

# 近世代数 (H) 笔记

林晓烁 2024 春

<https://xiaoshuo-lin.github.io>

# 目 录

<b>导言</b> . . . . .	1
<b>第一部分 课堂笔记</b> . . . . .	2
<b>第一章 预备知识</b> . . . . .	4
1.1 集合与映射 . . . . .	4
<b>第二章 环论</b> . . . . .	7
2.1 环的定义 . . . . .	7
2.2 理想与商环 . . . . .	10
2.3 分式域与商域 . . . . .	14
2.4 一元多项式环 . . . . .	18
2.5 Euclid 整环 . . . . .	25
2.6 Gauss 素数 . . . . .	29
2.7 唯一分解整环 . . . . .	35
2.8 中国剩余定理 . . . . .	43
<b>第三章 域论</b> . . . . .	47
3.1 域扩张与单扩张 . . . . .	47
3.2 域的代数扩张 . . . . .	52
3.3 分裂域 . . . . .	55
3.4 有限域 . . . . .	61
3.5 分圆域 . . . . .	65
<b>第四章 群论</b> . . . . .	69
4.1 群的定义 . . . . .	69
4.2 循环群 . . . . .	72
4.3 正规子群与商群 . . . . .	74

4.4 对称群 . . . . .	77
4.5 群作用 . . . . .	83
4.6 Sylow 定理 . . . . .	90
4.7 自由群与群的展示 . . . . .	92
4.8 有限生成 Abel 群 . . . . .	95
4.9 群的合成列 . . . . .	99
4.10 半直积 . . . . .	102
<b>第五章 Galois 理论 . . . . .</b>	<b>103</b>
5.1 Galois 扩张 . . . . .	103
5.2 Galois 对应 . . . . .	106
5.3 根式扩张 . . . . .	110
5.4 判别式 . . . . .	115
<b>第二部分 往年真题 . . . . .</b>	<b>117</b>
<b>第六章 期中考试题目 . . . . .</b>	<b>119</b>
6.1 2020 春期中考试 . . . . .	119
6.2 2022 春期中考试 . . . . .	120
6.3 2023 春期中考试 . . . . .	121
6.4 2024 春期中考试 . . . . .	125
<b>第七章 期末考试题目 . . . . .</b>	<b>127</b>
7.1 2020 春期末考试 . . . . .	127
7.2 2021 春期末考试 . . . . .	128
7.3 2023 春期末考试 . . . . .	128
7.4 2024 春期末考试 . . . . .	129

# 导言

## 简要说明

**旨趣** 这是 2024 年春季学期近世代数 (H) 课堂笔记, 课程由中国科学技术大学数学科学学院陈小伍教授讲授.

### 附记

(1) 相关资料:

- ◊ Évariste Galois 档案: <http://www.galois-group.net>
- ◊ <https://grothendieck.umontpellier.fr/archives-grothendieck/>

(2) 访问我的个人主页查看本文档最新版本: <https://xiaoshuo-lin.github.io>

## 致谢

这份笔记所用 L<sup>A</sup>T<sub>E</sub>X 模板来自北京国际数学研究中心李文威教授, 在此表示谢意.

# 第一部分

## 课堂笔记



# 第一章 预备知识

## 1.1 集合与映射

**例 1.1.1 (映射的例子)** (1) 恒等映射  $\text{Id}_X : X \rightarrow X, x \mapsto x$ .

(2) 设  $S \subset X$ . 包含映射  $\text{inc} : S \rightarrow X, s \mapsto s$ .

**注记 1.1.2** 根据映射相等的要求, 当  $S \subsetneq X$  时, 上述  $\text{inc} \neq \text{Id}_X$ .

**约定 1.1.3** 用  $X \xrightarrow{f} Y$  表示单射, 用  $X \xrightarrow{f} Y$  表示满射, 用  $X \xrightarrow{\sim} Y$  表示双射.

**例 1.1.4** 有如下交换图表:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow \bar{f} & \swarrow \text{inc} \\ & \text{Im}(f) & \end{array}$$

即  $f = \text{inc} \circ \bar{f}$ , 其中  $\bar{f} : X \rightarrow \text{Im}(f), x \mapsto f(x)$ .

**练习 1.1.5 (范畴意义下单满射的内蕴刻画)** 设  $f : X \rightarrow Y$ . 证明:

- (1)  $f$  是单射  $\iff [f \text{ 满足左消去律: } \forall g, g' : W \rightarrow X, f \circ g = f \circ g' \implies g = g']$ .
- (2)  $f$  是满射  $\iff [f \text{ 满足右消去律: } \forall h, h' : Y \rightarrow Z, h \circ f = h' \circ f \implies h = h']$ .
- (3)  $f$  是双射  $\iff [\exists! g : Y \rightarrow X, \text{ s.t. } g \circ f = \text{Id}_X, f \circ g = \text{Id}_Y]$ .

**例 1.1.6**

$$\begin{aligned} \text{Map}(X, \{0, 1\}) &\xrightarrow{\sim} \mathcal{P}(X) \\ f &\longmapsto S_f := \{x \in X : f(x) = 1\}. \end{aligned}$$

其逆映射为

$$\mathcal{P}(X) \rightarrow \text{Map}(X, \{0, 1\})$$

$$S \mapsto \chi_S,$$

其中  $\chi_S$  为  $S$  的特征函数.

**定义 1.1.7 (无交并的集合论定义)** 设  $(A_i : i \in I)$  是以  $I$  为指标集的一族集合, 其无交并定义为

$$\bigsqcup_{i \in I} A_i = \bigcup_{i \in I} \{(x, i) : x \in A_i\}.$$

**例 1.1.8** 典范双射

$$\begin{aligned} \text{Map}(X \sqcup Y, Z) &\xrightarrow{\sim} \text{Map}(X, Z) \times \text{Map}(Y, Z) \\ f &\longmapsto (f|_X, f|_Y). \end{aligned}$$

**例 1.1.9** 典范双射

$$\begin{aligned} \text{Map}(X, Y \times Z) &\xrightarrow{\sim} \text{Map}(X, Y) \times \text{Map}(Y, Z) \\ g &\longmapsto (g_1, g_2), \end{aligned}$$

其中

$$\begin{aligned} g : X &\rightarrow Y \times Z \\ x &\mapsto (g_1(x), g_2(x)). \end{aligned}$$

**例 1.1.10 (伴随双射)** 存在典范双射

$$\begin{aligned} \text{Map}(X \times Y, Z) &\xrightarrow{\sim} \text{Map}(X, \text{Map}(Y, Z)) \\ f &\longmapsto (x \mapsto \phi_{f,x}), \end{aligned}$$

其中

$$\begin{aligned} \phi_{f,x} : Y &\rightarrow Z \\ y &\mapsto f(x, y). \end{aligned}$$

**注记 1.1.11** 集合  $X$  上最小的等价关系即“等号”:

$$E = \{(x, x) : x \in X\}.$$

**定义 1.1.12** 给定  $X$  上的等价关系  $\overset{R}{\sim}$ .

- (1)  $\forall a \in X$ ,  $a$  的等价类  $[a] := \{x \in X : x \overset{R}{\sim} a\}.$
- (2) 关于  $\overset{R}{\sim}$  的商集  $X / \overset{R}{\sim} := \{\text{所有的等价类}\} \subset \mathcal{P}(X).$
- (3) 商映射  $\pi_R : X \twoheadrightarrow X / \overset{R}{\sim}, a \mapsto [a].$
- (4) 关于  $\overset{R}{\sim}$  的完全代表元系为  $S \subset X$ , s.t.  $\forall x \in X, \exists! s \in S, s \in [x].$

**练习 1.1.13 (完全代表元系的等价刻画)** 设  $\overset{R}{\sim}$  是  $X$  上的等价关系,  $S \subset X$ . 证明:  $S$  是完全代表元系当且仅当复合映射

$$S \xrightarrow{\text{inc}} X \xrightarrow{\pi_R} X / \overset{R}{\sim}$$

是双射.

**定义 1.1.14** 集合  $X$  的分拆为  $\mathcal{R} = \{X_i : i \in I\} \subset \mathcal{P}(X)$ , 满足

- (1)  $X_i \neq \emptyset, \forall i \in I$ .
- (2)  $X_i \cap X_j = \emptyset, \forall i \neq j$ .
- (3)  $X = \bigcup_{i \in I} X_i$ .

**性质 1.1.15** 集合  $X$  上的等价关系与分拆有如下关系:

- (1) 若  $R$  是  $X$  上的等价关系, 则  $X / \overset{R}{\sim}$  是  $X$  的一个分拆.
- (2) 若  $\mathcal{R} = \{X_i : i \in I\}$  是  $X$  的分拆, 定义关系  $\overset{T}{\sim}: x \overset{T}{\sim} y \iff \exists i \in I, \text{s.t. } x, y \in X_i$ , 则  $\overset{T}{\sim}$  是  $X$  上的等价关系, 且  $X / \overset{T}{\sim} = \mathcal{R}$ .

**定义 1.1.16** 映射  $f: X \rightarrow Y$  给出  $X$  上的等价关系  $\overset{f}{\sim}: x \overset{f}{\sim} x' \iff f(x) = f(x')$ . 对任意  $y \in Y$ , 记  $f^{-1}(y) := \{x \in X : f(x) = y\}$ , 称为  $f$  在  $y$  上的原像集(或纤维).

**注记 1.1.17**  $f^{-1}(y) \neq \emptyset \iff y \in \text{Im}(f)$ .

**练习 1.1.18** 关于  $\overset{f}{\sim}$  的等价类  $[x] = f^{-1}(f(x))$ .

**定理 1.1.19 (映射基本定理)** 设  $f: X \rightarrow Y$ , 则  $f$  诱导双射

$$\begin{aligned} \tilde{f}: X / \overset{f}{\sim} &\xrightarrow{\sim} \text{Im}(f) \\ [x] &\mapsto f(x). \end{aligned}$$

也即有如下交换图表:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \pi_f \downarrow & & \uparrow \text{inc} \\ X / \overset{f}{\sim} & \xrightarrow{\tilde{f}} & \text{Im}(f) \end{array}$$

**练习 1.1.20** 设集合  $X$  上的二元运算  $\cdot$  满足结合律:  $(x \cdot y) \cdot z = x \cdot (y \cdot z), \forall x, y, z \in X$ . 证明:

$$((x \cdot y) \cdot z) \cdot w = x \cdot (y \cdot (z \cdot w)), \quad \forall x, y, z, w \in X.$$

## 第二章 环论

### 2.1 环的定义

**定义 2.1.1** (含幺) 环是三元组  $(R, +, \cdot)$ , 其中  $R \neq \emptyset$ , 加法  $+ : R \times R \rightarrow R, (a, b) \mapsto a + b$  与乘法  $\cdot : R \times R \rightarrow R, (a, b) \mapsto a \cdot b$  满足以下八条公理:

(A1) 加法结合律:  $(a + b) + c = a + (b + c), \forall a, b, c \in R.$

(A2) 加法交换律:  $a + b = b + a, \forall a, b \in R.$

(A3) 加法有零元:  $\exists 0_R \in R$ , s.t.  $a + 0_R = a, \forall a \in R.$

(A4) 加法有负元:  $\forall a \in R, \exists b \in R$ , s.t.  $a + b = 0_R.$

(M1) 乘法结合律:  $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in R.$

(M2) 乘法有幺元:  $\exists 1_R \in R$ , s.t.  $a \cdot 1_R = a = 1_R \cdot a, \forall a \in R.$

(D1) 关于第一个分量的分配律:  $(a + b) \cdot c = a \cdot c + b \cdot c, \forall a, b, c \in R.$

(D2) 关于第二个分量的分配律:  $a \cdot (b + c) = a \cdot b + a \cdot c, \forall a, b, c \in R.$

**注记 2.1.2** (1) 由 (A2) 易得加法零元唯一.

(2) 由 (A1) 与 (A2) 易得加法负元唯一. 把  $a$  的加法负元记作  $-a$ .

(3) 定义  $R$  上减法:  $a - b := a + (-b), \forall a, b \in R.$

(4) 由定义易得乘法幺元唯一性.

**例 2.1.3 (环的例子)** (1) 整数环  $\mathbb{Z} = (\mathbb{Z}, +, \cdot).$

(2) Gauss 整数环  $\mathbb{Z}[\sqrt{-1}] := \{m + n\sqrt{-1} : m, n \in \mathbb{Z}\}.$

(3) 一元有理系数多项式环  $\mathbb{Q}[x].$

(4) 模  $n(n \geq 2)$  同余类环  $\overline{0}, \overline{1}, \dots, \overline{n-1}.$

(5)  $n$  阶复方阵  $M_n(\mathbb{C})$  是非交换环的基本例子.

**定义 2.1.4**  $\forall a \in R, n \in \mathbb{Z}$ , 定义  $a$  的  $n$  倍  $na$  如下:  $0a := 0_R, 1a := a$ , 对  $n > 0$ ,

$$na := \underbrace{a + \cdots + a}_{n \uparrow}, \quad (-n)a := \underbrace{(-a) + \cdots + (-a)}_{n \uparrow}.$$

**练习 2.1.5**  $\forall a \in R, \forall m, n \in \mathbb{Z}$ , 总有  $(m+n)a = ma + na$ . [提示] 留心对  $m, n$  异号情形的讨论.

**练习 2.1.6**  $\forall a \in R, n \in \mathbb{Z}$ , 总有  $na = (n1_R) \cdot a$ . 特别地, 当  $n = 0$  时, 可得  $0_R = 0_R \cdot a, \forall a \in R$ .

**练习 2.1.7 (广义分配律)**  $\left(\sum_{i=1}^m a_i\right) \left(\sum_{j=1}^n b_j\right) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j$ . [提示] 运用双重归纳.

**练习 2.1.8**  $\forall n \in \mathbb{Z}, a, b \in R, (na) \cdot b = n(a \cdot b) = a \cdot (nb)$ .

**例 2.1.9 (零环)** 以下等价:

(1)  $0_R = 1_R$ .

(2)  $R = \{0_R\}$ .

(3)  $R$  仅含一个元素.

[提示] (2)  $\Rightarrow$  (3)  $\Rightarrow$  (1) 是平凡的.

#### 阅读提示

以下如不另作说明, 环皆指非零的含幺环.

**例 2.1.10 (二元环)** 由例 2.1.9 可知二元环中  $0_R \neq 1_R$ , 进而可定出加法表与乘法表. 易见二元环本质上即  $\mathbb{Z}_2$ .

#### 阅读提示

以下总假定环  $R$  为含幺交换环.

**定义 2.1.11 ( $a$  的  $n$  次幂)**

$$\text{当 } n \geq 1 \text{ 时, } a^n := \underbrace{a \cdots a}_{n \uparrow}; \quad a^0 := 1_R.$$

**性质 2.1.12**  $a^n \cdot a^m = a^{n+m}$ .

**定理 2.1.13 (二项式定理)** 设  $a, b \in R, n \geq 1$ , 则

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^i \cdot b^{n-i}.$$

**定义 2.1.14**  $a \in R$  称为乘法可逆元(或单位), 若存在  $b \in R$ , 使得  $a \cdot b = 1_R$ .

**注记 2.1.15** 若  $a$  可逆, 对应的  $b$  是唯一的, 记  $b = a^{-1}$ , 称为  $a$  的逆. 易知  $(a^{-1})^{-1} = a$ .

**定义 2.1.16 (除法)** 若  $a$  可逆,  $c \div a := c \cdot a^{-1}$ .

**注记 2.1.17** (1) 由于  $0_R \neq 1_R$ ,  $0_R$  一定不可逆.

(2) 若  $a$  可逆, 可对全体  $n \in \mathbb{Z}$  定义  $a^n$ .

(3) 对可逆元有乘法消去律.

**定义 2.1.18** 环  $R$  的可逆元子集  $U(R) := \{a \in R : a \text{ 可逆}\}$  对  $R$  的乘法构成一个 Abel 群, 称为  $R$  的单位群.

**例 2.1.19** (1)  $U(\mathbb{Z}) = \{1, -1\}$ .

(2)  $U(\mathbb{Q}) = \mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ .

(3)  $U(\mathbb{Z}_n) = \{[m] : (m, n) = 1\}$ .

(4)  $U(\mathbb{Z}[\sqrt{-1}]) = \{\pm 1, \pm \sqrt{-1}\}$ .

**定义 2.1.20** 非零环  $R$  称为整环, 若  $ab = 0_R$  蕴含  $a = 0_R$  或  $b = 0_R$ .

**定义 2.1.21** 非零环  $R$  称为域, 若非零元均可逆.

**注记 2.1.22** (1) 整环中满足乘法消去律:  $ab = ac \implies a(b - c) = 0_R \xrightarrow{\text{若 } a \neq 0_R} b = c$ .

(2) 域是整环.

**例 2.1.23**  $\mathbb{Z}[\sqrt{-1}]$  是整环, 但不是域.

**命题 2.1.24** 设  $n \geq 2$ , 则以下等价:

(1)  $\mathbb{Z}_n$  是整环.

(2)  $n$  是素数.

(3)  $\mathbb{Z}_n$  是域.

**提示** (3)  $\implies$  (1)  $\implies$  (2)  $\implies$  (3).

**注记 2.1.25** 若  $\mathbb{Z}_p$  是域, 记之为  $\mathbb{F}_p$ .

**练习 2.1.26** 设  $R$  为有限环, 则  $R$  是整环  $\iff R$  是域.

**定义 2.1.27** 设  $R$  为环. 子集  $S \subset R$  称为子环, 若满足  $1_R \in S$ ,  $S$  对加法、减法、乘法封闭.

### 阅读提示

我们强烈要求  $1_R \in S$ .

**定义 2.1.28** 设  $K$  为域. 子环  $S \subset K$  称为子域, 若满足  $0_R \neq a \in S$ , 则  $a^{-1} \in S$ , 即对除法也封闭.

**注记 2.1.29** 子环自然成为环; 子域自身作为环是域.

**练习 2.1.30**  $\mathbb{Z}$  与  $\mathbb{Z}_n$  均没有真子环.

**练习 2.1.31**  $\mathbb{Q}$  与  $\mathbb{F}_p$  均没有真子域.

**练习 2.1.32**  $\mathbb{Q}(\sqrt{-1}) := \{a + b\sqrt{-1} : a, b \in \mathbb{Q}\} \subset \mathbb{C}$  是子域.

**练习 2.1.33** 若  $S \subset \mathbb{Q}(\sqrt{-1})$  是子域, 则  $S = \mathbb{Q}$  或  $S = \mathbb{Q}(\sqrt{-1})$ .

**练习 2.1.34** 设  $p$  是素数, 则  $R(p) := \left\{ \frac{m}{p^a} : a \geq 0, m \in \mathbb{Z} \right\} \subset \mathbb{Q}$  是子环.

## 2.2 理想与商环

设  $R = (R, +, \cdot)$ ,  $S = (S, +, \cdot)$  为两环.

**定义 2.2.1** 映射  $\theta : R \rightarrow S$  称为环同态, 若

- (1)  $\theta(a + b) = \theta(a) + \theta(b), \theta(a \cdot b) = \theta(a) \cdot \theta(b), \forall a, b \in R.$
- (2)  $\theta(1_R) = 1_S.$

双射的环同态称为环同构, 记为  $\theta : R \xrightarrow{\sim} S$ .

**性质 2.2.2** (1)  $\theta(0_R) = 0_S, \theta(a - b) = \theta(a) - \theta(b), \forall a, b \in R.$

- (2)  $\theta(a^m) = \theta(a)^m.$

(3) 环同态的复合仍是环同态.

(4) 若  $\theta : R \rightarrow S$  为环同构, 则  $\theta^{-1} : S \rightarrow R$  亦为环同构.

**例 2.2.3** 不存在  $\mathbb{Q} \rightarrow \mathbb{Z}_n$  的环同态. 提示 考虑  $\frac{1}{n} \in \mathbb{Q}$ .

**引理 2.2.4** 设  $\theta : R \rightarrow S$  为环同态, 则  $a \in U(R) \implies \theta(a) \in U(S)$ , 即  $\theta$  诱导  $U(R) \rightarrow U(S)$  群同态.

**证明** 若  $a \in U(R)$ , 则  $\theta(a^{-1}) = \theta(a)^{-1}$ . □

**定义 2.2.5**  $\text{Aut}(R) := \left\{ \theta : R \xrightarrow{\sim} R \text{ 环自同构} \right\}$  称为环  $R$  的自同构群.

**例 2.2.6**  $\text{Aut}(\mathbb{Z}) = \{\text{Id}_{\mathbb{Z}}\}$ .

**例 2.2.7**  $\text{Aut}(\mathbb{Z}[\sqrt{-1}]) = \left\{ \text{Id}_{\mathbb{Z}[\sqrt{-1}]}, \sigma \right\}$ , 其中  $\sigma : \mathbb{Z}[\sqrt{-1}] \rightarrow \mathbb{Z}[\sqrt{-1}], z \mapsto \bar{z}$ .

提示 考虑  $\sqrt{-1}$  在环同态下的像, 结合环同态保乘法的性质.

**练习 2.2.8**  $\text{Aut}(\mathbb{Q}) = \{\text{Id}_{\mathbb{Q}}\}$ .

**练习 2.2.9**  $\text{Aut}(\mathbb{Q}(\sqrt{-1})) = \left\{ \text{Id}_{\mathbb{Q}(\sqrt{-1})}, \sigma \right\}$ , 其中  $\sigma : \mathbb{Q}(\sqrt{-1}) \rightarrow \mathbb{Q}(\sqrt{-1}), z \mapsto \bar{z}$ .

**注记 2.2.10** 同构的环“本质一样”, 即具有相同的性质:

- (1)  $\forall a \in R, a \text{ 可逆} \iff \theta(a) \in S \text{ 可逆}.$
- (2) 有群同构  $U(R) \xrightarrow{\sim} U(S).$
- (3) 有群同构  $\text{Aut}(R) \xrightarrow{\sim} \text{Aut}(S), \phi \mapsto \theta \circ \phi \circ \theta^{-1}.$
- (4)  $R$  是整环  $\iff S$  是整环.
- (5)  $R$  是域  $\iff S$  是域.

**例 2.2.11 (特征同态)** 对于任何环  $R$ , 存在唯一的环同态  $\mathbb{Z} \rightarrow R, n \mapsto n1_R$ , 称为特征同态.

回顾定理 1.1.19, 考虑环同态  $\theta : R \rightarrow S$ , 注意到:

- 像  $\text{Im } \theta \subset S$  为子环.

- ◊  $a \stackrel{\theta}{\sim} b \iff \theta(a) = \theta(b) \iff a - b \in \theta^{-1}(0_S) =: \text{Ker } \theta$  ( $\theta$  的核).
- ◊ 相应的等价类  $[a] = \theta^{-1}(\theta(a)) = a + \text{Ker } \theta := \{a + r : r \in \text{Ker } \theta\}$  (核的“平移”).
- ◊ 商集  $R/\stackrel{\theta}{\sim}$  等于  $\{\text{Ker } \theta\}$  的平移}.

观察到核  $\text{Ker } \theta$  有以下特性:

- ◊ 核  $\text{Ker } \theta$  完全确定了等价关系  $\stackrel{\theta}{\sim}$ .
- ◊  $\text{Ker } \theta \subset R$  对加法、减法、乘法封闭, 但不是子环 ( $R$  非零环  $\implies 1_R \notin \text{Ker } \theta$ ).
- ◊ 对任意  $x \in \text{Ker } \theta, a \in R$ , 均有  $ax \in \text{Ker } \theta$ , 即核  $\text{Ker } \theta$  对于  $R$  中求“倍元”封闭 (这远强于乘法封闭性).

**定义 2.2.12** 非空子集  $I \subset R$  称为理想, 若  $I$  对加、减法以及倍元封闭, 即

- (1)  $a + b \in I, \forall a, b \in I$ .
- (2)  $a \cdot r \in I, \forall a \in I, r \in R$ .

记为  $I \triangleleft R$ .

**注记 2.2.13** (1) 虽然  $R \triangleleft R$ , 但我们通常仅考虑真理想. 理想  $I$  是真理想当且仅当  $1_R \notin I$ .

- (2)  $\{0_R\}$  与  $R$  是  $R$  的平凡理想.
- (3) 任意元素  $a \in R$  给出  $a$  生成的主理想  $(a) = aR := \{a \cdot r : r \in R\}$ . 特别地,  $(0_R) = \{0_R\}, (1_R) = R$ .
- (4) 环同态的核是真理想.

**引理 2.2.14** 环  $R$  为域当且仅当  $R$  仅有平凡理想.

**例 2.2.15**  $\mathbb{Z}$  的所有理想为  $\{n\mathbb{Z} : n \in \mathbb{N}_{\geq 0}\}$ .

**证明** 设  $\{0\} \neq I \triangleleft \mathbb{Z}$ , 则存在  $0 \neq n \in I$ , 使得  $|n|$  最小. 我们断言  $I = n\mathbb{Z}$ . 注意到:

- ◊  $n\mathbb{Z} \subset I$ .
- ◊ 对任意  $r \in I$ , 作带余除法  $r = qn + r'$ , 其中  $q \in \mathbb{Z}, 0 \leq r' < |n|$ . 由  $r' = r - qn \in I$  及  $r' < |n|$  即知  $r' = 0$ . 故  $n \mid r, \forall r \in I$ .  $\square$

**约定 2.2.16** 将  $a \stackrel{\theta}{\sim} b$  记为  $a \equiv b \pmod{\text{Ker } \theta}$ .

**定义 2.2.17** 给定  $I \triangleleft R$ , 定义商环  $R/I$  如下:

- (1) 同余等价关系  $a \equiv b \pmod{I} \iff a - b \in I$ . 等价类  $\bar{a} = a + I$ .
- (2) 商集  $R/\equiv$  记为  $R/I$ , 其上有自然运算  $\bar{a} + \bar{b} := \overline{a + b}, \bar{a} \cdot \bar{b} := \overline{a \cdot b}$ . 故  $R/I$  自然成为环.

**例 2.2.18**  $n\mathbb{Z} \triangleleft \mathbb{Z}$  且  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ .

考虑理想  $I \triangleleft R$ , 典范同态  $\text{can} : R \rightarrow R/I, a \mapsto \bar{a}$ , 则有  $\text{Ker}(\text{can}) = I$ .

**命题 2.2.19 (典范同态的泛性质)** 设  $\theta : R \rightarrow S$  为环同态,  $I \triangleleft R$ . 则  $I \subset \text{Ker } \theta$  当且仅当  $\theta = \theta' \circ \text{can}$ , 其中  $\theta' : R/I \rightarrow S$  为某个环同态. 此时, 由典范同态  $\text{can}$  为满射可知同态  $\theta'$  是唯一的, 称其由  $\theta$  诱导.

$$\begin{array}{ccc} R & \xrightarrow{\theta} & S \\ & \searrow \text{can} & \nearrow \exists! \theta' \text{ 环同态} \\ & R/I & \end{array}$$

**证明** ( $\Leftarrow$ )  $\text{Ker } \theta = \text{Ker}(\theta' \circ \text{can}) \supset \text{Ker}(\text{can}) = I$ .

( $\Rightarrow$ ) 定义映射  $\theta' : R/I \rightarrow S, [a] \mapsto \theta(a)$ . 检验其良定性: 对任意  $a, b \in R$ , 若  $[a] = [b]$ , 则  $a - b \in I \subset \text{Ker } \theta$ , 从而  $\theta(a) = \theta(b)$  即  $\theta'([a]) = \theta'([b])$ . 易见  $\theta'$  为环同态.  $\square$

**定理 2.2.20 (环同态基本定理)** 设  $\theta : R \rightarrow S$  为环同态, 则唯一存在环同构

$$\bar{\theta} : R/\text{Ker } \theta \xrightarrow{\sim} \text{Im } \theta$$

使得下图交换:

$$\begin{array}{ccc} R & \xrightarrow{\theta} & S \\ \text{can} \downarrow & & \uparrow \text{inc} \\ R/\text{Ker } \theta & \dashrightarrow \bar{\theta} & \text{Im } \theta \end{array}$$

**提示** 由定理 1.1.19, 只需验证  $\bar{\theta}$  为环同态.

**注记 2.2.21** (1) 设  $\theta : R \rightarrow S$  是单的, 则  $\text{Ker } \theta = \{0_R\}$ , 有环同构  $R \simeq \text{Im } \theta$ , 可将  $R$  “等同于”  $S$  的子环. 单的环同态又称为环嵌入.

(2) 设  $\theta : R \rightarrow S$  是满的, 则有环同构  $R/\text{Ker } \theta \simeq S$ , 可将  $S$  “等同于”  $R$  的商环.

**定义 2.2.22** 由例 2.2.15 知特征同态  $\mathbb{Z} \rightarrow R$  的核为  $n\mathbb{Z}$ , 其中  $n = 0$  或  $n \geq 2$ . 记  $n = \text{char}(R)$ , 称为环  $R$  的特征.

**注记 2.2.23** 由定理 2.2.20,

- ◊ 若  $\text{char}(R) = 0$ , 则有环嵌入  $\mathbb{Z} \hookrightarrow R$ .
- ◊ 若  $\text{char}(R) = n \geq 2$ , 则有环嵌入  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \hookrightarrow R$ .

**推论 2.2.24** 整环的特征为 0 或素数  $p$ .

**证明** 设整环  $R$  的特征为  $n$ , 则  $\mathbb{Z}/n\mathbb{Z}$  同构于  $R$  的子环, 从而也是整环, 再利用命题 2.1.24 即可.  $\square$

**注记 2.2.25** 特别地, 当  $K$  为域时, 若  $\text{char}(K) = 0$ , 则  $\mathbb{Z} \hookrightarrow K$ ; 若  $\text{char}(K) = \text{素数 } p$ , 则  $\mathbb{F}_p \hookrightarrow K$  为子域. 对于特征 0 域  $K$  及其特征同态  $\phi$ , 我们进一步断言, 可将  $\phi$  延拓为单同态

$$\begin{aligned} \tilde{\phi} : \mathbb{Q} &\hookrightarrow K \\ \frac{n}{m} &\mapsto \phi(n) \cdot \phi(m)^{-1}, \end{aligned}$$

其中  $n \in \mathbb{Z}, m \in \mathbb{Z} \setminus \{0\}$ . 由  $\phi$  是环同态可验证  $\tilde{\phi}$  是良定的.

**练习 2.2.26** 验证注记 2.2.25 中的映射  $\tilde{\phi}$  是单的环同态.

**例 2.2.27** 考虑环  $R$  的两个理想  $I \subset J$ , 有典范同态

$$R/I \rightarrow R/J, \quad a + I \mapsto a + J.$$

其良定性可由  $I \subset J$  得到, 亦可借助命题 2.2.19, 由  $I \subset J = \text{Ker}(\text{can}_J)$  得到如下交换图表:

$$\begin{array}{ccc} R & \xrightarrow{\text{can}_J} & R/J \\ & \searrow \text{can}_I & \nearrow \exists! \text{环同态} \\ & R/I & \end{array}$$

- ◊ 此典范同态的核为  $\{a + I : a + J = 0_{R/J}\} = \{a + I : a \in J\} \triangleleft R/I$ , 记为  $J/I$ .
- ◊ 由定理 2.2.20, 此典范同态诱导环同构

$$(R/I)/(J/I) \xrightarrow{\sim} R/J, \quad (a + I) + J/I \mapsto a + J.$$

- ◊ (对应定理) 固定  $I \triangleleft R$ , 则存在双射

$$\begin{array}{ccc} \{J \triangleleft R : J \supseteq I\} & \xleftrightarrow{1:1} & \{R/I \text{ 的理想}\} \\ J & \longleftarrow \longrightarrow & J/I \\ \{a \in R : a + I \in J\} & \xleftarrow{\psi} & J. \end{array}$$

**练习 2.2.28** 对例 2.2.27 中的映射  $\psi$ , 验证以下断言:

- (1)  $\psi(\bar{J}) \in \{J \triangleleft R : J \supseteq I\}, \forall \bar{J} \triangleleft R/I.$
- (2)  $\psi(\bar{J})/I = \bar{J}, \forall \bar{J} \triangleleft R/I.$
- (3)  $\psi(J/I) = J.$

**例 2.2.29 ( $\mathbb{Z}_n$  的理想)** 由例 2.2.27 对应定理,  $\{\mathbb{Z}/n\mathbb{Z} \text{ 的理想}\} \xleftrightarrow{1:1} \{J \triangleleft \mathbb{Z} : J \supseteq n\mathbb{Z}\}$ . 再结合例 2.2.15, 有  $\{\mathbb{Z}/n\mathbb{Z} \text{ 的理想}\} \xleftrightarrow{1:1} \{d\mathbb{Z} : d \geq 1, d \mid n\}$ . 换言之, 存在双射

$$\{d : d \geq 1, d \mid n\} \xrightarrow{\sim} \{\mathbb{Z}/n\mathbb{Z} \text{ 的理想}\}, \quad d \mapsto d\mathbb{Z}/n\mathbb{Z}.$$

特别地, 当  $p$  为素数时, 域  $\mathbb{F}_p$  仅有平凡理想, 这回应了引理 2.2.14.

**练习 2.2.30 (例 2.2.27 对应定理的子环版本)** 固定  $I \triangleleft R$ , 则存在双射

$$\{S \subset R \text{ 子环} : S \supseteq I\} \xrightarrow{\sim} \{R/I \text{ 的子环}\}, \quad S \mapsto S/I.$$

**练习 2.2.31** 设  $R$  为环,  $S \subset R$  为子环,  $I \triangleleft R$  为理想. 则

- (1)  $S + I = \{a + x : a \in S, x \in I\}$  为子环.
- (2)  $S \cap I$  为  $S$  的理想.
- (3) 存在环同构

$$S/(S \cap I) \xrightarrow{\sim} (S + I)/I, \quad a + (S \cap I) \mapsto a + I.$$

**提示** 考虑满射  $S \rightarrow (S + I)/I$ .

**练习 2.2.32** 证明：有限环的特征必然为正数.

**练习 2.2.33** 设  $D$  为整环,  $m$  和  $n$  为互素的正整数,  $a, b \in D$ . 如果  $a^m = b^m, a^n = b^n$ , 求证  $a = b$ .

**练习 2.2.34** 对任意  $n \geq 0$ , 记  $R_n = \{a + b\sqrt{-1} : a \in \mathbb{Z}, b \in n\mathbb{Z}\}$ .

- (1)  $R_n$  为  $\mathbb{Z}[\sqrt{-1}]$  的子环.
- (2) 对任意  $\mathbb{Z}[\sqrt{-1}]$  的子环  $S$ , 存在唯一  $n \geq 0$  使得  $S = R_n$ .
- (3) 若  $n \neq m$ , 则  $R_n \not\simeq R_m$ .

这样就分类了  $\mathbb{Z}[\sqrt{-1}]$  的子环.

**证明** (3) 若存在环同态  $\theta : R_n \rightarrow R_m$ , 则  $\theta|_{\mathbb{Z}} = \text{Id}_{\mathbb{Z}}$ . 由  $\theta(n\sqrt{-1})^2 = \theta(-n^2) = -n^2$  得  $\theta(n\sqrt{-1}) \in \text{Root}_{\mathbb{C}}(x^2 + n^2) = \{\pm n\sqrt{-1}\}$ , 进而  $R_n \subset R_m$ . 故若  $R_n \simeq R_m$ , 则  $R_n = R_m$ .  $\square$

**练习 2.2.35** 对全体素数的子集  $S$ , 记  $\mathbb{Z}_S = \left\{ \frac{m}{n} : (m, n) = 1, n \text{ 的素因子} \in S \right\} \cup \{0\}$ .

- (1)  $\mathbb{Z}_S$  为  $\mathbb{Q}$  的子环.
- (2) 对任意  $\mathbb{Q}$  的子环  $R$ , 存在唯一素数集合  $S$  使得  $\mathbb{Z}_S = R$ .
- (3) 若  $S \neq S'$  为全体素数的两个子集, 则  $\mathbb{Z}_S \not\simeq \mathbb{Z}_{S'}$ .

这样就分类了  $\mathbb{Q}$  的子环.

**证明** (3) 设存在环同态  $\theta : \mathbb{Z}_S \rightarrow \mathbb{Z}_{S'}$ . 对任意  $p \in S$ , 有  $\frac{1}{p} \in \mathbb{Z}_S$ . 由于  $1 = \theta(1) = \theta(p) \cdot \theta(\frac{1}{p}) = p \cdot \theta(\frac{1}{p})$ , 而  $x = \frac{1}{p}$  是方程  $px = 1$  在  $\mathbb{Q}$  上的唯一解, 因此  $\theta(\frac{1}{p}) = \frac{1}{p}$ . 这说明  $p \in S'$ , 因此  $S \subset S'$ . 故若  $\mathbb{Z}_S \simeq \mathbb{Z}_{S'}$ , 则  $S = S'$ .  $\square$

## 2.3 分式域与商域

设  $R$  为整环, 记  $R^\times := R \setminus \{0_R\}$ . 考虑  $R \times R^\times$  上的关系

$$(a, x) \simeq (b, y) \iff ay = bx.$$

**练习 2.3.1** 证明如上关系  $\simeq$  是  $R$  上的等价关系. **提示** 传递性需要用到整环的性质.

相应的等价类记为

$$\frac{a}{x} := \{(b, y) \in R \times R^\times : (b, y) \simeq (a, x)\},$$

称为分式. 分式的全体记为  $\text{Frac}(R) = R \times R^\times / \simeq$ . 在  $\text{Frac}(R)$  上自然定义加法和乘法

$$\frac{a}{x} + \frac{b}{y} = \frac{ay + bx}{xy}, \quad \frac{a}{x} \cdot \frac{b}{y} = \frac{ab}{xy}.$$

注意定义的合理性需要整环的性质:  $x, y \neq 0_R \implies xy \neq 0_R$ .

**命题 2.3.2**  $\text{Frac}(R)$  是域, 称为  $R$  的分式域.

考虑典范同态  $\text{can}_R : R \hookrightarrow \text{Frac}(R), r \mapsto \frac{r}{1_R}$ , 它是单的, 因而可将  $R$  视作域  $\text{Frac}(R)$  的子环.

**命题 2.3.3**  $\text{can}_R$  是同构当且仅当  $R$  是域.

**定理 2.3.4 (典范同态的泛性质)** 设  $R$  为整环,  $K$  为域,  $\phi : R \hookrightarrow K$  为环的单同态. 则存在唯一的域嵌入  $\tilde{\phi} : \text{Frac}(R) \hookrightarrow K$  使得下图交换:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & K \\ \text{can}_R \searrow & & \swarrow \exists! \tilde{\phi} \text{ 域嵌入} \\ \text{Frac}(R) & & \end{array}$$

进一步,  $\tilde{\phi}$  是同构当且仅当任意  $w \in K$  均可表为  $w = \phi(a)\phi(x)^{-1}$ , 其中  $a \in R, x \in R^\times$ .

**证明** (1) 先证明  $\tilde{\phi}$  的至多唯一性. 对任意  $\frac{a}{x} \in \text{Frac}(R)$  (其中  $a \in R, x \in R^\times$ ),

$$\tilde{\phi}\left(\frac{a}{x}\right) = \tilde{\phi}\left(\frac{a}{1_R} \cdot \left(\frac{x}{1_R}\right)^{-1}\right) = \tilde{\phi}\left(\frac{a}{1_R}\right)\phi\left(\frac{x}{1_R}\right)^{-1} \xrightarrow{\tilde{\phi} \circ \text{can}_R = \phi} \phi(a)\phi(x)^{-1}.$$

(2) 再验证如上  $\tilde{\phi}\left(\frac{a}{x}\right) = \phi(a)\phi(x)^{-1}$  构造的良定性:

- ◊ 因为  $\phi$  为单同态, 所以  $x \neq 0_R \implies \phi(x) \neq 0_K, \phi(x)$  可逆.
- ◊  $\tilde{\phi}$  不依赖于代表元的选取.

(3) 易验证  $\tilde{\phi}$  是域同态, 再由练习 2.3.6 知  $\tilde{\phi}$  是域嵌入.

(4)  $\tilde{\phi}$  是同构  $\iff \tilde{\phi}$  是满射, 再由 (1) 中  $\tilde{\phi}$  的构造即得定理最后的断言.  $\square$

**注记 2.3.5** (1) 可认为  $\tilde{\phi}$  延拓了  $\phi$ .

(2) 分式域  $\text{Frac}(R)$  是包含  $R$  的最小域.

**练习 2.3.6** 设  $\theta : K \rightarrow L$  为域之间的同态, 则  $\theta$  是单同态.

**例 2.3.7**  $\mathbb{Z} \subset \mathbb{Q}$  诱导了域同构  $\text{Frac}(\mathbb{Z}) \simeq \mathbb{Q}$ .

**练习 2.3.8** 考虑练习 2.2.35 中的  $\mathbb{Z}_S$ , 证明  $\text{Frac}(\mathbb{Z}_S) \simeq \mathbb{Q}$ .

**证明** 由定理 2.3.4, 存在唯一的域嵌入  $\theta : \text{Frac}(\mathbb{Z}_S) \hookrightarrow \mathbb{Q}$  使得下图交换:

$$\begin{array}{ccc} \mathbb{Z}_S & \xrightarrow{\text{inc}} & \mathbb{Q} \\ \text{can}_{\mathbb{Z}_S} \searrow & & \swarrow \exists! \theta \text{ 域嵌入} \\ \text{Frac}(\mathbb{Z}_S) & & \end{array}$$

由练习 2.1.31,  $\mathbb{Q}$  没有真子域, 因此  $\text{Frac}(\mathbb{Z}_S) \simeq \mathbb{Q}$ .  $\square$

**练习 2.3.9**  $\mathbb{Z}[\sqrt{-1}] \subset \mathbb{Q}(\sqrt{-1})$  诱导了域同构  $\text{Frac}(\mathbb{Z}[\sqrt{-1}]) \simeq \mathbb{Q}(\sqrt{-1})$ . [提示] 利用注记 2.3.5 (2).

### 阅读提示

一般来说, 很难确定等价关系  $\simeq$  的完全代表元系, 因而集合  $\text{Frac}(R)$  难以捉摸. 但当整环  $R$  具有某些性质(例如是唯一分解整环)时, 我们对  $\text{Frac}(R)$  能作进一步了解(例如可定义既约分式). 例如, 由于有理数具有既约表达式, 我们对集合  $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$  的大小是有所了解的.

**例 2.3.10** 设  $F$  为域. 由注记 2.2.25,

◇ 若  $\text{char}(F) = 0$ , 则  $\mathbb{Z} \hookrightarrow F$ . 根据定理 2.3.4, 由  $\text{can}_{\mathbb{Z}}$  的泛性质, 存在唯一的域嵌入

$$\begin{aligned}\theta : \mathbb{Q} &\hookrightarrow F \\ \frac{n}{m} &\mapsto (n1_F)(m1_F)^{-1}.\end{aligned}$$

因此  $\mathbb{Q}$  可视为  $F$  的子域,  $F$  自然成为  $\mathbb{Q}$ -线性空间, 其上的数乘运算. 定义为

$$\lambda \cdot v = \theta(\lambda)v, \quad \forall \lambda \in \mathbb{Q}, v \in F.$$

◇ 若  $\text{char}(F) = p > 0$ , 则存在唯一的域嵌入

$$\begin{aligned}\theta : \mathbb{F}_p &\hookrightarrow F \\ \bar{n} &\mapsto n1_F.\end{aligned}$$

因此  $F$  自然成为  $\mathbb{F}_p$ -线性空间, 其上的数乘运算. 定义为

$$\lambda \cdot v = \theta(\lambda)v, \quad \forall \lambda \in \mathbb{F}_p, v \in F.$$

**定义 2.3.11** 设  $R$  为环. 真理想  $\mathfrak{p} \trianglelefteq R$  称为素理想, 若  $ab \in \mathfrak{p}$  蕴含着  $a \in \mathfrak{p}$  或  $b \in \mathfrak{p}$ .

**注记 2.3.12** (1)  $\{0_R\}$  为素理想  $\iff R$  为整环.

(2) 设  $\mathfrak{p} \trianglelefteq R$ , 则  $\mathfrak{p}$  为素理想  $\iff R/\mathfrak{p}$  是整环.

**例 2.3.13** 设  $p \geq 1$ , 则  $p\mathbb{Z} \triangleleft \mathbb{Z}$  为素理想  $\iff p$  为素数.

**定义 2.3.14** 记环  $R$  中素理想构成的集合为  $\text{Spec}(R)$ , 称为  $R$  的素谱.

**例 2.3.15**  $\text{Spec}(\mathbb{Z}) = \{(0)\} \sqcup \{(p) : p \text{ 为素数}\}$ .

**注记 2.3.16** 参阅 Zariski topology 与 Spectrum of a ring 词条, 以了解  $\text{Spec}(R)$  如何在 Zariski 拓扑下成为一个拓扑空间. 例子:  $\text{Spec}(\mathbb{Z})$ .

**定义 2.3.17** 设  $R$  为环. 真理想  $\mathfrak{m} \trianglelefteq R$  称为极大理想, 若  $\mathfrak{m} \subset I \triangleleft R$  蕴含  $I = \mathfrak{m}$  或  $I = R$ .

**定义-命题 2.3.18** 真理想  $\mathfrak{m} \trianglelefteq R$  是极大理想当且仅当  $R/\mathfrak{m}$  是域. 此时, 称域  $R/\mathfrak{m}$  为商域. 特别地, 极大理想是素理想.

**证明** 由例 2.2.27 对应定理, 存在双射

$$\{R/\mathfrak{m} \text{ 的理想}\} \xleftrightarrow{1:1} \{I \triangleleft R : I \supset \mathfrak{m}\}.$$

因此  $\mathfrak{m} \trianglelefteq R$  为极大理想  $\iff \{I \triangleleft R : I \supset \mathfrak{m}\} = \{\mathfrak{m}, R\} \iff \{R/\mathfrak{m} \text{ 的理想}\} = \{\{0_{\mathfrak{m}}\}, R/\mathfrak{m}\} \xrightarrow{\text{引理 2.2.14}} R/\mathfrak{m}$  是域. 由注记 2.3.12, 极大理想是素理想.  $\square$

上面的证明堪称简洁, 而下面对  $(\Rightarrow)$  的另证则给出求  $R/\mathfrak{m}$  中非零元的逆的具体方法:

**证明**  $(\Rightarrow)$  设  $\bar{0} \neq \bar{a} \in R/\mathfrak{m}$ , 其中  $a \in R$ . 则  $a \notin \mathfrak{m}$ , 进而两理想之和  $Ra + \mathfrak{m} \supsetneq \mathfrak{m}$ . 由  $\mathfrak{m}$  是极大理想知  $Ra + \mathfrak{m} = R$ . 因此有“Bézout 等式”

$$1_R = ba + \omega, \quad b \in R, \omega \in \mathfrak{m}.$$

在  $R/\mathfrak{m}$  中, 上式变为

$$1_{R/\mathfrak{m}} = \bar{b} \cdot \bar{a}.$$

故  $\bar{a}$  可逆, 其逆为  $\bar{b}$ . □

**注记 2.3.19** 考虑零理想  $\{0_R\} \trianglelefteq R$ , 则  $R$  仅有平凡理想  $\iff \{0_R\}$  是  $R$  的极大理想  $\iff R/\{0_R\}$  是域  $\iff R$  是域. 这回应了引理 2.2.14.

**定义 2.3.20** 记环  $R$  中极大理想构成的集合为  $\text{MaxSpec}(R)$ , 称为  $R$  的极大理想谱.

**注记 2.3.21**  $\emptyset \neq \text{MaxSpec}(R) \subset \text{Spec}(R)$ .

**例 2.3.22**  $\text{MaxSpec}(\mathbb{Z}) = \{(p) : p \text{ 为素数}\}$ .

**注记 2.3.23** Hilbert's Nullstellensatz 联系代数与几何:

$$\text{MaxSpec}(\mathbb{C}[x_1, \dots, x_n]) \xleftarrow{1:1} \mathbb{C}^n.$$

**定义 2.3.24** 设  $R$  为整环,  $a \neq 0_R$ .  $a$  在  $R$  中整除  $b$  (记为  $a | b$ )  $\iff b \in (a)$ .

**定义 2.3.25** 设  $R$  为整环. 非零元  $a \in R$  称为素元, 若  $(a)$  为素理想.

**注记 2.3.26** (1) 设  $a$  非零非单位, 则  $a$  为素元  $\iff a | xy$  蕴含  $a | x$  或  $a | y$ .

(2) 若  $a$  为素元, 则  $(a) \neq R$ , 因此  $a \notin U(R)$ .

(3) 域上元素元.

