) : F\big) = 2 \times 3 = 6.
\end{aligned}$$

α is a root of $x^3 - a$. Then,

$$\big(F(\alpha) : F\big) = 3.$$

Therefore, $E \neq F(\alpha)$, which is $F(\alpha)$ is not the splitting field of the polynomial $x^3 - a$ over F.

□

练习 4.4.3. Suppose the following m irreducible monic polynomials over F:

$$p_1(x),\ p_2(x),\ \ldots,\ p_m(x).$$

Prove that there exists a finite field extension

$$F(\alpha_1, \alpha_2, \ldots, \alpha_m)$$

where the minimal polynomial of α_i over F is $p_i(x)$.

证明. Consider

$$F(x) = p_1(x)p_2(x)\ldots p_m(x).$$

Construct E as the splitting field of $f(x)$ over F.

E has all the roots of $f(x)$, which means $\alpha_1, \alpha_2, \ldots, \alpha_m \in E$ where α_i is the root of $p_i(x)$. Thus,

$$F(\alpha_1, \alpha_2, \ldots, \alpha_m) \subseteq E.$$

Since $p_i(x)$ is irreducible monic polynomial over F, they are the minimal polynomial of α_i over F. That is α_i is algebraic over F, thus $F(\alpha_1, \alpha_2, \ldots, \alpha_m)$ is a finite field extension of F.

□

练习 4.4.4. Suppose P is a field with $char(P) = p$ where p is prime number. $F = P(\alpha)$ is a simple field extension of P. Suppose α is a root of the polynomial $x^p - a \in P[x]$. Is $P(\alpha)$ a splitting field of $x^p - a$ over P?

解答. Since α is a root of $x^p - a$, thus $\alpha^p = a$. The field P and thus the field $F \supset P$ has characteristic of the prime number p. So in $F[x]$,

$$x^p - a = x^p - \alpha^p = (x - \alpha)^p.$$

Thus, $P(\alpha)$ can be considered as the field extension by adding p roots of $x^p - a$. Thus, $P(\alpha)$ is the splitting field of the polynomial $x^p - a$ over P.