**定义 2.3.27** 设  $R$  为整环. 非零元  $a \in R$  称为不可约元, 若  $a \notin U(R)$ , 且  $a = bc$  蕴含  $b \in U(R)$  或  $c \in U(R)$ .

**注记 2.3.28** 任意  $u \in U(R)$  给出  $a$  的平凡分解  $a = u \cdot (u^{-1}a) = (u^{-1}a) \cdot u$ , 因此不可约元可理解为“只有平凡分解的元素”.

**例 2.3.29** 在  $\mathbb{Z}$  中, 素元 = 不可约元 =  $\pm p$ ,  $p$  为素数.

**命题 2.3.30** 素元总不可约.

**证明** 设  $a \in R$  是素元, 则  $a \notin U(R)$ . 设  $a = bc$ , 则  $a | bc$ , 进而  $a | b$  或  $a | c$ . 不妨设  $a | b$ , 则存在  $c' \in R$  使得  $b = ac'$ . 于是  $a = bc = ac'c$ , 即  $a(1_R - c'c) = 0_R$ . 因为  $R$  是整环,  $a \neq 0_R$ , 所以  $c'c = 1_R, c \in U(R)$ . □

**例 2.3.31** 令  $\mathbb{Z}[\sqrt{-3}] := \{m + n\sqrt{-3} : m, n \in \mathbb{Z}\}$ , 则  $\mathbb{Z}[\sqrt{-3}]$  是  $\mathbb{C}$  的子环, 进而是整环. 断言: 在  $\mathbb{Z}[\sqrt{-3}]$  中, 2 不可约, 但非素.

**证明 (2 不可约)** 设  $2 = (m + n\sqrt{-3})(m' + n'\sqrt{-3})$ , 其中  $m, n, m', n' \in \mathbb{Z}$ . 两边取模再平方即得

$$4 = (m^2 + 3n^2)((m')^2 + 3(n')^2).$$

由于  $4 \in \mathbb{Z}_{\geq 0}$  只有  $4 = 1 \cdot 4 = 2 \cdot 2$  两种分解, 而  $m^2 + 3n^2$  不可能为 2, 所以  $m^2 + 3n^2 = 1$  或 4. 不妨设  $m^2 + 3n^2 = 1$ , 则  $m = \pm 1, n = 0, m + n\sqrt{-3} = \pm 1$  可逆. 故 2 在  $\mathbb{Z}[\sqrt{-3}]$  中不可约.

**(2 非素)** 注意到  $2 | 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ , 但  $2 \nmid (1 + \sqrt{-3}), 2 \nmid (1 - \sqrt{-3})$ . □

**练习 2.3.32** 令  $\omega := \frac{-1 + \sqrt{-3}}{2}$ , 定义 Eisenstein 整数环  $\mathbb{Z}[\omega] := \{m + n\omega : m, n \in \mathbb{Z}\}$ .

(1) 验证  $\mathbb{Z}[\omega]$  是  $\mathbb{C}$  的子环, 进而是整环.

(2) 证明 2 是  $\mathbb{Z}[\omega]$  中的素元.

**证明** (2) 定义范数映射

$$\begin{aligned} N : \mathbb{Z}[\omega] &\rightarrow \mathbb{Z}_{\geq 0} \\ a + b\omega &\mapsto a^2 - ab + b^2. \end{aligned}$$

由于  $a^2 - ab + b^2 = \frac{1}{4}[(2a - b)^2 + 3b^2]$ ,  $N(x) = 0 \iff x = 0$ . 容易验证,  $N(a + b\omega)$  为偶数  $\iff a, b$  均为偶数. 设  $2 \mid xy$ , 其中  $x, y \in \mathbb{Z}[\omega]$ . 则  $4 \mid N(x)N(y)$ , 进而  $N(x), N(y)$  至少有一个为偶数, 因此  $2 \mid x$  或  $2 \mid y$ . 故 2 是  $\mathbb{Z}[\omega]$  中的素元.  $\square$

**注记 2.3.33** 从例 2.3.31 和练习 2.3.32 看到, 2 在  $\mathbb{Z}[\sqrt{-3}]$  中非素, 但在  $\mathbb{Z}[\omega]$  中是素元.

**练习 2.3.34** 证明: 含幺交换有限环的素理想必是极大理想. 提示 利用练习 2.1.26.

**练习 2.3.35** 设  $f : R \rightarrow S$  是环的满同态,  $K = \text{Ker } f$ . 求证:

- (1) 若  $P$  是  $R$  的素理想并且  $P \supset K$ , 则  $f(P)$  也是  $S$  的素理想.
- (2) 若  $Q$  是  $S$  的素理想, 则  $f^{-1}(Q) = \{a \in R : f(a) \in Q\}$  也是  $R$  的素理想.
- (3)  $S$  中素理想和  $R$  中包含  $K$  的素理想是一一对应的. 将“素理想”换成“极大理想”则此论断也成立.

## 2.4 一元多项式环

**定义 2.4.1** 设  $x$  为字母(形式符号). 环  $R$  上关于  $x$  的(形式)多项式

$$f(x) = a_nx^n + \cdots + a_2x^2 + a_1x + a_0,$$

系数  $a_i \in R$ , 其中的  $a_i x^i$  为单项式. 约定  $x^0 := 1_R$ , 则可记  $f(x) = \sum_{i=0}^n a_i x^i$ . 若  $a_n \neq 0_R$ , 则称  $a_n x^n$  为首项,  $a_n$  为首项系数, 定义次数  $\deg(f) = n$ . 称  $a_0$  为常数项.

**注记 2.4.2** 零多项式  $0_R$  不定义其次数. 其他常值多项式  $a$  的次数为 0.

**约定 2.4.3**  $0_R x^i$  可以略去,  $1_R x^i$  简记为  $x^i$ .

**定义 2.4.4** 多项式  $f(x) = \sum_{i=0}^n a_i x^i$  称为首一的, 若  $a_n = 1_R$ .

**定义 2.4.5** 称两多项式相等, 若它们对应系数相等.

**命题 2.4.6** 记  $R$  上多项式全体为  $R[x]$ , 则  $R[x]$  自然成为环, 称为  $R$  上的一元多项式环.

◇ 加法: 对应系数相加.

◇ 乘法: 若  $f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{j=0}^m b_j x^j$ , 定义  $f(x)g(x) = \sum_{l=0}^{m+n} c_l x^l$ , 其中  $c_l = \sum_{i=0}^l a_i b_{l-i}$  (若下标超出范围则取为 0).

**练习 2.4.7** 验证多项式环中的乘法运算满足结合律.

**注记 2.4.8** 有典范环嵌入  $R \hookrightarrow R[x]$ ,  $a \mapsto a$  常值多项式.

**命题 2.4.9** 提示 考虑首项系数. 若  $R$  为整环, 则  $R[x]$  亦为整环. 特别地, 若  $k$  为域, 则  $k[x]$  为整环.

**性质 2.4.10** 设  $R$  是整环,  $f(x), g(x) \neq 0_R$ , 则  $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ .

**推论 2.4.11**  $R[x]$  绝不是域, 因为  $U(R[x]) \simeq U(R)$ .

**练习 2.4.12 ( $R[x]$  的等价定义)** 考虑

$$\overline{R} := \{\underline{a} = (a_0, a_1, \dots) : a_i \in R, \text{ 当 } i \text{ 充分大时 } a_i = 0_R\}.$$

定义加法和乘法如下:

$$\begin{aligned}\underline{a} + \underline{b} &= (a_0 + b_0, a_1 + b_1, \dots), \\ \underline{a} \cdot \underline{b} &= (c_0, c_1, \dots),\end{aligned}$$

其中  $c_0 = \sum_{i=0}^l a_i b_{l-i}$ . 证明:

(1)  $\overline{R}$  是环.

(2) 存在环同构

$$R[x] \xrightarrow{\sim} \overline{R}, \quad f(x) = \sum_{i \geq 0} a_i x^i \mapsto \underline{a} = (a_0, a_1, \dots).$$

**命题 2.4.13 (典范环嵌入的泛性质)** 设  $R$  为环. 对于任给的环同态  $\psi : R \rightarrow S$  以及  $s \in S$ , 唯一存在环同态

$$\tilde{\psi} : R[x] \rightarrow S$$

使得  $\tilde{\psi}|_R = \psi$  且  $\tilde{\psi}(x) = s$ .

**证明** (1) 先证明  $\tilde{\psi}$  的至多唯一性:

$$\tilde{\psi}(a_n x^n + \dots + a_1 x + a_0) = \psi(a_n)s^n + \dots + \psi(a_1)s + \psi(a_0).$$

(2) 再验证如上  $\tilde{\psi}$  是环同态(留作练习). □

**例 2.4.14** 考虑  $\text{Id}_R$  以及  $a \in R$ , 则  $a$  处的赋值同态

$$\text{ev}_a : R[x] \rightarrow R$$

使得  $f(x) \mapsto f(a)$ , 称为多项式  $f(x)$  在  $a$  处的取值.

**练习 2.4.15** 对任意集合  $X$ ,  $\text{Map}(X, R)$  为环(加法、乘法由  $R$  中运算诱导).

**例 2.4.16** 固定  $f(x) \in R[x]$ , 则有多项式函数

$$f : R \rightarrow R, \quad a \mapsto f(a),$$

即  $f \in \text{Map}(R, R)$ . 定义函数环  $\text{Map}(R, R)$  以及赋值同态

$$\text{ev} : R[x] \rightarrow \text{Map}(R, R), \quad f(x) \mapsto f.$$

该映射一般不是单射.

**例 2.4.17** 固定  $a \in R$ , 则有投影同态

$$p_a : \text{Map}(R, R) \rightarrow R, \quad \theta \mapsto \theta(a).$$

并且  $\text{ev}_a = p_a \circ \text{ev}$ , 其中  $\text{ev}_a$  来自例 2.4.14,  $\text{ev}$  来自例 2.4.16.

设  $k$  为域, 则  $k$  中非零元均可逆, 进而可对多项式作首一化:  $f(x) = a \cdot \bar{f}(x)$ , 其中  $a$  为  $f$  的首项系数,  $\bar{f}(x)$  为首一多项式. 由于  $a_n \in U(k[x])$ ,  $f(x)$  与  $\bar{f}(x)$  本质一样.

**定理 2.4.18 ( $k[x]$  中的带余除法)** 给定  $f(x) \in k[x], 0_k \neq h(x) \in k[x]$ , 则存在  $q(x), r(x) \in k[x]$ , 使得

$$f(x) = q(x) \cdot h(x) + r(x),$$

且  $r(x) = 0$  或  $\deg(r) < \deg(h)$ . 这样的  $q(x)$  与  $r(x)$  是唯一的, 分别称为商式与余式.

**定理 2.4.19 (余数定理)** 给定多项式  $f(x)$  以及  $a \in k$ , 则唯一存在多项式  $q(x) \in k[x]$  使得

$$f(x) = q(x) \cdot (x - a) + f(a).$$

特别地,  $(x - a) | f(x)$  当且仅当  $f(a) = 0_k$ .

**注记 2.4.20** 解集  $\text{Root}_k(f) := \{a \in k : f(a) = 0_k\} \xleftrightarrow{1:1} \{a \in k : (x - a) | f(x)\}$ .

**定义 2.4.21** 整环  $R$  称为主理想整环 (PID), 若其任何理想均为主理想.

**注记 2.4.22** 按定义, 域为 PID, 但我们仅考虑非域的 PID.

**命题 2.4.23**  $\mathbb{Z}$  与  $k[x]$  ( $k$  是域) 均为 PID. 提示 利用带余除法, 数的绝对值  $\rightsquigarrow$  多项式的次数.

**定义 2.4.24** 设  $R$  为整环, 非零元  $a, b$  的最大公因子  $d = \gcd(a, b)$  满足:

◇  $d | a$  且  $d | b$ .

◇ 若  $d' | a$  且  $d' | b$ , 则  $d' | d$ .

**注记 2.4.25** (1) 最大公因子不一定存在.

(2) 若  $\gcd(a, b)$  存在, 则它在相伴意义下唯一, 即若  $d$  和  $e$  都是  $a, b$  的最大公因子, 则存在  $u \in U(R)$ , 使得  $e = ud$  (这等价于  $(e) = (d)$ ).

**练习 2.4.26** 在整环  $R$  中,  $d = \gcd(a, b) \iff (d) \supseteq (a) + (b)$  是包含  $(a) + (b)$  的最小主理想.

**命题 2.4.27** 若  $R$  是 PID, 则对任意非零元  $a, b \in R$ ,  $\gcd(a, b)$  存在.

**证明** 由于  $R$  是 PID,  $R$  中任何理想都有生成元. 特别地, 存在  $d \in R$  使得  $(a) + (b) = (d)$ . 由练习 2.4.26 的 ( $\Leftarrow$ ) 即知  $d = \gcd(a, b)$ .  $\square$

**推论 2.4.28** 若  $R$  是 PID, 则  $R$  上存在 Bézout 等式: 对任意非零元  $a, b \in R$ , 存在  $u, v \in R$ , 使得

$$\gcd(a, b) = u \cdot a + v \cdot b.$$

**例 2.4.29 (最大公因子不一定存在)** 在  $\mathbb{Z}[\sqrt{-3}]$  中,  $4$  与  $(1 - \sqrt{-3})^2$  无最大公因子.

**证明** 定义范数映射

$$\begin{aligned} N : \mathbb{Z}[\sqrt{-3}] &\rightarrow \mathbb{Z}_{\geq 0} \\ m + n\sqrt{-3} &\mapsto m^2 + 3n^2. \end{aligned}$$

假设  $d = \gcd_{\mathbb{Z}[\sqrt{-3}]}(4, (1 - \sqrt{-3})^2)$  存在, 则存在  $a, b \in \mathbb{Z}$ , 使得

$$d \cdot (a + b\sqrt{-3}) = 4,$$

从而

$$N(d) \cdot (a^2 + 3b^2) = 16.$$

观察到  $1 \pm \sqrt{-3}$  均是 4 与  $(1 - \sqrt{-3})^2$  的公因子,  $N(1 + \sqrt{-3}) = N(1 - \sqrt{-3}) = 4$ , 因此  $4 \mid N(d)$ . 又  $U(\mathbb{Z}[\sqrt{-3}]) = \{1, -1\}$ ,  $1 \pm \sqrt{-3}$  非相伴元,  $N(d) > 4$ . 而显然  $N(d) \neq 8$ , 故  $N(d) = 16$ , 这意味着  $a = \pm 1, b = 0, d = \pm 4$ , 但  $d = \pm 4$  不是  $(1 - \sqrt{-3})^2$  的因子.  $\square$

**命题 2.4.30** 若  $R$  是 PID, 则  $R$  中素元 = 不可约元.

**证明** 由命题 2.3.30, 只需证  $R$  中不可约元是素元. 设  $a \in R$  不可约,  $a \mid bc$ . 假设  $a \nmid b$ , 下证  $a \mid c$ . 由  $a$  不可约可知  $\gcd(a, b)$  相伴于  $1_R$ , 由 Bézout 等式, 存在  $u, v \in R$  使得

$$1_R = u \cdot a + v \cdot b.$$

两边同乘  $c$  得

$$c = (uc) \cdot a + v \cdot (bc) \in (a).$$

$\square$

**命题 2.4.31** 设  $R$  是非域的 PID,  $\{0_R\} \neq \mathfrak{p} \in \text{Spec}(R)$ , 则  $\mathfrak{p} \in \text{MaxSpec}(R)$ . 故  $R$  的任何非零素理想均极大,  $\text{Spec}(R) = \{0_R\} \sqcup \text{MaxSpec}(R)$ .

**证明** 由于  $R$  是 PID, 存在素元  $a \in R$  使得  $\mathfrak{p} = (a)$ . 假设  $\mathfrak{p}$  不是极大理想, 则存在  $I \lhd R$ , 使得

$$\mathfrak{p} \subsetneq I \subsetneq R.$$

设  $I = (b)$ , 则由  $(b) \supset (a)$  知  $b \mid a$ . 由  $a$  是素元,  $b \in U(R)$  或  $b$  与  $a$  相伴. 若  $b \in U(R)$ , 则  $(b) = R$ , 矛盾; 若  $b$  与  $a$  相伴, 则  $(b) = (a)$ , 也矛盾. 故  $\mathfrak{p}$  是极大理想.  $\square$

**推论 2.4.32** 设  $R$  是非域的 PID,  $\{0_R\} \neq \mathfrak{p} \in \text{Spec}(R)$ , 则  $R/\mathfrak{p}$  是域.

在  $k[x]$  中可以约定仅考虑首一多项式. 例如:

- ◊ 多项式  $f(x), g(x) \in k[x]$  的最大公因式是指首一多项式  $h(x)$  满足:  $h(x) \mid f(x), h(x) \mid g(x)$ , 且若  $a(x) \mid f(x), a(x) \mid g(x)$ , 总有  $a(x) \mid h(x)$ .
- ◊  $k[x]$  中不可约元称为域  $k$  上的不可约多项式, 故

$$\text{MaxSpec}(k[x]) \xleftrightarrow{1:1} \{k \text{ 上首一不可约多项式}\}.$$

特别地,  $k \hookrightarrow \text{MaxSpec}(k[x]), \lambda \mapsto x - \lambda$ .

**练习 2.4.33** 设  $f(x)$  是域  $k$  上的不可约非零多项式,  $\deg(f(x)) \leq 3$ , 则  $f(x)$  在  $k$  上不可约  $\iff \text{Root}_k(f) = \emptyset$ .

**命题 2.4.34**  $|\text{Root}_k(f)| \leq \deg(f(x))$ . 提示 利用定理 2.4.19 归纳可证, 若  $\alpha_1, \dots, \alpha_m \in k$  是  $f(x)$  不同的零点, 则  $(x - \alpha_1) \cdots (x - \alpha_m) \mid f(x)$ .

**域扩张** 设有域的包含关系  $k \subset K$ , 则  $f(x) \in k[x]$  可视为  $K[x]$  中的元素, 且

- ◊  $\text{Root}_k(f) \subset \text{Root}_K(f)$ .
- ◊  $f(x) \in k[x]$  不可约  $\Rightarrow f(x) \in K[x]$  不可约.
- ◊ 设  $f(x), g(x) \in k[x]$ . 总有  $\text{gcd}_{k[x]}(f(x), g(x)) = \text{gcd}_{K[x]}(f(x), g(x))$ .

上面最后一条断言可由辗转相除法不随域扩张而改变直接得到, 也可如下证明:

**证明** 记  $d_1(x) = \text{gcd}_{k[x]}(f(x), g(x))$ ,  $d_2(x) = \text{gcd}_{K[x]}(f(x), g(x))$ , 则  $d_1(x) \mid d_2(x)$ . 由  $k[x]$  上的 Bézout 等式, 存在  $u(x), v(x) \in k[x]$  使得

$$d_1(x) = u(x)f(x) + v(x)g(x),$$

在  $K[x]$  中,  $d_2(x) \mid f(x), d_2(x) \mid g(x)$ , 由上式即得  $d_2(x) \mid d_1(x)$ . 又  $d_1(x), d_2(x)$  均为首一多项式, 故  $d_1(x) = d_2(x)$ .  $\square$

通常情况并不如上文中域的包含关系这么理想. 考虑域同态  $\theta : k \hookrightarrow K$  (由练习 2.3.6, 域同态一定是单的, 因此  $k \simeq \text{Im } \theta$ ), 则自然地有环嵌入 (仍用  $\theta$  标识)

$$\begin{aligned} \theta : k[x] &\hookrightarrow K[x] \\ f(x) = \sum_{i=0}^n a_i x^i &\mapsto \theta(f(x)) = \sum_{i=0}^n \theta(a_i)x^i. \end{aligned}$$

并且

- ◊  $\theta(\text{Root}_k(f)) \subset \text{Root}_K(\theta(f))$ .
- ◊  $f(x) \in k[x]$  不可约  $\Rightarrow \theta(f(x)) \in K[x]$  不可约.
- ◊ 设  $f(x), g(x) \in k[x]$ . 总有  $\theta\left(\text{gcd}_{k[x]}(f(x), g(x))\right) = \text{gcd}_{K[x]}(\theta(f(x)), \theta(g(x)))$ .

**练习 2.4.35** 证明以上第 1 条和第 3 条断言.

**Kronecker 添根构造** 设  $k$  为域,  $f(x) \in k[x]$  为首一不可约多项式. 考虑典范同态

$$\begin{aligned} \theta : \quad k &\xrightarrow{\text{can}} k[x] \xrightarrow{\text{can}} k[x]/(f(x)) = K \\ \lambda &\longmapsto \lambda \longmapsto \bar{\lambda} = \lambda + (f(x)). \end{aligned}$$

**练习 2.4.36** 设  $a \in k$ , 则存在域同构

$$k \xrightarrow{\sim} k[x]/(x - a).$$

提示 用带余除法.

**注记 2.4.37** 当  $f(x)$  为一次首一多项式时, 由  $k[x]/(f(x))$  得不到新的域. 因此以下设  $\deg(f(x)) = n \geq 2$ . 此时  $\text{Root}_k(f) = \emptyset$ .

记  $u = x + (f(x)) \in K$ . 对任意  $\bar{g}(x) \in K$ , 由  $k[x]$  上的带余除法, 有

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

其中  $r(x) = 0$  或  $\deg(r(x)) < n$ . 故  $\overline{g(x)} = \overline{r(x)}$ , 进而有双射

$$\begin{array}{ccc} K & \xleftarrow{1:1} & \{r(x) \in k[x] : r(x) = 0 \text{ 或 } \deg(r(x)) < n\} \\ \overline{r(x)} & \longleftrightarrow & r(x) \\ \theta(c_{n-1})u^{n-1} + \cdots + \theta(c_1)u + \theta(c_0) & \longleftarrow & c_{n-1}x^{n-1} + \cdots + c_1x + c_0. \end{array}$$

**例 2.4.38 (四元域)** 记  $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ . 考虑不可约多项式  $x^2 + x + \bar{1} \in \mathbb{F}_2[x]$ , 有双射

$$\begin{array}{ccc} \{a + bx : a, b \in \mathbb{F}_2\} & \xleftarrow{1:1} & \mathbb{F}_4 := \mathbb{F}_2[x]/(x^2 + x + \bar{1}) \\ a + bx & \longmapsto & \theta(a) + \theta(b)u. \end{array}$$

因此  $\mathbb{F}_4 = \{\theta(\bar{0}), \theta(\bar{1}), u, u + \theta(\bar{1})\}$ .

在以上尝试中, 我们自然希望将  $k$  等同于  $K$  的子域, 以便摆脱繁琐的  $\theta$ .

**练习 2.4.39** 设  $k, L$  为域. 考虑域同态  $\theta : k \hookrightarrow L$  (由练习 2.3.6, 域同态一定是单的), 则  $L$  自然成为  $k$ -线性空间. 其上的加法即域  $L$  上加法, 而数乘运算定义为:

$$\lambda \cdot a := \theta(\lambda) \cdot a, \quad \forall \lambda \in k, a \in L.$$

**注记 2.4.40**  $L$  作为  $k$ -线性空间与域同态  $\theta$  有关.

有了练习 2.4.39, 我们可以将  $K$  视为  $k$ -线性空间, 于是

$$\theta(c_{n-1})u^{n-1} + \cdots + \theta(c_1)u + \theta(c_0) = c_{n-1} \cdot u^{n-1} + \cdots + c_1 \cdot u + c_0 \cdot 1_k,$$

上式右边是  $k$ -线性组合,  $\{1_k, u, \dots, u^{n-1}\}$  是  $K$  的  $k$ -线性基,  $\dim_k K = n = \deg(f)$ .

**约定 2.4.41** 由于  $\theta(\lambda) = \lambda \cdot 1_k$ , 下面仍记  $\theta(\lambda) = \lambda + (f(x))$  为  $\lambda$ . 例如, 在这种约定下, 练习 2.4.39 中  $\mathbb{F}_4 = \{\bar{0}, \bar{1}, u, u + \bar{1}\}$ .

**练习 2.4.42**  $\mathbb{F}_4$  的加法表与乘法表.

**解答** 见表 2.1.

表 2.1:  $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + \bar{1})$  的加法表与乘法表

$+$	$\bar{0}$	$\bar{1}$	$u$	$u + \bar{1}$	$\times$	$\bar{0}$	$\bar{1}$	$u$	$u + \bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$u$	$u + \bar{1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$u + \bar{1}$	$u$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$u$	$u + \bar{1}$
$u$	$u$	$u + \bar{1}$	$\bar{0}$	$\bar{1}$	$u$	$\bar{0}$	$u$	$u + \bar{1}$	$\bar{1}$
$u + \bar{1}$	$u + \bar{1}$	$u$	$\bar{1}$	$\bar{0}$	$u + \bar{1}$	$\bar{1}$	$\bar{0}$	$u$	$\bar{1}$

**练习 2.4.43** (1) 不存在  $\mathbb{F}_4 \rightarrow \mathbb{Z}_4$  的同态.

(2) 存在唯一的  $\mathbb{Z}_4 \rightarrow \mathbb{F}_4$  的同态.

在约定 2.4.41 下, 可将  $k[x]$  中多项式  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$  等同于  $K[x]$  中多项式  $x^n + \theta(a_{n-1})x^{n-1} + \cdots + \theta(a_1)x + \theta(a_0)$ . 有如下重要观察:

**命题 2.4.44**  $u \in \text{Root}_K(f)$ , 即  $f(u) = u^n + \theta(a_{n-1})u^{n-1} + \cdots + \theta(a_1)u + \theta(a_0) = 0_K$ .

**例 2.4.45** 考虑不可约多项式  $x^2 + 1 \in \mathbb{R}[x]$  以及域嵌入

$$\begin{aligned}\theta : \mathbb{R} &\rightarrow \mathbb{R}[x]/(x^2 + 1) = K \\ a &\mapsto \theta(a) = a + (x^2 + 1) \text{ (仍记为 } a\text{).}\end{aligned}$$

记  $u = x + (x^2 + 1) \in K$ , 则  $K$  作为  $\mathbb{R}$ -线性空间有  $\mathbb{R}$ -基  $\{1, u\}$ ,  $K$  中元素为  $a + bu$ , 其中  $a, b \in \mathbb{R}$ . 有同构

$$K \xrightarrow{\sim} \mathbb{C}, \quad a + bu \mapsto a + b\sqrt{-1}.$$

但  $K$  未必就是  $\mathbb{C}$ , 因为另有同构

$$K \xrightarrow{\sim} \mathbb{C}, \quad a + bu \mapsto a - b\sqrt{-1}.$$

又  $u \in \text{Root}_K(x^2 + 1)$ , 由定理 2.4.19 可得  $x^2 + 1$  在  $K[x]$  中的分解 (运用 Vieta 定理):

$$x^2 + 1 = (x - u)(x + u).$$

**例 2.4.46** 由于  $u \in \text{Root}_{\mathbb{F}_4}(x^2 + x + \bar{1})$ ,  $\mathbb{F}_2$  上不可约多项式  $x^2 + x + \bar{1}$  在  $\mathbb{F}_4$  上有分解 (运用 Vieta 定理及表 2.1)

$$x^2 + x + \bar{1} = (x + u)(x + u + \bar{1}).$$

**定理 2.4.47 ( $\theta$  的泛性质)** 考虑  $K = k[x]/(f(x))$ ,  $u = x + (f(x))$ , 域同态  $\delta : k \rightarrow F$ , 以及  $\alpha \in \text{Root}_F(\delta(f))$ . 则唯一存在域同态  $\delta' : K \rightarrow F$  使得  $\delta = \delta' \circ \theta$  且  $\delta'(u) = \alpha$ .

$$\begin{array}{ccccc} k & \xleftarrow{\theta} & K & \ni & u \\ & \searrow \delta & \swarrow \exists! \delta' \text{ 域同态} & & \nearrow \\ & F & & & \alpha \\ & \uparrow \psi & & & \end{array}$$

**证明** (1) 先证明  $\delta'$  的至多唯一性:  $\{1_k, u, \dots, u^{n-1}\}$  是  $K$  的  $k$ -线性基, 且

$$\delta'(\theta(c_{n-1})u^{n-1} + \cdots + \theta(c_1)u + \theta(c_0)) = \delta(c_{n-1})\alpha^{n-1} + \cdots + \delta(c_1)\alpha + \delta(c_0).$$

(2) 再给出  $\delta'$  的构造. 由命题 2.4.13, 唯一存在环同态  $\tilde{\delta} : k[x] \rightarrow F$ , 使得  $\tilde{\delta}|_k = \delta$  且  $\tilde{\delta}(x) = \alpha$ , 进而  $\tilde{\delta}(f(x)) = \delta(f)(\alpha) = 0_F$ . 于是  $(f(x)) \subset \text{Ker } \tilde{\delta}$ . 由命题 2.2.19,  $\tilde{\delta}$  诱导环同态

$$\begin{aligned}\delta' : K = k[x]/(f(x)) &\rightarrow F \\ \overline{g(x)} &\mapsto \tilde{\delta}(g(x)).\end{aligned}$$

$\delta'$  使得  $\delta = \delta' \circ \theta$  且  $\delta'(u) = \tilde{\delta}(x) = \alpha$ . □

**注记 2.4.48** 等式  $\delta = \delta' \circ \theta$  意味着  $\delta'$  延拓  $\delta$ .

**练习 2.4.49 (九元域)** 记  $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ . 考虑不可约多项式  $x^2 + \bar{1} \in \mathbb{F}_3[x]$ , 以及域同态

$$\mathbb{F}_3 \hookrightarrow \mathbb{F}_3[x]/(x^2 + \bar{1}) =: \mathbb{F}_9.$$

记  $v = x + (x^2 + \bar{1}) \in \mathbb{F}_9$ .

(1)  $\mathbb{F}_9$  的加法表与乘法表.

(2) 在  $\mathbb{F}_9[x]$  中分解  $x^2 + \bar{1}$ .

**解答** (2)  $x^2 + \bar{1} = (x - u)(x - \bar{2}u)$ . □

**练习 2.4.50** 记  $K = \mathbb{R}[x]/(x^2 + 2)$ ,  $v = x + (x^2 + 2) \in K$ . 证明  $K \cong \mathbb{C}$ .

**练习 2.4.51** 如果  $D$  为整环但不是域, 求证  $D[x]$  不是 PID.

**例 2.4.52** 在  $\mathbb{F}_9$  中求  $(\bar{2}u + \bar{1})^{-1}$ .

**解答** 由于  $\gcd_{\mathbb{F}_9[x]}(\bar{2}x + \bar{1}, x^2 + \bar{1}) = \bar{1}$ , 通过带余除法可得 Bézout 等式:

$$x^2 + \bar{1} = (\bar{2}x + \bar{2})(\bar{2}x + \bar{1}) + \bar{2}.$$

因此在  $\mathbb{F}_9$  中

$$\bar{0} = (\bar{2}u + \bar{2})(\bar{2}u + \bar{1}) + \bar{2} \iff \bar{1} = (\bar{2}u + \bar{2})(\bar{2}u + \bar{1}),$$

即  $(\bar{2}u + \bar{1})^{-1} = \bar{2}u + \bar{2}$ . □

## 2.5 Euclid 整环

**定义 2.5.1** 整环  $R$  称为 Euclid 整环 (ED), 若存在 Euclid 函数

$$\phi : R^\times = R \setminus \{0_R\} \rightarrow \mathbb{Z}_{\geq 0},$$

使得任给  $a, b \in R^\times$ , 存在  $q, r \in R$  满足

$$a = qb + r,$$

其中  $r = 0_R$  或  $\phi(r) < \phi(b)$ .

**例 2.5.2** 整数环  $\mathbb{Z}$  是 ED. 此时 Euclid 函数  $\phi = |\cdot|$ , 而表达式不唯一, 如

$$33 = 3 \cdot 9 + 6 = 4 \cdot 9 - 3.$$

第二个表达式更好, 因为  $\phi(-3) = |-3|$  更小.

**例 2.5.3** 域上的一元多项式环  $k[x]$  是 ED. 此时 Euclid 函数  $\phi = \deg(\cdot)$ .

**定理 2.5.4** ED 是 PID.

**证明** 设  $R$  是 ED. 对任意非零理想  $I \triangleleft R$ , 取非零元  $b \in I$  使  $\phi(b)$  最小. 断言:  $I = (b)$ . 对任意  $a \in I$ , 由  $R$  是 ED 有

$$a = qb + r,$$

其中  $r = 0_R$  或  $\phi(r) < \phi(b)$ . 由于  $r = a - qb \in I$ , 由  $b$  的最小性知  $r = 0_R$ . 故  $b \mid a$ . □

**命题 2.5.5**  $\mathbb{Z}[\sqrt{-1}]$  是 ED, 从而是 PID.

**证明** 范数映射

$$\begin{aligned} N : \mathbb{Q}(\sqrt{-1})^\times &\rightarrow \mathbb{Q}_+ \\ z &\mapsto z \cdot \bar{z} \end{aligned}$$

是积性函数 (因复共轭  $\sigma \in \text{Aut}(\mathbb{C})$ ):

$$N(z \cdot w) = N(z) \cdot N(w), \quad \forall z, w \in \mathbb{Q}(\sqrt{-1})^\times.$$

$N$  限制在  $\mathbb{Z}[\sqrt{-1}]^\times \subset \mathbb{Q}(\sqrt{-1})^\times$  为 Euclid 函数. 对任意  $x, y \in \mathbb{Z}[\sqrt{-1}]^\times$ , 记

$$\frac{x}{y} = \frac{x \cdot \bar{y}}{N(y)} = \alpha + \beta\sqrt{-1} \in \mathbb{Q}(\sqrt{-1})^\times, \quad \alpha, \beta \in \mathbb{Q}.$$

取  $m, n \in \mathbb{Z}$  使得

$$|\alpha - m| \leq \frac{1}{2}, \quad |\beta - n| \leq \frac{1}{2}.$$

则由

$$\frac{x}{y} = (m + n\sqrt{-1}) + [(\alpha - m) + (\beta - n)\sqrt{-1}]$$

可得

$$x = qy + r,$$

其中  $q = m + n\sqrt{-1}$ ,  $r = [(\alpha - m) + (\beta - n)\sqrt{-1}] \cdot y \in \mathbb{Z}[\sqrt{-1}]$ . 若  $r \neq 0$ , 则

$$N(r) = [(\alpha - m)^2 + (\beta - n)^2] \cdot N(y) \leq \left(\frac{1}{4} + \frac{1}{4}\right)N(y) < N(y).$$

故  $\mathbb{Z}[\sqrt{-1}]$  是 ED. □

**练习 2.5.6** 利用范数映射证明例 2.1.19 (4).

**练习 2.5.7** 记  $i = \sqrt{-1}$ . 在  $\mathbb{Z}[\sqrt{-1}]$  上计算  $\gcd(4 + 7i, 3 + 4i)$ .

**解答** 由辗转相除法:

$$\diamond \frac{4 + 7i}{3 + 4i} = \frac{8}{5} + \frac{1}{5}i = 2 + \left(-\frac{2}{5} + \frac{1}{5}i\right) \implies 4 + 7i = 2 \cdot (3 + 4i) - (2 + i).$$

$$\diamond \frac{3 + 4i}{2 + i} = 2 + i \implies \gcd(4 + 7i, 3 + 4i) = \gcd(3 + 4i, 2 + i) = 2 + i. \quad \square$$

**命题 2.5.8**  $\mathbb{Z}[\sqrt{-2}]$  是 ED, 从而是 PID. 提示  $(\frac{1}{2})^2 + (\frac{1}{2})^2 \cdot 2 < 1$ .

**练习 2.5.9** 利用范数映射证明  $U(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$ .

**命题 2.5.10** 由例 2.3.31 与命题 2.4.30 知,  $\mathbb{Z}[\sqrt{-3}]$  不是 PID, 因此也不是 ED.

**注记 2.5.11** 由于  $(\frac{1}{2})^2 + (\frac{1}{2})^2 \cdot 3 = 1$ , 命题 2.5.5 的证明方法在此处失效.

**命题 2.5.12** Eisenstein 整数环  $\mathbb{Z}[\omega]$  是 ED, 从而是 PID.

**证明**  $\omega$  满足方程  $\omega^2 + \omega + 1 = 0$ . 范数映射

$$\begin{aligned} N : \mathbb{Q}(\omega)^\times &\rightarrow \mathbb{Q}_+ \\ a + b\omega &\mapsto a^2 - ab + b^2 \end{aligned}$$

限制在  $\mathbb{Z}[\omega]^\times \subset \mathbb{Q}(\omega)^\times$  为 Euclid 函数. 对任意  $x, y \in \mathbb{Z}[\omega]^\times$ , 记

$$\frac{x}{y} = \frac{x \cdot \bar{y}}{N(y)} = \alpha + \beta\omega \in \mathbb{Q}(\omega)^\times, \quad \alpha, \beta \in \mathbb{Q}.$$

取  $m, n \in \mathbb{Z}$  使得

$$|\alpha - m| \leq \frac{1}{2}, \quad |\beta - n| \leq \frac{1}{2}.$$

则由

$$\frac{x}{y} = (m + n\omega) + [(\alpha - m) + (\beta - n)\omega]$$

可得

$$x = qy + r,$$

其中  $q = m + n\omega, r = [(\alpha - m) + (\beta - n)\omega] \cdot y \in \mathbb{Z}[\omega]$ . 若  $r \neq 0$ , 则

$$\begin{aligned} N(r) &= [(m + n\omega)^2 + ((\alpha - m) + (\beta - n)\omega)^2 - (m + n\omega)(\alpha - m) - ((\alpha - m) + (\beta - n)\omega)m] \cdot N(y) \\ &\leq \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right)N(y) < N(y). \end{aligned}$$

故  $\mathbb{Z}[\omega]$  是 ED. □

**练习 2.5.13** 利用范数映射证明  $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm \omega, \pm \omega^2\}$ .

**代数整数环** 考虑  $\mathbb{Z} \subset R \subset F = \text{Frac}(R)$  使得  $\dim_{\mathbb{Q}} F < \infty$ . 这里  $\mathbb{Z} \subset R$  应理解为  $\text{char}(R) = 0$  (参考注记 2.2.23).

**定义 2.5.14**  $\alpha \in F$  称为代数整数, 若  $\alpha$  满足首一的整系数方程:

$$\alpha^m + b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0 = 0_F, \quad b_i \in \mathbb{Z}, m \geq 1.$$

记  $F$  中代数整数全体为  $\mathcal{O}_F$ .

有如下重要事实 (可参阅 James S. Milne 的 [A Primer of Commutative Algebra](#) 中定理 6.5):

**性质 2.5.15**  $\mathcal{O}_F$  是  $F$  的子环, 且  $\text{Frac}(\mathcal{O}_F) \simeq F$ .

**命题 2.5.16** 假设  $R \subset \mathcal{O}_F$ . 若  $R$  是 PID (或更弱点, 为 UFD), 则  $R = \mathcal{O}_F$ .

**注记 2.5.17** 为对以上“若”字之前的诸条件加深理解, 可参考以下实例:

$$\begin{array}{ccccccc} \mathbb{Z} & \subset & R & \subset & F = \text{Frac}(R) & & \\ & & \parallel & & \parallel & & \\ & & \mathbb{Z}[\sqrt{-3}] & & \mathbb{Q}(\sqrt{-3}) & & \end{array}$$

此时  $\dim_{\mathbb{Q}} F = 2$ . 由  $(x - m)^2 + 3n^2$  零化  $m + n\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$  可知  $\mathbb{Z}[\sqrt{-3}] \subset \mathcal{O}_F$ . 由于  $\omega$  满足  $\omega^2 + \omega + 1 = 0, \omega \in \mathcal{O}_F \setminus \mathbb{Z}[\sqrt{-3}]$  (也可由命题 2.5.24,  $-3 \equiv 1 \pmod{4}$ , 因此  $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\omega] \supsetneq \mathbb{Z}[\sqrt{-3}]$ ),

由命题 2.5.16 即知  $\mathbb{Z}[\sqrt{-3}]$  不是 PID. 而 Eisenstein 整数环  $\mathbb{Z}[\omega]$  是 PID, 由命题 2.5.16,  $\mathbb{Z}[\omega] = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ .

### 练习 2.5.18 考虑映射

$$\begin{aligned}\sigma : \mathbb{Q}(\sqrt{2}) &\rightarrow \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} &\mapsto a - b\sqrt{2}.\end{aligned}$$

证明:

$$(1) \ \sigma \in \text{Aut}(\mathbb{Q}(\sqrt{2})).$$

$$(2) \ \text{Aut}(\mathbb{Q}(\sqrt{2})) = \{\text{Id}_{\mathbb{Q}(\sqrt{2})}, \sigma\}.$$

(3)  $\sigma$  不能延拓为  $\mathbb{R}$  的自同构, 即不存在  $\delta \in \text{Aut}(\mathbb{R})$ , 使得  $\delta|_{\mathbb{Q}(\sqrt{2})} = \sigma$ .

**证明** (2) 设  $f \in \text{Aut}(\mathbb{Q}(\sqrt{2}))$ , 则  $f|_{\mathbb{Z}} = \text{Id}_{\mathbb{Z}}$ . 对任意  $q = \frac{n}{m}$ ,  $n, m \in \mathbb{Z}$ , 由  $q$  是方程  $f(m) \cdot q = f(n)$  的唯一解可知  $f(q) = q$ , 故  $f|_{\mathbb{Q}} = \text{Id}_{\mathbb{Q}}$ . 只需确定  $f(\sqrt{2})$  即可确定  $f$ . 由  $f(\sqrt{2})^2 = f(\sqrt{2} \cdot \sqrt{2}) = 2$  可知  $f(\sqrt{2}) = \pm\sqrt{2}$ .

◊ 若  $f(\sqrt{2}) = \sqrt{2}$ , 则  $f = \text{Id}_{\mathbb{Q}(\sqrt{2})}$ .

◊ 若  $f(\sqrt{2}) = -\sqrt{2}$ , 则  $f = \sigma$ .

(3) 若  $\delta \in \text{Aut}(\mathbb{R})$ , 则对任意  $x = y^2 \in \mathbb{R}_+$ ,  $\delta(x) = \delta(y)^2 > 0$ . □

### 命题 2.5.19 $\mathbb{Z}[\sqrt{2}]$ 是 ED, 从而是 PID.

**证明** 定义范数映射

$$\begin{aligned}N : \mathbb{Q}(\sqrt{2})^\times &\rightarrow \mathbb{Q}_+ \\ a + b\sqrt{2} &\mapsto |a^2 - 2b^2|.\end{aligned}$$

根据练习 2.5.18, 由  $N(x) = |x \cdot \sigma(x)|$  可知  $N$  是积性函数:

$$N(x \cdot y) = N(x) \cdot N(y), \quad \forall x, y \in \mathbb{Q}(\sqrt{2})^\times.$$

$N$  限制在  $\mathbb{Z}[\sqrt{2}]^\times \subset \mathbb{Q}(\sqrt{2})^\times$  为 Euclid 函数. 对任意  $x, y \in \mathbb{Z}[\sqrt{2}]^\times$ , 记

$$\frac{x}{y} = \frac{x \cdot \sigma(y)}{y \cdot \sigma(y)} = \alpha + \beta\sqrt{2} \in \mathbb{Q}(\sqrt{2})^\times, \quad \alpha, \beta \in \mathbb{Q}.$$

取  $m, n \in \mathbb{Z}$  使得

$$|\alpha - m| \leq \frac{1}{2}, \quad |\beta - n| \leq \frac{1}{2}.$$

则由

$$\frac{x}{y} = (m + n\sqrt{2}) + [(\alpha - m) + (\beta - n)\sqrt{2}]$$

可得

$$x = qy + r,$$

其中  $q = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ ,  $r = [(\alpha - m) + (\beta - n)\sqrt{2}] \cdot y$ . 若  $r \neq 0$ , 则

$$N(r) = |(\alpha - m)^2 - 2(\beta - n)^2| \cdot N(y) \leq \left[ \left( \frac{1}{2} \right)^2 + \left( \frac{1}{2} \right)^2 \cdot 2 \right] N(y) < N(y).$$

故  $\mathbb{Z}[\sqrt{2}]$  是 ED.  $\square$

**练习 2.5.20**  $U(\mathbb{Z}[\sqrt{2}])$  为无限群.

**证明** 注意到  $1 + \sqrt{2} \in U(\mathbb{Z}[\sqrt{2}])$ , 因此  $(1 + \sqrt{2})^n \in U(\mathbb{Z}[\sqrt{2}])$ ,  $\forall n \geq 0$ .  $\square$

**注记 2.5.21** 由 Dirichlet 单位定理可证  $U(\mathbb{Z}[\sqrt{2}]) = \{\pm(1 + \sqrt{2})^n : n \geq 0\}$ .

**命题 2.5.22**  $\mathbb{Z}[\sqrt{3}]$  是 ED, 从而是 PID.

**证明** 可仿照命题 2.5.19 证明, 区别仅在最后的放缩:

$$|(\alpha - m)^2 - 3(\beta - n)^2| \leq \frac{3}{4} < 1. \quad \square$$

**注记 2.5.23** Squarefree values of  $n$  for which the quadratic field  $\mathbb{Q}(\sqrt{n})$  is norm-Euclidean: -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73. 关于 norm-Euclidean fields 可参阅 [https://en.wikipedia.org/wiki/Euclidean\\_domain#Norm-Euclidean\\_fields](https://en.wikipedia.org/wiki/Euclidean_domain#Norm-Euclidean_fields).

**命题 2.5.24** 设  $d \in \mathbb{Z}$  无平方因子, 则

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{若 } d \equiv 2, 3 \pmod{4}, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{若 } d \equiv 1 \pmod{4}. \end{cases}$$

**定理 2.5.25** 设  $d \in \mathbb{Z}$  无平方因子, 则存在基本单位  $u \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ , 满足  $u > 1$ , 且  $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$  中所有单位都可表为  $\pm u^m$ , 其中  $m \in \mathbb{Z}$ .

**命题 2.5.26**  $\mathbb{Z}[\sqrt{5}]$  不是 ED.

**证明** 记  $\delta = \frac{1+\sqrt{5}}{2}$ . 因为  $5 \equiv 1 \pmod{4}$ , 由命题 2.5.24,  $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\delta] \supsetneq \mathbb{Z}[\sqrt{5}]$ . 由命题 2.5.16,  $\mathbb{Z}[\sqrt{5}]$  不是 UFD, 进而不是 ED.  $\square$

## 2.6 Gauss 素数

**定义 2.6.1** 整环  $R$  中非零元  $a, b$  称为相伴的, 若存在  $u \in U(R)$  使得  $a = bu$ . 这等价于  $(a) = (b)$ .

**注记 2.6.2** 相伴是等价关系.

**例 2.6.3** 由  $N(m + ni) = m^2 + n^2 = 1 \iff m + ni \in U(\mathbb{Z}[i])$  可知  $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ . 因此在相伴关系下,  $m + ni, -m - ni, -n + mi, n - mi \in \mathbb{Z}[i]$  应视为一体.

**命题 2.6.4** 设  $R$  为 PID, 则存在双射

$$\{a \in R : a \text{ 为素元}\}/\text{相伴关系} \leftrightarrow \text{MaxSpec}(R), \quad a \mapsto (a).$$

回顾命题 2.4.31, 此时  $\text{Spec}(R) = \{0\} \sqcup \text{MaxSpec}(R)$ .

**定义 2.6.5** Gauss 整数环  $\mathbb{Z}[i]$  中的素元称为 Gauss 素数.

**注记 2.6.6** 因为  $\mathbb{Z}[i]$  是 PID,  $\mathbb{Z}[i]$  中素元 = 不可约元.

**例 2.6.7**  $2 = (1+i)(1-i) = -i(1+i)^2$  不是 Gauss 素数, 且相伴于“平方数”.

**练习 2.6.8**  $1+i$  是 Gauss 素数.

**练习 2.6.9**  $\mathbb{Z}[i]/(1+i) \simeq \mathbb{F}_2$ .

**证明** 由于  $N(1+i) = 2$ , 任意  $x \in \mathbb{Z}[i]$  作带余除法:

$$x = q(1+i) + r,$$

其中  $r = 0$  或  $N(r) = 1$ . 因此只需考虑  $r = 0, \pm 1, \pm i$ . 由

$$1 - (-i) = 1 + i, \quad i - (-1) = 1 + i, \quad 1 - (-1) = (1+i)(1-i)$$

知  $\pm 1, \pm i$  模  $(1+i)$  同余,  $\mathbb{Z}[i]/(1+i) = \{\bar{0}, \bar{1}\}$  是二元域. 由例 2.1.10 知  $\mathbb{Z}[i]/(1+i) \simeq \mathbb{F}_2$ .  $\square$

以下是一个更富技巧性的证明 (思路与定理 2.6.15 的证明相仿):

**证明** 定理 2.6.15 证明中给出了环同构

$$\begin{aligned} \varphi : \mathbb{Z}[i] &\xrightarrow{\sim} \mathbb{Z}[x]/(x^2 + 1) \\ a + bi &\mapsto \overline{a + bx}. \end{aligned}$$

由  $\varphi(1+i) = \overline{x+1}$  可得

$$(1+i) \xrightarrow{\varphi} (\overline{x+1}).$$

由练习 2.6.16 即得环同构

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

由  $(x+1)(1-x) \equiv 1 - x^2 \equiv 2 \pmod{(x^2 + 1)}$  可知  $(\bar{2}) \subset (\overline{x+1})$ . 记  $R = \mathbb{Z}[x]/(x^2 + 1)$ , 由例 2.2.27, 存在环同构

$$(R/(\bar{2})) / ((\overline{x+1})/(\bar{2})) \simeq R/(\overline{x+1}).$$

注意到

$$(R/(\bar{2})) / ((\overline{x+1})/(\bar{2})) = \mathbb{F}_2[x]/(\overline{x+1}) \simeq \mathbb{F}_2,$$

于是

$$\mathbb{Z}[i]/(1+i) \simeq R/(\overline{x+1}) \simeq \mathbb{F}_2. \quad \square$$

**注记 2.6.10** (1) 由注记 2.3.12 (2),  $\mathbb{Z}[i]/(1+i)$  是域  $\implies 1+i$  是 Gauss 素数.

(2)  $\{0, 1\}$  是模  $(1+i)$  同余的完全代表元系也可如下证明:

$$\diamond (1+i) \not\leq \mathbb{Z}[i] \implies 1 \notin (1+i) \implies 0 \not\equiv 1 \pmod{(1+i)}.$$

◊ 注意到  $2 = (1 + i)(1 - i) \in (1 + i)$ , 因此对任意  $m + ni \in \mathbb{Z}[i]$ ,

$$m + ni \equiv m - n \equiv \begin{cases} 0, & \text{若 } m - n \text{ 为偶数,} \\ 1, & \text{若 } m - n \text{ 为奇数} \end{cases} \pmod{(1 + i)}.$$

(3) 更一般的结论见练习 2.6.26.

**练习 2.6.11** 记  $R = \mathbb{Z}[i]/(2)$ .

(1) 证明:  $R$  有 4 个元素.

(2)  $R$  是否同构于  $\mathbb{Z}_4$ ?

(3)  $R$  是否同构于  $\mathbb{F}_2[x]/(x^2)$ ?

**解答** (1) 易知  $\{0, 1, i, 1+i\}$  是  $\mathbb{Z}[i]$  模 (2) 的完全代表元系. 也可在定理 2.6.15 证明用到的环同构中令  $p = 2$  得到  $\mathbb{Z}[i]/(2) \simeq \mathbb{F}_2[x]/(x^2 + 1)$ .

(2) 不同构, 因为  $\text{char}(R) = 2 \neq 4$ .

$$(3) \mathbb{Z}[i]/(2) \simeq \mathbb{F}_2[x]/(x^2 + 1) = \mathbb{F}_2[x]/((x + 1)^2) \xrightarrow[x \mapsto x - 1]{} \mathbb{F}_2[x]/(x^2). \quad \square$$

**引理 2.6.12** 设  $z \in \mathbb{Z}[i]$ . 若  $N(z) = p$  为素数 (这样的  $p$  只能是 2 或  $4k + 1$ ), 则  $z$  是 Gauss 素数.

**提示** 只需证  $z$  是不可约元.

**引理 2.6.13** 设奇素数  $p = 4k + 3$ , 则  $p$  是 Gauss 素数.

**证明** 假设  $p$  在  $\mathbb{Z}[i]$  中有非平凡分解  $p = xy$ , 则  $p^2 = N(x)N(y)$ . 由于  $N(x), N(y) > 1$ ,  $N(x) = N(y) = p$ . 因此  $p$  是两个整数 (一个奇数与一个偶数) 的平方和, 但一个奇数与一个偶数的平方和为  $4k + 1$  型整数, 矛盾. 故  $p$  是不可约元, 即  $p$  是 Gauss 素数.  $\square$

**例 2.6.14 ( $4k + 1$  型素数不是 Gauss 素数)**

$$5 = (1 + 2i)(1 - 2i), \quad 13 = (3 + 2i)(3 - 2i), \quad 17 = (4 + i)(4 - i).$$

**定理 2.6.15 (Fermat 二平方和定理)** 设  $p$  为奇素数, 则  $p = 4k + 1$  当且仅当  $p = a^2 + b^2$ . 此时, 这样的  $0 < a < b$  唯一.

**证明** ( $\Leftarrow$ ) 一个奇数与一个偶数的平方和为  $4k + 1$  型整数.

( $\Rightarrow$ ) ① 由于  $4 \mid (p - 1)$ , 由命题 4.2.8, 循环群  $\mathbb{F}_p^\times$  中有四阶元, 因此方程  $x^2 + 1 = 0$  在  $\mathbb{F}_p^\times$  中有解, 即  $x^2 + 1$  在  $\mathbb{F}_p[x]$  中可约. 注意到存在环同构

$$\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[x]/(x^2 + 1),$$

由注记 2.3.12 (2),  $p$  不是 Gauss 素数. 设  $p$  在  $\mathbb{Z}[i]$  中有非平凡分解  $p = xy$ , 则  $p^2 = N(x)N(y)$ . 由于  $N(x), N(y) > 1$ ,  $N(x) = N(y) = p$ . 故存在  $a, b \in \mathbb{N}$  使得  $p = a^2 + b^2$ .

② 设  $p = a^2 + b^2 = c^2 + d^2$ , 其中  $0 < a < b, 0 < c < d$ . 由引理 2.6.12,

$$a + bi, \quad a - bi, \quad c + di, \quad c - di$$

均为 Gauss 素数. 由  $p = (a+bi)(a-bi) = (c+di)(c-di)$  知  $(a+bi) \mid (c+di)$  或  $(a+bi) \mid (c-di)$ . 但  $c \pm di$  也是 Gauss 素数, 因此  $a+bi$  与  $c+di$  相伴或与  $c-di$  相伴. 设  $a+bi = u(c \pm di)$ , 容易验证,  $u \neq -1, \pm i$ . 故  $a+bi = c+di$ . 这证明了  $a, b \in \mathbb{N}$  的唯一性.

**(环同构补证)** 以下分三步给出 ( $\Rightarrow$ ) 中环同构的证明:

① 对环同态  $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ , 由命题 2.4.13, 唯一存在环同态

$$\begin{aligned}\varphi : \mathbb{Z}[x] &\rightarrow \mathbb{Z}[i] \\ f(x) &\mapsto f(i).\end{aligned}$$

显然  $\varphi$  是满射, 且  $\text{Ker } \varphi = (x^2 + 1)$ . 由定理 2.2.20, 存在环同构

$$\bar{\varphi} : \mathbb{Z}[x]/(x^2 + 1) \xrightarrow{\sim} \mathbb{Z}[i]$$

② 观察到 ① 中环同构  $\bar{\varphi}$  使得

$$(x^2 + 1, p)/(x^2 + 1) \xrightarrow{\bar{\varphi}} (p).$$

其中  $(x^2 + 1, p) := (x^2 + 1) + (p)$  表示包含  $x^2 + 1$  和  $p$  的最小理想. 由例 2.2.27 与练习 2.6.16, 存在如下两个环同构:

$$\begin{array}{ccc} (\mathbb{Z}[x]/(x^2 + 1))/((x^2 + 1, p)/(x^2 + 1)) & \xrightarrow[\text{练习 2.6.16}]{\sim} & \mathbb{Z}[i]/(p) \\ \downarrow \text{例 2.2.27} \wr & & \\ \mathbb{Z}[x]/(x^2 + 1, p) & & \end{array}$$

③ 由模  $p$  约化

$$\mathbb{Z}[x] \twoheadrightarrow \mathbb{F}_p[x], \quad \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \bar{a}_i x^i$$

及定理 2.2.20, 存在环同构

$$\psi : \mathbb{Z}[x]/(p) \xrightarrow{\sim} \mathbb{F}_p[x].$$

观察到

$$(x^2 + 1, p)/(p) \xrightarrow{\psi} (x^2 + \bar{1}),$$

再次运用例 2.2.27 与练习 2.6.16 就得到如下两个环同构:

$$\begin{array}{ccc} (\mathbb{Z}[x]/(p))/((x^2 + 1, p)/(p)) & \xrightarrow[\text{练习 2.6.16}]{\sim} & \mathbb{F}_p[x]/(x^2 + \bar{1}) \\ \downarrow \text{例 2.2.27} \wr & & \\ \mathbb{Z}[x]/(x^2 + 1, p) & & \end{array}$$

再结合 ② 中环同构就得到欲证的环同构:

$$\mathbb{Z}[i]/(p) \xrightarrow{\sim} \mathbb{F}_p[x]/(x^2 + \bar{1}), \quad \overline{m+n\bar{i}} \mapsto \overline{m+\bar{n}x}.$$

□

**练习 2.6.16** 设  $\theta : R \xrightarrow{\sim} S$  为环同构,  $I \triangleleft R$ ,  $\theta(I) \triangleleft S$ , 则  $R/I \simeq S/\theta(I)$ .

**定理 2.6.17 (Gauss 素数分类)** 在相伴的意义下, Gauss 素数可分为以下三类:

- ◊  $1 + i$ .
- ◊  $4k + 3$  型素数.
- ◊  $a \pm bi$ , 其中  $p = a^2 + b^2$  为  $4k + 1$  型素数,  $0 < a < b$ .

**证明** 由于这三类数都是 Gauss 素数且互不相伴, 只需验证任一 Gauss 素数 (在相伴的意义下) 均从属于其中一类. 设  $z \in \mathbb{Z}[i]$  是 Gauss 素数, 则

$$z \mid z \cdot \bar{z} = N(z) = p_1^{n_1} \cdots p_k^{n_k},$$

其中  $p_1, \dots, p_k \in \mathbb{N}$  为素数, 注意到每个  $p_i$  必为以下三类数之一:

- ◊  $p_i = 2 = -i \cdot (1 + i)^2$ .
- ◊  $p_i$  为  $4k + 3$  型素数.
- ◊  $p_i = a^2 + b^2 = (a + bi)(a - bi)$  为  $4k + 1$  型素数.

因此  $N(z) = z_1 \cdots z_s$ , 其中每个  $z_i$  均为定理所述三类数之一. 由  $z \mid z_1 \cdots z_s$  可知存在  $1 \leq j \leq s$  使得  $z \mid z_j$ . 又  $z$  与  $z_j$  均为 Gauss 素数, 故  $z$  与  $z_j$  相伴.  $\square$

**注记 2.6.18**  $4k + 3$  与  $4k + 1$  型素数均有无穷个. (直接证明或由 Dirichlet 定理: 设正整数  $a, d$  互素, 则  $a + nd$  型素数有无穷个.)

**命题 2.6.19**  $\mathbb{Z}[i]$  中任一元素  $z$  有素分解

$$z \stackrel{\text{相伴}}{\sim} z_1 \cdots z_t,$$

其中  $z_1, \dots, z_t$  均为 Gauss 素数.

**证明** 由于  $\mathbb{Z}[i]$  是 PID, 这等价于证明有不可约分解. 设  $z \in \mathbb{Z}[i]$ , 若  $z$  是不可约元, 则已满足要求; 若  $z = xy$  是非平凡分解, 则  $N(x), N(y) < N(z)$ , 由递降法即得证.  $\square$

**定理 2.6.20 (二平方和定理)** 设  $n \geq 2$ , 则  $n$  可写成二平方和当且仅当有标准分解

$$n = 2^r p_1^{m_1} \cdots p_t^{m_t},$$

其中若  $p_i = 4k + 3$ , 相应的  $m_i$  为偶数.

**证明** ( $\Leftarrow$ ) 注意到恒等式

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2$$

蕴含着: 若两个整数均可表示成两个整数的平方和, 则它们的积也是两个整数的平方和 (这本质上是  $\mathbb{Z}[i]$  中范数映射的积性). 由已知条件, 结合定理 2.6.15, 易知  $n$  可写成若干平方和的乘积, 进而可写成二平方和.

( $\Rightarrow$ ) 设  $n = a^2 + b^2, z = a + bi \in \mathbb{Z}[i]$ . 由命题 2.6.19,  $z$  在  $\mathbb{Z}[i]$  中有标准分解

$$z = u \cdot z_1 \cdots z_t,$$

其中  $u \in \{\pm 1, \pm i\}$ ,  $z_1, \dots, z_t$  均为 Gauss 素数. 于是

$$n = N(z) = N(z_1) \cdots N(z_t).$$

由定理 2.6.17 即知  $n$  有所给的标准分解.  $\square$

**例 2.6.21** 在  $\mathbb{Z}[i]$  中分解  $z = 29 - 2i$ .

**解答**  $N(z) = 5 \cdot 13^2$ . 由定理 2.6.17 知  $z$  的不可约因子只能在  $1 \pm 2i, 2 \pm 3i$  之中. 通过试除即知  $z = -1 \cdot (1 + 2i) \cdot (2 + 3i)^2$ .  $\square$

**练习 2.6.22** 分别将 60 和  $81 + 8i$  在  $\mathbb{Z}[i]$  中分解成不可约元之积.

**解答**  $60 = -1 \cdot 3 \cdot (1 + 2i) \cdot (1 - 2i) \cdot (1 + i)^4$ ,  $81 + 8i = -i \cdot (2 - 7i) \cdot (1 - 2i)^3$ .  $\square$

**命题 2.6.23** 任一环同态  $\theta : R \rightarrow S$  诱导映射

$$\text{Spec}(S) \rightarrow \text{Spec}(R), \quad \mathfrak{q} \mapsto \theta^{-1}(\mathfrak{q}).$$

特别地, 若  $R$  是  $S$  的子环, 则有映射

$$\text{Spec}(S) \rightarrow \text{Spec}(R), \quad \mathfrak{q} \mapsto \mathfrak{q} \cap R.$$

**注记 2.6.24** 诱导映射的良定性见练习 2.3.35 (2), 它是 Zariski 拓扑下的连续映射. 此时还有整环间的嵌入映射

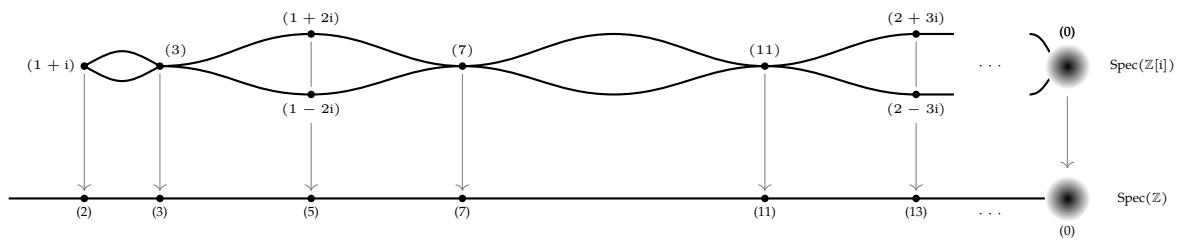
$$R/(\mathfrak{q} \cap R) \hookrightarrow S/\mathfrak{q}.$$

**练习 2.6.25**  $\mathbb{Z}[i]$  的素理想与  $\mathbb{Z}$  的交集有以下三类情形:

- (1)  $(1 + i) \cap \mathbb{Z} = 2\mathbb{Z}$ .
- (2) 若  $p$  为  $4k + 3$  型素数, 则  $(p) \cap \mathbb{Z} = p\mathbb{Z}$ .
- (3) 若  $p = a^2 + b^2$  ( $0 < a < b$ ) 为  $4k + 1$  型素数, 则  $(a + bi) \cap \mathbb{Z} = (a - bi) \cap \mathbb{Z} = p\mathbb{Z}$ .

**提示** RHS  $\subset$  LHS 均显然, 再由命题 2.6.23 及  $p\mathbb{Z} \in \text{MaxSpec}(\mathbb{Z})$  可得 LHS = RHS.

由命题 2.6.23, 考虑  $\mathbb{Z} \subset \mathbb{Z}[i]$ , 利用练习 2.6.25, 可得  $\text{Spec}(\mathbb{Z}[i]) \rightarrow \text{Spec}(\mathbb{Z})$  的图像:



◇  $\mathbb{Z}[i]/(1 + i) \cong \mathbb{F}_2$  (练习 2.6.9).

◇ 若  $p$  为  $4k + 3$  型素数, 定理 2.6.15 证明中给出环同构

$$\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[x]/(x^2 + \bar{1}),$$

注意到  $x^2 + \bar{1} \in \mathbb{F}_p[x]$  是不可约多项式, 上式两边均为  $p^2$  元域.

◊ 若  $p = a^2 + b^2$  ( $0 < a < b$ ) 为  $4k + 1$  型素数, 则  $\mathbb{Z}[\mathbf{i}]/(a + \mathbf{bi}) \simeq \mathbb{F}_p$  (练习 2.6.26).

**练习 2.6.26** 设  $a, b \in \mathbb{Z}$ . 若  $\gcd(a, b) = 1$ , 则  $\mathbb{Z}[\mathbf{i}]/(a + \mathbf{bi}) \simeq \mathbb{Z}/(a^2 + b^2)$ .

**证明** 因为  $\gcd(a, b) = 1$ , 由 Bézout 等式, 存在  $u, v \in \mathbb{Z}$  使得  $au + bv = 1$ , 从而

$$(a + \mathbf{bi})(v + u\mathbf{i}) = (av - bu) + (au + bv)\mathbf{i} = av - bu + \mathbf{i}.$$

因此在  $\mathbb{Z}[\mathbf{i}]/(a + \mathbf{bi})$  中  $\mathbf{i} \equiv bu - av \pmod{(a + \mathbf{bi})}$ , 进而

$$c + d\mathbf{i} \equiv c + d(bu - av) \pmod{(a + \mathbf{bi})}, \quad \forall c, d \in \mathbb{Z}.$$

而  $c + d(bu - av) \in \mathbb{Z}$ , 这说明环同态

$$\begin{aligned} \theta : \mathbb{Z} &\rightarrow \mathbb{Z}[\mathbf{i}]/(a + \mathbf{bi}) \\ m &\mapsto \overline{m} \end{aligned}$$

是满的. 再由

$$\begin{aligned} m \in \text{Ker } \theta &\iff (a + \mathbf{bi}) \mid m \iff \frac{m}{a + \mathbf{bi}} = \frac{m(a - \mathbf{bi})}{a^2 + b^2} \in \mathbb{Z}[\mathbf{i}] \\ &\iff (a^2 + b^2) \mid ma \text{ 且 } (a^2 + b^2) \mid mb \iff (a^2 + b^2) \mid \gcd(ma, mb) \\ &\iff (a^2 + b^2) \mid m \cdot \gcd(a, b) \iff (a^2 + b^2) \mid m \end{aligned}$$

得  $\text{Ker } \theta = (a^2 + b^2)\mathbb{Z}$ . 故由定理 2.2.20,

$$\mathbb{Z}[\mathbf{i}]/(a + \mathbf{bi}) = \text{Im } \theta \simeq \mathbb{Z}/\text{Ker } \theta = \mathbb{Z}/(a^2 + b^2)\mathbb{Z}. \quad \square$$

## 2.7 唯一分解整环

**定义 2.7.1** 整环  $R$  称为唯一分解整环 (UFD), 若满足以下两条:

(1) (存在不可约分解) 每个非零非单位元素  $a \in R$  均可写成

$$a = c_1 c_2 \cdots c_r,$$

其中  $c_i$  均为不可约元.

(2) (分解的唯一性) 若  $a = c_1 c_2 \cdots c_r = c'_1 c'_2 \cdots c'_s$  是  $a$  的任意两个上述不可约分解, 则  $r = s$ , 且存在置换  $\sigma \in S_r$ , 使得  $c_i$  与  $c'_{\sigma(i)}$  ( $1 \leq i \leq r$ ) 相伴.

**注记 2.7.2** 由推论 2.7.23, 条件 (2) 可替换成 “ $R$  中素元 = 不可约元”.

**命题 2.7.3** 若  $R$  是 UFD, 则  $R$  中素元 = 不可约元. 故 UFD 中任一元素有素分解.

**命题 2.7.4** 若  $R$  是 UFD, 则  $R$  中任一非零非单位元素  $a$  有标准分解

$$a = up_1^{n_1} \cdots p_r^{n_r},$$

其中  $u \in U(R)$ ,  $p_1, \dots, p_r$  为素元且互不相伴,  $n_i \geq 1$  ( $1 \leq i \leq r$ ). 进而  $a$  的因子总形如

$$vp_1^{m_1} \cdots p_r^{m_r},$$

其中  $v \in U(R)$ ,  $0 \leq m_i \leq n_i$  ( $1 \leq i \leq r$ ). 在相伴的意义下,  $a$  恰有  $\prod_{i=1}^r (1 + n_i)$  个因子.

**命题 2.7.5** 若  $R$  是 UFD, 则对任意非零元  $a, b \in R$ ,  $\gcd(a, b)$  和  $\text{lcm}(a, b)$  均存在. 若  $a, b$  有标准分解

$$a = up_1^{n_1} \cdots p_r^{n_r}, \quad b = vp_1^{m_1} \cdots p_r^{m_r},$$

其中  $u, v \in U(R)$ ,  $n_i, m_j \geq 0$ , 则

$$\gcd(a, b) \text{ 相伴于 } \prod_{i=1}^r p_i^{\min\{n_i, m_i\}}, \quad \text{lcm}(a, b) \text{ 相伴于 } \prod_{i=1}^r p_i^{\max\{n_i, m_i\}}.$$

**引理 2.7.6** 设  $R$  为 UFD,  $a, b$  为  $R$  中非零元.

(1)  $\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right)$  相伴于 1.

(2) 若  $\gcd(a, b)$  相伴于 1 (即  $a, b$  互素) 且  $a \mid bc$ , 则  $a \mid c$ .

**命题 2.7.7** 若  $R$  为 UFD, 则  $\text{Frac}(R)$  中任一元素  $\frac{a}{b}$  有既约表达  $\frac{a}{b} = \frac{a'}{b'}$ , 其中  $\gcd(a', b')$  相伴于 1.

现在可以证明命题 2.5.16.

**命题 2.5.16** UFD 是整闭环.

**证明** 设  $R$  为 UFD. 任取  $\frac{a}{b} \in \text{Frac}(R) \setminus R$ , 由命题 2.7.7, 可设  $\frac{a}{b}$  为既约形式, 则存在  $R$  中素元  $p$  使得  $p \mid b$  但  $p \nmid a$ . 若  $\frac{a}{b} \in \mathcal{O}_{\text{Frac}(R)}$ , 设

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_0 = 0, \quad c_i \in R.$$

两边同乘  $b^n$  得到

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_0b^n = 0.$$

由  $p \mid b$  即知  $p \mid a^n$ , 但这与  $R$  为 UFD 且  $p \nmid a$  矛盾. 故  $R = \mathcal{O}_{\text{Frac}(R)}$ .  $\square$

**练习 2.7.8** 设  $R$  为 UFD, 且在  $\text{Frac}(R)$  中有  $\frac{a}{b} = \frac{c}{d}$ , 其中  $\gcd(a, b)$  与  $\gcd(c, d)$  均相伴于 1, 则  $a$  与  $c$  相伴,  $b$  与  $d$  相伴.

**定义 2.7.9** 整环  $R$  称为 Bézout 整环, 若  $R$  中任意两个主理想之和仍为主理想.

**注记 2.7.10** (1) Bézout 整环中 Bézout 等式成立.

(2) PID 是 Bézout 整环.

**定理 2.7.11**  $R$  是 PID 当且仅当  $R$  是 UFD 且是 Bézout 整环.

**例 2.7.12 (一般 UFD 无 Bézout 等式)** 在  $\mathbb{Z}[x]$  中  $\gcd(2, x) = 1$ , 但不存在  $f(x), g(x) \in \mathbb{Z}[x]$ , 使得  $2f(x) + xg(x) = 1$ .

**定义 2.7.13** 设  $X \subset R$ . 称包含  $X$  的最小理想为  $X$  生成的理想, 记为

$$(X) = RX = \left\{ \text{有限和 } \sum_i a_i \cdot x_i, \text{ 其中 } a_i \in R, x_i \in X \right\}.$$

**定义 2.7.14**  $I \triangleleft R$  称为有限生成理想, 若存在有限集  $X$ , 使得  $I = (X)$ ,  $X$  称为生成元集.

**定义 2.7.15** 环  $R$  称为 Noether 环, 若任何理想均有限生成.

**例 2.7.16** PID 是 Noether 环.

**定理 2.7.17 (Hilbert 基定理)** 设  $R$  为 Noether 环, 则  $R[x_1, \dots, x_n]$  及其商环均为 Noether 环.

**提示** 由于  $R[x_1, \dots, x_{n+1}] \simeq R[x_1, \dots, x_n][x_{n+1}]$ , 断言的第一类化约为证明 “ $R$  为 Noether 环  $\implies R[x]$  为 Noether 环”; 再由例 2.2.27 对应定理, 其商环的任何理想均有限生成.

下面的定理说明定义 2.7.1 中条件 (1) 对绝大多数环均成立.

**定理 2.7.18** 设  $R$  为 Noether 整环, 则  $R$  中每个非零非单位元素均有不可约分解.

**证明** 用反证法, 假设  $a \in R$  无不可约分解. 特别地,  $a$  可约. 设有非平凡分解  $a = a_1 \cdot a_2$ , 则  $a_1$  与  $a_2$  至少有一个无不可约分解. 不妨设  $a_1$  无不可约分解, 特别地,  $a_1$  可约. 设有非平凡分解  $a_1 = a_{11} \cdot a_{12}$ , 并不妨设  $a_{11}$  无不可约分解,  $a_{11} = a_{111} \cdot a_{112}$ ,  $a_{111}$  无不可约分解. 由此递推可得  $R$  中理想的无限严格升链:

$$(a_1) \subsetneq (a_{11}) \subsetneq (a_{111}) \subsetneq \dots,$$

由练习 2.7.19 得矛盾. 故假设不成立.  $\square$

**练习 2.7.19** 设  $R$  为 Noether 环, 则  $R$  中不存在理想的无限严格升链:

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots, \quad I_i \triangleleft R.$$

**证明** 用反证法, 假设存在如上严格升链. 令  $I = \bigcup_{n=1}^{\infty} I_n$ , 则  $I \triangleleft R$ . 由  $R$  是 Noether 环知  $I$  是有限生成的, 设  $\{a_1, \dots, a_m\}$  为其生成元集. 由  $I$  的定义, 存在映射

$$\sigma : \{1, \dots, m\} \rightarrow \mathbb{Z}_{\geq 1},$$

使得  $a_i \in I_{\sigma(i)}$ . 令  $M = \max\{\sigma(1), \dots, \sigma(m)\}$ , 则由升链可得  $a_1, \dots, a_m \in I_M$ ,  $I_M \subset I \subset I_M$ . 故  $I_M = I$ , 矛盾.  $\square$

**注记 2.7.20** 事实上, 这一性质可用作 Noether 环的等价定义.

**命题 2.7.21** 设  $R$  为整环. 若  $a \in R$  有素分解, 则  $a$  的不可约分解唯一 (在定义 2.7.1 (2) 意义下).

**提示** 利用素元与整环性质逐一消去.

**注记 2.7.22** 由此可知素分解强于不可约分解.

**推论 2.7.23** 设整环  $R$  中每个非零非单位元素均有不可约分解 (如 Noether 整环), 则  $R$  是 UFD 当且仅当  $R$  中素元 = 不可约元.

**例 2.7.24** PID 是 UFD.

**定理 2.7.25 (Gauss 定理)** 设  $R$  为 UFD, 则  $R[x]$  亦为 UFD.

**例 2.7.26**  $\mathbb{Z}[x]$  为 UFD, 但不是 PID. 因为  $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$ , 说明非零素理想  $(x)$  不是极大理想.

**例 2.7.27**  $\mathbb{Z}[x_1, \dots, x_n]$  和  $k[x_1, \dots, x_n]$  ( $k$  为域) 均为 UFD.

为了证明定理 2.7.25, 需要一些准备工作.

**定义 2.7.28** 设  $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$  且  $f(x) \neq 0$ . 定义  $f(x)$  的容度为  $c(f) = \gcd(a_0, a_1, \dots, a_n)$ . 称  $f(x)$  为本原的, 若  $c(f)$  相伴于 1.

**定义 2.7.29** 设  $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$  且  $f(x) \neq 0$ , 则可将  $f(x)$  本原化:  $f(x) = c(f) \cdot f_0(x)$ , 其中  $f_0(x) = \sum_{i=0}^n \frac{a_i}{c(f)} \cdot x^i$  是本原多项式.

**引理 2.7.30 (Gauss 引理)** 设  $f(x), g(x) \in R[x]$ , 则  $c(f \cdot g)$  相伴于  $c(f) \cdot c(g)$ . 特别地, 本原多项式的乘积仍是本原的.

**证明** 通过本原化, 只需证本原多项式的乘积仍是本原的. 设存在两个本原多项式

$$f(x) = a_n x^n + \dots + a_1 x + a_0, \quad g(x) = b_m x^m + \dots + b_1 x + b_0$$

使得  $f(x)g(x)$  不是本原的, 则存在素元  $p$  使得  $f(x)g(x)$  中所有系数. 由于  $f(x)$  本原,  $p$  不能整除所有  $a_i$ , 设  $r$  是最小下标使  $p \nmid a_r$ . 类似地, 设  $s$  是最小下标使  $p \nmid b_s$ . 考虑  $f(x)g(x)$  中  $x^{r+s}$  的系数

$$a_0 b_{r+s} + \dots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \dots + a_{r+s} b_0,$$

该和式中只有  $a_r b_s$  一项不被  $p$  整除, 因此  $x^{r+s}$  系数不被  $p$  整除, 这与假设矛盾.  $\square$

以下用模  $p$  约化手法给出另证:

**证明** 用反证法, 同前面证明的假设. 考虑模  $p$  约化

$$\begin{aligned} \pi : R[x] &\rightarrow (R/pR)[x] \\ \sum_{i=0}^n a_i x^i &\mapsto \sum_{i=0}^n \bar{a}_i x^i. \end{aligned}$$

显然  $\pi$  是环同态且  $\text{Ker } \pi = p(R[x])$ . 由  $(R/pR)[x]$  是整环且  $\pi(f(x)g(x)) = \bar{0}$ ,  $f(x) \in \text{Ker } \pi$  或  $g(x) \in \text{Ker } \pi$ , 即  $p \mid f(x)$  或  $p \mid g(x)$ , 矛盾.  $\square$

**注记 2.7.31** Gauss 引理一个常用的特例如下: 记  $K = \text{Frac}(R)$ , 设  $f(x), g(x) \in K[x]$  是首一多项式, 则  $f(x)g(x) \in R[x] \implies f(x), g(x) \in R[x]$ .

现在可以给出定理 2.7.25 的证明:

**证明** 记  $K = \text{Frac}(R)$ . 将  $R[x]$  中非零多项式  $f(x)$  本原化:

$$f(x) = c(f) \cdot f_0(x) = c_1 c_2 \cdots c_r \cdot f_0(x),$$

其中  $c_i \in R$  为素元. 下面给出  $f(x) \in R[x]$  的不可约分解.

- (1) 由练习 2.7.32, 若  $c$  为  $R$  中素元, 则  $c$  作为常值多项式亦为  $R[x]$  中素元. 此断言亦可如下证明. 设  $c \mid g(x)h(x)$ , 作本原化:  $g(x) = c(g) \cdot g_0(x), h(x) = c(h) \cdot h_0(x)$ . 由引理 2.7.30,  $g_0(x)h_0(x)$  为本原多

项式, 因此  $c \mid c(g)c(h)$ . 而  $c$  为  $R$  中素元, 不妨设  $c \mid c(g)$ , 则  $c \mid c(g) \cdot g_0(x) = g(x)$ . 故  $c$  亦为  $R[x]$  中素元.

(2) 将  $f_0(x)$  在  $K[x]$  上作不可约分解:

$$f_0(x) = f_1(x) \cdots f_s(x),$$

其中  $f_i(x) \in K[x]$  不可约. 对每个  $f_i(x)$ , 可先通分为  $f_i(x) = \frac{1}{a} \cdot \tilde{f}_i(x)$ , 其中  $\frac{1}{a} \in K$ ,  $\tilde{f}_i(x) \in R[x]$ ; 再将  $\tilde{f}_i(x)$  本原化:  $\tilde{f}_i(x) = c(\tilde{f}_i) \cdot \bar{f}_i(x)$ . 于是

$$f_i(x) = \frac{c(f_i)}{a} \cdot \bar{f}_i(x).$$

由于  $\frac{c(f_i)}{a} \in K \setminus \{0_K\}$ ,  $f_i(x)$  与  $\bar{f}_i(x)$  在  $K[x]$  中相伴,  $\bar{f}_i(x) \in K[x]$  不可约. 故

$$f_0(x) = \frac{b}{a} \cdot \bar{f}_1(x) \cdots \bar{f}_s(x),$$

其中  $\frac{b}{a} \in K$ ,  $\bar{f}_i(x) \in K[x]$  不可约. 此时

$$a \cdot f_0(x) = b \cdot \bar{f}_1(x) \cdots \bar{f}_s(x).$$

由引理 2.7.30,  $\bar{f}_1(x) \cdots \bar{f}_s(x)$  为本原多项式, 上式两边取容度即得  $a$  与  $b$  在  $R$  中相伴. 因此  $u = \frac{b}{a} \in U(R)$ ,

$$f_0(x) = u \cdot \bar{f}_1(x) \cdots \bar{f}_s(x),$$

其中  $\bar{f}_i(x) \in K[x]$  不可约 (在  $K[x]$  中等价于素), 在  $R[x]$  中本原.

(3) 由练习 2.7.33 可得  $\bar{f}_i(x)$  是  $R[x]$  中不可约元. 亦可如下证明  $\bar{f}_i(x)$  是  $R[x]$  中素元. 设在  $R[x]$  中有  $\bar{f}_i(x) \mid g(x)h(x)$ , 由  $\bar{f}_i(x)$  是  $K[x]$  中素元, 可不妨设在  $K[x]$  中有  $\bar{f}_i(x) \mid g(x)$ ,  $g(x) = \bar{f}_i(x) \cdot d(x)$ . 设

$$d(x) = \frac{b'}{a'} \cdot \bar{d}(x),$$

其中  $a', b' \in R$ ,  $\bar{d}(x) \in R[x]$  本原. 此时

$$a' \cdot g(x) = b' \cdot \bar{f}_i(x) \cdot \bar{d}(x).$$

由引理 2.7.30,  $\bar{f}_i(x) \cdot \bar{d}(x)$  本原, 两边取容度即得  $a' \cdot c(g)$  相伴于  $b'$ . 故  $d(x)$  在  $R[x]$  中相伴于  $c(g) \cdot \bar{d}(x)$ , 进而在  $R[x]$  中  $\bar{f}_i(x) \mid g(x)$ . 这就说明  $\bar{f}_i(x)$  是  $R[x]$  中素元.  $\square$

**练习 2.7.32** 设  $R$  为 UFD,  $c \in R$  为素元, 则存在环同构

$$R[x]/(c) \simeq (R/Rc)[x].$$

此时,  $R/Rc$  为整环  $\Rightarrow (R/Rc)[x]$  为整环  $\Rightarrow R[x]/(c)$  为整环  $\Rightarrow c$  为  $R[x]$  中素元.

**练习 2.7.33** 设  $R$  为 UFD,  $K = \text{Frac}(R)$ . 若  $f(x)$  是  $R[x]$  中的本原多项式, 且在  $K[x]$  中不可约, 则存在环单同态

$$R[x]/(f(x)R[x]) \hookrightarrow K[x]/(f(x)K[x]).$$

此时, 由  $K[x]/(f(x)K[x])$  是域可得  $R[x]/(f(x)R[x])$  是整环, 从而  $f(x) \in R[x]$  不可约.

从定理 2.7.25 证明的 (3) 和练习 2.7.33 可提取出以下重要命题:

**命题 2.7.34** 设  $R$  为 UFD,  $K = \text{Frac}(R)$ . 若  $f(x) \in R[x]$  为本原多项式, 则  $f(x)$  在  $R[x]$  中不可约当且仅当  $f(x)$  是  $K$  上的不可约多项式.

**例 2.7.35**  $f(x) = x^3 + 3x - 2$  在  $\mathbb{Q}$  上不可约.

**解答** 因  $f(x)$  是  $\mathbb{Z}[x]$  中的本原多项式, 由命题 2.7.34, 只需证  $f(x)$  在  $\mathbb{Z}[x]$  中不可约. 若  $f(x)$  在  $\mathbb{Z}[x]$  中可约, 则它在  $\mathbb{Z}[x]$  中有分解  $f(x) = (x - m)(x^2 + ax + b)$ , 其中  $m, a, b \in \mathbb{Z}$ . 于是  $f(m) = 0$  且  $-mb = 2$ . 依次代入  $m = \pm 1, \pm 2$  知无解.  $\square$

**例 2.7.36** 设  $k$  为域, 则  $y^3 - x^2 \in k[x, y]$  不可约.

**解答** 因为  $k[x, y] \simeq k[x][y]$ , 若  $y^3 - x^2$  在  $k[x, y]$  中可约, 则它在  $k[x][y]$  中有分解  $y^3 - x^2 = [y - m(x)] \cdot [y^2 + a(x)y + b(x)]$ , 其中  $m(x), a(x), b(x) \in k[x]$ . 于是  $m(x)^3 - x^2 = 0$ , 但这无解.  $\square$

**注记 2.7.37** 因为  $y^3 - x^2 \in k[x][y]$  本原, 由命题 2.7.34,  $y^3 - x^2 \in k(x)[y]$  不可约, 其中  $k(x)$  表示  $k[x]$  的分式域.

**练习 2.7.38** 设  $A = k[x, y]/(y^3 - x^2)$ . 由于  $k[x, y]$  是 UFD, 由例 2.7.36 知  $y^3 - x^2$  是  $k[x, y]$  中素元, 因此  $A$  是整环. 视  $k[x, y]$  为  $k$ -线性空间,  $(y^3 - x^2)$  为  $k[x, y]$  的线性子空间, 则  $A$  为商空间.

(1) 求  $A$  的一组  $k$ -基.

(2)  $A$  是否为 UFD?

(3) 考虑  $k[t]$  的子环  $S = \{a_0 + a_2t^2 + a_3t^3 + \dots : a_i \in k\}$ . 证明:  $S \simeq A$ .

**解答** (1) 对任意  $f(x, y) \in k[x, y] = k[x][y]$ , 由于  $y^3 - x^2$  是  $k[x][y]$  中的首一多项式, 有带余除法

$$f(x, y) = g(x, y)(y^3 - x^2) + h_1(y)x + h_0(y).$$

因此  $B = \{\overline{x^n y^m} : 0 \leq n \leq 1, m \geq 0\}$  是  $A$  的生成元. 下证  $B$  是  $A$  的一组  $k$ -基. 设  $\sum_{n, m} a_{n, m} \overline{x^n y^m} = \bar{0}$ , 则存在  $F(x, y) \in k[x, y]$ , 使得

$$\sum_{n, m} a_{n, m} x^n y^m = (y^3 - x^2) F(x, y).$$

在  $k[y][x]$  中考虑上式: 若 LHS  $\neq 0$ , 则  $\deg(\text{LHS}) \leq 1$ ; 若 RHS  $\neq 0$ , 则  $\deg(\text{RHS}) \geq 2$ . 因此 LHS = RHS = 0, 即所有系数  $a_{n, m} = 0$ . 故  $B$  线性无关.

(2) 假设  $A$  为 UFD. 注意到  $\frac{\bar{x}}{\bar{y}} \in \text{Frac}(A)$  满足

$$\left(\frac{\bar{x}}{\bar{y}}\right)^2 = \frac{\bar{x}^2}{\bar{y}^2} = \frac{\bar{y}^3}{\bar{y}^2} = \bar{y},$$

即  $\frac{\bar{x}}{\bar{y}} \in \mathcal{O}_{\text{Frac}(A)}$ . 由命题 2.5.16, UFD 是整闭环, 因此  $\frac{\bar{x}}{\bar{y}} \in A$ . 设  $r(x, y) \in k[x, y]$  使得  $\frac{\bar{x}}{\bar{y}} = \overline{r(x, y)}$ , 则  $\bar{x} = \bar{y} \cdot \overline{r(x, y)}$ . 故存在  $q(x, y) \in k[x, y]$  使得

$$x = y \cdot r(x, y) + (y^2 - x^2) q(x, y).$$

考虑  $k[x][y]$  在 0 处的赋值同态  $\text{ev}_0$ , 它作用于上式便得到  $k[x]$  中等式

$$x = -x^3 \cdot q(x, 0).$$

但这不可能成立. 故  $A$  不是 UFD.

(3) 考虑环同态

$$\theta : k[x, y] \rightarrow S$$

使得

$$\theta(x) = t^3, \quad \theta(y) = t^2.$$

下证  $\text{Ker } \theta = (y^3 - x^2)$ . 显然  $(y^3 - x^2) \subset \text{Ker } \theta$ , 故只需证  $\text{Ker } \theta \subset (y^3 - x^2)$ . 设  $f(x, y) \in \text{Ker } \theta$ , 同(1) 作带余除法

$$f(x, y) = g(x, y)(y^3 - x^2) + h_1(y)x + h_0(y).$$

将  $\theta$  作用于上式两端即得

$$0 = h_1(t^2) \cdot t^3 + h_0(t^2).$$

注意到: 若  $h_1(t^2) \cdot t^3 \neq 0$ , 则其次数为奇数; 若  $h_0(t^2) \neq 0$ , 则其次数为偶数. 因此  $h_1(t^2) = h_0(t^2) = 0$  即  $h_1(y) = h_0(y) = 0$ . 故  $f(x, y) \in (y^3 - x^2)$ . 于是

$$\text{Ker } \theta = (y^3 - x^2).$$

又  $\theta$  显然是满射, 由定理 2.2.20, 存在环同构

$$k[x, y]/(y^3 - x^2) \simeq S.$$

□

**注记 2.7.39** 在  $S = k[t^2, t^3]$  中,  $t^6$  有两种分解:

$$t^6 = t^2 \cdot t^2 \cdot t^2 = t^3 \cdot t^3.$$

由于  $t^2$  和  $t^3$  不相伴且均为  $S$  中不可约元, 这两种分解本质不同. 故  $S$  不是 UFD.

**命题 2.7.40 (Eisenstein 判别法)** 设  $R$  为 UFD,  $K = \text{Frac}(R)$ ,  $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$  本原,  $p \in R$  为素元. 若  $p \mid a_{n-1}, \dots, p \mid a_1, p \mid a_0, p^2 \nmid a_0$  (从而  $p \nmid a_n$ ), 则  $f(x) \in R[x]$  不可约 (由命题 2.7.34,  $f(x) \in K[x]$  也不可约).

**证明** 设  $f(x)$  在  $R[x]$  中有非平凡分解  $f(x) = g(x)h(x)$ , 其中

$$g(x) = b_r x^r + \dots + b_1 x + b_0, \quad h(x) = c_{n-r} x^{n-r} + \dots + c_1 x + c_0,$$

则  $r, n-r > 0$ . 由于  $p \mid b_0 c_0$  而  $p^2 \nmid b_0 c_0$ ,  $b_0$  与  $c_0$  中恰有一个被  $p$  整除. 不妨设  $p \mid b_0$  且  $p \nmid c_0$ . 取最小下标  $i_0$  使得  $p \nmid b_{i_0}$ , 则  $0 < i_0 \leq r < n$ . 注意到

$$a_{i_0} = b_{i_0} c_0 + b_{i_0-1} c_1 + \dots + b_0 c_{i_0},$$

上式右端只有第一项  $b_{i_0} c_0$  不被  $p$  整除, 因此  $p \nmid a_{i_0}$ , 但  $0 < i_0 < n$ , 矛盾. □

以下用模  $p$  约化手法给出另证:

**证明** 设  $f(x)$  在  $R[x]$  中有非平凡分解  $f(x) = g(x)h(x)$ , 其中

$$g(x) = b_r x^r + \cdots + b_1 x + b_0, \quad h(x) = c_{n-r} x^{n-r} + \cdots + c_1 x + c_0.$$

考虑模  $p$  约化

$$\begin{aligned}\pi : R[x] &\rightarrow (R/pR)[x] \\ \sum_{i=0}^n a_i x^i &\mapsto \sum_{i=0}^n \bar{a}_i x^i.\end{aligned}$$

显然  $\pi$  是环同态, 于是在  $(R/pR)[x]$  中有

$$\bar{a}_n x^n = \pi(f(x)) = \pi(g(x)) \cdot \pi(h(x)).$$

由于  $p$  为素元,  $R/pR$  为整环, 可取  $K' = \text{Frac}(R/pR)$ . 由于

$$R[x] \xrightarrow{\pi} (R/pR)[x] \xrightarrow{\text{inc}} K'[x],$$

而  $K'[x]$  为 UFD, 利用唯一分解性可知  $\pi(g(x))$  与  $\pi(h(x))$  均为单项式. 故  $\bar{b}_0 = \bar{c}_0 = \bar{0}$ , 即  $p \mid b_0$  且  $p \mid c_0$ , 从而  $p^2 \mid a_0$ , 矛盾.  $\square$

**例 2.7.41**  $x^n - 2 \in \mathbb{Q}[x]$  ( $n \geq 1$ ) 均不可约. 故  $\mathbb{Q}[x]$  中存在任意次数的不可约多项式.

**例 2.7.42** 设  $f(x) \in \mathbb{Q}[x]$  使得  $f(\sqrt[n]{2}) = 0$ , 则  $(x^n - 2) \mid f(x)$ . 特别地,  $\deg(f(x)) \geq n$ .

**证明** 用反证法, 假设  $(x^n - 2) \nmid f(x)$ . 由  $x^n - 2 \in \mathbb{Q}[x]$  不可约,  $\gcd_{\mathbb{Q}[x]}(x^n - 2, f(x)) = 1$ . 由 Bézout 等式, 存在  $a(x), b(x) \in \mathbb{Q}[x]$  使得

$$a(x)(x^n - 2) + b(x)f(x) = 1.$$

将  $\sqrt[n]{2}$  处的赋值同态作用于上式两端即得矛盾.  $\square$

**例 2.7.43** 视  $\mathbb{C}$  为  $\mathbb{Q}$ -线性空间, 则  $\left\{1, \sqrt[n]{2}, \sqrt[n]{2^2}, \dots, \sqrt[n]{2^{n-1}}\right\}$  是  $\mathbb{Q}$ -线性无关的.

**练习 2.7.44** (1)  $2x + 2$  在  $\mathbb{Z}[x]$  和  $\mathbb{Q}[x]$  中是否为不可约元?

(2)  $x^2 + 1$  在  $\mathbb{R}[x]$  和  $\mathbb{C}[x]$  中是否为不可约元?

**练习 2.7.45** 设  $f(x) \in \mathbb{Z}[x]$  为首一多项式,  $p$  为素数. 考虑模  $p$  约化

$$\begin{aligned}\pi : \mathbb{Z}[x] &\rightarrow \mathbb{F}_p[x] \\ \sum_{i=0}^n a_i x^i &\mapsto \sum_{i=0}^n \bar{a}_i x^i.\end{aligned}$$

(1) 证明: 如果对某个素数  $p$ ,  $\pi(f(x))$  在  $\mathbb{F}_p[x]$  中不可约, 则  $f(x)$  在  $\mathbb{Z}[x]$  中不可约.

(2) 如果  $f(x) \in \mathbb{Z}[x]$  不是首一多项式, (1) 中的结论是否成立?

**练习 2.7.46** 设  $R$  为整环,  $f(x) \in R[x]$ ,  $c \in R$ ,  $g(x) = f(x + c) \in R[x]$ . 求证:

(1)  $f(x)$  在  $R[x]$  中本原  $\iff g(x)$  在  $R[x]$  中本原.

(2)  $f(x)$  在  $R[x]$  中不可约  $\iff g(x)$  在  $R[x]$  中不可约.

**证明** 由命题 2.4.13, 环嵌入  $R \xrightarrow{\text{inc}} R[x]$  诱导环同态

$$\theta : R[x] \rightarrow R[x]$$

使得  $\theta|_R = \text{Id}_R$  且  $\theta(x) = x + c$ . 显然  $\theta$  可逆, 其逆映射为

$$\begin{aligned}\theta^{-1} : R[x] &\rightarrow R[x] \\ f(x) &\mapsto f(x - c).\end{aligned}$$

故  $\theta$  是环同构. 显然  $\theta$  保持多项式的本原性与不可约性.  $\square$

**例 2.7.47**  $u(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1} \in \mathbb{Z}[x]$  不可约.

**证明** 由练习 2.7.46 (2), 等价于证明  $u(x+1) \in \mathbb{Z}[x]$  不可约. 而

$$u(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{i=0}^{p-1} \binom{p}{i+1} x^i,$$

由 Eisenstein 判别法,  $u(x+1) \in \mathbb{Z}[x]$  不可约.  $\square$

## 2.8 中国剩余定理

**定义 2.8.1** 设  $\{R_i : i \in I\}$  为一族环. 其直积  $\prod_{i \in I} R_i$  中的加法和乘法运算定义为

$$(r_i)_{i \in I} + (s_i)_{i \in I} = (r_i + s_i)_{i \in I}, \quad (r_i)_{i \in I} \cdot (s_i)_{i \in I} = (r_i \cdot s_i)_{i \in I}.$$

**注记 2.8.2** 任两个环的直积  $R \times S$  不是整环.

**练习 2.8.3** 投影同态

$$\begin{aligned}p : R \times S &\twoheadrightarrow S \\ (r, s) &\mapsto s\end{aligned}$$

诱导环同构

$$(R \times S)/(R \times \{0_S\}) \xrightarrow{\sim} S.$$

**定理 2.8.4 (中国剩余定理)** 设  $R$  为环,  $I_1, \dots, I_n$  为  $R$  的理想, 且对每个  $i \neq j$  皆有  $I_i + I_j = R$ , 则环同态

$$\begin{aligned}\theta : R &\rightarrow \prod_{i=1}^n R/I_i \\ r &\mapsto (r + I_1, \dots, r + I_n)\end{aligned}$$

诱导环同构

$$R/(I_1 \cap \dots \cap I_n) \xrightarrow{\sim} \prod_{i=1}^n R/I_i.$$

且  $I_1 \cap \dots \cap I_n = I_1 \cdots I_n$ .

**证明** (1)  $\text{Ker } \theta = \{r \in R : r \in I_1, \dots, r \in I_n\} = I_1 \cap \dots \cap I_n$ .

(2) 下证  $\theta$  是满的, 即对任意  $a_1, \dots, a_n \in R$ , 同余方程组

$$\begin{cases} b \equiv a_1 \pmod{I_1} \\ b \equiv a_2 \pmod{I_2} \\ \vdots \\ b \equiv a_n \pmod{I_n} \end{cases}$$

有解. 我们断言  $I_1 + I_2 \dots + I_n = R$ . 由

$$\begin{aligned} R &= RR = (I_1 + I_2)(I_1 + I_3) = I_1(I_1 + I_2 + I_3) + I_2I_3 \\ &\subset I_1 + I_2I_3 \subset R \end{aligned}$$

知  $I_1 + I_2I_3 = R$ . 由  $I_1 + I_2 \dots + I_{n-1} = R$  可得

$$\begin{aligned} R &= RR = (I_1 + I_2 \dots + I_{n-1})(I_1 + I_n) = I_1(I_1 + I_n + I_2 \dots + I_{n-1}) + I_2 \dots + I_n \\ &\subset I_1 + I_2 \dots + I_n \subset R, \end{aligned}$$

故  $R = I_1 + I_2 \dots + I_n$ . 由归纳法断言得证. 于是存在  $u_1 \in I_1$  与  $b_1 \in I_2 \dots + I_n$  使得

$$u_1 + b_1 = 1.$$

由  $I_2 \dots + I_n \subset I_2 \cap \dots \cap I_n$  即知  $b_1$  是同余方程组

$$\begin{cases} b \equiv 1 \pmod{I_1} \\ b \equiv 0 \pmod{I_2} \\ \vdots \\ b \equiv 0 \pmod{I_n} \end{cases}$$

的解. 同理可求得另  $n - 1$  个同余方程组

$$\begin{array}{ccc} \begin{cases} b \equiv 0 \pmod{I_1} \\ b \equiv 1 \pmod{I_2} \\ \vdots \\ b \equiv 0 \pmod{I_n} \end{cases} & \dots & \begin{cases} b \equiv 0 \pmod{I_1} \\ b \equiv 0 \pmod{I_2} \\ \vdots \\ b \equiv 1 \pmod{I_n} \end{cases} \end{array}$$

的解  $b_2, \dots, b_n$ . 令  $b = a_1b_1 + \dots + a_nb_n$ , 则  $b$  即最初的同余方程组的解.

(3) 由定理 2.2.20,  $\theta$  诱导环同构

$$R/(I_1 \cap \dots \cap I_n) \xrightarrow{\sim} \prod_{i=1}^n R/I_i.$$

由练习 2.8.6, 结合 (2) 中断言, 归纳即得  $I_1 \cap \dots \cap I_n = I_1 \dots + I_n$ . □

**注记 2.8.5**  $I_i + I_j = R$  这一条件通常称为 “ $I_i$  与  $I_j$  互素”. 例如对  $a, b \in \mathbb{Z}$ ,  $\gcd(a, b) = 1 \iff (a) + (b) = R$ .

$\mathbb{Z}$ .

**练习 2.8.6** 设  $I, J$  为环  $R$  的理想,  $I + J = R$ , 则  $I \cap J = IJ$ .

**证明** 由于  $I + J = R$ , 存在  $i \in I$  与  $j \in J$ , 使得  $i + j = 1$ . 任取  $a \in I \cap J$ , 则有  $a = ai + aj$ . 由  $a \in J$  且  $i \in I$  可知  $ai \in IJ$ , 由  $a \in I$  且  $j \in J$  可知  $aj \in IJ$ , 因此  $a \in IJ$ ,  $I \cap J \subset IJ$ . 又  $IJ \subset I \cap J$  是显然的, 故  $I \cap J = IJ$ .  $\square$

**例 2.8.7** 设  $\gcd(m, n) = 1$ , 则存在环同构

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z}).$$

**练习 2.8.8** 设  $R, S$  为环, 则有群同构  $U(R \times S) \simeq U(R) \times U(S)$ .

**例 2.8.9** 由例 2.8.7 与练习 2.8.8,  $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \implies U(\mathbb{Z}_{15}) \simeq U(\mathbb{Z}_3) \times U(\mathbb{Z}_5)$ .

**练习 2.8.10** 设  $R, S$  为环, 是否一定有  $\text{Aut}(R \times S) \simeq \text{Aut}(R) \times \text{Aut}(S)$ ?

**解答** 否. 取  $R = S = \mathbb{F}_2$ , 考虑

$$\begin{aligned} \theta : R \times S &\xrightarrow{\sim} R \times S \\ (a, b) &\mapsto (b, a) \end{aligned}$$

则  $\theta \in \text{Aut}(R \times S)$  且  $\theta \neq \text{Id}_{R \times S}$ . 但  $|\text{Aut}(R)| = |\text{Aut}(S)| = 1$ , 从而

$$|\text{Aut}(R \times S)| \geq 2 > 1 = |\text{Aut}(R) \times \text{Aut}(S)|.$$

$\square$

**练习 2.8.11** 设  $R, S$  为环, 则  $\text{Spec}(R \times S) = (\text{Spec}(R) \times \{S\}) \sqcup (\{R\} \times \text{Spec}(S))$ .

**解答** 任取  $\mathfrak{p} \in \text{Spec}(R \times S)$ , 令  $\mathfrak{p}_R = \pi_R(\mathfrak{p}), \mathfrak{p}_S = \pi_S(\mathfrak{p})$ , 其中  $\pi_R, \pi_S$  分别为关于  $R, S$  的投影同态. 对  $r, r' \in R$ , 注意到

$$\begin{array}{ccc} rr' \in \mathfrak{p}_R & \iff & (r, 0)(r', 0) \in \mathfrak{p} \\ \Downarrow & & \Downarrow \\ r \in \mathfrak{p}_R \text{ 或 } r' \in \mathfrak{p}_R & \iff & (r, 0) \in \mathfrak{p} \text{ 或 } (r', 0) \in \mathfrak{p} \end{array}$$

因此

$$\begin{aligned} \mathfrak{p}_R \in \text{Spec}(R) &\iff \mathfrak{p}_R \neq R, \\ \mathfrak{p}_S \in \text{Spec}(S) &\iff \mathfrak{p}_S \neq S. \end{aligned}$$

进而

$$\begin{aligned} \mathfrak{p}_R \times S \in \text{Spec}(R \times S) &\iff \mathfrak{p}_R \neq R, \\ R \times \mathfrak{p}_S \in \text{Spec}(R \times S) &\iff \mathfrak{p}_S \neq S. \end{aligned}$$

对于欲证等式, RHS  $\subset$  LHS 是显然的, 只需证 LHS  $\subset$  RHS. 结合前述讨论, 只需证  $\mathfrak{p}_R \neq R$  与  $\mathfrak{p}_S \neq S$  有且仅有一者成立.

**(至多一者成立)** 假设  $\mathfrak{p}_R \neq R$ , 则  $1_R \notin \mathfrak{p}_R$ . 任取  $s \in \mathfrak{p}_S$ , 存在  $r \in R$  使得  $(r, s) \in \mathfrak{p}$ . 因

$$(r, 1_S)(1_R, s) = (r, s) \in \mathfrak{p}, \quad (1_R, s) \notin \mathfrak{p},$$

必有  $(r, 1_S) \in \mathfrak{p}$ , 从而  $1_S \in \mathfrak{p}_S$ , 即  $\mathfrak{p}_S = S$ . 同理, 当  $\mathfrak{p}_S \neq S$  时, 必有  $\mathfrak{p}_R = R$ . 故  $\mathfrak{p}_R \neq R$  与  $\mathfrak{p}_S \neq S$  至多有一者成立.

**(至少一者成立)** 假设二者皆不成立, 即  $\mathfrak{p}_R = R$  且  $\mathfrak{p}_S = S$ , 则存在  $r \in R$  与  $s \in S$  使得  $(1_R, s), (r, 1_S) \in \mathfrak{p}$ , 从而

$$(1_R, 1_S) = (1_R, 0_S)(1_R, s) + (0_R, 1_S)(r, 1_S) \in \mathfrak{p},$$

即  $\mathfrak{p} = R \times S$ , 与  $\mathfrak{p} \in \text{Spec}(R \times S)$  矛盾. 故  $\mathfrak{p}_R \neq R$  与  $\mathfrak{p}_S \neq S$  总有一者成立.  $\square$

**注记 2.8.12** 若采用代数几何术语, 有拓扑空间范畴中的同构(即同胚)

$$\text{Spec}(R \times S) \simeq \text{Spec}(R) \sqcup \text{Spec}(S),$$

这里的无交并采用定义 1.1.7 的集合论定义. 参考 <https://stacks.math.columbia.edu/tag/00ED>.

## 第三章 域论

### 3.1 域扩张与单扩张

**定义 3.1.1** 域扩张是指域同态  $\theta : k \hookrightarrow K$ , 简记为  $K/k$ .

**注记 3.1.2** 之所以选用  $K/k$  这一记号, 是因为  $k \simeq \theta(k) \subset K$ , 我们将  $k$  等同于  $\theta(k)$ , 而后者是  $K$  的子域. 于是域扩张  $\theta : k \hookrightarrow K$  等同于包含映射  $\text{inc} : \theta(k) \hookrightarrow K$ . 此记号恰略去最关键的信息  $\theta$ , 见练习 3.1.4.

**例 3.1.3 (域扩张的例子)** (1)  $\mathbb{R}/\mathbb{Q}$  和  $\mathbb{C}/\mathbb{R}$  均是域扩张.

(2) Kronecker 添根构造:  $k \hookrightarrow k[x]/(f(x))$ .

(3) 考虑  $k[x]$  的分式域  $k(x)$ , 称为有理函数域. 典范嵌入  $k[x] \hookrightarrow k(x)$  诱导域扩张

$$k \hookrightarrow k(x), \quad \lambda \mapsto \frac{\lambda}{1}.$$

**练习 3.1.4** 设  $k$  为域, 记  $F = k(t), K = k(x)$ . 考虑域扩张

$$\begin{aligned} \theta : F &\hookrightarrow K \\ \frac{f(t)}{g(t)} &\mapsto \frac{f(x^2)}{g(x^2)}. \end{aligned}$$

通过  $\theta$  将  $K$  视为  $F$ -线性空间, 求  $\dim_F K$ . 提示 注意到  $K = \theta(F)(x)$ , 再用定理 3.1.23.

**定义 3.1.5** 设  $\theta : k \hookrightarrow K$  与  $\theta' : k \hookrightarrow K'$  是两个域扩张. 称  $\theta$  与  $\theta'$  作为域扩张同构, 若存在域同构  $\phi : K \xrightarrow{\sim} K'$ , 使得下图交换:

$$\begin{array}{ccc} & K & \\ \theta \swarrow & \downarrow & \searrow \exists \phi \text{域同构} \\ k & & K' \\ \theta' \swarrow & \downarrow & \searrow \\ & & K' \end{array}$$

若  $\theta = \theta'$ , 则  $\theta$  的自同构  $\phi : K \xrightarrow{\sim} K$  又称为域扩张  $K/k$  的自同构.

**注记 3.1.6** (1) 后文中练习 3.1.22 有助于体会  $\phi \circ \theta = \theta'$  这一条件.

(2)  $\theta$  的自同构  $\phi$  满足  $\phi \circ \theta = \theta$ , 即  $\phi|_{\theta(k)} = \text{Id}_{\theta(k)}$ .

**练习 3.1.7** 在定义 3.1.5 中,  $\phi : K \rightarrow K'$  是  $k$ -线性空间同构, 从而  $\dim_k K = \dim_k K'$ .

**注记 3.1.8**  $\text{Aut}(K/k) := \{\theta \text{ 的自同构}\} \leq \text{Aut}(K)$  为子群. 由练习 3.1.7 可见, “可视为线性同构” 是域扩张的自同构与一般的域自同构的一大区别.

**定义 3.1.9** 设  $\theta : R \hookrightarrow S$  为环的单同态,  $\alpha, \alpha_1, \alpha_2 \in S$ .

(1) 定义  $R$  与  $\alpha$  生成的子环为  $S$  中包含  $\theta(R)$  及  $\alpha$  的最小子环, 记为

$$R[\alpha] = \left\{ \text{有限和 } \sum \theta(r_i)\alpha^i : r_i \in R \right\}.$$

(2) 记  $S$  中包含  $\theta(R)$  及  $\alpha_1, \alpha_2$  的最小子环为

$$R[\alpha_1, \alpha_2] = \left\{ \text{有限和 } \sum \theta(r_{ij})\alpha_1^i \alpha_2^j : r_{ij} \in R \right\}.$$

**注记 3.1.10** (1) 由命题 2.4.13, 环嵌入  $R \xrightarrow{\text{inc}} S$  诱导环同态

$$\tilde{\psi} : R[x] \rightarrow S$$

使得  $\tilde{\psi}|_R = \text{Id}_R$  且  $\theta(x) = \alpha$ . 此时  $\text{Im } \tilde{\psi} = R[\alpha]$ .

(2)  $R[\alpha_1, \alpha_2] = R[\alpha_1][\alpha_2] = R[\alpha_2][\alpha_1]$ .

**例 3.1.11**  $\mathbb{Z}[i] \subset \mathbb{C}$ .

**定义 3.1.12** 设  $\theta : k \hookrightarrow K$  为域同态,  $\alpha, \alpha_1, \alpha_2 \in K$ .

(1) 记  $K$  中包含  $\theta(k)$  及  $\alpha$  的最小子域为

$$k(\alpha) = \left\{ \frac{\sum \theta(r_i)\alpha^i}{\sum \theta(r'_j)\alpha^j} : r_i, r'_j \in k, \sum \theta(r'_j)\alpha^j \neq 0_K \right\}.$$

(2) 记  $K$  中包含  $\theta(k)$  及  $\alpha_1, \alpha_2$  的最小子域为

$$k(\alpha_1, \alpha_2) = \left\{ \frac{\sum \theta(r_{ij})\alpha_1^i \alpha_2^j}{\sum \theta(r'_{ij})\alpha_1^i \alpha_2^j} : r_{ij}, r'_{ij} \in k, \sum \theta(r'_{ij})\alpha_1^i \alpha_2^j \neq 0_K \right\}$$

**注记 3.1.13** (1) 一般而言,  $k(\alpha)$  与  $k[x]$  无关.

(2)  $k[\alpha] \subset k(\alpha)$ .

(3) 有如下交换图表:

$$\begin{array}{ccc} k & \xrightarrow{\theta} & K \\ & \searrow & \swarrow \text{inc} \\ & k(\alpha) & \end{array}$$

(4)  $k(\alpha_1, \alpha_2) = k(\alpha_1)(\alpha_2) = k(\alpha_2)(\alpha_1)$ .

**例 3.1.14**  $\mathbb{Q}(i) \subset \mathbb{C}$ .

**定义 3.1.15** 称域扩张  $K/k$  为单扩张, 若存在  $\alpha \in K$  使得  $K = k(\alpha)$ .

**例 3.1.16** (1) Kronecker 添根构造:  $k \hookrightarrow k[x]/(f(x))$ ,  $K = k(u) = k[u]$ .

(2) 有理函数域  $k \subset k(x)$ :  $k[x] \subsetneq k(x)$ .

(3)  $\mathbb{Q} \subset \mathbb{Q}(i) = \mathbb{Q}[i]$ .

(4)  $\mathbb{R} \subset \mathbb{C}$ :  $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$ .

**定义 3.1.17** 考虑域扩张  $K/k$  及  $\alpha \in K$ . 称  $\alpha$  为  $k$  上代数元, 若存在非零多项式  $f(x) \in k[x]$  使得  $f(\alpha) = 0_K$ . 否则, 称  $\alpha$  为  $k$  上超越元.

**例 3.1.18** 考虑域扩张  $\mathbb{C}/\mathbb{Q}$ , 则  $\sqrt{2}, e^{\frac{2\pi i}{3}}$  均为 ( $\mathbb{Q}$  上) 代数元;  $\pi, e$  均为 ( $\mathbb{Q}$  上) 超越元.

**定理 3.1.19** 考虑域扩张  $K/k$  以及  $\alpha \in K$  在  $k$  上代数, 则唯一存在首一不可约多项式  $f(x) \in k[x]$  满足:

(1)  $f(\alpha) = 0$ .

(2) 若  $g(x) \in k[x]$  满足  $g(\alpha) = 0$ , 则  $f(x) \mid g(x)$ .

这样的多项式  $f(x)$  称为  $\alpha$  关于  $k$  的最小多项式.

**证明** 考虑在  $\alpha$  处的赋值同态

$$\begin{aligned} \text{ev}_\alpha : k[x] &\rightarrow K \\ g(x) &\mapsto g(\alpha), \end{aligned}$$

由  $k[x]$  是 PID, 设其核  $\text{Ker}(\text{ev}_\alpha) = (f(x))$ , 其中  $f(x) \in k[x]$ . 由定理 2.2.20, 存在环同构

$$k[x]/(f(x)) \xrightarrow{\sim} k[\alpha].$$

由于  $k[\alpha] \subset K$  为整环,  $f(x) \in k[x]$  为素元, 即  $f(x) \in k[x]$  为不可约多项式. □

**注记 3.1.20** 由命题 2.4.31,  $k[x]/(f(x))$  为域, 因此  $k[\alpha] \subset K$  为子域, 即  $k[\alpha] = k(\alpha)$ . 这可用来解释例 3.1.16 中 (1)(3)(4) 与 (2) 的不同, 即在于  $\alpha$  是否为  $k$  上代数元.

**例 3.1.21** 关于域扩张  $\mathbb{C}/\mathbb{Q}$ ,  $\sqrt[3]{2}$  的最小多项式为  $x^3 - 2$ ,  $e^{\frac{2\pi i}{3}}$  的最小多项式为  $x^2 + x + 1$ .

**练习 3.1.22** 考虑域扩张  $\theta : k \rightarrow K$  与  $\theta' : k \rightarrow K'$ ,  $\alpha \in K$ . 若存在域扩张的同构  $\phi : K \rightarrow K'$ , 则

(1)  $\alpha$  在  $k$  上代数  $\iff \phi(\alpha)$  在  $k$  上代数.

(2) 若  $\alpha$  在  $k$  上代数, 则  $\alpha$  和  $\phi(\alpha)$  的最小多项式相同.

**定理 3.1.23 (单扩张的结构定理)** 设有单扩张  $K/k$  与  $\alpha \in K$  使得  $K = k(\alpha)$ .

(1) 若  $\alpha$  在  $k$  上代数, 最小多项式为  $f(x)$ ,  $\deg(f(x)) = d$ , 则

- ◊  $\dim_k K = d < \infty$ .
- ◊  $\{1, \alpha, \dots, \alpha^{d-1}\}$  是  $K$  的一组  $k$ -基, 且  $K = k[\alpha]$ .
- ◊ 有域扩张同构  $K \cong k[x]/(f(x))$ .

(2) 若  $\alpha$  在  $k$  上超越, 则

- ◊  $\dim_k K = \infty$ .
- ◊  $k[\alpha] \subsetneq K$ .
- ◊ 有域扩张同构  $K \simeq k(x)$ .

**提示** 考虑赋值同态  $\text{ev}_\alpha$ : 若  $\alpha$  代数, 用定理 2.2.20; 若  $\alpha$  超越, 用定理 2.3.4.

**注记 3.1.24** 本质上仅有两种单扩张, 我们主要研究有限维域扩张.

**例 3.1.25** (1) 考虑  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ . 则  $\mathbb{Q}(\sqrt[3]{2})$  有  $\mathbb{Q}$ -基  $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ , 且存在域同构

$$\mathbb{Q}[x]/(x^3 - 2) \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2})$$

使得  $u = x + (x^3 - 2) \mapsto \sqrt[3]{2}$  且它在  $\mathbb{Q}$  上为恒等映射.

(2) 考虑  $\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}$ . 则  $\mathbb{Q}(\sqrt[3]{2}\omega)$  有  $\mathbb{Q}$ -基  $\{1, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega^2\}$ , 且存在域同构

$$\mathbb{Q}[x]/(x^3 - 2) \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2}\omega)$$

使得  $u = x + (x^3 - 2) \mapsto \sqrt[3]{2}\omega$  且它在  $\mathbb{Q}$  上为恒等映射.

**注记 3.1.26** 作为  $\mathbb{C}$  的子域,  $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{2}\omega)$ . 但由例 3.1.25 可得交换图表

$$\begin{array}{ccccc} & \mathbb{Q}(\sqrt[3]{2}) & & \sqrt[3]{2} & \\ & \nearrow \text{inc} & \uparrow \wr & \downarrow u & \uparrow \lambda \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}[x]/(x^3 - 2) & \mathbb{Q}(\sqrt[3]{2}\omega) & \lambda \in \mathbb{Q} \\ & \searrow \text{inc} & \downarrow \wr & \downarrow \sqrt[3]{2}\omega & \downarrow \lambda \end{array}$$

于是域扩张  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  同构于  $\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}$ :

$$\mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2}\omega), \quad a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + b\sqrt[3]{2}\omega + c\sqrt[3]{4}\omega^2.$$

**应用于  $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$  的证明** 用反证法, 设

$$\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}, \quad a, b, c \in \mathbb{Q},$$

即

$$3 = (a + b\sqrt[3]{2} + c\sqrt[3]{4})^3, \quad a, b, c \in \mathbb{Q}.$$

由注记 3.1.26, 域扩张  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  同构于  $\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}$ , 因此

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})^3 = 3 = (a + b\sqrt[3]{2}\omega + c\sqrt[3]{4}\omega^2)^3,$$

从而

$$a + b\sqrt[3]{2}\omega + c\sqrt[3]{4}\omega^2 = (a + b\sqrt[3]{2} + c\sqrt[3]{4})\omega^k,$$

其中  $k = 0$  或  $1$  或  $2$ . 利用  $\omega^2 = -\omega - 1$  化简可得:

- ◊ 若  $k = 0$ , 则  $(b\sqrt[3]{2} - c\sqrt[3]{4})\omega = b\sqrt[3]{2} + 2c\sqrt[3]{4}$ , 易知与  $\omega \notin \mathbb{R}$  矛盾.
- ◊ 若  $k = 1$ , 则  $c\sqrt[3]{4}\omega = a$ , 易知与  $\omega \notin \mathbb{R}$  矛盾.
- ◊ 若  $k = 2$ , 则  $(a + 2b\sqrt[3]{2})\omega + 2a + b\sqrt[3]{2} = 0$ , 易知与  $\omega \notin \mathbb{R}$  矛盾.

故假设不成立,  $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$ .

**定义 3.1.27** 定义域扩张  $K/k$  的次数为  $[K : k] := \dim_k K$ .

**练习 3.1.28** 设  $F/K$  为域扩张,  $u \in F$  是  $K$  上奇次代数元. 求证  $K(u) = K(u^2)$ .

**练习 3.1.29** 给出域扩张  $F/K$  的例子, 使得  $F = K(u, v)$ ,  $u$  和  $v$  均是  $K$  上超越元, 但  $F \not\simeq K(x_1, x_2)$ .

**解答**  $K = \mathbb{Q}, u = \pi, v = \sqrt{\pi}$ ,  $u$  和  $v$  在  $K$  上超越, 但  $F = K(\pi, \sqrt{\pi}) = \mathbb{Q}(\sqrt{\pi}) \simeq \mathbb{Q}(t) \not\simeq \mathbb{Q}(x_1, x_2)$ .  $\square$

**练习 3.1.30** 设  $p$  为素数, 分别求扩张  $\mathbb{Q}(e^{\frac{2\pi i}{p}})/\mathbb{Q}$  和  $\mathbb{Q}(e^{\frac{2\pi i}{8}})/\mathbb{Q}$  的次数. 提示  $p-1$  和  $4$ .

**练习 3.1.31** 求元素  $a$  在域  $K$  上的最小多项式, 其中

- (1)  $a = \sqrt{2} + \sqrt{3}, K = \mathbb{Q}$ . 提示  $x^4 - 10x^2 + 1$ .
- (2)  $a = \sqrt{2} + \sqrt{3}, K = \mathbb{Q}(\sqrt{2})$ . 提示  $x^2 - 2\sqrt{2}x - 1$ .
- (3)  $a = \sqrt{2} + \sqrt{3}, K = \mathbb{Q}(\sqrt{6})$ . 提示  $x^2 - (5 + 2\sqrt{6})$ .

**解答** (1)  $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$  零化  $a$ . 下证  $f(x) \in \mathbb{Q}[x]$  不可约. 令

$$r_1 = \sqrt{2} + \sqrt{3}, \quad r_2 = \sqrt{2} - \sqrt{3}, \quad r_3 = \sqrt{3} - \sqrt{2}, \quad r_4 = -\sqrt{2} - \sqrt{3}.$$

由  $f(x) = (x - r_1)(x - r_2)(x - r_3)(x - r_4)$ ,  $r_i \notin \mathbb{Q}$ , 且对任意  $i \neq j$ , 均有  $(x - r_i)(x - r_j) \notin \mathbb{Q}[x]$  可知  $f(x) \in \mathbb{Q}[x]$  不可约.

(2)  $f(x) = (x - \sqrt{2})^2 - 3 = x^2 - 2\sqrt{2}x - 1 \in \mathbb{Q}(\sqrt{2})[x]$  零化  $a$ . 下证  $f(x) \in \mathbb{Q}(\sqrt{2})[x]$  不可约. 否则,  $a \in \mathbb{Q}(\sqrt{2})$ , 考虑域扩张塔  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2})$ . 由 (1) 知  $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$ , 这与  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$  矛盾.

(3)  $f(x) = x^2 - (\sqrt{2} + \sqrt{3})^2 = x^2 - (5 + 2\sqrt{6}) \in \mathbb{Q}(\sqrt{6})[x]$  零化  $a$ . 下证  $f(x) \in \mathbb{Q}(\sqrt{6})[x]$  不可约. 否则,  $a \in \mathbb{Q}(\sqrt{6})$ , 考虑域扩张塔  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{6})$ . 由 Eisenstein 判别法知  $x^2 - 6 \in \mathbb{Q}[x]$  不可约, 因此  $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2$ . 由 (1) 知  $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4 > 2$ , 矛盾.  $\square$

## 3.2 域的代数扩张

**定义 3.2.1** 域扩张  $K/k$  称为代数扩张, 若任何  $\alpha \in K$  均在  $k$  上代数.

**例 3.2.2**  $\mathbb{R}/\mathbb{Q}$  不是代数扩张, 例如  $\pi$  与  $e$  均为 ( $\mathbb{Q}$  上) 超越元.

**引理 3.2.3** 有限维域扩张总是代数扩张, 即若  $\dim_k K < \infty$ , 则  $K/k$  代数.

**证明** 对任意  $\alpha \in K$ ,  $k(\alpha)$  是  $K$  的  $k$ -线性子空间, 因此  $\dim_k k(\alpha) < \infty$ . 由定理 3.1.23,  $\alpha$  是  $k$  上代数元.  $\square$

由线性代数可得另证:

**证明** 对任意  $\alpha \in K$ ,  $\{1, \alpha, \alpha^2, \dots\}$  是  $k$ -线性相关的, 即存在  $k$  上多项式零化  $\alpha$ .  $\square$

**定理 3.2.4 (维数公式)** 考虑域扩张塔  $k \subset E \subset K$ . 若  $E/k$  与  $K/E$  均为有限维域扩张, 则  $K/k$  亦为有限维域扩张, 且其次数具有塔性质:

$$[K : k] = [E : k][K : E].$$

**提示** 若  $(x_i)_{i \in I}$  和  $(y_j)_{j \in J}$  分别是  $K$  在  $E$  上和  $E$  在  $k$  上的一组基, 则  $(x_i y_j)_{(i,j) \in I \times J}$  是  $K$  在  $k$  上的一组基.

**例 3.2.5** 设  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . 考虑域扩张  $K/\mathbb{Q}$ , 求  $[K : \mathbb{Q}]$ .

**解答** 考虑域扩张塔  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset K$ , 由定理 3.2.4,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}][K : \mathbb{Q}(\sqrt{2})].$$

由例 2.7.41,  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ . 由  $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$  知  $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$  不可约, 因此  $[K : \mathbb{Q}(\sqrt{2})] = 2$ . 故  $[K : \mathbb{Q}] = 4$ .  $\square$

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$  的证明 设  $\sqrt{3} = a + b\sqrt{2}$ , 其中  $a, b \in \mathbb{Q}$ , 两边平方得

$$3 = a^2 + 2b^2 + 2ab\sqrt{2},$$

因此  $ab = 0$ . 但不论  $a = 0$  或  $b = 0$  均矛盾.

**注记 3.2.6** 从  $\mathbb{Q}(\sqrt{2})$  的  $\mathbb{Q}$ -基  $\{1, \sqrt{2}\}$  和  $K$  的  $\mathbb{Q}(\sqrt{2})$ -基  $\{1, \sqrt{3}\}$  可得  $K$  的  $\mathbb{Q}$ -基  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ .

**例 3.2.7** 设  $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ . 考虑域扩张  $K/\mathbb{Q}$ , 求  $[K : \mathbb{Q}]$ .

**解答** 考虑域扩张塔  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset K$ , 由定理 3.2.4,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][K : \mathbb{Q}(\sqrt[3]{2})].$$

由例 2.7.41,  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ . 由于  $x^2 + x + 1 = (x - \omega)(x - \omega^2)$  零化  $\omega$ , 且其在  $\mathbb{C}$  上的根  $\omega, \omega^2 \notin \mathbb{Q}(\sqrt[3]{2})$ ,  $x^2 + x + 1$  在  $\mathbb{Q}(\sqrt[3]{2})$  上不可约, 因此  $[K : \mathbb{Q}(\sqrt[3]{2})] = 2$ . 故  $[K : \mathbb{Q}] = 6$ . 从  $\mathbb{Q}(\sqrt[3]{2})$  的  $\mathbb{Q}$ -基  $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$  和  $K$  的  $\mathbb{Q}(\sqrt[3]{2})$ -基  $\{1, \omega\}$  可得  $K$  的  $\mathbb{Q}$ -基  $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega\}$ .  $\square$

**练习 3.2.8** 求  $\sqrt[3]{2}$  在  $\mathbb{Q}(\omega)$  上的最小多项式.

**解答** 假设  $\sqrt[3]{2} \in \mathbb{Q}(\omega)$ , 则有域扩张塔  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\omega)$ . 由定理 3.2.4,

$$2 = [\mathbb{Q}(\omega) : \mathbb{Q}] = \left[\mathbb{Q}(\omega) : \mathbb{Q}(\sqrt[3]{2})\right] \left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] \geq 3,$$

矛盾. 故  $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \notin \mathbb{Q}(\omega)$  即  $x^3 - 2 \in \mathbb{Q}(\omega)[x]$  不可约. 因此  $x^3 - 2$  为  $\sqrt[3]{2}$  在  $\mathbb{Q}(\omega)$  上的最小多项式.  $\square$

**练习 3.2.9** 设  $K/k$  为有限维域扩张,  $\alpha \in K$  的最小多项式  $f(x) \in k[x]$ , 则  $\deg(f(x)) \mid [K : k]$ .

**定义 3.2.10** 考虑域扩张  $K/k$ . 若一族  $K$  中的元素  $\{\alpha_i : i \in I\}$  满足  $k(\alpha_i : i \in I) = K$ , 则称  $\{\alpha_i\}_{i \in I}$  是  $K/k$  的生成元集. 具有有限生成集  $\{\alpha_1, \dots, \alpha_n\}$  的扩张称为有限生成扩张, 此时有域扩张塔

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \dots \subset K.$$

**定理 3.2.11** 域扩张  $K/k$  是有限维的  $\iff K/k$  是有限生成的代数扩张.

**命题 3.2.12** 考虑域扩张塔  $k \subset E \subset K$ , 则  $K/k$  代数  $\iff K/E$  和  $E/k$  均代数.

**证明** ( $\Rightarrow$ ) 由  $K/k$  代数,

- ◊ 对任意  $\alpha \in K$ , 存在  $f(x) \subset k[x] \subset E[x]$  使得  $f(\alpha) = 0_K$ , 因此  $K/E$  代数.
- ◊ 对任意  $\beta \in E \subset K$ , 存在  $g(x) \subset k[x]$  使得  $g(\beta) = 0_E$ , 因此  $E/k$  代数.

( $\Leftarrow$ ) 对任意  $\alpha \in K$ , 由  $K/E$  代数, 存在  $u_0, u_1, \dots, u_{n-1} \in E$ , 使得

$$\alpha^n + u_{n-1}\alpha^{n-1} + \dots + u_1\alpha + u_0 = 0_K.$$

因此  $\alpha$  在  $k(u_0, u_1, \dots, u_{n-1})$  上代数. 由定理 3.1.23,

$$[k(u_0, u_1, \dots, u_{n-1}, \alpha) : k(u_0, u_1, \dots, u_{n-1})] < \infty.$$

又  $k(u_0, u_1, \dots, u_{n-1}) \subset E$ ,  $E/k$  代数,  $k(u_0, u_1, \dots, u_{n-1})/k$  是有限生成的代数扩张. 由定理 3.2.11,

$$[k(u_0, u_1, \dots, u_{n-1}) : k] < \infty.$$

由定理 3.2.4 即得

$$[k(u_0, u_1, \dots, u_{n-1}, \alpha) : k] < \infty.$$

而  $k \subset k(\alpha) \subset k(u_0, u_1, \dots, u_{n-1}, \alpha)$ , 故  $[k(\alpha) : k] < \infty$ . 再由定理 3.1.23,  $\alpha$  在  $k$  上代数. 故  $K/k$  代数.  $\square$

**定义-定理 3.2.13** 考虑域扩张  $K/k$ . 定义  $E = \{\alpha \in K : \alpha$  在  $k$  上代数 $\}$ , 则  $E \subset K$  为子域, 它称为  $k$  在  $K$  中的代数闭包.

**证明** 对任意  $\alpha, \beta \in K$ , 考虑域扩张塔  $k \subset k(\alpha) \subset k(\alpha, \beta)$ . 由  $\alpha, \beta$  在  $k$  上代数,

$$[k(\alpha) : k] < \infty, \quad [k(\alpha, \beta) : k(\alpha)] < \infty.$$

由定理 3.2.4,  $[k(\alpha, \beta) : k] < \infty$ . 再由定理 3.2.11,  $k(\alpha, \beta)/k$  是有限生成的代数扩张. 特别地,  $\alpha \pm \beta, \alpha \cdot \beta \in k(\alpha, \beta)$  均在  $k$  上代数; 若  $\beta \neq 0_K$ ,  $\beta^{-1} \in k(\alpha, \beta)$  亦在  $k$  上代数.  $\square$

**练习 3.2.14** 考虑域扩张  $K/k$ . 若  $\beta \in K$  关于  $k$  的最小多项式为  $f(x)$ ,  $\deg(f(x)) = d$ , 则  $\beta^{-1}$  的最小多项式为  $x^d \cdot f\left(\frac{1}{x}\right)$ .

**练习 3.2.15** 在定义-定理 3.2.13 中, 若  $E \subsetneq K$ , 任取  $u \in K \setminus E$ , 则  $u$  在  $E$  上超越.

**定义 3.2.16** 域  $K$  称为代数闭域, 若它没有非平凡的代数扩张, 亦即:  $E/K$  为代数扩张  $\iff [E : K] = 1$  ( $E = K$ ).

**命题 3.2.17** 域  $K$  是代数闭域当且仅当  $K[x]$  中任意不可约多项式均为一次的.

**命题 3.2.18** 域  $K$  是代数闭域当且仅当  $K[x]$  中每个非常值多项式完全分裂, 亦即有一次因子.

**练习 3.2.19** 若域  $K$  是代数闭域, 则  $K$  必为无限域.

**证明** 假设  $|K| < \infty$ . 考虑  $f(x) = \prod_{\lambda \in K} (x - \lambda) + 1_K \in K[x]$ , 则  $f(x)$  在  $K$  上无根. 由命题 3.2.18 即得矛盾. 故  $K$  为无限域.  $\square$

**定理 3.2.20 (代数基本定理)**  $\mathbb{C}$  是代数闭域.

**练习 3.2.21** 记  $\overline{\mathbb{Q}}$  为  $\mathbb{Q}$  在  $\mathbb{C}$  中的代数闭包, 则  $\overline{\mathbb{Q}}$  是代数闭域.

**证明** 任取  $f(x) \in \overline{\mathbb{Q}}[x]$ , 由定理 3.2.20 与命题 3.2.18, 设  $f(x) = \prod_{i=1}^n (x - \lambda_i)$ , 其中  $\lambda_i \in \mathbb{C}$ . 记  $K$  为  $\overline{\mathbb{Q}}$  在  $\mathbb{C}$  中的代数闭包, 则由  $f(x) \in \overline{\mathbb{Q}}[x]$  知  $\lambda_i \in K$ . 由于  $K/\overline{\mathbb{Q}}$  与  $\overline{\mathbb{Q}}/\mathbb{Q}$  均为代数扩张, 根据命题 3.2.12,  $K/\mathbb{Q}$  为代数扩张, 即  $K \subset \overline{\mathbb{Q}}$ . 故  $\lambda_i \in \overline{\mathbb{Q}}$ , 再由命题 3.2.18 即知  $\overline{\mathbb{Q}}$  是代数闭域.  $\square$

**注记 3.2.22**  $\overline{\mathbb{Q}}$  为可数域, 其中的元素称为代数数.

**定理 3.2.23** 对任意域  $k$ , 均存在(同构意义下)唯一的代数扩张  $k \hookrightarrow \overline{k}$  使得  $\overline{k}$  为代数闭域. 这样的  $\overline{k}$  称为  $k$  的代数闭包.

**例 3.2.24**  $\mathbb{C}$  为  $\mathbb{R}$  的代数闭包, 练习 3.2.21 中  $\overline{\mathbb{Q}}$  为  $\mathbb{Q}$  的代数闭包.

**练习 3.2.25** 设  $u$  是域  $K$  的某扩域中的元素, 且  $x^n - a$  是  $u$  在  $K$  上的最小多项式. 对于  $m | n$ , 求  $u^m$  在域  $K$  上的最小多项式.

**练习 3.2.26** 设  $u$  是多项式  $x^3 - 6x^2 + 9x + 3$  的一个实根.

(1) 求证  $[\mathbb{Q}(u) : \mathbb{Q}] = 3$ .

(2) 试将  $u^4, (u+1)^{-1}, (u^2 - 6u + 8)^{-1}$  表示成  $1, u, u^2$  的  $\mathbb{Q}$ -线性组合.

**练习 3.2.27** 设  $u = \frac{x^3}{x+1}$ , 求  $[\mathbb{Q}(x) : \mathbb{Q}(u)]$ . 提示  $[\mathbb{Q}(x) : \mathbb{Q}(u)] = 3$ .

**练习 3.2.28** 设  $M/K$  为域扩张,  $M$  中元素  $u, v$  分别是  $K$  上的  $m$  次和  $n$  次代数元,  $F = K(u), E = K(v)$ .

(1) 求证  $[FE : K] \leq mn$ .

(2) 若  $\gcd(m, n) = 1$ , 则  $[FE : K] = mn$ .

我们可以将上面的练习 3.1.4 与练习 3.2.27 推广为如下命题.

**命题 3.2.29** 设  $k$  为域,  $u \in k(x) \setminus k$ , 则  $u$  在  $k$  上超越,  $x$  在  $k(u)$  上代数, 且  $[k(x) : k(u)] = \deg(u)$ , 这里  $\deg(u)$  定义为  $u$  的既约表达中分子、分母次数的较高者.

**证明** 由命题 2.7.7, 可设  $u(x) = \frac{a(x)}{b(x)}$ , 其中  $a(x), b(x) \in k[x]$  互素. 则  $a(t) - b(t)u \in k(u)[t]$  有根  $x$ , 从而  $x$  在  $k(u)$  上代数. 进而  $u$  在  $k$  上超越, 否则  $k \hookrightarrow k(u) \hookrightarrow k(x)$  是代数扩张的复合, 由命题 3.2.12,  $k(x)/k$  亦为代数扩张, 矛盾. 由于  $u$  在  $k$  上超越, 由命题 2.4.13 易知

$$k[y, t] \simeq k[u, t], \quad y \leftrightarrow u, \quad t \leftrightarrow t.$$

由于  $a(t) - b(t)y \in k[y, t]$  显然不可约, 因此  $a(t) - b(t)u \in k[u, t]$  亦不可约, 再由命题 2.7.34 知  $a(t) - b(t)u \in k(u)[t]$  不可约, 而  $x$  是它的根, 因此 (在至多相差常数倍的意义下) 它是  $x$  在  $k(u)$  上的最小多项式, 其次数为  $\deg(u)$ .  $\square$

## 3.3 分裂域

**引理 3.3.1 (关键引理)** 考虑下图

$$\begin{array}{ccc} \alpha \in E & & E' \\ \uparrow \text{域扩张} & & \uparrow \text{域扩张} \\ k & \xrightarrow[\sim]{\sigma \text{ 域同构}} & k' \end{array}$$

设  $\alpha$  关于  $k$  的最小多项式为  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x]$ . 令  $\sigma(f) = x^n + \sigma(a_{n-1})x^{n-1} + \cdots + \sigma(a_0) \in k'[x]$ . 则

(1) 若  $\beta \in \text{Root}_{E'}(\sigma(f))$ , 则唯一存在  $\sigma$  的延拓

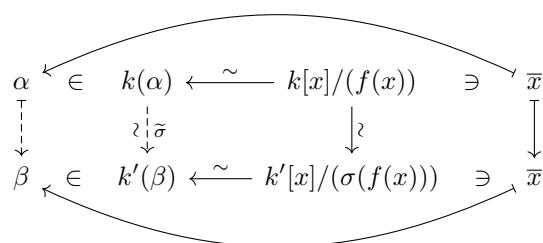
$$\tilde{\sigma} : k(\alpha) \xrightarrow{\sim} k'(\beta)$$

满足  $\tilde{\sigma}(\alpha) = \beta$ .

(2) 恰有  $|\text{Root}_{E'}(\sigma(f))|$  个这样的延拓  $\tilde{\sigma} : k(\alpha) \hookrightarrow E'$ .

**证明** (1) 设存在  $\beta \in \text{Root}_{E'}(\sigma(f))$ .

- ① 先证明  $\tilde{\sigma}$  的至多唯一性. 设  $\deg(f(x)) = d$ . 由定理 3.1.23,  $\{1, \alpha, \dots, \alpha^{d-1}\}$  是  $k(\alpha)$  的一组  $k$ -基, 而  $\tilde{\sigma}(\alpha) = \beta$ , 且对任意  $\lambda \in k$ ,  $\tilde{\sigma}(\lambda) = \sigma(\lambda)$ .
- ② 再验证如上  $\tilde{\sigma} : k(\alpha) \rightarrow k'(\beta)$  满足要求. 由  $\sigma$  是域同构知  $\sigma(f) \in k'[x]$  是首一不可约多项式, 又  $\beta \in \text{Root}_{E'}(\sigma(f))$ , 因此  $\sigma(f)$  是  $\beta$  关于  $k'$  的最小多项式. 又域同构  $\sigma : k \xrightarrow{\sim} k'$  自然诱导环同构  $k[x] \xrightarrow{\sim} k'[x]$  (仍用  $\sigma$  标识), 它使得  $(f(x)) \xrightarrow{\sigma} (\sigma(f(x)))$ . 由练习 2.6.16, 有环同构  $k[x]/(f(x)) \xrightarrow{\sim} k'[x]/(\sigma(f(x)))$ . 再结合定理 3.1.23 即可得到如下图表:



由此图表显见欲求  $\tilde{\sigma}$  (即虚线箭头) 的存在性.

(2) 设  $\delta : k(\alpha) \hookrightarrow E'$  为 (1) 中所述的延拓:

$$\begin{array}{ccc} k(\alpha) & \xhookrightarrow{\delta} & E' \\ \downarrow & & \downarrow \\ k & \xrightarrow[\sim]{\sigma} & k' \end{array}$$

将  $\delta$  作用在等式

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0_{k(\alpha)}$$

两端即得

$$\delta(\alpha)^n + \sigma(a_{n-1})\delta(\alpha)^{n-1} + \cdots + \sigma(a_0) = 0_{E'},$$

即  $\delta(\alpha) \in \text{Root}_{E'}(\sigma(f))$ . 再由 (1) 即得证.  $\square$

**注记 3.3.2** 由定理 3.1.23, 当  $\beta \in \text{Root}_{E'}(\sigma(f))$  时, 有如下图表:

$$\begin{array}{ccc} \alpha \in E & & E' \ni \beta \\ \uparrow & & \uparrow \\ k[x]/(f(x)) & \xleftarrow[\sim]{} & k'(\beta) \xrightarrow[\sim]{} k'[x]/(\sigma(f(x))) \\ \uparrow & \dashrightarrow_{\exists! \tilde{\sigma} \text{域同构}}^{\alpha \mapsto \beta} & \uparrow \\ k & \xrightarrow[\sim]{\sigma} & k' \end{array}$$

**定义 3.3.3** 设  $k$  为域, 非常值多项式  $f(x) \in k[x]$  的分裂域是指域扩张  $E/k$  满足:

- (1)  $f(x)$  在  $E$  上分裂:  $f(x) = (x - \alpha_1) \cdots (x - \alpha_n), \alpha_i \in E$ .
- (2)  $E = k(\alpha_1, \dots, \alpha_n)$ .

**注记 3.3.4** 由每个  $\alpha_i$  均被  $f(x) \in k[x]$  零化知它们在  $k$  上代数, 再由定理 3.1.23 知域扩张塔  $k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset E$  中相邻扩张均是有限维的. 由定理 3.2.4 得  $[E : k] < \infty$ .

**定理 3.3.5** 设  $k$  为域, 则非常值多项式  $f(x) \in k[x]$  在  $k$  上的分裂域总是存在的.

**证明** (1) 先证明存在域扩张  $K/k$  使得  $f(x)$  在  $K$  上完全分裂. 提示 添根构造.

- (2) 由 (1), 设  $f(x) = (x - \beta_1) \cdots (x - \beta_n), \beta_i \in K$ . 取  $E = k(\beta_1, \dots, \beta_n) \subset K$ , 则  $E/k$  为分裂域.  $\square$

**例 3.3.6** 设  $f(x) \in \mathbb{Q}[x]$ , 由定理 3.2.20,

$$f(x) = (x - z_1) \cdots (x - z_n), \quad z_i \in \mathbb{C}.$$

则  $E = \mathbb{Q}(z_1, \dots, z_n)$  为  $f(x)$  的分裂域.

**例 3.3.7**  $x^3 - 2 \in \mathbb{Q}[x]$  的分裂域为  $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ .

**例 3.3.8**  $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$  的分裂域为  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ .

**例 3.3.9**  $x^2 + x + 1 \in \mathbb{F}_2[x]$  的分裂域为  $\mathbb{F}_2(u, u + 1) = \mathbb{F}_4$ .

**定义 3.3.10** 设  $E/k$  为  $f(x) \in k[x]$  的分裂域, 称  $\text{Gal}(E/k) := \text{Aut}(E/k) = \{\delta \in \text{Aut}(E) : \delta|_k = \text{Id}_k\}$  为  $E/k$  的 Galois 群 (或方程  $f(x) = 0$  的 Galois 群  $\text{Gal}_k(f)$ ).

**注记 3.3.11** 由下面的定理 3.3.13, Galois 群的定义不依赖于域扩张  $E/k$  的选取.

**命题 3.3.12** 任取  $\alpha \in \text{Root}_E(f(x))$  与  $\sigma \in \text{Gal}_k(f)$ , 则  $\sigma(\alpha) \in \text{Root}_E(f(x))$ .

**定理 3.3.13** 给定域同构  $\sigma : k \xrightarrow{\sim} k'$ ,  $f(x) \in k[x]$  及相应的  $\sigma(f(x)) \in k'[x]$ . 取  $E/k$  为  $f(x)$  的一个分裂域,  $E'/k'$  为  $\sigma(f(x))$  的一个分裂域. 则  $\sigma$  可延拓为域同构

$$\delta : E \xrightarrow{\sim} E'.$$

这样的域同构  $\delta$  至多有  $[E : k] = [E' : k']$  个.

**证明** 对  $[E : k]$  归纳. 若  $[E : k] = 1$ , 则  $E = k$ . 因此  $f(x)$  在  $k$  上完全分裂,  $\sigma(f(x))$  在  $k'$  上完全分裂,  $E' = k'$ . 此时  $\sigma$  自身即为所求  $\delta$  (自然个数为 1). 现设  $[E : k] < N$  时结论成立, 考虑  $[E : k] = N \geq 2$  的情形. 设  $f(x)$  在  $E$  上完全分裂为

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_i \in E.$$

由于  $[E : k] > 1$ , 不妨设  $\alpha_1 \notin k$ . 设  $\alpha_1$  关于  $k$  的最小多项式为  $g(x)$ , 则  $\deg(g(x)) \geq 2$  且  $g(x) \mid f(x)$ , 进而  $\sigma(g(x)) \mid \sigma(f(x))$ . 由  $\sigma(f(x))$  在  $E'$  上完全分裂即知  $\sigma(g(x))$  亦在  $E'$  上完全分裂. 于是可取  $\beta_1 \in \text{Root}_{E'}(\sigma(g(x)))$ . 由引理 3.3.1, 唯一存在  $\sigma$  的延拓  $\tilde{\sigma} : k(\alpha_1) \xrightarrow{\sim} k'(\beta_1)$  满足  $\tilde{\sigma}(\alpha_1) = \beta_1$ . 由分裂域的定义可知  $E/k(\alpha_1)$  是  $f(x) \in k(\alpha_1)[x]$  的分裂域,  $E/k'(\beta_1)$  是  $\sigma(f(x)) \in k'(\beta_1)[x]$  的分裂域. 由定理 3.2.4,

$$[E : k(\alpha_1)] = \frac{[E : k]}{[k(\alpha_1) : k]} < [E : k].$$

由归纳假设, 存在域同构  $\delta : E \xrightarrow{\sim} E'$  延拓  $\tilde{\sigma}$ , 且这样的域同构至多有  $[E : k(\alpha_1)]$  个. 而由引理 3.3.1, 恰有  $|\text{Root}_{E'}(\sigma(g(x)))|$  个  $\tilde{\sigma} : k(\alpha_1) \xrightarrow{\sim} k'(\beta_1)$ . 于是这样的  $\delta$  的个数为

$$[E : k(\alpha_1)] \cdot \underbrace{|\text{Root}_{E'}(\sigma(g(x)))|}_{\leq \deg(g(x)) = [k(\alpha_1) : k]} \leq [E : k(\alpha_1)][k(\alpha_1) : k] \xrightarrow{\text{定理 3.2.4}} [E : k].$$

□

**推论 3.3.14** 在定理 3.3.13 中取  $\delta = \text{Id}_k$  (从而  $k' = k$ ,  $\sigma(f(x)) = f(x)$ ), 可得

$$\begin{array}{ccc} E & \xrightarrow[\text{---}]{\sim} & E' \\ \uparrow & & \uparrow \\ k & \xrightarrow{\text{Id}_k} & k \end{array}$$

(1) (分裂域的唯一性) 分裂域在域扩张同构的意义下唯一.

(2)  $|\text{Gal}_k(f)| := |\text{Aut}(E/k)| \leq [E : k]$ .

**例 3.3.15** 考虑  $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ , 由例 3.3.7, 其分裂域  $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ , 因此  $\text{Gal}_{\mathbb{Q}}(f) = \text{Aut}(E/\mathbb{Q})$ . 同练习 2.5.18 (2) 证明手法可知,  $E$  上任一自同构限制在  $\mathbb{Q}$  上均为恒等映射. 于是域  $E$  的自同构均为域扩张  $E/\mathbb{Q}$  的自同构,  $\text{Aut}(E/\mathbb{Q}) = \text{Aut}(E)$ . 记

$$\text{Root}_E(x^3 - 2) = \left\{ \beta_0 = \sqrt[3]{2}, \beta_1 = \sqrt[3]{2}\omega, \beta_2 = \sqrt[3]{2}\omega^2 \right\},$$

$$\text{Root}_E(x^2 + x + 1) = \left\{ \alpha_1 = \omega, \alpha_2 = \omega^2 \right\}.$$

由引理 3.3.1, 存在  $\text{Id}_{\mathbb{Q}}$  的延拓

$$\sigma_i : \mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sim} \mathbb{Q}(\beta_i)$$

满足  $\sigma_i(\sqrt[3]{2}) = \beta_i$ . 再次运用引理 3.3.1, 存在  $\delta_{i,j}$  的延拓

$$\delta_{i,j} : \mathbb{Q}(\sqrt[3]{2})(\omega) \xrightarrow{\sim} \mathbb{Q}(\beta_i)(\alpha_j)$$

满足  $\delta_{i,j}(\omega) = \alpha_j$ . 故

$$\text{Aut}(E) = \{\delta_{i,j} : i = 0, 1, 2; j = 1, 2\}.$$

此时  $|\text{Aut}(E/\mathbb{Q})| = 6 = [E : \mathbb{Q}]$ .

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2})(\omega) & \xrightarrow[\sim]{\delta_{i,j}} & \mathbb{Q}(\beta_i)(\alpha_j) \\ \uparrow^{x^2+x+1} & & \uparrow^{\sigma_i(x^2+x+1)} \\ \mathbb{Q}(\sqrt[3]{2}) & \xrightarrow[\sim]{\sigma_i} & \mathbb{Q}(\beta_i) \\ \uparrow^{x^3-2} & & \uparrow^{\text{Id}_{\mathbb{Q}}(x^3-2)} \\ \mathbb{Q} & \xrightarrow{\text{Id}_{\mathbb{Q}}} & \mathbb{Q} \end{array}$$

**练习 3.3.16** 例 3.3.15 中  $\text{Aut}(E)$  的乘法表.

**解答** 见表 3.1. 注意  $\text{Aut}(E)$  是非 Abel 群.

表 3.1: 例 3.3.15 中  $\text{Aut}(E)$  的乘法表

$\downarrow \circ \rightarrow$	$\delta_{0,1}$	$\delta_{0,2}$	$\delta_{1,1}$	$\delta_{1,2}$	$\delta_{2,1}$	$\delta_{2,2}$
$\delta_{0,1}$	$\delta_{0,1}$	$\delta_{0,2}$	$\delta_{1,1}$	$\delta_{1,2}$	$\delta_{2,1}$	$\delta_{2,2}$
$\delta_{0,2}$	$\delta_{0,2}$	$\delta_{0,1}$	$\delta_{2,2}$	$\delta_{2,1}$	$\delta_{1,2}$	$\delta_{1,1}$
$\delta_{1,1}$	$\delta_{1,1}$	$\delta_{1,2}$	$\delta_{2,1}$	$\delta_{2,2}$	$\delta_{0,1}$	$\delta_{0,2}$
$\delta_{1,2}$	$\delta_{1,2}$	$\delta_{1,1}$	$\delta_{0,2}$	$\delta_{0,1}$	$\delta_{2,2}$	$\delta_{2,1}$
$\delta_{2,1}$	$\delta_{2,1}$	$\delta_{2,2}$	$\delta_{0,1}$	$\delta_{0,2}$	$\delta_{1,1}$	$\delta_{1,2}$
$\delta_{2,2}$	$\delta_{2,2}$	$\delta_{2,1}$	$\delta_{1,2}$	$\delta_{1,1}$	$\delta_{0,2}$	$\delta_{0,1}$

**例 3.3.17** 考虑  $f(x) = x^2 + x + \bar{1} \in \mathbb{F}_2[x]$ , 由例 3.3.9, 其分裂域  $\mathbb{F}_2(u, u + \bar{1}) = \mathbb{F}_4$ . 因此  $\text{Gal}_{\mathbb{F}_2}(f) = \text{Aut}(\mathbb{F}_4/\mathbb{F}_2)$ . 由于  $\mathbb{F}_4$  上任一自同构限制在  $\mathbb{F}_2$  上均为恒等映射,  $\text{Aut}(\mathbb{F}_4/\mathbb{F}_2) = \text{Aut}(\mathbb{F}_4)$ . 记

$$\text{Root}_{\mathbb{F}_4}(x^2 + x + \bar{1}) = \{\alpha_0 = u, \alpha_1 = u + \bar{1}\}.$$

由引理 3.3.1, 存在  $\text{Id}_{\mathbb{F}_2}$  的延拓

$$\delta_i : \mathbb{F}_4 \xrightarrow{\sim} \mathbb{F}_2(\alpha_i)$$

满足  $\delta_i(u) = \alpha_i$ . 故

$$\text{Aut}(\mathbb{F}_4) = \{\delta_0, \delta_1\}.$$

此时  $|\text{Aut}(\mathbb{F}_4/\mathbb{F}_2)| = 2 = [\mathbb{F}_4 : \mathbb{F}_2]$ .

$$\begin{array}{ccc} \mathbb{F}_2(u) & = & \mathbb{F}_4 \xrightarrow{\sim} \mathbb{F}_4 \\ & & \uparrow \delta_i \\ & & \mathbb{F}_2 \xrightarrow{\text{Id}_{\mathbb{F}_2}} \mathbb{F}_2 \\ \uparrow x^2+x+\bar{1} & & \uparrow \text{Id}_{\mathbb{F}_2}(x^2+x+\bar{1}) \end{array}$$

**练习 3.3.18** 例 3.3.17 中,  $\delta_0 = \text{Id}_{\mathbb{F}_4}$ , 而对每个  $a \in \mathbb{F}_4$  均有  $\delta_1(a) = a^2$ .

**定义 3.3.19** 称非零多项式  $f(x) \in k[x]$  (在某个扩域里) 有重根, 若存在域扩张  $E/k$  使得对某个  $a \in E$  有  $(x - a)^2 \mid f(x)$ .

**定义 3.3.20** 设  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in k[x]$ . 定义  $f(x)$  的形式微分为

$$f'(x) = n a_n x^{n-1} + \dots + 2 a_2 x + a_1.$$

**注记 3.3.21** 若  $n1_k \neq 0_k$ , 则对任意  $n$  次多项式  $f(x)$ ,  $\deg(f'(x)) = \deg(f(x)) - 1$ .

**性质 3.3.22 (Leibniz 法则)** 设  $f(x), g(x) \in k[x]$ , 则

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x).$$

**引理 3.3.23** 非零多项式  $f(x) \in k[x]$  无重根当且仅当  $\gcd_{k[x]}(f(x), f'(x)) = 1$ .

**定义 3.3.24** 非零多项式  $f(x) \in k[x]$  称为  $k$  上可分的, 若  $f(x)$  在  $k[x]$  中的不可约因子均无重根.

**引理 3.3.25** 若  $\text{char}(k) = 0$ , 则  $k$  上的任意多项式均可分.

**证明** 设  $g(x)$  是  $f(x) \in k[x]$  的不可约因子. 由注记 3.3.21,  $\deg(g'(x)) = \deg(g(x)) - 1$ . 因此

$$\gcd_{k[x]}(g(x), g'(x)) = 1.$$

由引理 3.3.23,  $g(x)$  无重根. 故  $f(x)$  在  $k$  上可分.  $\square$

**例 3.3.26 (不可分多项式)** 考虑有理函数域  $k = \mathbb{F}_p(t)$ , 其中  $p$  为素数,  $t$  为未定元. 由  $t \in \mathbb{F}_p[t]$  为素元, 根据 Eisenstein 判别法,  $x^p - t \in \mathbb{F}_p[t][x]$  不可约. 而  $\mathbb{F}_p[t]$  为 UFD, 由命题 2.7.34,  $x^p - t \in k[x]$  不可约. 设  $\alpha$  是  $x^p - t$  在  $k$  的某个扩域上的根, 则由

$$x^p - t = x^p - \alpha^p = (x - \alpha)^p$$

可知  $\alpha$  是重根. 故  $x^p - t \in k[x]$  是不可分多项式.

**练习 3.3.27** 考虑域扩张  $K/k$  与  $f(x) \in k[x]$ . 若  $f(x)$  在  $k$  上可分, 则  $f(x)$  在  $K$  上亦可分.

**定理 3.3.13 续** 给定域同构  $\sigma : k \xrightarrow{\sim} k'$ ,  $f(x) \in k[x]$  及相应的  $\sigma(f(x)) \in k'[x]$ . 取  $E/k$  为  $f(x)$  的一个分裂域,  $E'/k'$  为  $\sigma(f(x))$  的一个分裂域. 则  $f(x) \in k[x]$  可分当且仅当  $\sigma$  仅有  $[E : k]$  个延拓  $\delta : E \xrightarrow{\sim} E'$ . 此时  $|\text{Aut}(E/k)| = [E : k]$ .

**有限维域扩张** 设  $E/k$  为有限维域扩张, 由定理 3.2.11,  $E/k$  是有限生成的代数扩张. 因此任意  $u \in E$  均有关于  $k$  的最小多项式  $g(x)$ . 对任意  $\sigma \in \text{Aut}(E/k)$ , 由  $\sigma|_k = \text{Id}_k$  知, 对  $g(x) \in k[x]$ , 有  $g(u) = 0 \implies g(\sigma(u)) = 0$ , 即  $\sigma(u) \in \text{Root}_E(g(x))$ , 它仅有有限种可能取值. 设  $E = k(u_1, \dots, u_n)$ , 我们有以下事实:

**练习 3.3.28** 设  $\sigma, \tau \in \text{Aut}(E/k)$ . 若  $\sigma(u_i) = \tau(u_i), \forall i$ , 则  $\sigma = \tau$ .

也即域扩张  $E/k$  的自同构完全由其在生成元集上的作用确定. 故  $\text{Aut}(E/k)$  是有限群.

**例 3.3.29**  $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \text{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \{\text{Id}_{\mathbb{Q}(\sqrt[3]{2})}\}$ . 它是平凡群的原因在于  $x^3 - 2$  在  $\mathbb{Q}(\sqrt[3]{2})$  中的根仅有  $\sqrt[3]{2}$ .

**定理 3.3.30** 设  $E/k$  是有限维域扩张, 则  $|\text{Aut}(E/k)| \leq [E : k]$ , 等号成立当且仅当  $E/k$  是  $k$  上某个可分多项式的分裂域. 此时, 对任意  $a \in E$ , 有  $a \in k$  当且仅当对任意  $\sigma \in \text{Aut}(E/k)$  均有  $\sigma(a) = a$ .

**证明** (1) 由定理 3.2.11,  $E/k$  是有限生成的代数扩张, 设  $E = k(u_1, \dots, u_n)$ . 不妨只考虑  $n = 2$  的情形. 取  $u_1$  关于  $k$  的最小多项式  $g_1(x) \in k[x]$ , 任取  $\beta_1 \in \text{Root}_E(g_1(x))$ . 由引理 3.3.1, 对于每个取定的  $\beta_1$ , 唯一存在  $\text{Id}_k$  的延拓  $\sigma_1 : k(u_1) \xrightarrow{\sim} k(\beta_1)$  满足  $\sigma_1(u_1) = \beta_1$ . 这样的延拓  $\sigma_1$  恰有  $|\text{Root}_E(g_1(x))|$  个, 而  $|\text{Root}_E(g_1(x))| \leq \deg(g_1(x)) = [k(\beta_1) : k]$ . 再取  $u_2$  关于  $k(u_1)$  的最小多项式  $g_2(x) \in k(u_1)[x]$ , 任取  $\beta_2 \in \text{Root}_E(\sigma_1(g_2(x)))$ . 再由引理 3.3.1, 对于给定的  $\sigma_1$  与取定的  $\beta_2$ , 唯一存在  $\sigma_1$  的延拓  $\sigma_2 : E \xrightarrow{\sim} E$  满足  $\sigma_2(u_2) = \beta_2$ . 这样的延拓恰有  $|\text{Root}_E(\sigma_1(g_2(x)))|$  个, 而  $|\text{Root}_E(\sigma_1(g_2(x)))| \leq \deg(g_2(x)) = [E : k(\beta_1)]$ . 故

$$\begin{aligned} |\text{Aut}(E/k)| &= |\text{Root}_E(g_1(x))| \cdot |\text{Root}_E(\sigma_1(g_2(x)))| \\ &\leq [k(\beta_1) : k][E : k(\beta_1)] \xrightarrow{\text{定理 3.2.4}} [E : k]. \end{aligned}$$

- (2) 设  $|\text{Aut}(E/k)| = [E : k]$ . 由 (1) 中第一处 “ $\leq$ ” 为 “ $=$ ” 知,  $u_1$  关于  $k$  的最小多项式  $h_1(x) \in k[x]$  在  $E$  上分裂且无重根. 由于从  $k$  到  $E$  的扩张不依赖于  $u_1, \dots, u_n$  的顺序, 对域扩张  $k(u_i)/k$  如上分析即知,  $u_i$  关于  $k$  的最小多项式  $h_i \in k[x]$  在  $E$  上分裂且在  $k$  上可分. 记  $f(x) = \prod_{i=1}^n h_i(x) \in k[x]$ , 则  $f(x)$  在  $E$  上分裂且在  $k$  上可分,  $E/k$  即  $f(x)$  的分裂域.
- (3) 设  $E/k$  为  $k$  上可分多项式  $f(x)$  的分裂域,  $f(x) = (x - u_1) \cdots (x - u_n)$ . 由于  $u_1$  关于  $k$ 、 $u_2$  关于  $k(u_1)$  直至  $u_n$  关于  $k(u_1, \dots, u_{n-1})$  的最小多项式均为  $f(x)$  的因子, 因此它们在  $E$  上分裂且无重根. 由此可知 (1) 中每处 “ $\leq$ ” 均为 “ $=$ ”, 故  $|\text{Aut}(E/k)| = [E : k]$ .
- (4) 设  $E/k$  是  $k$  上可分多项式  $f(x)$  的分裂域,  $a \in E$ , 且对任意  $\sigma \in \text{Aut}(E/k)$  均有  $\sigma(a) = a$ . 下证  $a \in k$ . 用反证法, 假设  $a \notin k$ , 则  $a$  关于  $k$  的最小多项式  $g(x)$  满足  $\deg(g(x)) \geq 2$ . 同 (2) 知  $g(x)$  在  $E$  上分裂且无重根, 因此  $|\text{Root}_E(g(x))| = \deg(g(x)) \geq 2$ , 存在  $b \neq a$  使得  $g(b) = 0$ . 由引理 3.3.1, 存在  $\text{Id}_k$  的延拓  $\sigma : k(a) \xrightarrow{\sim} k(b)$  满足  $\sigma(a) = b$ . 由于  $\sigma(f(x)) = f(x)$ ,  $E/k(a)$  为  $f(x) \in k(a)[x]$  的分裂域,  $E/k(b)$  为  $f(x) \in k(b)[x]$  的分裂域, 由定理 3.3.13, 存在  $\sigma$  的延拓  $\delta \in \text{Aut}(E)$ . 因此  $\delta \in \text{Aut}(E/k)$ , 但  $\delta(a) = \sigma(a) = b \neq a$ , 矛盾.

$$\begin{array}{ccc} E & \xrightarrow{\sim} & E \\ \uparrow & & \uparrow \\ k(a) & \xrightarrow{\sim} & k(b) \\ \uparrow & & \uparrow \\ k & \xrightarrow{\text{Id}_k} & k \end{array}$$

□

**不动子域** 设  $E/k$  为有限维域扩张,  $H \leqslant \text{Aut}(E/k)$  为子群. 定义  $H$ -不动子域为

$$E^H := \{z \in E : \sigma(z) = z, \forall \sigma \in H\}.$$

此时有域扩张塔  $k \subset E^H \subset E$ .

**中间域** 考虑域扩张塔  $k \subset K \subset E$ . 此时对中间域  $K$  有

$$\text{Aut}(E/K) = \{\sigma \in \text{Aut}(E) : \sigma|_K = \text{Id}_K\} \leqslant \text{Aut}(E/k)$$

为子群.

## 3.4 有限域

**有限域的概念** 设  $E$  为有限域. 由推论 2.2.24,  $\text{char}(R) = p$  ( $p$  为素数). 再由注记 2.2.25, 存在域嵌入  $\mathbb{F}_p \hookrightarrow E$ . 由练习 2.4.39, 可视  $E$  为  $\mathbb{F}_p$ -线性空间. 设  $n = \dim_{\mathbb{F}_p} E$ , 则有线性同构  $E \simeq \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ . 于是  $|E| = p^n$ .

**定义 3.4.1** 设有限域  $E$  特征为  $p$ . 定义  $E$  上的 Frobenius 自同构为

$$\begin{aligned}\sigma : E &\xrightarrow{\sim} E \\ a &\longmapsto a^p.\end{aligned}$$

**注记 3.4.2** 考虑域扩张  $E/\mathbb{F}_p$ , 由于  $\sigma \in \text{Aut}(E)$ ,  $\sigma|_{\mathbb{F}_p} = \text{Id}_{\mathbb{F}_p}$ . 因此对任意  $\bar{m} \in \mathbb{F}_p$ ,  $\sigma(\bar{m}) = \bar{m}^p = \bar{m}$ . 这便是 Fermat 小定理.

**例 3.4.3** 考虑域扩张  $\mathbb{F}_4/\mathbb{F}_2$ , 则  $\sigma|_{\mathbb{F}_2} = \text{Id}_{\mathbb{F}_2}$ ,  $\sigma(u) = u^2 = u + \bar{1}$ ,  $\sigma(u + \bar{1}) = u^2 + \bar{1} = u$ . 因此  $\sigma^2 = \text{Id}_{\mathbb{F}_4}$ . 而  $|\text{Aut}(\mathbb{F}_4/\mathbb{F}_2)| \leqslant [\mathbb{F}_4 : \mathbb{F}_2] = 2$ , 因此  $\text{Aut}(\mathbb{F}_4/\mathbb{F}_2) = \{\text{Id}_{\mathbb{F}_4}, \sigma\}$ .

**例 3.4.4** 有理函数域  $\mathbb{F}_p(t)$  的 Frobenius 自同态  $\sigma(x) = x^p$  不是满射. 例如, 假设  $t \in \text{Im } \sigma$ , 则存在  $f(t), g(t) \in \mathbb{F}_p[t]$ , 使得  $\left(\frac{f(t)}{g(t)}\right)^p = t$ . 两边取次数即  $p \cdot [\deg(f) - \deg(g)] = 1$ , 但这不可能. 故  $t \notin \text{Im } \sigma$ .

设  $|E| = p^n$ , 则  $E^\times = E \setminus \{0_E\}$  满足  $|E^\times| = p^n - 1$ . 我们有定理 4.1.18 的特殊情形:

**引理 3.4.5** 对任意  $a \in E^\times$  均有  $a^{p^n-1} = 1_E$ . 故任意  $a \in E$  均为  $x^{p^n} - x$  的根.

**证明** 固定  $a \in E^\times$ , 考虑无穷序列

$$1_E, a, a^2, \dots \in E.$$

由  $E$  是有限域, 必存在  $i < j$  使得  $a^i = a^j$ . 于是  $a^{j-i} = 1_E$ . 取最小的  $d \geqslant 1$  使得  $a^d = 1_E$ . 由于  $H = \{1_E, a, \dots, a^{d-1}\} \leqslant E^\times$  是子群, 由定理 4.1.18,  $|H| \mid (p^n - 1)$  即  $d \mid (p^n - 1)$ . 故  $a^{p^n-1} = 1_E$ .  $\square$

**定理 3.4.6** 对任意正整数  $n$  与素数  $p$ , 唯一存在  $p^n$  阶有限域, 通常记为  $\mathbb{F}_{p^n}$ .

**证明 (至多唯一性)** 设存在有限域  $E$  满足  $|E| = p^n$ . 由引理 3.4.5,  $E/\mathbb{F}_p$  是  $x^{p^n} - x \in \mathbb{F}_p[x]$  的分裂域, 它在域扩张同构的意义下唯一.

**(存在性)** 设  $K/\mathbb{F}_p$  为  $x^{p^n-1} - x \in \mathbb{F}_p[x]$  的分裂域. 由  $K/\mathbb{F}_p$  是有限生成的代数扩张知  $[K : \mathbb{F}_p] < \infty$ , 因此  $K$  为有限域. 取  $E = \text{Root}_K(x^{p^n} - x)$ . 考虑  $K$  上的 Frobenius 自同构  $\sigma$ , 对任意  $a, b \in E$ , 有

$$(a \pm b)^{p^n} = \sigma^n(a \pm b) = \sigma^n(a) \pm \sigma^n(b) = a \pm b, \quad (ab)^{p^n} = a^{p^n}b^{p^n} = ab,$$

因此  $E$  为  $K$  的子域. 由  $K$  的定义即得  $E = K$ . 只需说明  $|E| = p^n$  即  $x^{p^n} - x \in \mathbb{F}_p[x]$  无重根. 这来自

$$\gcd_{\mathbb{F}_p[x]} \left( x^{p^n} - x, (x^{p^n} - x)' \right) = \gcd_{\mathbb{F}_p[x]} \left( x^{p^n} - x, -1 \right) = 1. \quad \square$$

**注记 3.4.7** 特别地, 我们有  $\mathbb{F}_{p^n}[x]$  中的等式

$$x^{p^n} - x = \prod_{a \in \mathbb{F}_{p^n}} (x - a).$$

当  $n = 1$  时, 就得到  $\mathbb{F}_p[x]$  中的等式

$$x^p - x = x(x - 1) \cdots (x - \overline{p-1}),$$

两边约去  $x$  即

$$x^{p-1} - 1 = (x - 1) \cdots (x - \overline{p-1}).$$

令  $x = \bar{0}$  便是初等数论中的 Wilson 定理:

$$(p-1)! \equiv -1 \pmod{p}.$$

**命题 3.4.8** 对素数  $p$  与正整数  $n$ , 在  $\mathbb{F}_p[x]$  中有分解

$$x^{p^n} - x = \prod_{d|n} \prod_{\substack{\text{d 次首一不可约} \\ \text{多项式 } f(x) \in \mathbb{F}_p[x]}} f(x).$$

**证明** 取定  $E$  满足  $|E| = p^n$ . 任取  $x^{p^n} - x$  的不可约因子  $f(x) \in \mathbb{F}_p[x]$ , 则  $f(x)$  在  $E$  上完全分裂, 因此可取  $a \in E$  使得  $f(a) = \bar{0}$ . 考虑域扩张塔

$$\mathbb{F}_p \subset \mathbb{F}_p(a) \subset E.$$

由于  $[\mathbb{F}_p(a) : \mathbb{F}_p] = \deg(f(x))$ ,  $[E : \mathbb{F}_p] = n$ , 由定理 3.2.4,  $\deg(f(x)) \mid n$ . 又  $x^{p^n} - x$  无重根 (见定理 3.4.6 证明), 故  $f(x)$  在分解式中仅出现一次. 反过来, 设  $g(x) \in \mathbb{F}_p[x]$  为  $d$  次首一不可约多项式,  $d \mid n$ . 考虑 Kronecker 添根构造  $K = \mathbb{F}_p[x]/(g(x))$ , 记  $u = \bar{x}$ . 则  $K = \mathbb{F}_p(u)$ ,  $[K : \mathbb{F}_p] = d$ , 因此  $|K| = p^d$ . 由引理 3.4.5,  $u^{p^d} - u = \bar{0}$ . 又  $g(x)$  是  $u$  的最小多项式, 因此  $g(x) \mid (x^{p^d} - x)$ . 而  $(x^{p^d} - x) \mid (x^{p^n} - x)$ , 故  $g(x) \mid (x^{p^n} - x)$ .  $\square$

$(x^{p^d} - x) \mid (x^{p^n} - x)$  的证明  $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1, \forall a, m, n \in \mathbb{Z}_+$ .

**例 3.4.9** 在命题 3.4.8 中, 取  $p = 2$  可得  $\mathbb{F}_2[x]$  中分解

$$\begin{aligned} x^4 - x &= x(x + \bar{1})(x^2 + x + \bar{1}), \\ x^8 - x &= x(x + \bar{1})(x^3 + x^2 + \bar{1})(x^3 + x + \bar{1}), \\ x^{16} - x &= x(x + \bar{1})(x^2 + x + \bar{1})(x^4 + x^3 + x^2 + x + \bar{1})(x^4 + x^3 + \bar{1})(x^4 + x + \bar{1}). \end{aligned}$$

取  $p = 3$  可得  $\mathbb{F}_3[x]$  中分解

$$x^9 - x = x(x + \bar{1})(x - \bar{1})(x^2 + \bar{1})(x^2 + x - \bar{1})(x^2 - x - \bar{1}).$$

**命题 3.4.10** 取定  $p^n$  元域  $E$ .

- (1) 设  $K$  为  $E$  的子域, 则  $|K| = p^d$ , 其中  $d \mid n$ .
- (2) 设  $d \mid n$ , 则存在唯一的子域  $K \subset E$  满足  $|K| = p^d$ .

**证明** (1) 考虑域扩张塔  $\mathbb{F}_p \subset K \subset E$ , 由定理 3.2.4 得  $[K : \mathbb{F}_p] \mid [E : \mathbb{F}_p]$ .

- (2) (至多唯一性) 假设  $K \subset E$  满足  $|K| = p^d$ , 由引理 3.4.5,  $K \subset \text{Root}_E(x^{p^d} - x)$ . 但  $x^{p^d} - x$  无重根 (见定理 3.4.6 证明),  $|\text{Root}_E(x^{p^d} - x)| = p^d = |K|$ , 因此  $K = \text{Root}_E(x^{p^d} - x)$ .
- (存在性) 只需验证  $\text{Root}_E(x^{p^d} - x) \subset E$  是  $p^d$  阶子域. □

**例 3.4.11 ( $\mathbb{F}_{2^6}$  的子域格)** 取定域  $E$  使得  $|E| = 2^6$ . 由命题 3.4.10, 存在唯一子域  $K_1 \subset E$  与  $K_2 \subset E$  满足  $|K_1| = 2^2, |K_2| = 2^3$ .

$$\begin{array}{ccccc} & & K_1 & & \\ & \swarrow & & \searrow & \\ \mathbb{F}_2 & & \subset & & E \\ & \nwarrow & & \swarrow & \\ & & K_2 & & \end{array}$$

此时,  $K_1 = \{a \in E : a^4 = a\}, K_2 = \{b \in E : b^8 = b\}$ .

**练习 3.4.12** 设  $E, K_1, K_2$  如例 3.4.11 所述.

- (1) 证明:  $K_1 \cap K_2 = \mathbb{F}_2$ .
- (2) 求  $|\{u \in E : \mathbb{F}_2(u) = E\}|$ .

**解答** (1)  $K_1 \cap K_2 = \{a \in E : a^2 = a\} = \text{Root}_E(x^2 - x) = \mathbb{F}_2$ .

- (2) 结合 (1) 可知  $|\{u \in E : \mathbb{F}_2(u) = E\}| = |E \setminus (K_1 \cup K_2)| = 64 - (4 + 8 - 2) = 54$ . □

从例 3.4.11 可提取出如下结论: 设  $n$  有素因数分解  $n = q_1^{r_1} \cdots q_t^{r_t}$  ( $r_i \geq 1$ ), 则  $E$  的极大真子域  $K_i$  阶为  $p^{\frac{n}{q_i}}$ . 此时, 从练习 3.4.12 (2) 出发, 我们还有

**命题 3.4.13**  $E$  的全体极大真子域的并集  $\bigcup_{i=1}^t K_i \neq E$ . 故存在  $u \in E$  使得  $E = \mathbb{F}_p(u)$ .

**证明** 只需作简单的估计:

$$\left| \bigcup_{i=1}^t K_i \right| \leq \sum_{i=1}^t p^{\frac{n}{q_i}} \leq t \cdot p^{\frac{n}{2}} < \frac{n}{2} \cdot p^{\frac{n}{2}} \leq p^n.$$
□

从命题 3.4.13 可知  $E/\mathbb{F}_p$  为单扩张. 于是  $E \setminus (K_1 \cup \dots \cup K_t)$  中任一元素关于  $\mathbb{F}_p$  的最小多项式次数为  $[E : \mathbb{F}_p] = n$ . 故我们得到

**推论 3.4.14** 对任意正整数  $n$ ,  $\mathbb{F}_p[x]$  中总有  $n$  次不可约多项式.

**命题 3.4.15** 取定  $n$  次首一不可约多项式  $f(x) \in \mathbb{F}_p[x]$ . 设  $u \in \text{Root}_E(f(x))$ , 则

$$f(x) = \prod_{i=0}^{n-1} (x - \sigma^i(u)).$$

**证明** 由  $u \in \text{Root}_E(f(x))$  可知  $[\mathbb{F}_p(u) : \mathbb{F}_p] = \deg(f(x)) = n$ , 因此  $\mathbb{F}_p(u) = E$ .

(1) 先证明  $\sigma^i(u) \neq u, \forall 1 \leq i \leq n - 1$ . 假设存在  $i \leq n - 1$  使得  $\sigma^i(u) = u$ . 记

$$d = \gcd(i, n) = mi + rn, \quad m, r \in \mathbb{Z}.$$

由  $u \in E$  即知  $\sigma^n(u) = u$ . 于是

$$\sigma^d(u) = (\sigma^i)^m \circ (\sigma^n)^r(u) = (\sigma^i)^m(u) = u.$$

若  $d < n$ , 则  $u \in \mathbb{F}_{p^d} \subsetneq E, \mathbb{F}_p(u) \subsetneq E$ , 矛盾. 故  $d = n$ , 但这与  $i \leq n - 1$  矛盾.

(2) 由 (1) 可知  $\sigma^i(u) \neq \sigma^j(u), 0 \leq i < j \leq n - 1$ . 否则两边作用  $\sigma^{-i}$  即得矛盾.

(3) 由于  $\sigma \in \text{Aut}(E), u, \sigma(u), \dots, \sigma^{n-1}(u) \in \text{Root}_E(f(x))$  且两两不同.  $\square$

**注记 3.4.16**  $E/\mathbb{F}_p$  是  $\mathbb{F}_p$  上可分多项式  $f(x)$  的分裂域.

**例 3.4.17** 对任意  $w \in \mathbb{F}_9 \setminus \mathbb{F}_3$ ,  $w$  与  $\sigma(w) = w^3$  有相同的最小多项式, 为

$$(x - w)(x - \sigma(w)) \in \mathbb{F}_3[x].$$

**证明** 由 Fermat 小定理,  $\sigma|_{\mathbb{F}_3} = \text{Id}_{\mathbb{F}_3}$ . 视  $\mathbb{F}_9$  为  $\mathbb{F}_3$ -线性空间, 则

$$g(w) = \bar{0} \iff \sigma(g(w)) = \bar{0} \iff g(\sigma(w)) = \bar{0}.$$

又  $[\mathbb{F}_9 : \mathbb{F}_3] = 2$ ,  $w$  的最小多项式次数为 2,  $\sigma(w) \neq w$ , 因此  $w$  (与  $\sigma(w)$ ) 关于  $\mathbb{F}_3$  的最小多项式为  $(x - w)(x - \sigma(w)) \in \mathbb{F}_3[x]$ .  $\square$

**注记 3.4.18** 由此可知  $\mathbb{F}_3[x]$  中共有 3 个 2 次首一不可约多项式.

**定理 3.4.19** 设域  $E$  满足  $|E| = p^n$ , 则  $\text{Aut}(E) = \{\text{Id}_E, \sigma, \dots, \sigma^{n-1}\}$ .

**证明** 取定  $u$  使  $\mathbb{F}_p(u) = E$ , 设  $u$  关于  $\mathbb{F}_p$  的最小多项式为  $f(x)$ . 由命题 3.4.15 证明知  $\text{Id}_E, \sigma, \dots, \sigma^{n-1} \in \text{Aut}(E)$  两两不同, 且  $u, \sigma(u), \dots, \sigma^{n-1}(u) \in \text{Root}_E(f(x))$ . 任取  $\delta \in \text{Aut}(E)$ , 则  $\delta(u) \in \text{Root}_E(f(x))$ . 因此存在  $0 \leq i \leq n - 1$ , 使得  $\delta(u) = \sigma^i(u)$ . 又  $E$  的任一自同构限制在  $\mathbb{F}_p$  上均为恒等映射, 由  $E$  为  $\mathbb{F}_p$ -线性空间即知  $\delta = \sigma^i$ .  $\square$

**注记 3.4.20**  $\text{Aut}(E)$  为循环群. 对任意  $d | n$ ,

$$H_d = \{\text{Id}_E, \sigma^d, \sigma^{2d}, \dots, \sigma^{n-d}\} \leqslant \text{Aut}(E)$$

为子群, 且  $\text{Aut}(E)$  的任意子群均形如此.

由命题 3.4.10 与注记 3.4.20,  $E$  的子域与  $\text{Aut}(E)$  的子群均一一对应于  $n$  的(正)因子. 故我们得到

**定理 3.4.21 (有限域的 Galois 对应)** 设  $E$  为有限域,  $|E| = p^n$ . 存在 **格** 的反同构

$$\{H \leqslant \text{Aut}(E) \text{ 子群}\} \xleftarrow{1:1} \{K \subset E \text{ 子域}\}$$

$$H_d \xrightarrow{\begin{array}{c} K_d = \{a \in E : \sigma^d(a) = a\} \\ = \{a \in E : \delta(a) = a, \forall \delta \in H_d\} \\ = \text{Root}_E(x^{p^d} - x) \end{array}}$$

$$\text{Aut}(E/K_d) = \{\delta \in E : \delta|_{K_d} = \text{Id}_{K_d}\} \xleftarrow{\quad} K_d.$$

**注记 3.4.22** (1)  $K_d$  是由  $\sigma^d$  生成的子群  $H_d$  的不动子域.

(2) 由注记 3.4.16,  $E/K_d$  也是  $K_d$  上可分多项式  $f(x) = x^{p^n} - x$  的分裂域. 由定理 3.3.13 续,  $|\text{Aut}(E/K_d)| = [E : K_d]$ . 这与  $|\text{Aut}(E/K_d)| = |H_d| = \frac{n}{d}$  而  $[E : K_d] = \frac{n}{d}$  相符.

(3) Galois 对应反保持偏序关系(格结构).

## 3.5 分圆域

**定义 3.5.1** 称元素  $w \in k$  为  $n$  次单位根, 若满足  $w^n = 1_k$ . 定义单位根  $w$  的阶  $\text{ord}(w)$  为最小的正整数  $d$  使得  $w^d = 1_k$ . 此时, 称  $w$  为  $d$  次本原单位根.

**引理 3.5.2** 设单位根  $w \in k$  满足  $\text{ord}(w) = d$ , 则  $w^n = 1_k \iff d \mid n$ .

**引理 3.5.3** 设  $\text{char}(k) = p > 0$ , 单位根  $w \in k$  满足  $\text{ord}(w) = d$ , 则  $p \nmid d$ .

**证明** 用反证法, 假设  $d = pd_1$ , 则

$$0_k = w^d - 1_k = (w^{d_1})^p - 1_k^p = (w^{d_1} - 1_k)^p \implies w^{d_1} = 1_k.$$

这与  $d$  的最小性矛盾.  $\square$

**例 3.5.4** 设有限域  $E$  满足  $|E| = p^n$ . 任意  $w \in E^\times$  均满足  $w^{p^n-1} = 1_E$ , 故  $\text{ord}(w) \mid (p^n - 1)$ .

若  $w \in k$  为  $d$  次本原单位根, 则  $\{1, w, \dots, w^{d-1}\} = \text{Root}_k(x^d - 1)$  为  $k^\times$  的  $d$  阶子群. 事实上, 这是唯一可能的  $d$  阶子群:

**定理 3.5.5** 设  $k$  为域, 且  $H \leq k^\times$  为  $d$  阶子群, 则存在  $d$  阶本原单位根  $w$ , 且  $H = \{1, w, \dots, w^{d-1}\}$ . 特别地, 这样的  $H$  唯一.

**例 3.5.6** 设有限域  $E$  满足  $|E| = p^n$ , 则  $E^\times$  为  $p^n - 1$  阶群. 由定理 3.5.5, 存在  $p^n - 1$  次本原单位根  $u \in E$ , 使得  $E^\times = \{1, u, \dots, u^{p^n-2}\}$ . 于是  $E = \mathbb{F}_p(u)$ .

**例 3.5.7** 考虑九元域  $E = \mathbb{F}_3[x]/(x^2 + \bar{1})$ , 记  $u = \bar{x}$ . 在  $E^\times$  中, 由于  $\text{ord}(u + \bar{1}) \mid 8$ , 而  $(u + \bar{1})^2 = \bar{2}u$ ,  $(u + \bar{1})^4 = \bar{2}$ , 因此  $\text{ord}(u + \bar{1}) = 8$ ,  $u + \bar{1}$  是  $E^\times$  的生成元.

**复单位根** 设  $n \geq 2$ , 考虑  $\zeta = \zeta_n = e^{\frac{2\pi i}{n}}$ , 则  $\text{Root}_{\mathbb{C}}(x^n - 1) = \{1, \zeta, \dots, \zeta^{n-1}\}$ ,

$$x^n - 1 = (x - 1)(x - \zeta) \cdots (x - \zeta^{n-1}).$$

由定理 3.5.5,  $\{1, \zeta, \dots, \zeta^{n-1}\}$  是  $\mathbb{C}^\times$  的(唯一)  $n$  阶子群.

**练习 3.5.8** 设  $\zeta$  是  $n$  次本原单位根,  $m$  为正整数, 则  $\text{ord}(\zeta^m) = \frac{n}{\gcd(m, n)}$ .

**引理 3.5.9** 复  $n$  次本原单位根的全体恰为  $\{\zeta^d : 1 \leq d < n, \gcd(d, n) = 1\}$ , 共有  $\varphi(n)$  个, 这里  $\varphi(n)$  为 Euler 函数.

**定义 3.5.10**  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  恰为  $x^n - 1 \in \mathbb{Q}[x]$  的分裂域, 称为分圆域.

**例 3.5.11**  $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ ,  $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ ,  $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\mathbf{i})$ ,  $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$ .

**计算  $\zeta_5$**  将  $\zeta = \zeta_5$  满足的方程  $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$  写成

$$(\zeta + \zeta^{-1})^2 + (\zeta + \zeta^{-1}) - 1 = 0.$$

由此可得  $2 \cos \frac{2\pi}{5} = \zeta_5 + \zeta_5^{-1} = \frac{\sqrt{5}-1}{2}$ , 进而  $\zeta_5 = \frac{\sqrt{5}-1}{4} + \sqrt{\frac{5+\sqrt{5}}{8}}i$ . 由于  $\zeta_5, \zeta_5^{-1} \in \mathbb{Q}(\zeta_5)$ , 而  $\zeta_5 + \zeta_5^{-1} = \frac{\sqrt{5}-1}{2}$ , 因此  $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$ .

**定义 3.5.12** 对  $n \geq 2$ ,  $n$  级分圆多项式

$$\Phi_n(x) = \prod_{\text{ord}(w)=n} (x-w) = \prod_{\substack{1 \leq m < n \\ \gcd(m,n)=1}} (x - \zeta^m).$$

**注记 3.5.13** 补充定义  $\Phi_1(x) = x - 1$ . 我们有  $\deg \Phi_n(x) = \varphi(n)$ .

**引理 3.5.14**  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ .

**证明** 由练习 3.5.8, 对于  $1 \leq m \leq n$  与  $d | n$ ,

$$\text{ord}(\zeta^m) = d \iff \gcd(m, n) = \frac{n}{d} \iff m = \frac{n}{d} \cdot k \text{ 且 } \gcd(k, d) = 1.$$

因此  $n$  次单位根中阶为  $d$  的元素为

$$S_d = \{\zeta^{\frac{n}{d}k} : 1 \leq k \leq d, \gcd(k, d) = 1\}.$$

利用  $n$  次单位根之集的划分

$$\{1, \zeta, \dots, \zeta^{n-1}\} = \bigsqcup_{d|n} S_d$$

即得

$$x^n - 1 = (x - 1)(x - \zeta) \cdots (x - \zeta^{n-1}) = \prod_{d|n} \prod_{w \in S_d} (x - w) = \prod_{d|n} \Phi_d(x).$$

□

**注记 3.5.15** 由  $\{1, \zeta, \dots, \zeta^{n-1}\} = \bigsqcup_{d|n} S_d$  可得  $n = \sum_{d|n} \varphi(d)$ .

**例 3.5.16** 设  $p$  为素数, 则  $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$ .

**定理 3.5.17** 对任意正整数  $n$ ,  $\Phi_n(x) \in \mathbb{Z}[x]$ .

**证明** 用归纳法, 当  $n = 1$  时,  $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$ . 假设对所有正整数  $d < n$ , 均有  $\Phi_d(x) \in \mathbb{Z}[x]$ . 令

$$g(x) = \prod_{\substack{d|n \\ 1 \leq d < n}} \Phi_d(x),$$

则  $g(x) \in \mathbb{Z}[x]$ . 由引理 3.5.14,

$$x^n - 1 = g(x)\Phi_n(x).$$

由于  $g(x)$  首一, 由带余除法, 存在  $q(x), r(x) \in \mathbb{Z}[x]$  使得

$$x^n - 1 = q(x)g(x) + r(x),$$

其中  $r(x) = 0$  或  $\deg(r(x)) < \deg(g(x))$ . 将以上两式看作  $\mathbb{C}[x]$  中带余除法, 由定理 2.4.18 即知  $r(x) = 0$  且  $q(x) = \Phi_n(x)$ . 故  $\Phi_n(x) \in \mathbb{Z}[x]$ .  $\square$

**练习 3.5.18** 设域  $F$  为  $p^n$  元域,  $p$  为素数,  $f(x) \in F[x]$  为首一不可约多项式. 求证:

- (1)  $f(x)$  有重根  $\iff$  存在  $g(x) \in F[x]$ , 使得  $f(x) = g(x^p)$ .
- (2) 如果  $f(x) = g(x^{p^n})$ , 其中  $g(x) \in F[x]$ , 但不存在  $\bar{g}(x) \in F[x]$  使得  $f(x) = \bar{g}(x^{p^{n+1}})$ , 则  $p^n \mid m = \deg(f(x))$ , 并且  $f(x)$  共有  $\frac{m}{p^n}$  个不同的根, 每个根的重数均为  $p^n$ .

**证明** (1) 设  $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ , 则

$$\begin{aligned} f(x) \text{ 有重根} &\iff \gcd(f(x), f'(x)) \neq 1 \iff \begin{cases} f(x) \text{ 首一不可约} \\ \deg(f'(x)) < \deg(f(x)) \end{cases} \implies f'(x) = 0 \\ &\iff ma_m = 0, 0 \leq m \leq n \iff \text{若 } p \nmid m \text{ 则 } a_m = 0. \end{aligned}$$

- (2) 由  $f(x)$  首一不可约且  $f(x) = g(x^{p^{n+1}})$  知  $g(x)$  亦为首一不可约多项式. 由条件, 不存在  $h(x) \in F[x]$  使得  $g(x) = h(x^p)$ . 由(1), 这等价于  $g(x)$  无重根. 设

$$g(x) = \prod_{i=1}^{\frac{m}{p^n}} (x - u_i),$$

其中  $u_i$  互异. 取  $v_i$  使得  $v_i^{p^n} = u_i$ , 则  $v_i$  互异, 且

$$f(x) = g(x^{p^{n+1}}) = \prod_{i=1}^{\frac{m}{p^n}} (x^{p^n} - v_i^{p^n}) = \prod_{i=1}^{\frac{m}{p^n}} [\sigma^n(x) - \sigma^n(v_i)] = \prod_{i=1}^{\frac{m}{p^n}} (x - v_i)^{p^n}.$$

 $\square$ 

由例 3.5.16 与例 2.7.47, 对于素数  $p$ ,  $\Phi_p(x) \in \mathbb{Z}[x]$  不可约. 更一般地, 我们有

**定理 3.5.19**  $\Phi_n(x) \in \mathbb{Z}[x]$  不可约 (由命题 2.7.34,  $\Phi_n(x) \in \mathbb{Q}[x]$  也不可约), 它是任意  $n$  次本原单位根的最小多项式.

**证明** 取定  $n$  次本原单位根  $\zeta_n$  及其(首一)最小多项式  $P \in \mathbb{Q}[x]$ , 则  $P \mid \Phi_n$ . 如能证明每个  $n$  次单位根  $\zeta$  都是  $P$  的根, 则  $\deg P = \varphi(n) = \deg \Phi_n$ , 从而  $\Phi_n = P$  不可约. 为此只需证对  $\zeta$  如上及满足  $p \nmid n$  的素数  $p$ , 皆有  $P(\zeta) = 0 \implies P(\zeta^p) = 0$ ; 因为对任意满足  $\gcd(k, n) = 1$  及  $1 < k < n$  的正整数  $k$ , 可由素因数分解  $k = p_1 \cdots p_s$  ( $p_i \nmid n$ ) 得到  $P(\zeta) = 0 \implies P(\zeta^{p_1}) = 0 \implies P(\zeta^{p_1 p_2}) = 0 \implies \cdots \implies P(\zeta^{p_1 \cdots p_s}) = 0$ .

注意到  $\Phi_n(\zeta^p) = 0$ , 并且在  $\mathbb{Q}[x]$  中有分解  $\Phi_n = PQ$ , 其中  $Q$  首一, 而由注记 2.7.31 即得  $P, Q \in \mathbb{Z}[x]$ . 假设  $P(\zeta) = 0$  而  $P(\zeta^p) \neq 0$ , 则  $Q(\zeta^p) = 0$ . 此时  $P(x)$  与  $Q(x^p)$  有公共根  $\zeta$ , 因此  $P(x)$  与  $Q(x^p)$  在  $\mathbb{C}[x]$  中不互素, 由于  $\mathbb{Q}[x]$  中最大公因子不随域  $\mathbb{Q}$  的扩张而改变, 它们在  $\mathbb{Q}[x]$  中也不互素. 又  $P(x)$  在  $\mathbb{Q}$  上不可约, 因此在  $\mathbb{Q}[x]$  中  $P(x) \mid Q(x^p)$ , 即存在  $R(x) \in \mathbb{Q}[x]$  使得  $Q(x^p) = P(x)R(x)$ . 再次运用注记 2.7.31 即知  $R(x) \in \mathbb{Z}[x]$ . 考虑多项式的模  $p$  约化  $\pi : \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$ . 由 Fermat 小定理, 设  $Q(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$ , 则

$$\begin{aligned} \pi(Q(x^p)) &= \overline{b_m} x^{pm} + \overline{b_{m-1}} x^{p(m-1)} + \cdots + \overline{b_1} x^p + \overline{b_0} \\ &= (\overline{b_m} x^m)^p + (\overline{b_{m-1}} x^{m-1})^p + \cdots + (\overline{b_1} x)^p + (\overline{b_0})^p \\ &= (\overline{b_m} x^m + \overline{b_{m-1}} x^{m-1} + \cdots + \overline{b_1} x + \overline{b_0})^p = \pi(Q(x))^p. \end{aligned}$$

于是由  $Q(x^p) = P(x)R(x)$  可得

$$\pi(Q)^p = \pi(P)\pi(R).$$

由于  $\mathbb{F}_p[x]$  是 UFD,  $\pi(P)$  在  $\mathbb{F}_p[x]$  中任一不可约因子必整除  $\pi(Q)$ , 从而  $\pi(P)$  与  $\pi(Q)$  不互素. 而  $\pi(\Phi_n) = \pi(P)\pi(Q), \Phi_n(x) | (x^n - 1)$ , 故  $\pi(x^n - 1) = x^n - \bar{1} \in \mathbb{F}_p[x]$  有重根. 但由  $p \nmid n$  知  $(x^n - \bar{1})' = nx^{n-1} \in \mathbb{F}_p[x]$  非零,  $\gcd(x^n - \bar{1}, nx^{n-1}) = \bar{1}$ , 由引理 3.3.23 知  $x^n - \bar{1} \in \mathbb{F}_p[x]$  无重根, 矛盾.  $\square$

**推论 3.5.20** 分圆域  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  的维数  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ .

由于  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  是可分多项式  $x^n - 1 \in \mathbb{Q}[x]$  的分裂域, 由定理 3.3.13 续,

$$|\text{Aut}(\mathbb{Q}(\zeta_n))| = |\text{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

注意到域的自同构保持代数元的最小多项式, 因此对任意  $\sigma \in \text{Aut}(\mathbb{Q}(\zeta_n))$ ,  $\sigma(\zeta_n)$  仍为  $n$  次本原单位根, 记  $\sigma(\zeta_n) = \zeta_n^k$ , 其中  $1 \leq k \leq n$  且  $\gcd(k, n) = 1$ .

**定理 3.5.21** 存在群同构

$$\text{Aut}(\mathbb{Q}(\zeta_n)) \xrightarrow{\sim} U(\mathbb{Z}_n), \quad \sigma \mapsto \bar{k},$$

其中  $\sigma$  满足  $\sigma(\zeta_n) = \zeta_n^k$ .

**注记 3.5.22** 在此群同构下, 复共轭  $\sigma(z) = \bar{z}$  的像为  $-\bar{1}$ .

**练习 3.5.23**  $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\cos \frac{2\pi}{n})$ . 这便是  $\mathbb{Q}(\zeta_n)$  的不动子域  $\mathbb{Q}(\zeta_n)^{\{\text{Id}, \sigma\}}$ , 其中  $\sigma$  为复共轭.

**提示** 利用第一类 Chebyshev 多项式证明 LHS  $\subset$  RHS, 注意  $\mathbb{Q}(\zeta_n) = \mathbb{Q}[\zeta_n]$ .

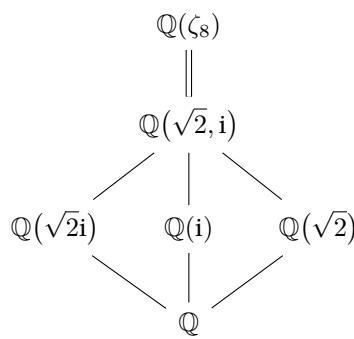
**例 3.5.24** 由定理 3.5.21,  $\text{Aut}(\mathbb{Q}(\zeta_8)) \simeq U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ , 元素间的对应关系为

$$\bar{1} \leftrightarrow (\zeta_8 \mapsto \zeta_8), \quad \bar{3} \leftrightarrow (\zeta_8 \mapsto \zeta_8^3), \quad \bar{5} \leftrightarrow (\zeta_8 \mapsto \zeta_8^5), \quad \bar{7} \leftrightarrow (\zeta_8 \mapsto \zeta_8^7).$$

易知  $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$ . 利用  $\zeta_8 + \zeta_8^7 = \sqrt{2}$  与  $\zeta_8^2 = i$ , 经计算可将上述  $\text{Aut}(\mathbb{Q}(\zeta_8))$  元素重新表述为

$\text{Id} : \sqrt{2} \mapsto \sqrt{2}, i \mapsto i$	$\sigma : \sqrt{2} \mapsto -\sqrt{2}, i \mapsto -i$	$\delta : \sqrt{2} \mapsto -\sqrt{2}, i \mapsto i$	$\tau : \sqrt{2} \mapsto \sqrt{2}, i \mapsto -i$
--	---	--	--

由定理 4.1.18, 四阶群  $\text{Aut}(\mathbb{Q}(\zeta_8)) = \{\text{Id}, \sigma, \delta, \tau\}$  的非平凡子群只能为二阶群, 而由上述可见  $\sigma, \delta, \tau$  均为二阶元, 故所有二阶子群为  $\{\text{Id}, \sigma\}, \{\text{Id}, \delta\}, \{\text{Id}, \tau\}$ . 再考虑余下两个平凡子群, 由 Galois 对应及下面的练习 3.5.25 结果可得  $\mathbb{Q}(\zeta_8)$  的所有子域为  $\mathbb{Q}(\zeta_8), \mathbb{Q}(\sqrt{2}i), \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}$ .



**练习 3.5.25** 例 3.5.24 中  $\{\text{Id}, \sigma\}, \{\text{Id}, \delta\}, \{\text{Id}, \tau\}$  对应的  $\mathbb{Q}(\zeta_8)$  的不动子域分别为  $\mathbb{Q}(\sqrt{2}i), \mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ .

**提示**  $\mathbb{Q}(\zeta_8)$  的一组  $\mathbb{Q}$ -基为  $\{1, \sqrt{2}, i, \sqrt{2}i\}$ .

## 第四章 群论

### 4.1 群的定义

**定义 4.1.1** 二元组  $(G, \cdot)$  称为群, 其中  $G$  为非空集合, 乘法  $\cdot$  为二元运算

$$G \times G \rightarrow G, \quad (a, b) \mapsto a \cdot b$$

满足如下三条公理:

**(G1) 结合律:**  $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in G.$

**(G2) 有幺元:** 存在  $1_G \in G$ , 使得  $1_G \cdot a = a = a \cdot 1_G, \forall a \in G.$

**(G3) 有逆元:** 对任意  $a \in G$ , 存在  $b \in G$ , 使得  $a \cdot b = 1_G = b \cdot a$ , 记  $b = a^{-1}$ .

有时简记  $(G, \cdot)$  为  $G$ , 乘法运算  $a \cdot b = ab$ .

**注记 4.1.2** 满足 **(G1)** 和 **(G2)** 的称为含幺半群.

**练习 4.1.3** 群中幺元和逆元均是唯一的.

**定义 4.1.4** 若群  $G$  中运算还满足交换律, 则称  $G$  为交换群或 Abel 群.

**引理 4.1.5** 设  $G$  为群, 则有

(1) 乘法消去律:  $ab = ac \implies b = c.$

(2)  $ab = 1_G \implies b = a^{-1}.$

(3)  $(a^{-1})^{-1} = a.$

(4)  $(ab)^{-1} = b^{-1}a^{-1}.$

(5)  $a^{n+m} = a^n \cdot a^m, \forall n, m \in \mathbb{Z}.$

**定义 4.1.6** 非空子集  $H \subset G$  称为  $G$  的子群, 若对任意  $a, b \in H$ , 均有  $a \cdot b \in H, a^{-1} \in H$ , 记作  $H \leq G$ . 此时,  $H$  也是群.

**注记 4.1.7** 每个群  $G$  均有平凡子群  $\{1_G\}$  和  $G$ .

**例 4.1.8 (一般线性群)**  $\mathrm{GL}(n, \mathbb{C}) = \{A \in M_n(\mathbb{C}) : \det(A) \neq 0\}$ .

**例 4.1.9 (特殊线性群)**  $\mathrm{SL}(n, \mathbb{C}) = \{A \in \mathrm{GL}(n, \mathbb{C}) : \det(A) = 1\}$ .

**例 4.1.10 (正交群)**  $\mathrm{O}(n) = \{A \in \mathrm{GL}(n, \mathbb{R}) : AA^\top = I_n\}$ .

**例 4.1.11 (特殊正交群)**  $\mathrm{SO}(n) = \{A \in \mathrm{O}(n) : \det(A) = 1\}$ .

**约定 4.1.12** 加法群意指 Abel 群  $A$ , 其二元运算记为  $+$ , 么元记为  $0$ , 元素  $a \in A$  的加法逆元(负元)记为  $-a$ .

**例 4.1.13** 给定环  $R$ , 自然有三个群: 加法群  $(R, +)$ , 单位群  $(U(R), \cdot)$ , 自同构群  $(\mathrm{Aut}(R), \circ)$ . 实例如下:

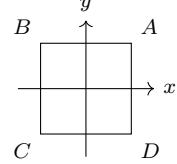
$R$	$\mathbb{Z}$	$\mathbb{Z}_n$	$\mathbb{Z}[\mathrm{i}]$
$(R, +)$	$(\mathbb{Z}, +)$	$(\mathbb{Z}_n, +)$	$(\mathbb{Z}[\mathrm{i}], +) \simeq (\mathbb{Z}, +) \times (\mathbb{Z}, +)$
$(U(R), \cdot)$	$\{\pm 1\}$	$\{\bar{m} : 1 \leq m \leq n, \gcd(m, n) = 1\}$	$\{\pm 1, \pm \mathrm{i}\}$
$(\mathrm{Aut}(\mathbb{Q}), \circ)$	$\{\mathrm{Id}_{\mathbb{Z}}\}$	$\{\mathrm{Id}_{\mathbb{Z}_n}\}$	$\{\mathrm{Id}_{\mathbb{Z}[\mathrm{i}]}, \sigma \text{ (复共轭)}\}$

**例 4.1.14** 考虑域扩张  $K/k$ , 则  $\mathrm{Aut}(K/k) = \{\sigma \in \mathrm{Aut}(K) : \sigma|_k = \mathrm{Id}_k\} \leqslant \mathrm{Aut}(K)$ .

**例 4.1.15** 图形  $P \subset \mathbb{R}^n$  的对称群  $\Sigma(P) = \{g \in \mathrm{O}(n) : g(P) = P\} \leqslant \mathrm{O}(n)$ . 称  $g \in \Sigma(P)$  为  $P$  的对称. 如  $\mathbb{R}^2$  中单位圆周  $\mathbb{S}^1$  的对称群即  $\mathrm{O}(2)$ .

**练习 4.1.16** 写出  $\mathbb{R}^2$  中以原点为中心的正方形的对称群(矩阵形式).

提示 四个旋转和四个镜面对称,  $|\Sigma(\square)| = 8$ .



**例 4.1.17** 抽象集  $X$  (无附加结构) 上的置换指双射  $\sigma : X \xrightarrow{\sim} X$ ,  $X$  的对称群  $S(X) = \{X \text{ 上的所有置换}\}$ . 如  $\mathrm{Aut}(R) \leqslant S(R)$ ,  $\mathrm{GL}(n, \mathbb{C})$  同构于  $S(\mathbb{C}^n)$  的子群.

**定理 4.1.18 (Lagrange 定理)** 设  $G$  为有限群,  $H \leqslant G$ , 则  $|H| \mid |G|$ .

**证明** 定义  $G$  上关系  $\approx$  为  $a \approx b \iff ab^{-1} \in H$ , 容易验证  $\approx$  是等价关系, 且任意  $a \in H$  关于  $\approx$  的等价类为  $Ha = \{ha : h \in H\}$ , 称其为  $H$  的右陪集. 设  $G = \bigsqcup_{i \in I} Ha_i$  为  $G$  关于  $H$  的右陪集分解, 称  $\{a_i\}_{i \in I}$  为  $G$  关于  $H$  的右陪集完全代表元系. 观察到对任意  $a \in G$ ,  $|Ha| = |H|$ , 因此  $|G| = |H| \cdot |I|$ .  $\square$

**注记 4.1.19**  $[G : H] := |I|$  称为  $H$  在  $G$  中的指数. 故 Lagrange 定理可表述为  $|G| = |H| \cdot [G : H]$ .

**练习 4.1.20** 设  $H \leqslant G$ .  $H$  的左陪集  $aH = \{ah : h \in H\}$  是  $a$  关于等价关系  $a \sim b \iff b^{-1}a \in H$  的等价类.

**练习 4.1.21** 设  $H \leqslant G$ . 若  $G = \bigsqcup_{i \in I} Ha_i$ , 则  $G = \bigsqcup_{i \in I} a_i^{-1}H$ .

**例 4.1.22** 设  $G = \mathrm{GL}(2, \mathbb{F}_2)$ . 考虑  $G$  的子群  $H = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix} \right\}$  与元素  $a = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}$ , 则  $Ha = \left\{ \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \right\} \neq \left\{ \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix} \right\} = aH$ .

**定义 4.1.23** 元素  $a \in G$  的阶是指最小的正整数  $d$  使得  $a^d = 1_G$ , 记为  $\text{ord}(a)$ . 若不存在这样的  $d$ , 则记  $\text{ord}(a) = \infty$ .

**注记 4.1.24** 若  $G$  是有限群, 则  $G$  中任意元素  $a$  具有有限的阶, 且  $\text{ord}(a) \mid |G|$ .

**例 4.1.25** 设  $p$  为素数. 由注记 4.1.24, 对任意  $\bar{m} \in \mathbb{F}_p^\times$ , 有  $\bar{m}^{p-1} = \bar{1}$ . 这即是 Fermat 小定理.

**命题 4.1.26** 设  $G$  为群,  $a \in G$ . 若  $\text{ord}(a) = d < \infty$ , 则  $a^n = 1_G$  当且仅当  $d \mid n$ .

**定义 4.1.27** 设  $G, G'$  为群. 称映射  $f : G \rightarrow G'$  为群同态, 若  $f(a \cdot b) = f(a) \cdot f(b), \forall a, b \in G$ . 双射的群同态称为群同构.

**注记 4.1.28**  $f$  是群同态蕴含了  $f(1_G) = 1_{G'}$  及  $f(a)^{-1} = f(a^{-1})$ .

**练习 4.1.29** 设  $f : G \rightarrow G'$  为群同态,  $a \in G$ , 则  $\text{ord}(f(a)) \mid \text{ord}(a)$ . 若  $f$  是群同构, 则  $\text{ord}(f(a)) = \text{ord}(a)$ .

**注记 4.1.30** 同构的群的阶表必定相同.

**例 4.1.31** 子群  $H \leqslant G$  诱导包含同态  $\text{inc} : H \rightarrow G$ .

**例 4.1.32** 行列式映射  $\det : \text{GL}(n, \mathbb{C}) \rightarrow \mathbb{C}^\times$  是群的满同态.

**例 4.1.33** 记  $n$  阶单位根群  $\mu_n = \{z \in \mathbb{C} : z^n = 1\} \leqslant \mathbb{C}^\times$ , 存在群同构

$$\mu_n \xrightarrow{\sim} (\mathbb{Z}_n, +), \quad e^{\frac{2k\pi}{n}} \mapsto \bar{k}.$$

**定义 4.1.34** 设  $G, H$  是两个群, 在  $G \times H = \{(g, h) : g \in G, h \in H\}$  中定义乘法为

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

则  $G \times H$  是一个群, 称为  $G$  与  $H$  的直积, 其中  $1_{G \times H} = (1_G, 1_H)$ ,  $(g, h)^{-1} = (g^{-1}, h^{-1})$ .

◊ 有自然同态

$$G \hookrightarrow G \times H, \quad g \mapsto (g, 1_H).$$

◊ 有投影同态

$$G \times H \twoheadrightarrow G, \quad (g, h) \mapsto g.$$

$$\diamond (g, h) = (g, 1_H) \cdot (1_G, h) = (1_G, h) \cdot (g, 1_H).$$

**练习 4.1.35** 考虑  $(g, h) \in G \times H$ , 若  $\text{ord}(g), \text{ord}(h) < +\infty$ , 则  $\text{ord}(g, h) = \text{lcm}(\text{ord}(g), \text{ord}(h))$ .

**例 4.1.36** Klein 四元群  $V_4 := \mu_2 \times \mu_2 = \{(\pm 1, \pm 1)\}$ , 其阶表如下:

	(1, 1)	(1, -1)	(-1, 1)	(-1, -1)
阶	1	2	2	2

特别地,  $V_4$  无四阶元, 因此  $V_4 \not\simeq \mathbb{Z}_4$ . 由命题 4.2.7,  $V_4$  不是循环群. 由推论 4.2.12,  $V_4$  是最小的非 Abel 群.

**练习 4.1.37** 存在群同构  $V_4 \simeq U(\mathbb{Z}_8)$ .

**定义 4.1.38** 设  $G$  为群,  $X \subset G$  是任意子集, 则包含  $X$  的最小子群称为由  $X$  生成的子群, 记为  $(X)$ . 若  $(X) = G$ , 则称  $X$  为  $G$  的生成元集. 当  $X$  是独点集  $\{x\}$  时, 简记  $(\{x\})$  为  $(x) := \{x^n : n \in \mathbb{Z}\}$ .

**注记 4.1.39**  $(X)$  中的元素是由  $X$  的元素出发, 经乘法及求逆运算所能得到的所有元素:

$$(X) = \{1_G\} \cup \{x_1 \cdots x_n : x_i \in X \text{ 或 } x_i^{-1} \in X, n \geq 1\}.$$

**练习 4.1.40** 证明:  $(\mathbb{Q}, +) \not\simeq (\mathbb{Q}^\times, \cdot)$ .

**证明** 假设存在群同构  $f : (\mathbb{Q}, +) \xrightarrow{\sim} (\mathbb{Q}^\times, \cdot)$ , 取  $a \in \mathbb{Q}$  使得  $f(a) = 2$ , 则  $2 = f(a) = f\left(\frac{a}{2} + \frac{a}{2}\right) = f\left(\frac{a}{2}\right)^2$ , 与  $\sqrt{2} \notin \mathbb{Q}$  矛盾.  $\square$

**练习 4.1.41** 设  $A, B$  是群  $G$  的两个子群. 试证:  $AB \leq G$  当且仅当  $AB = BA$ .

**练习 4.1.42** 设  $a, b$  是群  $G$  的任意两个元素. 试证:  $a$  和  $a^{-1}$ ,  $ab$  和  $ba$  有相同的阶.

## 4.2 循环群

**定义 4.2.1** 群  $G$  称为循环群, 若存在  $a \in G$  使  $(a) = G$ , 即  $G = \{a^n : n \in \mathbb{Z}\}$ . 此时称  $a$  为  $G$  的生成元.

**注记 4.2.2** 循环群是 Abel 群.

**练习 4.2.3** 设  $G \simeq H$ , 则  $G$  为循环群当且仅当  $H$  为循环群.

**例 4.2.4**  $(\mathbb{Z}, +)$  为循环群, 生成元为 1 或  $-1$ .

**例 4.2.5**  $(\mathbb{Z}_n, +)$  为循环群,  $\bar{1}$  或  $-\bar{1}$  是生成元.

**例 4.2.6**  $n$  阶单位根群  $\mu_n$  为循环群,  $e^{\frac{2\pi i}{n}}$  是生成元.

**命题 4.2.7** 设  $G$  为循环群, 则  $G$  同构于  $(\mathbb{Z}, +)$  或  $(\mathbb{Z}_n, +)$ .

利用命题 4.2.7 的同构可以得到

**命题 4.2.8** 设  $G$  为循环群, 生成元为  $a$ .

(1) 若  $|G| = \infty$ , 则  $G$  恰有两个生成元  $a$  和  $a^{-1}$ ,  $G$  的子群有  $\{1_G\}$  和  $(a^d)$ , 其中  $d \geq 1$ . 每个  $(a^d)$  均同构于  $\mathbb{Z}$ , 也同构于  $G$ .

(2) 若  $|G| = n < \infty$ , 则  $G$  恰有  $\varphi(n)$  个生成元  $a^k$ , 其中  $1 \leq k \leq n$ ,  $\gcd(k, n) = 1$ . 对于每个  $d | n$ , 存在唯一的子群  $H_d = (a^{\frac{n}{d}})$ , 满足  $|H_d| = d$ .

**提示** 对(2), 利用例 2.2.29 对环  $\mathbb{Z}_n$  理想的分类结果以及练习 4.2.10. 注意

群  $(\mathbb{Z}_n, +)$  的子群 = 环  $(\mathbb{Z}_n, +, \cdot)$  的理想

**注记 4.2.9** 由于  $\varphi(d)$  恰为  $G$  中  $d$  阶元的个数, 我们再次得到  $n = \sum_{d|n} \varphi(d)$ .

**练习 4.2.10** 设  $G$  为群,  $a \in G$ . 若  $\text{ord}(a) = n < \infty$ , 则  $\text{ord}(a^m) = \frac{n}{\gcd(m, n)}$ .

**命题 4.2.11**  $n$  阶群  $G$  为循环群当且仅当  $G$  中存在  $n$  阶元.

**推论 4.2.12** 对于素数  $p$ ,  $p$  阶群一定为循环群, 进而  $G \simeq (\mathbb{Z}_p, +)$ .

**证明** 设  $G$  为  $p$  阶群. 任取  $1_G \neq a \in G$ , 则  $\text{ord}(a) > 1$ , 但  $\text{ord}(a) \mid |G| = p$ , 因此  $\text{ord}(a) = p$ . 由命题 4.2.11,  $G$  为循环群.  $\square$

**定理 4.2.13** 设  $G$  为群,  $|G| = n < \infty$ , 则  $G$  为循环群当且仅当对任意  $d \mid n$ , 至多存在一个  $d$  阶子群.

**证明** ( $\Rightarrow$ ) 这即是命题 4.2.8 (2).

( $\Leftarrow$ ) 对任意  $d \mid n$ , 记  $S_d = \{g \in G : \text{ord}(g) = d\}$ , 由定理 4.1.18,

$$G = \bigsqcup_{d \mid n} S_d.$$

对任意  $g \in S_d$ ,  $(g) \leqslant G$  为  $d$  阶循环群, 由条件,  $(g)$  不依赖于  $g \in S_d$  的选取, 记之为  $H_d$ , 则  $S_d \subset H_d$ . 因此

$$n = |G| = \sum_{d \mid n} |S_d| \leqslant \sum_{d \mid n} \#\{H_d \text{ 生成元}\} = \sum_{d \mid n} \varphi(d) = n,$$

这说明  $|S_d| = \varphi(d), \forall d \mid n$ . 特别地,  $S_n \neq \emptyset$ , 由命题 4.2.11,  $G$  为循环群.  $\square$

**定理 4.2.14** 设  $k$  为域,  $G \leqslant k^\times$  为有限子群, 则  $G$  为循环群.

**证明** 设  $|G| = n$ , 对任意  $d \mid n$ , 假设存在  $G$  的  $d$  阶子群  $H$ , 下证  $H$  唯一. 注意到  $H \subset \text{Root}_k(x^d - 1_k)$ , 而  $|\text{Root}_k(x^d - 1_k)| \leqslant d$ , 故  $H = \text{Root}_k(x^d - 1)$ . 由定理 4.2.13,  $G$  为循环群.  $\square$

运用定理 4.2.14, 我们再次得到命题 3.4.13 的结论:

**例 4.2.15** 考虑有限域  $E/\mathbb{F}_p$ , 则  $E^\times$  为循环群, 即存在  $v \in E$  使得  $E^\times = (v)$ . 故  $E = \{\bar{0}\} \cup \{\bar{1}, v, \dots, v^{|E|-2}\}$ ,  $E = \mathbb{F}_p(v)$  为单扩张.

利用定理 4.2.14 还可以确定乘法群  $\mathbb{C}^\times$  的所有有限子群:

**例 4.2.16** 设  $G \leqslant \mathbb{C}^\times$  为有限子群,  $|G| = n$ , 则  $G = \mu_n$  ( $n$  阶单位根群).

**练习 4.2.17** 乘法群  $\mathbb{C}^\times$  不是循环群.

**证明** 假设  $\mathbb{C}^\times$  是循环群, 由命题 4.2.7,  $\mathbb{C}^\times \simeq \mathbb{Z}$ , 从而  $\mathbb{C}^\times$  中除去 1 外任意元素的阶为  $\infty$ . 这与  $\mathbb{C}^\times$  存在有限子群  $\mu_n$  矛盾.  $\square$

**例 4.2.18** 由定理 4.2.14,  $\mathbb{F}_9^\times = (\mathbb{F}_3[x]/(x^2 + \bar{1})) \setminus \{0\}$  是循环群. 由于  $u = \bar{x}$  满足  $u^2 = \bar{2}, u^3 = \bar{2}u, u^4 = \bar{1}$ , 因此  $\{\bar{1}, \bar{2}, u, \bar{2}u\}$  是  $\mathbb{F}_9^\times$  的 4 阶子群. 又  $\mathbb{F}_9^\times$  共有  $\varphi(8) = 4$  个生成元, 故余下的  $u + \bar{1}, u + \bar{2}, \bar{2}u + \bar{1}, \bar{2}u + \bar{2}$  均为  $\mathbb{F}_9^\times$  的生成元.

**练习 4.2.19**  $(\mathbb{Q}, +)$  不是循环群, 但它的任意有限生成的子群都是循环群.

**证明** 设  $\frac{m}{n} \in \mathbb{Q}$ . 取素数  $p$  满足  $p \nmid n$ , 则  $\frac{1}{p} \notin \left(\frac{m}{n}\right)$ . 这表明  $(\mathbb{Q}, +)$  不是循环群. 欲证  $(\mathbb{Q}, +)$  的有限生成子群是循环群, 由归纳法只需证由两个元素生成的子群是循环群. 设  $H = \left(\frac{m}{n}, \frac{t}{s}\right)$ , 令  $d = \gcd(ms, nt)$ . 则由 Bézout 等式, 存在  $\lambda, \mu \in \mathbb{Z}$  使得  $d = \lambda ms + \mu nt$ , 从而  $\frac{d}{ns} = \lambda \cdot \frac{m}{n} + \mu \cdot \frac{t}{s} \in H$ . 又

$$\frac{m}{n} = \frac{ms}{ns} \in \left(\frac{d}{ns}\right), \quad \frac{t}{s} = \frac{nt}{ns} \in \left(\frac{d}{ns}\right),$$

故  $H = \left(\frac{d}{ns}\right)$  为循环群.  $\square$

**练习 4.2.20** 设  $p$  为素数,  $G = \{x \in \mathbb{C} : \text{存在正整数 } n \text{ 使得 } x^{p^n} = 1\}$ , 则  $G$  对于复数的乘法构成群. 试证  $G$  的任意真子群都是有限阶的循环群.

**证明** 设  $H$  是  $G$  的真子群, 取  $g \in G \setminus H$ . 设  $\text{ord}(g) = p^n$ , 则  $H$  中任一元素的阶为  $p^m$ ,  $m < n$ . 否则,  $\mu_{p^m} \leqslant H$ , 而  $g \in \mu_{p^m}$ , 与  $g \notin H$  矛盾. 故可设  $h$  是  $H$  中阶最大的元素, 进而  $H = (h)$ .  $\square$

## 4.3 正规子群与商群

考虑群同态  $f: G \rightarrow H$ , 则  $f$  的像  $\text{Im}(f) \leqslant H$  是子群. 回顾定义 1.1.16,  $f$  诱导  $G$  上的等价关系:

$$a \sim b \iff f(ab^{-1}) = 1_H \iff f(b^{-1}a) = 1_H.$$

应该注意, 一般而言  $ab^{-1} \neq b^{-1}a$ , 但有相似(共轭)关系:  $ab^{-1} = a(b^{-1}a)a^{-1}$ .

**定义 4.3.1** 定义群同态  $f: G \rightarrow H$  的核为  $\text{Ker}(f) = \{g \in G : f(g) = 1_H\}$ .

**注记 4.3.2**  $\text{Ker}(f) \leqslant G$  为子群.

令  $N = \text{Ker}(f)$ , 则  $a \in Nb \iff ab^{-1} \in N \iff b^{-1}a \in N \iff a \in bN$ , 即  $Nb = bN, \forall b \in G$ .

**定义 4.3.3** 子群  $N \leqslant G$  称为正规子群, 若  $aN = Na, \forall a \in G$ , 记为  $N \triangleleft G$ .

**注记 4.3.4** (1) 设  $f: G \rightarrow H$  为群同态, 则  $\text{Ker}(f) \triangleleft G$ .

(2) 若群  $G$  为 Abel 群, 则  $G$  的任意子群均正规.

**定义 4.3.5** 群  $G$  的中心定义为  $Z(G) = \{g \in G : gh = hg, \forall h \in G\}$ .

**练习 4.3.6** 设  $G$  为群, 则  $Z(G) \triangleleft G$ .

**定义 4.3.7** 设  $G$  为群,  $H \leqslant G, a \in G$ . 定义  $H$  的共轭  $aHa^{-1} = \{aha^{-1} : h \in H\}$ .

**练习 4.3.8** 在定义 4.3.7 中,  $aHa^{-1} \leqslant G$ , 且有内自同构  $H \xrightarrow{\sim} aHa^{-1}$ .

**命题 4.3.9** 设  $H \leqslant G$  为子群, 则  $H \triangleleft G$  当且仅当  $H = aHa^{-1}, \forall a \in G$ .

**例 4.3.10** 设  $G = \text{GL}(n, \mathbb{C}) (n \geqslant 2)$ ,  $H$  为  $G$  中全体上三角方阵构成的集合, 则  $H \leqslant G$  但  $H$  不是正规子群, 因为总可用  $G$  中方阵将  $H$  中方阵相似下三角化.

**例 4.3.11** 由  $\text{SL}(n, \mathbb{C})$  是  $\det: \text{GL}(n, \mathbb{C}) \rightarrow \mathbb{C}^\times$  的核知,  $\text{SL}(n, \mathbb{C}) \triangleleft \text{GL}(n, \mathbb{C})$ .

**例 4.3.12** 设  $H \leqslant G$  为子群. 若  $[G : H] = 2$ , 则  $H \triangleleft G$ . 提示  $G = G \sqcup (G \setminus H)$ .

**例 4.3.13** 考虑  $G = \text{GL}(2, \mathbb{F}_2)$ . 设  $H = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \right\}, N = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}$ . 则  $H \leqslant G$  但  $H$  不是正规子群, 因为

$$\begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}^{-1} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \notin H.$$

而  $|N| = 3, |G| = 6, [G : N] = 2$ , 由例 4.3.12,  $N \triangleleft G$ .

**定义 4.3.14** 设  $G$  为群,  $N \triangleleft G$ . 在陪集空间  $G/N = \{\bar{a} = aN : a \in G\}$  上定义乘法运算

$$aN \cdot bN = abN, \quad a, b \in G.$$

这使得  $G/N$  构成一个群, 称为  $G$  模  $N$  的商群.

**注记 4.3.15** (1) 在商群  $G/N$  中,  $\bar{a} = \bar{b} \iff a^{-1}b \in N \iff ba^{-1} \in N$ . 由此可验证  $G/N$  中乘法的良定性与结合律.

(2)  $G/N$  中幺元为  $1_{G/N} = \bar{1}$ , 而逆由  $\bar{a}^{-1} = \overline{a^{-1}}$  给出.

(3) 有典范群同态

$$\begin{aligned}\text{can} : G &\twoheadrightarrow G/N \\ a &\mapsto \bar{a}.\end{aligned}$$

其核  $\text{Ker}(\text{can}) = N$ .

**定理 4.3.16 (群同态基本定理)** 设  $f : G \rightarrow H$  为群同态, 则唯一存在群同构

$$\bar{f} : R/\text{Ker}(f) \xrightarrow{\sim} \text{Im}(f)$$

使得下图交换:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \text{can} \downarrow & & \uparrow \text{inc} \\ G/\text{Ker}(f) & \dashrightarrow^{\bar{f}} & \text{Im}(f) \end{array}$$

提示 由定理 1.1.19, 只需验证  $\bar{f}$  为群同态.

**注记 4.3.17** (1) 若  $f$  是单的, 即  $\text{Ker}(f) = \{1_G\}$ , 则  $G \simeq \text{Im}(f) \leqslant H$ .

(2) 若  $f$  是满的, 即  $\text{Im}(f) = H$ , 则  $H \simeq G/\text{Ker}(f)$ .

**例 4.3.18** 在练习 4.1.16 中, 记  $V = \{A, B, C, D\}$ , 则任意  $g \in \Sigma(\square)$  均满足  $g|_V$  为  $V$  的置换. 因此有群同态

$$\begin{aligned}\phi : \Sigma(\square) &\rightarrow S(V) \\ g &\mapsto g|_V.\end{aligned}$$

由于  $\text{Ker } \phi = \{I_2\}$  即  $\phi$  是单射, 由定理 4.3.16,  $\Sigma(\square)$  同构于  $S(V)$  的一个 8 阶子群.

**例 4.3.19** 考虑  $x^3 - 2 \in \mathbb{Q}[x]$  的分裂域  $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$  及其根集  $X = \text{Root}_E(x^3 - 2) = \left\{ \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \right\}$ . 对任意  $\sigma \in \text{Aut}(E/\mathbb{Q}) = \text{Aut}(E)$ ,  $\sigma|_X \in S(X)$ , 因此有自然群同态

$$\begin{aligned}\phi : \text{Aut}(E) &\rightarrow S(X) \\ \sigma &\mapsto \sigma|_X.\end{aligned}$$

利用  $E$  是  $\mathbb{Q}$ -线性空间 ( $\mathbb{Q}$ -基见例 3.2.7) 可知  $\phi$  是单射. 又  $|\text{Aut}(E)| = 6 = |S(X)|$ , 由定理 4.3.16,  $\phi$  是群同构,  $\text{Aut}(E) \simeq S(X)$ . 特别地,  $\text{Aut}(E/\mathbb{Q})$  是非 Abel 群.

**练习 4.3.20** 在例 4.3.19 中, 存在群同构  $S(X) \simeq \text{GL}(2, \mathbb{F}_2)$ .

**证明** 记  $u = (\bar{1}, \bar{0})^\top, v = (\bar{0}, \bar{1})^\top, w = (\bar{1}, \bar{1})^\top$ . 观察到  $\text{GL}(2, \mathbb{F}_2)$  中任一方阵诱导集合  $\{u, v, w\}$  上的一个置换, 因此存在群同态  $f : \text{GL}(2, \mathbb{F}_2) \rightarrow S(X)$ . 可验证  $f$  是单的, 又  $|\text{GL}(2, \mathbb{F}_2)| = 6 = |S(X)|$ , 由定理

**4.3.16**,  $f$  是群同构. 具体而言, 群同构  $f : \mathrm{GL}(2, \mathbb{F}_2) \xrightarrow{\sim} S(3)$  如下:

$$\begin{aligned} \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} &\mapsto (123), \quad \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \mapsto (12), \quad \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix} \mapsto (132), \\ \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix} &\mapsto (13), \quad \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{pmatrix} \mapsto (23), \quad I \mapsto \mathrm{Id}. \end{aligned}$$

□

**定理 4.3.21 (对应定理)** 设  $G$  为群,  $N \triangleleft G$ , 则存在双射

$$\begin{aligned} \{K : N \leq K \leq G\} &\xleftrightarrow{1:1} \{G/N \text{ 的子群}\} \\ K &\longmapsto K/N \\ \{a \in G : aN \in \overline{K}\} &\longleftarrow \overline{K}. \end{aligned}$$

**定理 4.3.22** 设  $G$  为群,  $N \leq K \leq G$ ,  $N \triangleleft G$ . 则  $K \triangleleft G$  当且仅当  $K/N \triangleleft G/N$ . 此时, 有自然同构

$$(G/N)/(K/N) \xrightarrow{\sim} G/K, \quad (aN)K/N \mapsto aK.$$

**证明** (1) 若  $K \triangleleft G$ , 则有群的满同态

$$G/N \twoheadrightarrow G/K, \quad aN \mapsto aK.$$

其良定性检验:  $aN = a'N \iff a^{-1}a' \in N \implies a^{-1}a' \in K \iff aK = a'K$ . 此同态的核为  $\{aN : aK = 1_{G/K}\} = \{aN : a \in K\} = K/N$ . 因此  $K/N \triangleleft G/N$ .

(2) 若  $K/N \triangleleft G/N$ , 由命题 4.3.9, 对任意  $gN \in G/N$ ,  $(gN)(K/N) = (gN)^{-1}$ , 于是  $(gKg^{-1})/N = K/N, \forall g \in G$ . 又  $N \leq K, N \leq gKg^{-1}$ , 由定理 4.3.21 中的双射即得  $gKg^{-1} = K, \forall g \in G$ . 再由命题 4.3.9,  $K \triangleleft G$ .

(3) 若  $K \triangleleft G$ , 对 (1) 中满同态运用定理 4.3.16 即得  $(G/N)/(K/N) \xrightarrow{\sim} G/K$ . □

**定理 4.3.23** 设  $G$  为群,  $N \triangleleft G, H \leq G$ , 则

- (1)  $NH = HN \leq G$ .
- (2)  $(H \cap N) \triangleleft H$ .
- (3)  $H/(H \cap N) \simeq NH/N$ .

**证明** 由  $N \triangleleft G$  知  $Nh = hN, \forall h \in H$ , 令  $h$  遍历  $H$  即得  $NH = HN$ . 由此易得  $NH \leq G$ . 于是有群的满同态

$$H \twoheadrightarrow NH/N, \quad h \mapsto hN.$$

其核为  $\{h \in H : hN = 1_{NH/N}\} = \{h \in H : h \in N\} = N \cap H$ . 故  $(N \cap H) \triangleleft H$ , 且由定理 4.3.16, 存在群同构

$$H/(H \cap N) \xrightarrow{\sim} NH/N.$$

□

**例 4.3.24** 设  $G, H$  为群. 考虑投影同态

$$G \times H \twoheadrightarrow H, \quad (g, h) \mapsto h.$$

其核为  $(G \times \{1_H\}) \triangleleft (G \times H)$ . 由定理 4.3.16, 存在群同构

$$(G \times H)/(G \times \{1_H\}) \xrightarrow{\sim} H.$$

**练习 4.3.25** 设有群同构  $\theta : G \xrightarrow{\sim} G'$ ,  $N \triangleleft G$ ,  $N' = \theta(N) \triangleleft G'$ , 则  $G/N \simeq G'/N'$ .

**练习 4.3.26** 令  $G$  是实数对  $(a, b), a \neq 0$  带有乘法  $(a, b)(c, d) = (ac, ad + b)$  的群. 试证:  $K = \{(1, b) : b \in \mathbb{R}\} \triangleleft G$  且  $G/K \simeq (\mathbb{R}^\times, \cdot)$ . [提示] 第一分量投影同态.

**练习 4.3.27** 设  $f : G \rightarrow H$  是群同态,  $M \leqslant G$ . 试证  $f^{-1}(f(M)) = KM$ , 这里  $K = \text{Ker}(f)$ .

**练习 4.3.28** 设  $M$  和  $N$  均为群  $G$  的正规子群. 若  $M \cap N = \{1_G\}$ , 则对任意  $a \in M, b \in N$  有  $ab = ba$ . [提示]  $b^{-1}aba^{-1} \in M \cap N$ .

**练习 4.3.29** 若  $G/Z(G)$  是循环群, 则  $G$  是 Abel 群.

**证明** 设  $G/Z(G) = (gZ(G))$ , 其中  $g \in G$ . 对任意  $a, b \in G$ , 存在  $c, d \in Z(G)$  使得  $a = g^m c, b = g^n d$ . 由此可见  $ab = ba$ , 即  $G$  是 Abel 群.  $\square$

## 4.4 对称群

**定义 4.4.1** 记  $n$  元集合  $\underline{n} = \{1, \dots, n\}$  的对称群为  $S_n$ , 称为  $n$  次的对称群或置换群.

**注记 4.4.2**  $|S_n| = n!$ .

**命题 4.4.3** 设有集合间双射  $\delta : X \rightarrow Y$ , 则有群同构

$$S(X) \xrightarrow{\sim} S(Y), \quad \sigma \mapsto \delta \circ \sigma \circ \delta^{-1}.$$

**推论 4.4.4** 若集合  $X$  满足  $|X| = n$ , 则  $S(X) \simeq S_n$ .

**约定 4.4.5** 当  $j_1, j_2, \dots, j_n$  是  $1, 2, \dots, n$  的一个排列时, 可将一个置换  $\sigma \in S_n$  记为

$$\sigma = \begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ \sigma(j_1) & \sigma(j_2) & \cdots & \sigma(j_n) \end{pmatrix}.$$

**例 4.4.6** 在  $S_3$  中, 考虑  $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$  及  $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ , 则  $\sigma \circ \tau \neq \tau \circ \sigma$ .

**例 4.4.7** 对任意正整数  $n$ , 有群嵌入

$$S_n \hookrightarrow S_{n+1}, \quad \sigma \mapsto \bar{\sigma} = \begin{pmatrix} 1 & \cdots & n & n+1 \\ \sigma(1) & \cdots & \sigma(n) & n+1 \end{pmatrix}.$$

于是结合例 4.4.6 即知, 当  $n \geqslant 3$  时,  $S_n$  是非 Abel 群.

**定义 4.4.8** 设  $\{i_1, i_2, \dots, i_t\} \subset \{1, 2, \dots, n\}$ . 若  $c \in S_n$  满足

$$\begin{array}{ccc} i_1 & \xrightarrow{c} & i_2 \\ c \nearrow & & \swarrow c \\ i_t & & i_3 \\ \swarrow c & & \nearrow c \\ & \dots & \end{array} \quad \text{且 } c(j) = j, \forall j \in \underline{n} \setminus \{i_1, i_2, \dots, i_t\},$$

则称  $c$  为  $S_n$  中的一个  $t$ -轮换 (又称循环), 记为  $c = (i_1 i_2 \cdots i_t)$ . 称  $i_1, i_2, \dots, i_t$  为轮换  $c$  中的文字,  $t$  称为轮换  $c$  的长. 特别地, 2-轮换称为对换, 1-轮换实际上就是恒等置换.

**注记 4.4.9** (1)  $c^{-1} = (i_t \cdots i_2 i_1)$ .

(2)  $\text{ord}(c) = t$ .

(3) 任一个  $t$ -轮换都有  $t$  种表示法.

(4)  $S_n$  中  $t$ -轮换共有  $\frac{n!}{t}$  个.

**例 4.4.10 (辨结构)** 在  $S_3$  中,  $(12)(23)(12) = (23)(12)(23)$ . 提示 用引理 4.4.12 简算.

**定义 4.4.11** 在  $S_n$  中, 如果若干个轮换间没有共同文字, 则称它们是不相交的轮换.

**引理 4.4.12 (t-轮换的共轭)** 对任意  $\sigma \in S_n$  与  $t$ -轮换  $(i_1 i_2 \cdots i_t) \in S_n$ , 有

$$\sigma(i_1 i_2 \cdots i_t) \sigma^{-1} = (\sigma(i_1) \sigma(i_2) \cdots \sigma(i_t)).$$

提示 观察 LHS 在  $\sigma(i_r)$  上的作用.

**引理 4.4.13**  $S_n$  中两个不相交的轮换是可交换的.

**证明** 设  $\sigma, \tau \in S_n$  为两个不相交的轮换,  $\tau = (i_1 i_2 \cdots i_t)$ , 由引理 4.4.12,

$$\sigma \tau \sigma^{-1} = (\sigma(i_1) \sigma(i_2) \cdots \sigma(i_t)) \xrightarrow{\text{不相交}} (i_1 i_2 \cdots i_t) = \tau \implies \sigma \tau = \tau \sigma. \quad \square$$

**命题 4.4.14 (轮换分解)** 任何  $\sigma \in S_n$  均可表为  $\sigma = c_1 \cdots c_l$ , 其中  $c_i$  为互不相交的轮换 (不含 1-轮换). 如果不计次序, 则表法是唯一的. 提示 考虑  $n$  上的  $\sigma$ -轨道.

**定义 4.4.15** 称群  $G$  中元素  $a$  与  $b$  共轭, 若存在  $g \in G$  使得  $a = gbg^{-1}$ . 这是  $G$  上的等价关系, 其等价类称为共轭类. 通常记元素  $a$  所在的共轭类为  $C_a$ .

**注记 4.4.16**  $C_a = \{a\} \iff a \in Z(G)$ .

**定义 4.4.17** 设  $\sigma \in S_n$  可表为  $c_1 \cdots c_t$ , 其中  $c_i$  为互不相交的轮换 (包括 1-轮换), 并用  $\lambda_i$  表示其中长为  $i$  的轮换个数. 定义  $\sigma$  的循环型为  $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$ , 它满足  $\sum_{i=1}^n i \lambda_i = n$ .

**注记 4.4.18**  $\text{ord}(\sigma) = \text{lcm}(i : \lambda_i \neq 0)$ .

**定理 4.4.19**  $S_n$  中两元素共轭当且仅当它们具有相同的循环型.

**证明** ( $\Rightarrow$ ) 任取  $\sigma \in S_n$ , 设  $\sigma = c_1 \cdots c_t$ , 其中  $c_i$  为互不相交的轮换, 则对任意  $h \in S_n$ ,  $h\sigma h^{-1} = (hc_1 h^{-1}) \cdots (hc_t h^{-1})$ . 由引理 4.4.12 立见  $\sigma$  与  $h\sigma h^{-1}$  同型.

( $\Leftarrow$ ) 设  $\sigma, \tau \in S_n$  具有相同的循环型:

$$\begin{aligned}\sigma &= (a_1) \cdots (a_s)(i_1 i_2) \cdots (i_{2r-1} i_{2r}) \cdots, \\ \tau &= (b_1) \cdots (b_s)(j_1 j_2) \cdots (j_{2r-1} j_{2r}) \cdots.\end{aligned}$$

取  $h \in S_n$  满足  $h(a_1) = b_1, \dots, h(a_s) = b_s, h(i_1) = j_1, h(i_2) = j_2, \dots, h(i_{2r-1}) = j_{2r-1}, h(i_{2r}) = j_{2r}, \dots$ . 易见  $h\sigma h^{-1} = \tau$  即  $\sigma$  与  $\tau$  共轭.  $\square$

**例 4.4.20** 由定理 4.4.19 可得  $S_3$  的共轭类(表 4.1).

表 4.1:  $S_3$  的共轭类  $[6 = 1 + 3 + 2]$

循环型	$1^3$	$1^1 2^1$	$3^1$
元素	Id	$(12), (13), (23)$	$(123), (132)$

由此可知在  $S_3$  中  $(12)$  与  $(13)$  共轭, 为求  $h \in S_3$  使得  $h(12)h^{-1} = (13)$ , 利用引理 4.4.12, 只需求解  $(h(1)h(2)) = (13)$ . 故分别解

$$\begin{cases} h(1) = 1, \\ h(2) = 3 \end{cases} \quad \text{与} \quad \begin{cases} h(1) = 3, \\ h(2) = 1 \end{cases}$$

得  $h = (23)$  或  $h = (132)$ .

**例 4.4.21** 由定理 4.4.19 可得  $S_4$  的共轭类(表 4.2).

表 4.2:  $S_4$  的共轭类  $[24 = 1 + 6 + 3 + 8 + 6]$

循环型	$1^4$	$1^2 2^1$	$2^2$	$1^1 3^1$	$4^1$
元素	Id	$(12), (13), (14), (23), (24), (34)$	$(12)(34), (13)(24), (14)(23)$	$(123), (132), (124), (142), (134), (143), (234), (243)$	$(1234), (1243), (1324), (1342), (1423), (1432)$

观察到群嵌入  $S_3 \hookrightarrow S_4$  (例 4.4.7) 对共轭不封闭, 由命题 4.3.9,  $S_3$  不是  $S_4$  的正规子群.

**注记 4.4.22** 由注记 4.4.16, 从例 4.4.20 与例 4.4.21 可见,  $Z(S_3)$  与  $Z(S_4)$  均平凡.

**例 4.4.23** 在练习 4.1.16 中, 代  $A, B, C, D$  以  $1, 2, 3, 4$ . 映射  $\Sigma(\square) \hookrightarrow S_4$  的像  $H$  为

- (1) 四个旋转: Id,  $(1234), (13)(24), (1432)$ .
- (2) 四个镜面对称:  $(14)(23), (12)(34), (24), (13)$ .

由表 4.2 可见,  $H \leq S_4$  对共轭不封闭, 因此  $H$  不是  $S_4$  的正规子群.

**练习 4.4.24** 在例 4.4.23 中,

- (1)  $H = ((1234), (13))$ .
- (2) 另代练习 4.1.16 中的  $A, B, C, D$  以  $1, 3, 2, 4$ , 求映射  $\Sigma(\square) \hookrightarrow S_4$  的像  $H'$ .
- (3) 另代练习 4.1.16 中的  $A, B, C, D$  以  $1, 2, 4, 3$ , 求映射  $\Sigma(\square) \hookrightarrow S_4$  的像  $H''$ .

(4) 求  $H \cap H' \cap H''$ .

**解答** (1) 在  $S_4$  中,  $\text{ord}(1234) = 4$  且  $(13) \notin ((1234))$ , 因此  $|((1234), (13))| \geq 5$ . 又  $((1234), (13)) \leq H$ ,  $|H| = 8$ , 由定理 4.1.18,  $|((1234), (13))| = 8$ , 故  $H = ((1234), (13))$ .

(2)  $H' = \{\text{Id}, (1324), (12)(34), (1423), (14)(23), (13)(24), (12), (34)\}$ .

(3)  $H'' = \{\text{Id}, (1243), (14)(23), (1342), (13)(24), (12)(34), (14), (23)\}$ .

(4)  $H \cap H' \cap H'' = \{\text{Id}, (12)(34), (13)(24), (14)(23)\} \triangleleft S_4$ , 其正规性见表 4.2. □

**注记 4.4.25** (4) 中得到的子群记作  $K_4$ , 因其同构于 Klein 四元群 (例 4.1.36).

**引理 4.4.26** 任意  $\sigma \in S_n$  均能写成对换之积.

**证明** 任一  $t$ -轮换都可写成  $t - 1$  个对换之积:  $(i_1 i_2 \cdots i_t) = (i_{t-1} i_t) \cdots (i_2 i_t)(i_1 i_t)$ . □

**引理 4.4.27**  $S_n$  可由  $(12), (23), \dots, (n-1, n)$  生成.

**证明** 只需证任意  $(ij) \in ((12), (23), \dots, (n-1, n))$ . 对  $|j - i|$  归纳, 当  $|j - i| = 1$  时结论已成立. 当  $|j - i| > 1$  时,  $(ij) = (i+1, j)(i, i+1)(i+1, j)$ , 对  $(i+1, j)$  归纳即证. □

**注记 4.4.28** 对  $1 \leq i \leq n-1$ , 通常记  $s_i = (i, i+1) \in S_n$ . 因此  $S_n$  由  $s_1, s_2, \dots, s_{n-1}$  生成. 有如下辫子关系:

$$\begin{aligned} s_i s_{i+1} s_i &= s_{i+1} s_i s_{i+1}, \quad \forall 1 \leq i \leq n-2, \\ s_i s_j &= s_j s_i, \quad \forall |i - j| \geq 2, \\ s_i^2 &= \text{Id}, \quad \forall 1 \leq i \leq n-1. \end{aligned}$$

**例 4.4.29** 存在群同态

$$S_n \hookrightarrow \text{GL}(n, \mathbb{R}), \quad \sigma \mapsto P_\sigma \text{ 置换方阵.}$$

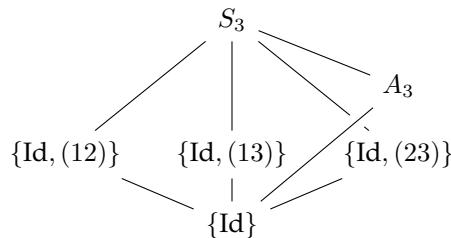
将其与行列式同态复合便得群同态

$$\begin{aligned} \text{sgn} : S_n &\rightarrow \{1, -1\} \\ \sigma &\mapsto \det(P_\sigma). \end{aligned}$$

若  $\text{sgn}(\sigma) = 1$ , 称  $\sigma$  为偶置换; 若  $\text{sgn}(\sigma) = -1$ , 称  $\sigma$  为奇置换. 定义  $A_n = \text{Ker}(\text{sgn})$ , 称为  $n$  元集合上的交错群, 则  $A_n$  的元素为全体偶置换,  $A_n \triangleleft S_n$ . 由定理 4.3.16,  $S_n/A_n \cong \{\pm 1\}$ ,  $|A_n| = \frac{n!}{2}$ . 由引理 4.4.26,  $\text{sgn}(i_1 i_2 \cdots i_t) = (-1)^{t-1}$ .

**例 4.4.30** 由表 4.1,  $A_3 = \{\text{Id}, (123), (132)\} \triangleleft S_3$ .

**例 4.4.31 ( $S_3$  的子群格)** 对  $S_3$  的子群作分类 (用线表示包含关系, 称为 Hasse 图):



**例 4.4.32** 在表 4.2 中,  $A_4$  为循环型  $1^4, 2^2, 1^1 3^1$  对应共轭类之并, 因此  $A_4 \triangleleft S_4$ .

**例 4.4.33** 对  $S_4$  的正规子群分类:  $\{\text{Id}\} \leq K_4 \leq A_4 \leq S_4$  (利用子群正规当且仅当是共轭类之并).

**定义 4.4.34** 若群  $G$  不具有除  $\{1_G\}, G$  之外的正规子群, 则称  $G$  为单群.

**练习 4.4.35** 设  $G \neq \{1_G\}$  为 Abel 群, 则  $G$  为单群当且仅当  $G$  为  $p$  阶循环群, 其中  $p$  为素数.

**证明** 由于  $G$  为 Abel 群,  $G$  的任意子群均是正规子群.

( $\Rightarrow$ ) 任取  $a \in G \setminus \{1_G\}$ , 则  $(a) \triangleleft G$ , 因此  $G = (a)$  为循环群. 由任意非  $1_G$  元素均为生成元即知  $G$  为素数阶循环群.

( $\Leftarrow$ ) 若  $G$  为  $p$  阶循环群, 由定理 4.1.18,  $G$  无非平凡子群, 进而为单群.  $\square$

**定理 4.4.36** 当  $n \geq 5$  时, 交错群  $A_n$  是单群.

**证明** (1) 先证明当  $n \geq 3$  时,  $A_n$  由所有 3-轮换生成. 对于互不相同的  $i, j, k, l$ , 有  $(ij)(ik) = (jik), (ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$ , 因此两个不同的对换之积一定是 3-轮换之积, 而  $A_n$  中任何元素都可以写成偶数个对换之积, 因此  $A_n$  由 3-轮换生成.

- (2) 再证明当  $n \geq 5$  时,  $A_n$  中所有 3-轮换是一个共轭类. 对任意 3-轮换  $(ijk)$ , 存在  $\sigma \in S_n$  使得  $\sigma(i) = 1, \sigma(j) = 2, \sigma(k) = 3$ . 若  $\sigma \in A_n$ , 则  $\sigma(ijk)\sigma^{-1} = (123)$ ; 若  $\sigma \notin A_n$ , 则  $(45)\sigma \in A_n$ , 且  $(45)\sigma(ijk)\sigma^{-1}(45) = (123)$ . 因此所有 3-轮换都与  $(123)$  共轭.
- (3) 下证  $A_n$  无非平凡正规子群. 由(1)(2), 只需证若  $\{\text{Id}\} \neq N \triangleleft A_n$ , 则  $N$  含有一个 3-轮换. 以下记任意置换  $\sigma$  的不动点集为  $\text{Fix}(\sigma) := \{i : \sigma(i) = i\}$ . 取  $\sigma \in N \setminus \{\text{Id}\}$  使得  $|\text{Fix}(\sigma)|$  最大, 下证  $\sigma$  即欲求的 3-轮换.

- ① 如果  $\sigma$  的轮换分解中只有对换, 那么分解中至少含两项如  $(ij)(kl)$ , 其中  $\{i, j\} \cap \{k, l\} = \emptyset$ . 由于  $n \geq 5$ , 可取  $r \notin \{i, j, k, l\}$  并定义

$$\tau := (klr), \quad \sigma' := \tau \sigma \tau^{-1} \sigma^{-1} \in N \quad (\because N \triangleleft A_n).$$

可直接验证  $i, j \in \text{Fix}(\sigma') \setminus \text{Fix}(\sigma), \sigma'(k) = r \neq k$ , 以及

$$\text{Fix}(\sigma) \setminus \{r\} = \text{Fix}(\sigma) \setminus \{k, l, r\} = (\text{Fix}(\sigma) \cap \text{Fix}(\tau)) \subset \text{Fix}(\sigma').$$

故  $|\text{Fix}(\sigma')| > |\text{Fix}(\sigma)|$ , 矛盾.

- ② 设  $\sigma$  的轮换分解中包含长  $> 2$  的项  $(ijk \dots)$ . 若  $\sigma = (ijk)$  则  $\sigma$  即所求的 3-轮换; 否则因为  $\sigma$  不可能是 4-轮换,  $\sigma$  除了  $i, j, k$  之外还挪动至少两个相异元  $r, l$ . 依然如①定义  $\sigma' \in N$ . 可以验证  $j \in \text{Fix}(\sigma'), \sigma'(k) = l \neq k$  和

$$\text{Fix}(\sigma) = \text{Fix}(\sigma) \setminus \{k, l, r\} = (\text{Fix}(\sigma) \cap \text{Fix}(\tau)) \subset \text{Fix}(\sigma').$$

仍得到矛盾  $|\text{Fix}(\sigma')| > |\text{Fix}(\sigma)|$ . 故  $\sigma$  只能为 3-轮换.  $\square$

**推论 4.4.37** 当  $n \geq 5$  时,  $A_n$  是  $S_n$  唯一的非平凡正规子群.

**证明** 设  $\{\text{Id}\} \neq N \triangleleft S_n$ , 结合  $A_n \triangleleft S_n$  即得  $(N \cap A_n) \triangleleft A_n$ .

- ◊ 若  $N \cap A_n = A_n$ , 则  $A_n \subset N$ , 而  $[S_n : A_n] = 2$ , 故  $N = A_n$ .

◊ 若  $N \cap A_n = \{\text{Id}\}$ , 考虑群同态

$$A_n \xrightarrow{\text{inc}} S_n \twoheadrightarrow S_n/N,$$

因其核即  $N \cap A_n = \{\text{Id}\}$ , 这是群嵌入. 因此  $|N| = 2$ . 取  $\sigma \in N \setminus \{\text{Id}\}$ , 则  $\text{ord}(\sigma) = 2$ . 由命题 4.4.14 与注记 4.4.18,  $\sigma$  是不交对换之积. 由定理 4.4.19 易见  $N$  对共轭不封闭, 与  $N \triangleleft S_n$  矛盾.  $\square$

**例 4.4.38** 由例 4.3.12 与定理 4.4.36 即知,  $A_5$  无 30 阶子群.

**练习 4.4.39** 在  $A_4$  中求解方程  $\sigma(12)(34)\sigma^{-1} = (13)(24)$ .

**解答** 由引理 4.4.12,  $\sigma(12)(34)\sigma^{-1} = (\sigma(12)\sigma^{-1})(\sigma(34)\sigma^{-1}) = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$ .

$$\diamond \begin{cases} (\sigma(1)\sigma(2)) = (13), \\ (\sigma(3)\sigma(4)) = (24) \end{cases} \implies \sigma = \underbrace{(23)}_{\notin A_4}, (132), \underbrace{(234)}_{\notin A_4}, \underbrace{(1342)}_{\notin A_4}.$$

$$\diamond \begin{cases} (\sigma(1)\sigma(2)) = (24), \\ (\sigma(3), \sigma(4)) = (13) \end{cases} \implies \sigma = \underbrace{(1243)}_{\notin A_4}, (143), (143), (124), \underbrace{(14)}_{\notin A_4}.$$

故  $\sigma = (132), (234), (143), (124)$ .  $\square$

照此计算可知  $A_4$  中  $(12)(34)$  与  $(14)(23)$  共轭, 但  $(123)$  与  $(132)$  不共轭 (尽管它们在  $S_4$  中共轭).

**练习 4.4.40** 分别求  $A_4$  中  $(123)$  和  $(132)$  的共轭类.

**解答**  $A_4$  中  $(123)$  和  $(132)$  的共轭类均为  $3^1$  型, 因此  $|C_{(123)}| + |C_{(132)}| \leq 8$ , 若能分别找到  $C_{(123)}$  与  $C_{(132)}$  中的 4 个元素, 则它们恰为欲求共轭类. 直接计算得:

$$\begin{aligned} (12)(34)(123)(34)^{-1}(12)^{-1} &= (142), \\ (13)(24)(123)(24)^{-1}(13)^{-1} &= (134), \\ (14)(23)(123)(23)^{-1}(14)^{-1} &= (243), \\ (12)(34)(132)(34)^{-1}(12)^{-1} &= (124), \\ (13)(24)(132)(24)^{-1}(13)^{-1} &= (143), \\ (14)(23)(132)(23)^{-1}(14)^{-1} &= (234). \end{aligned}$$

故  $C_{(123)} = \{(123), (134), (142), (243)\}$ ,  $C_{(132)} = \{(124), (132), (143), (234)\}$ .  $\square$

**练习 4.4.41**  $A_4$  没有 6 阶子群.

**证明** 假设  $G$  是  $A_4$  的 6 阶子群, 则  $[A_4 : G] = 2$ , 由例 4.3.12,  $G \triangleleft A_4$ , 因此  $G$  为  $A_4$  中若干共轭类之并. 由前述讨论可得  $A_4$  的共轭类 (表 4.3), 可见与  $|G| = 6$  矛盾.

表 4.3:  $A_4$  的共轭类  $12 = 1 + 3 + 4 + 4$

循环型	$1^4$	$2^2$	$1^1 3^1$	$1^1 3^1$
元素	$\text{Id}$	$(12)(34), (13)(24), (14)(23)$	$(123), (134), (142), (243)$	$(124), (132), (143), (234)$

**练习 4.4.42** 讨论置换  $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$  的奇偶性.

## 4.5 群作用

**定义 4.5.1** 设  $G$  为群,  $X$  为非空集合. 若映射

$$\begin{aligned}\psi : G \times X &\rightarrow X \\ (g, x) &\mapsto \psi(g, x)\end{aligned}$$

满足对任意  $x \in X$  与  $g_1, g_2 \in G$  都有

$$\begin{aligned}\psi(1_G, x) &= x, \\ \psi(g_1 g_2, x) &= \psi(g_1, \psi(g_2, x)),\end{aligned}$$

则称  $G$  左作用于  $X$ , 记为  $G^\sim X$ . 此时称  $X$  或  $(X, \psi)$  为左  $G$ -集. 常记  $\psi(g, x)$  为  $g \cdot x$ .

**例 4.5.2** 对任意非空集合  $X$ , 其对称群  $S(X)$  在  $X$  上有自然的左作用:  $(\sigma, x) \mapsto \sigma(x)$ .

**例 4.5.3**  $\mathrm{GL}(n, \mathbb{R})$  在  $\mathbb{R}^n$  上有自然的左(线性)作用:  $(A, x) \mapsto Ax$ .

**例 4.5.4** 设  $K/k$  为  $f(x) \in k[x]$  的分裂域, 则  $\mathrm{Aut}(K/k)^\sim \mathrm{Root}_K(f) : (\sigma, a) \mapsto \sigma(a)$ .

**例 4.5.5** 在练习 4.3.20 的证明中, 我们看到  $\mathrm{GL}(2, \mathbb{F}_2)^\sim \mathbb{F}_2^{\oplus 2}$ .

**例 4.5.6** 若  $G^\sim X$ , 则  $G$  自然作用于  $P$  的幂集  $\mathcal{P}(X)$ .

$\{G$  在  $X$  上的左作用 $\} \xleftrightarrow{1:1} \mathrm{Hom}(G, S(X))$  任意左  $G$ -集  $(X, \psi)$  诱导群同态(群的置换表示)

$$\begin{aligned}\rho : G &\rightarrow S(X) \\ g &\mapsto \rho(g),\end{aligned}$$

其中  $\rho(g)(x) := g \cdot x$ . 反过来, 给定群同态  $\rho : G \rightarrow S(X)$ , 可定义  $G$  在  $X$  上的左作用:

$$\begin{aligned}\psi : G \times X &\rightarrow X \\ (g, x) &\mapsto \rho(g)(x).\end{aligned}$$

### 阅读提示

请验证如上群同态的良定性, 如  $\rho(g) \in S(X)$  等.

**定义 4.5.7** 定义群作用  $G^\sim X$  的核  $N$  为如上群同态  $G \rightarrow S(X)$  的核, 即  $N = \bigcap_{x \in X} G_x$ .

**练习 4.5.8** 设  $K/k$  为  $f(x) \in k[x]$  的分裂域, 由例 4.5.4 可得群同态

$$\rho : \mathrm{Aut}(K/k) \rightarrow S(\mathrm{Root}_K(f)).$$

证明  $\rho$  是单同态. 由此再次得到  $\mathrm{Aut}(K/k)$  是有限群.

**定义 4.5.9** 给定群  $(G, \cdot)$ , 在集合  $G$  上定义新的二元运算  $\star$  使得  $x \star y = y \cdot x$ , 得到的新群  $(G, \star)$  记作  $G^{\mathrm{op}}$ , 称为  $G$  的反群.

**注记 4.5.10** 存在群同构  $G \xrightarrow{\sim} G^{\text{op}}, g \mapsto g^{-1}$ .

**定义 4.5.11** 设  $G$  为群,  $Y$  为非空集合. 若映射

$$\begin{aligned}\phi : Y \times G &\rightarrow Y \\ (y, g) &\mapsto \phi(y, g)\end{aligned}$$

满足对任意  $y \in Y$  与  $g_1, g_2 \in G$  都有

$$\begin{aligned}\phi(y, 1_G) &= y, \\ \phi(y, g_1 g_2) &= \phi(\phi(y, g_1), g_2),\end{aligned}$$

则称  $G$  右作用于  $y$ , 记为  $Y \curvearrowright G$ . 此时称  $Y$  或  $(Y, \phi)$  为右  $G$ -集. 常记  $\phi(y, g)$  为  $y \cdot g$ .

$\{G \text{ 在 } Y \text{ 上的右作用}\} \xleftarrow{1:1} \text{Hom}(G, S(Y)^{\text{op}})$  任意右  $G$ -集  $(Y, \phi)$  诱导群同态(群的置换表示)

$$\begin{aligned}\rho : G &\rightarrow S(Y)^{\text{op}} \\ g &\mapsto \rho(g),\end{aligned}$$

其中  $\rho(g)(y) := y \cdot g$ . 反过来, 给定群同态  $\rho : G \rightarrow S(Y)^{\text{op}}$ , 可定义  $G$  在  $Y$  上的右作用:

$$\begin{aligned}\phi : Y \times G &\rightarrow Y \\ (y, g) &\mapsto \rho(g)(y).\end{aligned}$$

左/右  $G$ -集本质相同:  $[G \curvearrowright X : (g, x) \mapsto g \cdot x] \rightleftharpoons [X \curvearrowright G : (x, g) \mapsto x \cdot g := g^{-1} \cdot x]$

**例 4.5.12** 设  $G$  为群,  $H \leqslant G$ .

- (1) 考虑左陪集空间  $G/H = \{aH : a \in G\}$  (未必为商群), 则有左诱导作用  $G \curvearrowright (G/H) : (g, aH) \mapsto gaH$ .
- (2) 对偶地, 考虑右陪集空间  $H \backslash G = \{Ha : a \in G\}$ , 则有右诱导作用  $(H \backslash G) \curvearrowright G : (Ha, g) \mapsto Hag$ , 与右正则作用对应的左作用为  $(g, Ha) \mapsto Hag^{-1}$ .
- (3) 特别地, 当  $H = \{1_G\}$  时, 得到左正则作用  $G \curvearrowright G : (g, a) \mapsto ga$  与右正则作用  $G \curvearrowright G : (a, g) \mapsto ag$ .

前文已谈及  $G$  在  $X$  上的左作用与  $\text{Hom}(G, S(X))$  间存在一一对应关系, 将其用于例 4.5.12 (3) 的左正则作用, 便得到群嵌入

$$G \hookrightarrow S(G), \quad g \mapsto \ell_g,$$

其中  $\ell_g(x) := gx$  (易验证此同态的核为  $\{1_G\}$ ). 故我们得到

**定理 4.5.13 (Cayley 定理)** 任何群  $G$  与对称群  $S(G)$  的一个子群同构.

**定义 4.5.14** 设  $G$  为群,  $X$  为左  $G$ -集, 称  $G \curvearrowright X$  是忠实的, 若相应的群同态

$$\begin{aligned}\rho : G &\rightarrow S(X) \\ g &\mapsto \rho(g)\end{aligned}$$

是单射, 其中  $\rho(g)(x) = g \cdot x, \forall x \in X$ . 这等价于说群作用  $G \curvearrowright X$  的核  $N = \{1_G\}$ .

**例 4.5.15** 例 4.5.12 中的左/右正则作用均是忠实的.

**例 4.5.16** 由练习 4.5.8,  $\text{Aut}(K/k)^\sim \text{Root}_K(f)$  是忠实的.

**例 4.5.17 (非忠实群作用)**  $(\mathbb{R}^2, +)^\sim \mathbb{S}^1 : ((x, y), e^{i\theta}) \mapsto e^{i(\theta+x+y)}$  非忠实.

**定义 4.5.18** 设  $G^\sim X, x \in X$ . 称  $\mathcal{O}_x = \{g \cdot x : g \in G\} \subset X$  为  $x$  的轨道.

**注记 4.5.19** 定义  $X$  上的等价关系为  $x \approx y \iff \exists g \in G, \text{s.t. } y = g \cdot x$ . 则  $x$  所在的等价类即  $\mathcal{O}_x$ ,  $X$  有  $G$ -轨道分解  $X = \bigsqcup_{x \in I} \mathcal{O}_x$ , 其中  $I$  为  $G$ -轨道的完全代表元系. 轨道的集合记为  $X/G$  或  $G \backslash X$ .

**定义 4.5.20** 设  $G^\sim X$ . 若对任意  $x, y \in X$ , 均存在  $g \in G$  使得  $y = g \cdot x$ , 则称群作用  $G^\sim X$  是可迁的.

**注记 4.5.21** (1)  $G^\sim X$  可迁当且仅当  $X$  仅有一个  $G$ -轨道.

(2) 对任意  $x \in X$ , 限制作用  $G^\sim \mathcal{O}_x$  总是可迁的.

**引理 4.5.22** 考虑无重根非零多项式  $f(x) \in k[x]$  及其分裂域  $K/k$ , 则  $f(x)$  不可约当且仅当群作用  $\text{Aut}(K/k)^\sim \text{Root}_K(f)$  是可迁的.

**证明** ( $\Rightarrow$ ) 对不可约的  $f(x)$  的任意一对根  $\alpha \neq \beta \in K$ , 由引理 3.3.1, 唯一存在  $\text{Id}_k$  的延拓  $\sigma : k(\alpha) \xrightarrow{\sim} k(\beta)$  满足  $\sigma(\alpha) = \beta$ . 此时  $K/k(\alpha)$  与  $K/k(\beta)$  分别为  $f(x) \in k(\alpha)[x]$  与  $\sigma(f(x)) \in k(\beta)[x]$  的分裂域, 由定理 3.3.13, 存在  $\sigma$  的延拓  $\delta \in \text{Aut}(K)$ . 故  $\delta \in \text{Aut}(K/k)$  满足  $\delta(\alpha) = \beta$ , 即  $\text{Aut}(K/k)^\sim \text{Root}_K(f)$  可迁.

$$\begin{array}{ccc} K & \xrightarrow[\sim]{\delta} & K \\ \downarrow & & \downarrow \\ k(\alpha) & \xrightarrow[\sim]{\sigma: \alpha \mapsto \beta} & k(\beta) \\ \downarrow & & \downarrow \\ k & \xrightarrow{\text{Id}_k} & k \end{array}$$

( $\Leftarrow$ ) 若  $f = gh$  可约,  $\deg(g), \deg(h) \geq 1$ , 则由  $f(x)$  无重根知  $\text{Root}_K(g) \cap \text{Root}_K(h) = \emptyset$ , 因此  $\text{Aut}(K/k)^\sim \text{Root}_K(f)$  不混合  $g$  和  $h$  的根集, 故不可迁, 矛盾.  $\square$

**定义 4.5.23** 设  $G^\sim X, x \in X$ . 定义  $x$  的稳定化子  $G_x = \{g \in G : g \cdot x = x\}$ .

**注记 4.5.24**  $G_x \leqslant G$  为子群.

**引理 4.5.25** 设  $G^\sim X, x, y \in X$ . 若存在  $h \in G$  使得  $x = h \cdot y$ , 则  $G_x = hG_yh^{-1}$ . 故同一轨道中的稳定化子是互相共轭的.

**注记 4.5.26** 再由练习 4.3.8 可知, 有群同构  $G_x \cong G_y$ .

**例 4.5.27** 将地球表面看作  $S^2$ . 地球绕南北极的自转可看作  $\text{SO}(2)$  在  $S^2$  上的作用, 其轨道就是纬线. 在非南北极点的稳定化子是  $\{\text{Id}\}$ ; 在南北极点的稳定化子是  $\text{SO}(2)$ .

**例 4.5.28**  $\text{GL}(n, \mathbb{R})$  在  $\mathbb{R}^n$  上的自然作用的轨道有  $\{\mathbf{0}\}$  和  $\mathbb{R}^n \setminus \{\mathbf{0}\}$  两个. 在  $\mathbf{0}$  点的稳定化子是  $\text{GL}(n, \mathbb{R})$ , 在  $\mathbf{e}_1$  点的稳定化子是

$$\left\{ \begin{pmatrix} 1 & \alpha \\ \mathbf{0} & A \end{pmatrix} \in \text{GL}(n, \mathbb{R}) : A \in \text{GL}(n-1, \mathbb{R}), \alpha \in \mathbb{R}^{n-1} \right\}.$$

**例 4.5.29**  $\mathrm{SO}(n)$  在  $\mathbb{R}^n$  上的作用的轨道是  $\{x \in \mathbb{R}^n : |x| = r\}$ ,  $r \geq 0$ . 当  $r > 0$  时, 在  $r\mathbf{e}_1$  点的稳定化子是  $\{\mathrm{diag}(1, A) : A \in \mathrm{SO}(n-1)\}$ .

**例 4.5.30** 根据例 4.4.7,  $S_{n-1}$  可看作  $S_n$  的子群.  $S_n \curvearrowright n$  在  $n$  的稳定化子为  $S_{n-1}$ .

**例 4.5.31**  $\mathrm{GL}(n, \mathbb{C})$  在  $M_n(\mathbb{C})$  上相似作用的轨道是  $\mathcal{O}_J = \{TJT^{-1} : T \in \mathrm{GL}(n, \mathbb{C})\}$ , 其中  $J$  是某个 Jordan 标准形, 而  $J$  的稳定化子为  $\{A \in \mathrm{GL}(n, \mathbb{C}) : AJ = JA\}$ .

**定理 4.5.32 (轨道-稳定化子定理)** 设  $G \curvearrowright X, x \in X$ , 则存在双射

$$\begin{aligned} f : G/G_x &\xrightarrow{\sim} \mathcal{O}_x \\ gG_x &\longmapsto g \cdot x. \end{aligned}$$

特别地, 我们有轨道-稳定化子公式

$$|\mathcal{O}_x| = |G/G_x| = [G : G_x] \quad \text{即} \quad |G| = |\mathcal{O}_x||G_x|.$$

**注记 4.5.33** 对集合间双射  $f : Y \rightarrow Z$  与群作用  $G \curvearrowright Y, G \curvearrowright Z$ , 称  $f$  与  $G$ -作用相容, 若

$$f(g \cdot y) = g \cdot f(y), \quad \forall g \in G, y \in Y.$$

在定理 4.5.32 中, 从  $G \curvearrowright X$  可得左诱导作用  $G \curvearrowright (G/G_x)$  (参见例 4.5.12 (1)) 与限制作用  $G \curvearrowright \mathcal{O}_x$ , 由于

$$f(h \cdot gG_x) = h \cdot f(gG_x), \quad \forall g, h \in G,$$

双射  $f$  与  $G$ -作用相容.

**例 4.5.34** 在例 4.4.23 中, 有  $\Sigma(\square) \curvearrowright 4$ . 由于  $\mathcal{O}_1 = 4$  而  $\Sigma(\square)_1 = \{\mathrm{Id}, (24)\}$ , 根据定理 4.5.32,  $|\Sigma(\square)| = 4 \cdot 2 = 8$ .

**定理 4.5.35 (Burnside 引理)** 设  $G$  是有限群,  $X$  是有限  $G$ -集. 对于  $g \in G$ , 考虑  $X^g = \{x \in X : g \cdot x = x\}$ , 则有

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

**证明** 通过将  $X$  拆分为轨道的并, 可不妨设  $G \curvearrowright X$  是可迁的, 从而只需证  $|G| = \sum_{g \in G} |X^g|$ . 定义函数  $f : G \times X \rightarrow \mathbb{R}$  如下:

$$f(g, x) = \begin{cases} 1, & \text{若 } g \cdot x = x, \\ 0, & \text{若 } g \cdot x \neq x. \end{cases}$$

下面用两种方式来计算  $S = \sum_{(g, x) \in G \times X} f(g, x)$ :

◇ 对任意  $x \in X$ , 由定理 4.5.32,  $|G_x| = \frac{|G|}{|\mathcal{O}_x|} = \frac{|G|}{|X|}$ . 因此  $S = |X||G_x| = |G|$ .

◇ 对任意  $g \in G$ ,  $\sum_{x \in X} f(g, x) = |X^g|$ , 因此  $S = \sum_{g \in G} |X^g|$ .

比较这两个等式即得  $|G| = \sum_{g \in G} |X^g|$ . □

**注记 4.5.36** 换言之, 轨道的个数是群中各个元素不动点个数的平均值.

**定义 4.5.37** 设  $G$  为群,  $X$  为  $G$ -集. 称作用  $G^\sim X$  为自由的, 若对任意  $x \in X$  都有  $G_x = \{1_G\}$ .

**注记 4.5.38** 由定理 4.5.32,  $G^\sim X$  是自由的  $\iff |O_x| = |G|, \forall x \in X$ . 此时  $|G| \mid |X|$ .

**例 4.5.39** 例 4.5.12 (3) 的左正则作用  $G^\sim G : (g, a) \mapsto ga$  是自由的.

**例 4.5.40** 设  $H \leqslant G$ , 则限制左正则作用  $H^\sim G : (h, x) \mapsto hx$  是自由的. 由注记 4.5.38,  $|H| \mid |G|$ , 这便是定理 4.1.18.

**定义 4.5.41** 设  $G$  为群,  $X$  为  $G$ -集. 称作用  $G^\sim X$  为平凡的, 若对任意  $g \in G$  与  $x \in X$  均有  $g \cdot x = x$ .

**注记 4.5.42**  $G^\sim X$  是平凡的  $\iff G_x = G, \forall x \in X \iff O_x = \{x\}, \forall x \in X$ .

**例 4.5.43** 设  $G^\sim X$ , 记  $X$  的不动点集为  $X^G = \{x \in X : g \cdot x = x, \forall g \in G\}$ . 若  $X^G \neq \emptyset$ , 则  $G^\sim X^G$  是平凡的.

**定义 4.5.44** 设  $G$  为群, 称作用  $G^\sim X = G : (g, x) \mapsto gxg^{-1}$  为共轭作用.

**注记 4.5.45** (1)  $G$  是 Abel 群  $\iff G^\sim X$  是平凡的. 故仅考虑非 Abel 群共轭作用.

(2) 共轭作用下的  $x$  的轨道即  $G$  中  $x$  所在的共轭类  $C_x$  (定义 4.4.15).

**定义 4.5.46** 定义  $x \in G$  的中心化子  $Z(x)$  为  $x$  在共轭作用下的稳定化子, 即

$$Z(x) = \{g \in G : gx = xg\} \leqslant G.$$

**注记 4.5.47** (1)  $Z(G) \subset Z(x), (x) \subset Z(x), \forall x$ .

(2) 定理 4.5.32 在共轭作用下可表述为  $|G| = |C_x||Z(x)|$ . 特别地,  $|C_x| \mid |G|$ .

(3)  $C_x = \{x\} \iff x \in Z(G) \iff Z(x) = G$ .

**例 4.5.48** 在练习 4.4.40 中, 我们看到  $A_4$  中  $|C_{(123)}| = 4$ . 这也可由注记 4.5.47 (2) 公式  $|G| = |C_x||Z(x)|$ , 化为求  $Z((123)) = \{\sigma \in A_4 : \sigma(123)\sigma^{-1} = (123)\}$ . 由引理 4.4.12,

$$\sigma(123)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)) = (123) \implies \sigma = \text{Id}, (123), (132).$$

$$\text{故 } |C_{(123)}| = \frac{|A_4|}{|Z((123))|} = \frac{12}{3} = 4.$$

由注记 4.5.47 (3) 可得

$$\text{命题 4.5.49 (类等式)} \quad |G| = |Z(G)| + \sum_{C_x : |C_x| > 1} |C_x|.$$

**注记 4.5.50** 表 4.1, 4.2, 4.3 分别给出了  $S_3, S_4, A_4$  的类等式.

**定义 4.5.51** 设  $p$  为素数. 有限群  $G$  称为  $p$ -群, 若  $|G| = p^n, n \in \mathbb{Z}_{\geq 0}$ .

**注记 4.5.52**  $p$ -群未必是 Abel 群, 如练习 4.1.16 的 8 阶群  $\Sigma(\square)$  是非 Abel 群.

**命题 4.5.53** 设  $G$  为非平凡的  $p$ -群, 则  $Z(G) \neq \{1_G\}$ .

**证明** 由命题 4.5.49 及注记 4.5.47 (2),  $p \mid |Z(G)|$ . □

**注记 4.5.54** 若  $G$  为非平凡  $p$ -群, 由练习 4.3.6, 商群  $G/Z(G)$  是阶数更小的  $p$ -群, 可以此递归研究  $p$ -群的结构. 下面的定理 4.5.55 与后面的例 5.3.6 (5) 即为二例.

**定理 4.5.55** 对任意非平凡  $p$ -群  $G$ , 存在  $H \triangleleft G$  使得  $[G : H] = p$ .

**证明** 设  $|G| = p^n$ , 对  $n$  归纳. 由推论 4.2.12,  $n = 1$  时结论显然成立. 下设结论对  $k < n$  ( $n \geq 2$ ) 成立. 由命题 4.5.53,  $Z(G) \neq \{1_G\}$ , 即  $Z(G)$  亦为非平凡  $p$ -群. 由定理 4.6.11, 存在  $p$  阶元  $a \in Z(G)$ . 令  $H = \langle a \rangle \leqslant Z(G)$ , 则  $H \triangleleft G$ . 由于  $|G/H| = p^{n-1}$ , 由归纳假设,  $G/H$  有指数为  $p$  的正规子群, 由定理 4.3.21 与定理 4.3.22, 它对应于  $G$  中包含  $H$  的正规子群, 且由定理 4.3.22 给出的群同构可知此正规子群指数为  $p$ .  $\square$

**命题 4.5.56** 设  $p$  为素数,  $G$  为  $p^2$  阶群, 则  $G$  为 Abel 群, 且  $G \simeq \mu_{p^2}$  或  $G \simeq \mu_p \times \mu_p$ .

**证明** 由命题 4.5.53, 可取  $g \in Z(G) \setminus \{1_G\}$ . 由  $\text{ord}(g) \mid |G|$  知  $\text{ord}(g) = p$  或  $p^2$ .

- ◊ 若  $\text{ord}(g) = p^2$ , 由命题 4.2.11 及命题 4.2.7,  $G$  为循环群且  $G \simeq \mu_{p^2}$ .
- ◊ 若  $\text{ord}(g) = p$ ,  $H = \langle g \rangle \subset Z(G)$ . 可取  $g' \in G \setminus H$ , 并不妨设  $\text{ord}(g') = p$  (否则,  $\text{ord}(p') = p^2$ ,  $G \simeq \mu_{p^2}$ ). 记  $K = \langle g' \rangle$ , 则由  $g \in Z(G)$  可得  $KH = HK \leqslant G$ . 由定理 4.1.18,  $|HK| \mid |G|$ , 但由  $H \subsetneq HK$  知  $|HK| \geq p + 1$ , 因此  $|HK| = p^2$ ,  $G = HK$  为 Abel 群. 考虑群同态

$$H \times K \rightarrow G, \quad (h, k) \mapsto hk.$$

由  $HK = G$  知这是满同态, 而  $|H \times K| = p^2 = |G|$ , 因此这是群同构,  $G \simeq H \times K$ . 而  $H \times K \simeq \mu_p \times \mu_p$ , 故  $G \simeq \mu_p \times \mu_p$ .  $\square$

**练习 4.5.57** 设  $G$  为群,  $p$  是  $|G|$  的最小素因子. 若  $p$  阶子群  $A \triangleleft G$ , 则  $A \leqslant Z(G)$ .

**证明** 因为  $A \triangleleft G$ , 所以  $G$  在  $A$  上有共轭作用. 由此可得群同态

$$\rho : G \rightarrow S(A) = S_p.$$

注意到  $\text{Im } \rho \leqslant \text{Aut}(A) \simeq \text{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$ . 由定理 4.1.18,  $|\text{Im } \rho| \mid (p-1)$ . 另一方面, 由定理 4.3.16,  $G/\text{Ker } \rho \simeq \text{Im } \rho$ , 因此  $|\text{Im } \rho| \mid |G|$ , 但  $|G|$  的最小素因子是  $p$ , 故  $|\text{Im } \rho| = 1$ , 进而  $G = \text{Ker } \rho$ . 这表明  $A \subset Z(G)$ .

$\text{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$  补证 注意到有群同构

$$\text{Aut}(\mathbb{Z}_p) \xrightarrow{\sim} \mathbb{Z}_p^\times, \quad f \mapsto f(\bar{1}).$$

由定理 4.2.14 知  $\mathbb{Z}_p^\times$  为循环群, 再由命题 4.2.7,  $\mathbb{Z}_p^\times \simeq \mathbb{Z}_{p-1}$ . 故  $\text{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$ .  $\square$

**例 4.5.58** 设  $H \leqslant G$ , 记  $X_H = \{H' \leqslant G : H' \text{ 共轭于 } H\} \ni H$ , 则有共轭作用

$$G^\sim X_H : (g, H') \mapsto gH'g^{-1}.$$

定义  $H$  的正规化子  $N_G(H)$  为  $H$  在  $G^\sim X_H$  下的稳定化子, 即

$$N_G(H) = \{g \in G : gHg^{-1} = H\} = \{g \in G : gH = Hg\}.$$

- ◊  $H \triangleleft N_G(H) \leqslant G$ .

- ◊ 定理 4.5.32 在共轭作用  $G^\sim X_H$  下可表述为  $|G| = |N_G(H)| |X_H|$ .

$$\diamond N_G(H) = G \iff H \triangleleft G \iff X_H = \{H\}.$$

**例 4.5.59** 共轭作用  $G^\sim X = G$  在  $G$  中元素  $x$  的轨道 (即共轭类) 上有限制作用  $G^\sim C_x$ . 例如  $S_4$  共轭作用于共轭类 (见表 4.2)

$$X = \{A = (12)(34), B = (13)(24), C = (14)(23)\}.$$

由此可得群同态

$$\rho : S_4 \rightarrow S(X) \simeq S_3.$$

由引理 4.4.12, 对  $\sigma \in S_4$ ,

$$\begin{aligned}\sigma A \sigma^{-1} &= (\sigma(1)\sigma(2))(\sigma(3)\sigma(4)), \\ \sigma B \sigma^{-1} &= (\sigma(1)\sigma(3))(\sigma(2)\sigma(4)), \\ \sigma C \sigma^{-1} &= (\sigma(1)\sigma(4))(\sigma(2)\sigma(3)).\end{aligned}$$

由此可计算得群同态  $\rho$  的如下信息:

像	纤维
Id	Id, $(12)(34), (13)(24), (14)(23)$
$(12)$	$(14), (23), (1243), (1342)$
$(13)$	$(13), (24), (1234), (1432)$
$(23)$	$(12), (34), (1324), (1423)$
$(123)$	$(124), (132), (143), (234)$
$(132)$	$(123), (134), (142), (243)$

特别地,  $\rho$  为满射, 且  $\text{Ker } \rho = \{\text{Id}, A, B, C\} = K_4$  (见注记 4.4.25). 由定理 4.3.16, 有群同构

$$S_4/K_4 \simeq S_3.$$

**练习 4.5.60** 设  $G^\sim X$  可迁,  $N \triangleleft G$ , 则  $X$  在  $N$  作用下的每个轨道有同样多的元素.

**证明** 由于  $G^\sim X$  可迁, 存在  $a \in X$  使  $X = Ga$ . 对任意  $x \in X$ , 设  $x = ga, g \in G$ , 则

$$\begin{aligned}N_x &= \{n \in N : nx = x\} = \{n \in N : nga = ga\} \\ &= \{n \in N : g^{-1}ng \in G_a\} = N \cap gG_a g^{-1}.\end{aligned}$$

由于  $N \triangleleft G$ ,  $N_x = N \cap gG_a g^{-1} = g(N \cap G_a)g^{-1} = gN_a g^{-1}$ . 由定理 4.5.32,

$$|Nx| = \frac{|N|}{|N_x|} = \frac{|N|}{|gN_a g^{-1}|} = \frac{|N|}{|N_a|} = |Na|.$$

即  $X$  在  $N$  作用下的每个轨道有同样多的元素. □

## 4.6 Sylow 定理

**定义 4.6.1** 设  $G$  为  $n$  阶有限群,  $p$  为素数. 设  $p^r \mid n$ , 满足  $|H| = p^r$  的子群  $H$  称为  $G$  的 Sylow  $p$ -子群.

**定理 4.6.2 (Sylow 定理)** 设  $G$  为有限群,  $p$  为任意素数.

- (1)  $G$  含有 Sylow  $p$ -子群.
- (2)  $G$  的任两个 Sylow  $p$ -子群  $P, P'$  皆共轭 (从而同构).
- (3) 设  $|G| = p^r m, p \nmid m$ , 则  $G$  中 Sylow  $p$ -子群的个数是  $m$  的因子, 且形如  $kp + 1$ .
- (4) 任意  $p$ -子群  $H \leq G$  皆包含于某个 Sylow  $p$ -子群.

**注记 4.6.3** 由 (2) 可知,  $G$  中存在正规的 Sylow  $p$ -子群当且仅当  $G$  有唯一的 Sylow  $p$ -子群.

我们仅对 (1) 作出证明.

**证明** (1) 设  $|G| = p^r m, p \nmid m$ , 考虑

$$X = \{U \subset G : |U| = p^r\} \subset \mathcal{P}(G).$$

由例 4.5.12 (3) 的左正则作用与例 4.5.6, 有群作用  $G^\sim \mathcal{P}(G) : (g, U) \mapsto gU$ , 而  $|gU| = |U|$ , 故此作用可限制在  $X$  上, 得到  $G^\sim X : (g, U) \mapsto gU$ . 由于

$$|X| = \binom{p^r m}{p^r} = \frac{p^r m(p^r m - 1) \cdots (p^r m - p^r + 1)}{p^r(p^r - 1) \cdots 1},$$

注意到  $i$  与  $p^r m - p^r + i$  所含  $p$  的幂次相同 ( $1 \leq i \leq p^r$ ), 因此  $p \nmid |X|$ . 设  $X$  有  $G$ -轨道分解  $X = \bigsqcup_U \mathcal{O}_U$ , 则存在  $U \in X$  使得  $p \nmid |\mathcal{O}_U|$ . 由定理 4.5.32,  $|G_U||\mathcal{O}_U| = |G| = p^r m$ , 因此  $|G_U| = p^r m'$ , 其中  $m' \mid m$ . 另一方面, 按定义  $G_U = \{g \in G : gU = U\}$ , 因此另有群作用  $G_U \curvearrowright U : (g, u) \mapsto gu$ . 由于此作用是自由的, 由注记 4.5.38,  $|G_U| \mid |U| = p^r$ . 故  $m' = 1, |G_U| = p^r$  即为所求.  $\square$

以下再给出定理 4.6.2 (1) 的另一个证明, 此证明依赖于下述引理:

**引理 4.6.4** 设  $G$  为有限群,  $H \leq G$ . 若  $G$  有 Sylow  $p$ -子群  $S$ , 则  $H$  亦有 Sylow  $p$ -子群. 更具体地, 存在  $g \in G$  使  $gSg^{-1} \cap H$  为  $H$  的 Sylow  $p$ -子群.

**证明** 考虑左诱导作用  $H^\sim(G/S) : (h, gS) \mapsto hgS$ . 由于  $S$  为 Sylow  $p$ -子群, 因此  $p \nmid |G/S|$ , 此作用有某个轨道  $\mathcal{O}_{gS}$ , 满足  $p \nmid |\mathcal{O}_{gS}|$ . 由定理 4.5.32,  $|H| = |\mathcal{O}_{gS}| |H_{gS}|$ , 因此  $|H|$  与  $|H_{gS}|$  所含  $p$  的幂次相同. 而

$$H_{gS} = \{h \in H : hgS = gS\} = \{h \in H : g^{-1}hg \in S\} = \{h \in H : h \in gSg^{-1}\} = gSg^{-1} \cap H,$$

由  $H_{gS} \leq gSg^{-1}$  知  $H_{gS}$  为  $p$ -群, 又  $|H|$  与  $|H_{gS}|$  所含  $p$  的幂次相同, 故  $H_{gS}$  为  $H$  的 Sylow  $p$ -子群.  $\square$

以下便是定理 4.6.2 (1) 的另证.

**证明** 设  $n = |G| = p^r m$ . 由例 4.5.12 (3) 的左正则作用可得群嵌入  $G \hookrightarrow S(G) \cong S_n$ . 而  $S_n$  亦可嵌入  $\mathrm{GL}(n, \mathbb{F}_p)$  中:  $\sigma \in S_n, (\mathbf{e}_i)_{1 \leq i \leq n}$  是  $\mathbb{F}_p^n$  的基, 我们将  $\sigma$  映为线性变换  $\mathbf{e}_i \mapsto \mathbf{e}_{\sigma(i)}$  对应的方阵. 注意到

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) \quad (\text{逐行考虑}),$$

其中  $p$  的幂次为  $1 + 2 + \dots + (n - 1) = \frac{n(n - 1)}{2}$ . 考虑对角线上元素均为 1 的上三角方阵的集合  $H$ , 则  $H \leq \mathrm{GL}(n, \mathbb{F}_p)$  且  $|H| = p^{\frac{n(n-1)}{2}}$ , 因此  $H$  为  $\mathrm{GL}(n, \mathbb{F}_p)$  的 Sylow  $p$ -子群. 由于  $G \hookrightarrow S_n \hookrightarrow \mathrm{GL}(n, \mathbb{F}_p)$ , 由引理 4.6.4 即知  $G$  有 Sylow  $p$ -子群.  $\square$

**例 4.6.5** 考虑  $S_4$ ,  $|S_4| = 3^1 \cdot 2^3$ .

(Sylow 3-子群) 由推论 4.2.12 与表 4.2 易见即为如下 4 个 3 阶子群.

$$\{\mathrm{Id}, (123), (132)\}, \quad \{\mathrm{Id}, (124), (142)\}, \quad \{\mathrm{Id}, (134), (143)\}, \quad \{\mathrm{Id}, (234), (243)\}.$$

(Sylow 2-子群) 由例 4.4.33 可知  $S_4$  无 8 阶正规子群, 再由注记 4.6.3 即得  $S_4$  的 Sylow 2-子群个数  $> 1$ ,

根据定理 4.6.2 (3) 即知  $S_4$  恰有 3 个 Sylow 2-子群. 由定理 4.6.2 (4), Klein 四元群  $K_4$  包含于某个 Sylow 2-子群, 而由练习 4.4.24 的解答 (4) 知  $K_4 \triangleleft S_4$ , 它对共轭封闭, 因此由定理 4.6.2 (2) 即知  $K_4$  包含于  $S_4$  的所有 Sylow 2-子群. 由定理 4.6.2 (2) 及定理 4.4.19, 这 3 个子群分别包含  $K_4$ , 2 个  $1^2 2^1$  型置换与 2 个  $4^1$  型置换. 注意到两个相交对换之积是 3-轮换, 但 8 阶群不含 3-轮换, 因此每个子群中恰含有 2 个不相交对换. 最后由  $2^2$  型置换与对换之积生成 4-轮换. 结果如下:

$$\begin{aligned} \{\mathrm{Id}, (12)(34), (13)(24), (14)(23), (12), (34), (1324), (1423)\} &= (K_4, (12)), \\ \{\mathrm{Id}, (12)(34), (13)(24), (14)(23), (13), (24), (1234), (1432)\} &= (K_4, (13)), \\ \{\mathrm{Id}, (12)(34), (13)(24), (14)(23), (14), (23), (1243), (1342)\} &= (K_4, (14)). \end{aligned}$$

这与练习 4.4.24 一致.

**例 4.6.6** 考虑  $A_4$ ,  $|A_4| = 3^1 \cdot 2^2$ .

(Sylow 3-子群) 由推论 4.2.12 与表 4.3 易见即为如下 4 个 3 阶子群.

$$\{\mathrm{Id}, (123), (132)\}, \quad \{\mathrm{Id}, (124), (142)\}, \quad \{\mathrm{Id}, (134), (143)\}, \quad \{\mathrm{Id}, (234), (243)\}.$$

(Sylow 2-子群) 由表 4.3 可知  $K_4$  是  $A_4$  的 2 个共轭类之并, 因此  $K_4 \triangleleft A_4$ . 由注记 4.6.3,  $K_4$  是  $A_4$  唯一的 Sylow 2-子群.

**命题 4.6.7** 35 阶群必同构于  $\mathbb{Z}_{35}$ .

**证明** 设  $G$  为 35 阶群, 由定理 4.6.2 (2) 即知  $G$  有唯一的 5 阶子群  $P$  和 7 阶子群  $Q$ , 再由注记 4.6.3,  $P \triangleleft G, Q \triangleleft G$ . 由推论 4.2.12,  $P \cong \mathbb{Z}_5, Q \cong \mathbb{Z}_7$ , 进而  $P \cap Q = \{1_G\}$ . 由练习 4.3.28,  $pq = qp, \forall p \in P, q \in Q$ . 由此可验证映射

$$P \times Q \rightarrow G, \quad (p, q) \mapsto pq$$

是群同态 (由可换性), 且是单的, 进而为群同构,  $G \cong P \times Q \cong \mathbb{Z}_5 \times \mathbb{Z}_7$ . 由练习 4.1.35, 对  $(\bar{1}, \bar{1}) \in \mathbb{Z}_5 \times \mathbb{Z}_7$ ,  $\mathrm{ord}(\bar{1}, \bar{1}) = \mathrm{lcm}(5, 7) = 35$ . 再由命题 4.2.11 知  $G$  为循环群, 由命题 4.2.7 即得  $G \cong \mathbb{Z}_{35}$ .  $\square$

**命题 4.6.8** 108 阶群总不是单群.

**证明** 设群  $G$  满足  $|G| = 108 = 2^2 \cdot 3^3$ . 由定理 4.6.2 (1) 即知  $G$  有 27 阶子群  $H$ . 由例 4.5.12 (1), 有左诱导作用  $G^\sim(G/H) : (g, aH) \mapsto gaH$ , 因此存在群同态  $\rho : G \rightarrow S(G/H)$ . 由定理 4.3.16,  $G/\mathrm{Ker} \rho \cong \mathrm{Im} \rho$ , 而  $\mathrm{Im} \rho \neq \{\mathrm{Id}\}$ , 因此  $\mathrm{Ker} \rho \not\leq G$ . 又  $|\mathrm{Im} \rho| \leq |S(G/H)| = |S_4| = 24$ , 因此  $|\mathrm{Ker} \rho| \neq 1$ ,  $\mathrm{Ker} \rho \neq \{1_G\}$ . 故  $\mathrm{Ker} \rho$  是  $G$  的非平凡正规子群, 即  $G$  非单群.  $\square$

**命题 4.6.9** 设  $G$  为有限 Abel 群,  $|G| = p_1^{s_1} \cdots p_r^{s_r}$ , 其中  $p_1, \dots, p_r$  为互异的素数. 则  $G$  的 Sylow  $p_i$ -子群  $P_i$  唯一 ( $1 \leq i \leq r$ ), 且  $G \simeq P_1 \times \cdots \times P_r$ .

**证明** 由于  $G$  的 Sylow  $p_i$ -子群是 Abel 群, 在共轭作用下不变, 由定理 4.6.2 (2) 即知唯一性. 由  $P_i$  ( $1 \leq i \leq r$ ) 均为 Abel 群可知映射

$$P_1 \times \cdots \times P_r \rightarrow G, \quad (g_1, \dots, g_r) \mapsto g_1 \cdots g_r$$

是群同态. 记  $H = P_1 \cdots P_r \leq G$ , 则  $P_i \leq H$  ( $1 \leq i \leq r$ ), 由定理 4.1.18,  $p_i^{s_i} \mid |H|$  ( $1 \leq i \leq r$ ), 而  $|H| \mid |G| = p_1^{s_1} \cdots p_r^{s_r}$ , 因此  $H = G$ . 故上述群同态是满的, 进而为群同构,  $G \simeq P_1 \times \cdots \times P_r$ .  $\square$

**注记 4.6.10** 有限 Abel 群的结构问题归结于 Abel  $p$ -群的结构问题.

**定理 4.6.11 (Cauchy 定理)** 设  $G$  为有限群, 素数  $p \mid |G|$ , 则  $G$  中存在  $p$  阶元, 即  $G$  含有  $p$  阶子群.

**证明** 由定理 4.6.2 (1),  $G$  含有 Sylow  $p$ -子群  $P$ , 设  $|P| = p^r$ . 任取  $g \in G \setminus \{1_G\}$ , 则  $\text{ord}(g) = p^s$ , 其中  $1 \leq s \leq r$ . 此时  $\text{ord}(g^{p^{s-1}}) = p$ .  $\square$

**练习 4.6.12** 设  $G$  是一个  $n$  阶群, 素数  $p \mid n$ . 证明: 方程  $x^p = 1$  在群  $G$  中解的个数是  $p$  的倍数.

**练习 4.6.13** 设  $N$  是有限群  $G$  的一个正规子群. 若  $p$  和  $|G/N|$  互素, 则  $N$  包含  $G$  的所有 Sylow  $p$ -子群.

**练习 4.6.14** 设  $G$  为有限群,  $N \triangleleft G$ ,  $P$  是  $G$  的一个 Sylow  $p$ -子群. 证明:

- (1)  $N \cap P$  是  $N$  的 Sylow  $p$ -子群.
- (2)  $PN/N$  是  $G/N$  的 Sylow  $p$ -子群.
- (3)  $(N_G(P)N)/N \simeq N_{G/N}(PN/N)$ .

**练习 4.6.15** 设  $P$  是  $G$  的 Sylow  $p$ -子群,  $N_G(P) \triangleleft G$ . 证明:  $P \triangleleft G$ .

## 4.7 自由群与群的展示

**定义 4.7.1** 考虑非空集合  $X$ , 添加其形式逆  $X^{-1} = \{x^{-1} : x \in X\}$ , 称  $X \sqcup X^{-1}$  为字母集.

- (1) 定义字  $w = x_1 x_2 \cdots x_n$ , 其中  $x_i \in X \sqcup X^{-1}$ . 称两个字相等, 若相应位置完全相等. 若  $n = 0$  则称为空字, 记为 1.
- (2) 称字是既约的, 若  $x_i \neq x_{i+1}^{-1}, \forall i$ .

**注记 4.7.2** 每个字均能约化为唯一的既约字.

**定义 4.7.3** 定义集合  $X$  上的自由群  $\mathbf{F}(X) = \{\text{以 } X \sqcup X^{-1} \text{ 为字母表得到的字}\}$ , 其上的乘法定义为字的连接并约化, 纥元为空字 1, 求逆操作为  $(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1} x_1^{-1}$ . 若  $|X| < +\infty$ , 则称  $\mathbf{F}(X)$  为有限生成自由群.

**例 4.7.4** 若  $X = \{a\}$ , 则  $\mathbf{F}(X) = \{1, a^k, a^{-k}, k \geq 1\} \simeq \mathbb{Z}$ .

**例 4.7.5** 若  $X = \{a, b\}$ , 则  $\mathbf{F}(X)$  中长度为 0 的字有 1 个, 长度为 1 的字有 4 个, 长度为 2 的字有  $4 \cdot 3$  个, 长度为 3 的字有  $4 \cdot 3^2$  个……

**约定 4.7.6** 有时将  $\mathbf{F}(\{x_1, \dots, x_n\})$  简记为  $\mathbf{F}(x_1, \dots, x_n)$ .

**命题 4.7.7 (自由群的泛性质)** 设  $G$  为群,  $X$  为集合, 则任意映射  $f : X \rightarrow G$  可唯一延拓为群同态  $\tilde{f} : \mathbf{F}(X) \rightarrow G$ , 使得下图交换:

$$\begin{array}{ccc} & G & \\ f \nearrow & \uparrow \tilde{f} & \\ X & & \downarrow \text{inc} \\ & \mathbf{F}(X) & \end{array}$$

**命题 4.7.8** 任何群  $G$  均为自由群的商群.

**证明** 在命题 4.7.7 中取  $X = G$  即得群的满同态  $\rho : \mathbf{F}(G) \twoheadrightarrow G$ . 由定理 4.3.16 即知  $\mathbf{F}(G)/\text{Ker } \rho \simeq G$ .  $\square$

**定义 4.7.9** 群  $G$  的有限展示是指

$$G = \langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle, \quad r_i \in \mathbf{F}(x_1, \dots, x_n).$$

这里等号右边意指

$$\mathbf{F}(x_1, \dots, x_n)/N(r_1, \dots, r_m),$$

其中  $N(r_1, \dots, r_m)$  为包含  $r_1, \dots, r_m$  的  $\mathbf{F}(x_1, \dots, x_n)$  的最小正规子群. 称  $x_i$  为生成元,  $r_i$  为生成关系.

**注记 4.7.10** 由于在商映射下  $r_1, \dots, r_m$  的像均为  $1_G$ , 有时也记

$$G = \langle x_1, \dots, x_n \mid r_1 = 1, \dots, r_m = 1 \rangle.$$

**命题 4.7.11** 在定义 4.7.9 中,  $N(r_1, \dots, r_m)$  是由  $\{\omega r_i \omega^{-1} : \omega \in \mathbf{F}(x_1, \dots, x_n), 1 \leq i \leq m\}$  生成的子群.

**例 4.7.12**  $\langle x \mid x^n \rangle \simeq \mu_n = \{1, \omega, \dots, \omega^{n-1}\}$ , 其中  $\omega = e^{\frac{2\pi i}{n}}$ . 这有两种看法:

(看法一) 由例 4.7.4 知  $\mathbf{F}(x) \simeq \mathbb{Z}$  为循环群, 因此  $\mathbf{F}(x)$  的子群均正规,  $N(x^n) \simeq n\mathbb{Z}$ . 故  $\langle x \mid x^n \rangle = \mathbf{F}(x)/N(x^n) \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mu_n$ .

(看法二) 设  $f : \{x\} \rightarrow \mu_n, x \mapsto \omega$ . 由命题 4.7.7,  $f$  可唯一延拓为群同态

$$\begin{aligned} \tilde{f} : \mathbf{F}(x) &\twoheadrightarrow \mu_n \\ x^m &\mapsto \omega^m. \end{aligned}$$

由  $\tilde{f}(x^n) = \omega^n = 1$  可知  $N(x^n) \subset \text{Ker } \tilde{f}$ . 由定理 4.3.16,  $\mathbf{F}(x)/N(x^n) \twoheadrightarrow \mathbf{F}(x)/\text{Ker } \tilde{f} \simeq \mu_n$ . 又  $|\mathbf{F}(x)/N(x^n)| = n = |\mu_n|$ , 因此  $\langle x \mid x^n \rangle = \mathbf{F}(x)/N(x^n) \simeq \mu_n$ .

**命题 4.7.13 (泛性质)** 设  $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle$ ,  $H$  为群, 则映射  $f : X = \{x_1, \dots, x_n\} \rightarrow H$  可(唯一)延拓至群同态  $G \rightarrow H$  当且仅当元素  $f(x_i) \in H$  满足关系  $r_i$  ( $1 \leq i \leq m$ ).

**证明** ( $\Rightarrow$ ) 是显然的, 下证 ( $\Leftarrow$ ). 由命题 4.7.7,  $f$  可唯一延拓为群同态

$$\begin{aligned} \phi : \mathbf{F}(X) &\rightarrow H \\ x_i &\mapsto f(x_i). \end{aligned}$$

由于  $f(x_i) \in H$  满足关系  $r_i$ , 因此  $\phi(r_i) = 1_H$  ( $1 \leq i \leq m$ ),  $N(r_1, \dots, r_m) \leq \text{Ker } \phi$ . 由定理 4.3.16,

$$G = \mathbf{F}(X)/N(r_1, \dots, r_m) \twoheadrightarrow \mathbf{F}(X)/\text{Ker } \phi \simeq \text{Im } \phi \xrightarrow{\text{inc}} H. \quad \square$$

**例 4.7.14** 考虑  $S_3 = \{\text{Id}, (12), (13), (23), (123), (132)\}$  与  $G = \langle a, b \mid a^2, b^2, (ab)^3 \rangle$ . 注意到  $(12)(13) = (123)$ , 因此由  $(12), (13)$  生成的群阶为 6 的倍数, 进而  $S_3 = ((12), (13))$ . 考虑映射

$$f : \{a, b\} \rightarrow S_3, \quad a \mapsto (12), \quad b \mapsto (13),$$

由命题 4.7.13,  $f$  可延拓为群的满同态  $\tilde{f} : G \rightarrow S_3$ , 故  $|G| \geq |S_3| = 6$ . 观察到  $G$  中有如下辫子关系 (参考注记 4.4.28):

$$\begin{array}{c} \boxed{a^2 = 1} \quad \boxed{b^2 = 1} \\ ababab = 1 \implies abab^{-1}a^{-1}b^{-1} = 1 \implies \boxed{aba = bab} \end{array}$$

这里的  $a, b$  实为商群中的  $\bar{a}, \bar{b}$ . 因此  $G$  中的元素共有以下三类 (注意  $a^{-1} = a, b^{-1} = b$ ):

- ◊ 1.
- ◊ 第一位为  $a$ :  $a, ab, aba$  (往后  $abab = babb = ba, \dots$ ).
- ◊ 第一位为  $b$ :  $b, ba, bab$  (往后  $baba = abaa = ab, \dots$ ).

于是  $|G| \leq 6$ , 从而  $|G| = 6, G \cong S_3$ .

**练习 4.7.15** 在例 4.7.14 中,  $G$  另有展示  $G = \langle a, b \mid a^2, b^2, abab^{-1}a^{-1}b^{-1} \rangle$ .

**例 4.7.16** 正  $n$  边形的对称群  $D_n$  (称为二面体群) 阶为  $2n$  ( $n$  个旋转与  $n$  个镜面对称), 有展示

$$D_n \cong \langle x, y \mid x^n, y^2, (xy)^2 \rangle.$$

**练习 4.7.17** 另有展示  $D_n \cong \langle s, t \mid s^2, t^2, (st)^n \rangle$ . 因此当  $n = 3$  时, 我们得到  $D_3 \cong S_3$  (参考例 4.7.14).

群的展示可用来构造群的同态, 以下是构造群同态  $D_4 \hookrightarrow S_4$  的例子 (参考例 4.4.23).

**例 4.7.18** 由例 4.7.16,  $D_4 = \langle x, y \mid x^4, y^2, (xy)^2 \rangle$ . 定义映射  $\phi$  满足  $\phi(x) = (1234), \phi(y) = (13)$ , 则

$$\phi(x)^4 = \text{Id}, \quad \phi(y)^2 = \text{Id}, \quad [\phi(x)\phi(y)]^2 = [(14)(23)]^2 = \text{Id}.$$

由命题 4.7.13,  $\phi$  可延拓为群同态  $\tilde{\phi} : D_4 \rightarrow S_4$ . 由  $(1234) \in \text{Im } \tilde{\phi}$  可知  $|\text{Im } \tilde{\phi}| \geq 4$ , 又  $(13) \in \text{Im } \tilde{\phi} \setminus ((1234))$ , 因此  $|\text{Im } \tilde{\phi}| > 4$ . 而  $|\text{Im } \tilde{\phi}| = |D_4 / \text{Ker } \tilde{\phi}|$  是  $|D_4| = 8$  的因子, 因此  $|\text{Im } \tilde{\phi}| = 8, |\text{Ker } \tilde{\phi}| = 1$ . 从而  $D_4 \cong \text{Im } \tilde{\phi} \hookrightarrow S_4$ .

**例 4.7.19 (四元数代数)** 考虑以  $1, i, j, k$  为基的实向量空间  $\mathbb{H} := \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ . 其上具有良定的乘法使得  $\mathbb{H}$  成环并满足:

- ◊ 乘法  $(x, y) \mapsto xy$  是  $\mathbb{H}$  上的双线性映射.
- ◊  $1$  是乘法单位元.
- ◊  $i^2 = j^2 = -1$ .
- ◊  $ij = k = -ji$ .

由此可以推导出  $k^2 = -1, jk = i = -kj, ki = j = -ik$ .  $\mathbb{H}$  是非交换可除环 (体). 考虑四元数群

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \leq \mathbb{H}^\times,$$

可知  $|Q_8| = |D_4|$ , 但  $Q_8 \not\simeq D_4$ , 因为  $Q_8$  中每个元素均为 4 阶元.

**练习 4.7.20**  $Q_8 \simeq \langle a, b \mid a^4, a^2b^{-2}, bab^{-1}a \rangle = \langle a, b \mid a^4 = 1, b^2 = a^2, ba = a^3b \rangle$ . 提示  $a \mapsto j, b \mapsto i$ .

**练习 4.7.21** 设  $D_\infty = \langle s, t \mid s^2, t^2 \rangle$ . 问是否有  $|D_\infty| = +\infty$ ?

## 4.8 有限生成 Abel 群

**约定 4.8.1** 两加法群  $A, B$  的直积通常记为直和  $A \oplus B = A \times B$ .

**例 4.8.2** 秩  $n$  的自由 Abel 群  $\mathbb{Z}^n = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$  有标准基  $(\mathbf{e}_i)_{1 \leq i \leq n}$ .

**定义 4.8.3** 设  $A$  是加法群, 有限集合  $S \subset A$  称为  $A$  的有限基, 若

- (1)  $S$  生成  $A$ .
- (2)  $S$  是  $\mathbb{Z}$ -线性无关的.

**注记 4.8.4** 不是所有的加法群都有基, 如  $\mathbb{Z}_n$  就没有基, 因为对任意  $v \in \mathbb{Z}_n$ ,  $nv = \bar{0}$ .

**命题 4.8.5 ( $\mathbb{Z}^n$  的泛性质)** 对任意加法群  $A$  与  $v_1, \dots, v_n \in A$ , 存在唯一的群同态  $f : \mathbb{Z}^n \rightarrow A$  使得  $f(\mathbf{e}_i) = v_i$  ( $1 \leq i \leq n$ ).

**命题 4.8.6**  $\mathbb{Z}^n \simeq \langle x_1, \dots, x_n \mid x_i x_j x_i^{-1} x_j^{-1}, \forall i \neq j \rangle = \langle x_1, \dots, x_n \mid x_i x_j = x_j x_i, \forall i \neq j \rangle$ .

**证明** 构造映射  $f : \{x_1, \dots, x_n\} \rightarrow \mathbb{Z}^n$ ,  $x_i \mapsto \mathbf{e}_i$ , 则  $f(x_i) + f(x_j) = f(x_j) + f(x_i)$ ,  $\forall i \neq j$ . 由命题 4.7.13,  $f$  可唯一延拓为群同态  $\tilde{f} : G \rightarrow \mathbb{Z}^n$ .

◦ 由于  $\tilde{f}(x_1^{a_1} \cdots x_n^{a_n}) = a_1 \mathbf{e}_1 + \cdots + a_n \mathbf{e}_n = (a_1, \dots, a_n)$ ,  $\tilde{f}$  是满射.

◦ 若  $\tilde{f}(x_1^{a_1} \cdots x_n^{a_n}) = \mathbf{0}$ , 则  $a_1 = \cdots = a_n = 0$ , 因此  $\tilde{f}$  为单射.

故  $\tilde{f}$  为群同构,  $\mathbb{Z}^n \simeq \langle x_1, \dots, x_n \mid x_i x_j = x_j x_i, \forall i \neq j \rangle$ . □

**注记 4.8.7** 自由 Abel 群  $\mathbb{Z}^n$  是自由群当且仅当  $n = 1$ .

**命题 4.8.8** 有限生成 Abel 群  $A$  是自由 Abel 群当且仅当  $A$  有一组基.

**命题 4.8.9** 设  $A$  为有限生成 Abel 群, 则存在正整数  $n$  与  $K \leq \mathbb{Z}^n$ , 使得  $A \simeq \mathbb{Z}^n / K$ .

**证明** 取  $A$  的一个生成元集  $S = \{v_1, \dots, v_n\}$ , 定义映射  $f : \{x_1, \dots, x_n\} \rightarrow S$ ,  $x_i \mapsto v_i$ , 则  $f(x_i) + f(x_j) = f(x_j) + f(x_i)$ ,  $\forall i \neq j$ . 由命题 4.7.13 与命题 4.8.6,  $f$  可唯一延拓为群同态  $\tilde{f} : \mathbb{Z}^n \rightarrow A$ . 由定理 4.3.16,  $\mathbb{Z}^n / \text{Ker } \tilde{f} \simeq A$ . □

**例 4.8.10**  $\mathbb{Z}_n$  可由  $\{\bar{1}\}$  生成,  $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$ .

**命题 4.8.11** 设  $K \leq \mathbb{Z}^n$ , 则  $K$  是有限生成的.

**证明** 对  $n$  归纳.

- 当  $n = 1$  时, 由命题 4.2.8 (1),  $\mathbb{Z}$  的子群形如  $d\mathbb{Z}$ , 其中  $d \geq 0$ , 它是循环群, 因此是有限生成的.
- 当  $n = 2$  时, 由  $K \leq \mathbb{Z}^2$  知  $(K \cap \mathbb{Z}\mathbf{e}_1) \leq \mathbb{Z}\mathbf{e}_1 \simeq \mathbb{Z}$ , 由命题 4.2.8 (1),  $K \cap \mathbb{Z}\mathbf{e}_1$  为循环群. 由定理 4.3.23 (3) 得

$$K / (K \cap \mathbb{Z}\mathbf{e}_1) \simeq (\mathbb{Z}\mathbf{e}_1 + K) / \mathbb{Z}\mathbf{e}_1 \leq \mathbb{Z}^2 / \mathbb{Z}\mathbf{e}_1 \simeq \mathbb{Z}\mathbf{e}_2,$$

因此  $K / (K \cap \mathbb{Z}\mathbf{e}_1)$  是循环群, 再由下面的练习 4.8.12 知  $K$  是有限生成的.

◇ 余下情形类似. □

**练习 4.8.12** 设  $G$  为群,  $N \triangleleft G$  是有限生成的, 且  $G/N$  也是有限生成的. 证明:  $G$  是有限生成的.

**证明** 设  $\{\bar{g}_1, \dots, \bar{g}_n\}$  是  $G/N$  的生成元集, 其中  $g_1, \dots, g_n \in G$ , 又设  $\{h_1, \dots, h_m\}$  是  $N$  的生成元集. 由  $G = (g_1, \dots, g_n)N = (g_1, \dots, g_n)(h_1, \dots, h_m)$  知  $(g_i h_j : 1 \leq i \leq n, 1 \leq j \leq m)$  是  $G$  的生成元集. □

**命题 4.8.13** 存在双射

$$M_{n \times m}(\mathbb{Z}) \xleftrightarrow{1:1} \text{Hom}(\mathbb{Z}^m, \mathbb{Z}^n), \quad A \mapsto \phi_A,$$

其中

$$\begin{aligned} \phi_A : \mathbb{Z}_{\text{col}}^m &\rightarrow \mathbb{Z}_{\text{col}}^n \\ \mathbf{v} &\mapsto A\mathbf{v}. \end{aligned}$$

**命题 4.8.14** 若  $\mathbb{Z}^n \simeq \mathbb{Z}^m$ , 则  $n = m$ .

**证明** 沿用命题 4.8.13 中的记号, 存在  $A \in M_{m \times n}(\mathbb{Z})$  与  $B \in M_{n \times m}(\mathbb{Z})$  使得  $\phi_A \in \text{Hom}(\mathbb{Z}^n, \mathbb{Z}^m)$ ,  $\phi_B \in \text{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$ , 且  $\phi_B \circ \phi_A = \text{Id}_{\mathbb{Z}^n}$ ,  $\phi_A \circ \phi_B = \text{Id}_{\mathbb{Z}^m}$ , 也即  $AB = I_m$ ,  $BA = I_n$ . 于是  $n = \text{tr}(BA) = \text{tr}(AB) = m$ . □

**定义 4.8.15** 设  $f : A \rightarrow B$  是 Abel 群之间的同态, 则称商群  $B / \text{Im } f$  为  $f$  的余核, 记作  $\text{Coker } f$ .

**注记 4.8.16** 与核是用来刻画同态的单性 ( $\text{Ker } f = 1 \iff f$  是单射) 相对应, 余核是用来刻画同态的满性 ( $\text{Coker } f = 1 \iff f$  是满射).

**命题 4.8.17** 设  $G$  为有限生成 Abel 群, 则存在整数矩阵  $A$ , 使得  $G \simeq \text{Coker}(\phi_A)$ .

**证明** 由命题 4.8.9, 存在  $K \leq \mathbb{Z}^n$  使得  $G \simeq \mathbb{Z}^n / K$ , 再由命题 4.8.11,  $K$  是有限生成的, 故存在  $\mathbf{v}_1, \dots, \mathbf{v}_m \in K$  使得  $K = \mathbb{Z}\mathbf{v}_1 + \dots + \mathbb{Z}\mathbf{v}_m$ . 取  $A = (\mathbf{v}_1, \dots, \mathbf{v}_m) \in M_{n \times m}(\mathbb{Z})$ , 则  $\text{Im}(\phi_A) = K$ , 得证. □

下面考虑可逆整方阵  $\text{GL}(n, \mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \det(A) = \pm 1\}$ .

**练习 4.8.18** 设  $A \in M_n(\mathbb{Z})$ , 则  $A \in \text{GL}(n, \mathbb{Z}) \iff \phi_A \in \text{Aut}(\mathbb{Z}^n)$ .

**定义 4.8.19** 称  $A, B \in M_{n \times m}(\mathbb{Z})$  为  $\mathbb{Z}$ -相抵的, 若存在  $P \in \text{GL}(n, \mathbb{Z})$  与  $Q \in \text{GL}(m, \mathbb{Z})$  使得  $B = PAQ$ .

**注记 4.8.20**  $\mathbb{Z}$ -相抵是  $M_{n \times m}$  上的等价关系.

**命题 4.8.21** 设  $A, B \in M_{n \times m}(\mathbb{Z})$  是  $\mathbb{Z}$ -相抵的, 则  $\text{Coker}(\phi_A) \simeq \text{Coker}(\phi_B)$ .

**证明** 设  $B = P^{-1}AQ$ , 其中  $P \in \text{GL}(n, \mathbb{Z})$ ,  $Q \in \text{GL}(m, \mathbb{Z})$ , 则有如下左半交换图 ( $\phi_A \circ \phi_Q = \phi_P \circ \phi_B$ ):

$$\begin{array}{ccccc} \mathbb{Z}^m & \xrightarrow{\phi_A} & \mathbb{Z}^n & \xrightarrow{\text{can}} & \text{Coker}(\phi_A) \\ \uparrow \phi_Q \wr & & \uparrow \phi_P \wr & & \uparrow \wr \\ \mathbb{Z}^m & \xrightarrow{\phi_B} & \mathbb{Z}^n & \xrightarrow{\text{can}} & \text{Coker}(\phi_B) \end{array}$$

由此可见  $\phi_P(\text{Im}(\phi_B)) = \text{Im}(\phi_A)$ , 由练习 4.3.25 即得  $\mathbb{Z}^n / \text{Im}(\phi_B) \simeq \mathbb{Z}^n / \text{Im}(\phi_A)$ . □

**定理 4.8.22 (Smith 标准形)** 设  $A \in M_{n \times m}(\mathbb{Z})$ , 则存在  $P \in \text{GL}(n, \mathbb{Z})$  与  $Q \in \text{GL}(m, \mathbb{Z})$  使得

$$P^{-1}AQ = \text{diag}(d_1, d_2, \dots, d_r, O),$$

其中  $r = \text{rank}(A)$ , 正整数  $d_1 | d_2 | \cdots | d_r$ .

**例 4.8.23**  $A := \begin{pmatrix} 2 & 4 \\ 6 & 5 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 \\ 0 & 7 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 7 & 7 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 1 & 7 \end{pmatrix} \sim \begin{pmatrix} 1 & 7 \\ 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix} =: B$ . 由命题 4.8.21,  $\text{Coker}(\phi_A) \simeq \text{Coker}(\phi_B)$ , 即

$$\mathbb{Z}^2 / \left\{ \begin{pmatrix} 2a + 4b \\ 6a + 5b \end{pmatrix} : a, b \in \mathbb{Z} \right\} \simeq \mathbb{Z}^2 / (\mathbb{Z} \times 14\mathbb{Z}) \simeq (\mathbb{Z}/\mathbb{Z}) \times (\mathbb{Z}/14\mathbb{Z}) \simeq \{0\} \times \mathbb{Z}_{14} \simeq \mathbb{Z}_{14}.$$

其中第二处同构用到了练习 4.8.24.

**练习 4.8.24** 设  $G_1, G_2$  为群,  $N_1 \triangleleft G_1, N_2 \triangleleft G_2$ , 则  $(N_1 \times N_2) \triangleleft (G_1 \times G_2)$ , 且  $(G_1 \times G_2)/(N_1 \times N_2) \simeq (G_1/N_1) \times (G_2/N_2)$ .

**定理 4.8.25 (有限生成 Abel 群结构定理)** 设  $G$  为有限生成 Abel 群, 则存在群同构

$$G \simeq (\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}) \oplus \mathbb{Z}^s,$$

其中  $s \geq 0$ , 正整数  $d_1 | \cdots | d_r$  称为  $G$  的不变因子. 特别地, 当  $G$  为有限群时,  $s = 0$ , 从而

$$G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}.$$

**证明** 由命题 4.8.17, 存在  $A \in M_{n \times m}(\mathbb{Z})$  使得  $G \simeq \text{Coker}(\phi_A)$ . 设  $A$  相抵于  $B = \text{diag}(d_1, \dots, d_r, O)$ , 由命题 4.8.21 与练习 4.8.24,

$$\text{Coker}(\phi_A) \simeq \text{Coker}(\phi_B) = \mathbb{Z}^n / (d_1\mathbb{Z} \times \cdots \times d_r\mathbb{Z} \times 0\mathbb{Z} \cdots \times 0\mathbb{Z}) \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z}) \times \mathbb{Z}^{n-r},$$

记  $s = n - r$ , 则

$$G \simeq (\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}) \oplus \mathbb{Z}^s.$$

□

**推论 4.8.26** 设  $A \in M_n(\mathbb{Z})$ , 则  $\text{Coker}(\phi_A)$  有限当且仅当  $\det(A) \neq 0$ . 此时,  $|\text{Coker}(\phi_A)| = |\det(A)|$ .

**推论 4.8.27** 设  $K \leqslant \mathbb{Z}^n$ , 则

(1) 存在  $\mathbb{Z}^n$  的一组基  $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ , 以及正整数  $d_1 | d_2 | \cdots | d_r$ , 使得  $\{d_1\mathbf{e}_1, \dots, d_r\mathbf{e}_r\}$  恰为  $K$  的基. 特别地,  $K$  是自由 Abel 群,  $\text{rank}(A) = r \leqslant n$ .

(2)  $\mathbb{Z}^n / K \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z}^{n-r}$ .

**证明** 取  $K$  的一个生成元集  $\{\mathbf{v}_1, \dots, \mathbf{v}_m\} \subset \mathbb{Z}^n$ , 令  $A = (\mathbf{v}_1, \dots, \mathbf{v}_m)$ , 其 Smith 标准形为  $B = P^{-1}AQ = \text{diag}(d_1, \dots, d_r, O)$ , 其中  $P \in \text{GL}(n, \mathbb{Z}), Q \in \text{GL}(m, \mathbb{Z})$ . 在命题 4.8.21 证明的交换图中, 取  $\mathbb{Z}^n$  的标准正交基  $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ , 则  $\{d_1\mathbf{f}_1, \dots, d_r\mathbf{f}_r\}$  为的  $\text{Im}(\phi_B)$  的基. 而  $\phi_P(\text{Im}(\phi_B)) = \text{Im}(\phi_A) = K$ , 令  $\mathbf{e}_i = \phi_P(\mathbf{f}_i)$ , 则  $\{d_1\mathbf{e}_1, \dots, d_r\mathbf{e}_r\}$  为  $K$  的基. □

**定义 4.8.28** 定义 Abel 群  $G$  的扭子群  $t(G) = \{g \in G : g \text{ 有限阶}\} = \{g \in G : \text{存在 } n > 0 \text{ 使 } ng = 0_G\}$ .

**注记 4.8.29**  $t(G) \leqslant G$ .

用扭子群的概念可以将定理 4.8.25 内蕴表述为以下定理.

**定理 4.8.30** 设  $G$  为有限生成 Abel 群, 则存在内直和分解  $G = t(G) \oplus F$ , 使得  $F$  为有限生成自由 Abel 群 (称其为  $t(G)$  的补),  $|t(G)| < +\infty$ , 且  $t(G) \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$ .

**证明** 由定理 4.8.25, 设存在群同构  $\theta : (\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}) \oplus \mathbb{Z}^s \xrightarrow{\sim} G$ . 记  $U = \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$ ,  $V = \mathbb{Z}^s$ , 则  $U \simeq \theta(U) \leqslant G, V \simeq \theta(V) \leqslant G$ . 由  $|\theta(U)| < +\infty$  即知  $\theta(U) \subset t(G)$ , 而  $V \simeq \theta(V)$  中的元素显然为无限阶的, 因此  $\theta(U) = t(G)$ . 取  $F = \theta(V)$  即得证.  $\square$

**注记 4.8.31** (1) 此分解中  $F$  不唯一, 但在同构意义下唯一,  $F \simeq G/t(G)$ .

(2) 若  $F \simeq \mathbb{Z}^s$ , 则称  $s$  为  $G$  的秩, 记为  $\text{rank}(G)$ .

**不变因子与初等因子** 在定理 4.8.25 中, 当  $G$  为有限群时,  $G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$ , 其中  $d_1 | \cdots | d_r$  为  $G$  的不变因子. 对这些不变因子进行标准素分解:

$$d_i = p_1^{s_{1i}} \cdots p_t^{s_{ti}}, \quad s_{1i}, \dots, s_{ti} \geq 0.$$

对互异的素数  $p_1, \dots, p_t$ , 由定理 2.8.4 可得环同构  $\mathbb{Z}_{p_1^{s_{1i}} \cdots p_t^{s_{ti}}} \simeq \mathbb{Z}_{p_1^{s_{1i}}} \times \cdots \times \mathbb{Z}_{p_t^{s_{ti}}}$ , 仅保留加法结构便得到群同构  $\mathbb{Z}_{p_1^{s_{1i}} \cdots p_t^{s_{ti}}} \simeq \mathbb{Z}_{p_1^{s_{1i}}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{s_{ti}}}$ . 因此

$$\begin{aligned} G &\simeq \left( \mathbb{Z}_{p_1^{s_{11}}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{s_{t1}}} \right) \oplus \cdots \oplus \left( \mathbb{Z}_{p_1^{s_{1r}}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{s_{tr}}} \right) \\ &\simeq \underbrace{\left( \mathbb{Z}_{p_1^{s_{11}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{s_{1r}}} \right)}_{\text{Sylow } p_1\text{-子群}} \oplus \cdots \oplus \underbrace{\left( \mathbb{Z}_{p_t^{s_{t1}}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{s_{tr}}} \right)}_{\text{Sylow } p_t\text{-子群}}, \end{aligned}$$

其中  $s_{11} \leq \cdots \leq s_{1r}, \dots, s_{t1} \leq \cdots \leq s_{tr}$ . 我们将第一个分解中的  $p_1^{s_{11}} \cdots p_t^{s_{t1}}, \dots, p_1^{s_{1r}} \cdots p_t^{s_{tr}}$  称为  $G$  的初等因子. 回顾线性代数知识, 这里第一种分解可类比于 Jordan 块, 第二种分解可类比于根子空间分解.

**例 4.8.32** 分类 1500 阶 Abel 群.

**解答** 设群  $G$  满足  $|G| = 1500 = 2^2 \cdot 3^1 \cdot 5^3$ , 则

- ◊  $G$  的 Sylow 2-子群在同构意义下有  $\mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2$  共 2 种.
- ◊  $G$  的 Sylow 3-子群在同构意义下有  $\mathbb{Z}_3$  共 1 种.
- ◊  $G$  的 Sylow 5-子群在同构意义下有  $\mathbb{Z}_{125}, \mathbb{Z}_5 \oplus \mathbb{Z}_{25}, \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$  共 3 种.

故  $G$  共有  $2 \cdot 1 \cdot 3 = 6$  种可能.  $\square$

**例 4.8.33** 在例 4.8.32 中, 若  $G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$ , 则  $G$  的初等因子 (按降序) 为  $2^2 \cdot 3^1 \cdot 5^2, 2^0 \cdot 3^0 \cdot 5^1$ ; 若  $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$ , 则  $G$  的初等因子 (按降序) 为  $2^1 \cdot 3^1 \cdot 5^2, 2^1 \cdot 3^0 \cdot 5^1$ .

**练习 4.8.34** 设 Abel 群  $A \simeq B$ , 整数  $m \mid n$ , 则  $mA/nA \simeq mB/nB$ . 特别地,  $A/nA \simeq B/nB$ .

下面的命题表明不变因子与初等因子均由群  $G$  唯一确定.

**命题 4.8.35** 设  $p$  为素数,  $\mathbb{Z}_{p^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{s_n}} \simeq \mathbb{Z}_{p^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{t_m}}$ , 其中  $1 \leq s_1 \leq \cdots \leq s_n, 1 \leq t_1 \leq \cdots \leq t_m$ , 则  $n = m, s_i = t_i$  ( $1 \leq i \leq n$ ).

**证明** 记  $A = \text{LHS}, B = \text{RHS}$ . 由练习 4.8.24,

$$A/pA \simeq (\mathbb{Z}_{p^{s_1}}/p\mathbb{Z}_{p^{s_1}}) \oplus \cdots \oplus (\mathbb{Z}_{p^{s_n}}/p\mathbb{Z}_{p^{s_n}}).$$

注意到对  $1 \leq i \leq n$ ,  $\mathbb{Z}_{p^{s_i}}/p\mathbb{Z}_{p^{s_i}}$  是循环群的商群, 因此均为循环群, 且  $\text{ord}(\bar{1}) = p$ , 因此  $\mathbb{Z}_{p^{s_i}}/p\mathbb{Z}_{p^{s_i}} \simeq \mathbb{Z}_p$ , 从而  $A/pA \simeq (\mathbb{Z}_p)^n$ . 同理可得  $B/pB \simeq (\mathbb{Z}_p)^m$ , 由练习 4.8.34 即知  $(\mathbb{Z}_p)^n \simeq (\mathbb{Z}_p)^m$ , 从而  $n = m$ . 再次运用

练习 4.8.24 可得

$$pA/p^2A \simeq (p\mathbb{Z}_{p^{s_1}}/p^2\mathbb{Z}_{p^{s_1}}) \oplus \cdots \oplus (p\mathbb{Z}_{p^{s_n}}/p^2\mathbb{Z}_{p^{s_n}}) \simeq (\mathbb{Z}_p)^{\#\{1 \leq i \leq n : s_i \geq 2\}}.$$

同理  $pB/p^2B \simeq (\mathbb{Z}_p)^{\#\{1 \leq j \leq m : t_j \geq 2\}}$ , 由练习 4.8.34 即知  $\#\{1 \leq i \leq n : s_i \geq 2\} = \#\{1 \leq j \leq m : t_j \geq 2\}$ , 结合  $n = m$  及  $1 \leq s_1 \leq \cdots \leq s_n, 1 \leq t_1 \leq \cdots \leq t_m$  即得  $s_1 = t_1$ . 余下类似可证.  $\square$

**练习 4.8.36** 证明: 有限生成 Abel 群  $G$  是自由 Abel 群当且仅当  $G$  的每个非零元都是无限阶元素.

**练习 4.8.37** 设  $A$  为有限 Abel 群, 证明: 对于  $|A|$  的每个正因子  $d$ ,  $A$  均有  $d$  阶子群和  $d$  阶商群.

**练习 4.8.38** 设  $H$  是有限 Abel 群  $A$  的子群, 证明:  $A$  有同构于  $A/H$  的子群.

**练习 4.8.39** 若有限 Abel 群  $A$  不是循环群, 则存在素数  $p$  使得  $A$  有同构于  $\mathbb{Z}_p^2 = \mathbb{Z}_p \oplus \mathbb{Z}_p$  的子群.

**练习 4.8.40** 证明: 当  $(m, n) = 1$  时,  $\mathbb{Z}_m \oplus \mathbb{Z}_n$  的不变因子为  $\{mn\}$ ; 而当  $(m, n) > 1$  时,  $\mathbb{Z}_m \oplus \mathbb{Z}_n$  的不变因子为  $\{(m, n), [m, n]\}$ .

**练习 4.8.41** 求  $\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{35}$  的初等因子和不变因子.

## 4.9 群的合成列

**定义 4.9.1** 群  $G$  的递降子群链

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

如满足  $G_{i+1} \triangleleft G_i, \forall 0 \leq i < n$ , 则称之为正规列, 而群族

$$G_i/G_{i+1}, \quad i = 0, \dots, n-1$$

称为该列的子商.

**定义 4.9.2** 若群  $G$  的正规列  $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1_G\}$  满足子商皆为单群, 则称之为合成列. 我们称整数  $n$  为该合成列的长度.

**注记 4.9.3** 在合成列中, 群  $G$  由子商“拼成”.

**例 4.9.4** 群  $G$  为单群当且仅当  $G \supset \{1_G\}$  为合成列.

**引理 4.9.5** 有限群  $G$  必有合成列.

**证明** 若  $|G| = 1$ , 取平凡合成列. 若  $G$  为非平凡单群, 取合成列  $G \supsetneq \{1_G\}$ . 对余下情形, 对  $|G|$  归纳: 取  $G$  的阶最大的正规的真子群  $N$ , 则  $G/N$  为单群. 由于  $|N| < |G|$ , 归纳假设给出了  $N$  的合成列  $(N_i)$ , 取  $(G, N_0, N_1, \dots)$  作为  $G$  的合成列即可.  $\square$

**注记 4.9.6** 无限群未必有合成列, 例如  $\mathbb{Z}$ .

**例 4.9.7 (合成列未必唯一)** 由例 4.4.33 与例 4.3.12 可得合成列  $S_4 \supsetneq A_4 \supsetneq K_4 \supsetneq \{1, \sigma_i\} \supsetneq \{\text{Id}\}$ , 其中

$$\sigma_1 = (12)(34), \quad \sigma_2 = (13)(24), \quad \sigma_3 = (14)(23).$$

由于  $i$  可任选为 1, 2 或 3, 因此上述合成列的选取并不唯一.

**定义 4.9.8** 设  $G = G_0 \supset \dots$  为正规列, 我们视其子商  $(G_i/G_{i+1})_{i \geq 0}$  为不计顺序, 但计入重数的集合. 如果两个正规列长度相同, 而且其子商在上述意义下相等, 则称两正规列等价.

**定义 4.9.9** 考虑一列群同态

$$\dots \xrightarrow{f_0} G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \dots \xrightarrow{f_i} G_{i+1} \rightarrow \dots,$$

长度或有限或无限. 若对所有  $i$  都有

$$\text{Im}(f_i) = \text{Ker}(f_{i+1}),$$

则称此列正合. 我们经常把  $\{1\}$  简写为 1, 或用加性符号记为 0.

**例 4.9.10** (1) 对于任意同态  $\varphi : G \rightarrow G'$ , 列  $G \rightarrow G' \rightarrow 1$  正合当且仅当  $\varphi$  是满的, 列  $1 \rightarrow G \rightarrow G'$  正合当且仅当  $\varphi$  是单的.

(2) 我们恒有正合列

$$1 \rightarrow \text{Ker}(\varphi) \rightarrow G \xrightarrow{\varphi} \text{Im}(\varphi) \rightarrow 1$$

其中  $\text{Ker}(\varphi) \rightarrow G$  是自然的包含映射.

**定理 4.9.11 (Jordan-Hölder 定理)** 群  $G$  的任两个合成列皆等价.

**证明** 设  $(G_i)_{0 \leq i \leq n}$  为群  $G$  的合成列, 对每个单群  $S$ , 记  $n(G, (G_i), S)$  为在同构意义下  $S$  在  $G$  的全体子商中出现的次数, 只需证  $n(G, (G_i), S)$  与合成列  $(G_i)$  的选取无关. 注意到若  $H \leq G$ , 则通过定义  $H_i = G_i \cap H$ , 正规列  $(G_i)$  诱导出  $H$  的正规列  $(H_i)$ . 类似地, 若  $N \triangleleft G$ , 则  $(G/N)_i = G_i/(G_i \cap N)$  定义出  $G/N$  的正规列  $((G/N)_i)$ . 正合列  $1 \rightarrow N \rightarrow G \rightarrow G/N \rightarrow 1$  诱导出正合列

$$1 \rightarrow N_i/N_{i+1} \rightarrow G_i/G_{i+1} \rightarrow (G/N)_i/(G/N)_{i+1} \rightarrow 1.$$

由于  $(G_i)$  为合成列, 从而  $G_i/G_{i+1}$  均为单群, 因此  $N_i/N_{i+1}$  必为 1 或  $G_i/G_{i+1}$ . 据此, 我们将指标集  $I = \{0, \dots, n-1\}$  分为两部分

$$I_1 = \{i : N_i/N_{i+1} = G_i/G_{i+1}\}, \quad I_2 = \{i : N_i/N_{i+1} = 1\}.$$

分别利用  $I_1$  和  $I_2$  作为指标集, 我们得到  $N$  和  $G/N$  上的合成列, 且  $|I_1| + |I_2| = n$ . 为证明定理, 我们对合成列的长度  $n$  进行归纳. 当  $n \leq 1$  时, 不证自明. 现假定  $n \geq 2$ , 则  $G$  不是平凡群也不是单群, 因此可取  $G$  的一个非平凡正规真子群  $N$ . 根据上述讨论,  $|I_1|$  和  $|I_2|$  都小于  $n$ , 从而可以对  $N$  以及  $G/N$  用归纳假设, 这表明  $n(N, (N_i)_{i \in I_1}, S)$  和  $n(G/N, ((G/N)_i)_{i \in I_2}, S)$  与合成列的选取无关. 又因为

$$n(G, (G_i), S) = n(N, (N_i)_{i \in I_1}, S) + n(G/N, ((G/N)_i)_{i \in I_2}, S),$$

所以  $n(G, (G_i), S)$  与合成列的选取无关.  $\square$

因此, 一旦群  $G$  有合成列, 则其子商在定义 4.9.8 的意义下无关合成列的选取.

**定义 4.9.12** 假设群  $G$  有合成列, 定义其合成因子或 Jordan-Hölder 因子集  $\text{JH}(G)$  为其任意合成列的全体子商(不计顺序, 计入重数), 并将合成列的长度称为群  $G$  的长度, 记作  $\ell(G)$ . 如果一个群没有合成列, 我们约定其长度为  $\infty$ .

**命题 4.9.13** 设  $G$  为有限群, 则  $G$  为可解群当且仅当  $\text{JH}(G)$  中任一合成因子均为素数阶循环群.

**证明** ( $\Rightarrow$ ) 由练习 4.4.35 立得.

( $\Leftarrow$ ) 循环群是 Abel 群. □

**练习 4.9.14** 证明: 若群  $G$  有合成列,  $N \triangleleft G$ , 则  $N$  亦有合成列. 若  $N \leqslant G$ , 结论是否成立?

**定义 4.9.15** 设  $G$  为群, 对于  $x, y \in G$ , 定义换位子  $[x, y] = xyx^{-1}y^{-1}$ .

**注记 4.9.16**  $xy = yx$  当且仅当  $[x, y] = 1_G$ .

**定义 4.9.17** 设  $G$  为群, 对任意子集  $A, B \subset G$ , 定义  $[A, B] \triangleleft G$  为由  $\{[a, b] : a \in A, b \in B\}$  生成的最小正规子群. 我们称  $G_{\text{der}} := [G, G]$  为  $G$  的导出子群或换位子群, 而  $G_{\text{ab}} := G/G_{\text{der}}$  称为  $G$  的 Abel 化.

**注记 4.9.18** (1)  $G_{\text{der}}$  亦可直接定义为由群  $G$  中换位子生成的子群, 可证它是正规子群.

(2) 若  $G$  是 Abel 群, 则  $G_{\text{der}} = \{1_G\}$ .

(3)  $G_{\text{ab}}$  是 Abel 群.

按照定义, 我们有

**命题 4.9.19** 设  $G$  为群,  $H \leqslant G$ , 则以下等价:

(1)  $H \supseteq G_{\text{der}}$ .

(2)  $H \triangleleft G$  且  $G/H$  为 Abel 群.

**例 4.9.20** 考虑例 4.7.19 中的  $Q_8$ , 由练习 4.7.20,  $[b, a] = bab^{-1}a^{-1} = (bab^{-1}a)a^{-2} = a^{-2}a^4 = a^2 \in (Q_8)_{\text{der}}$ . 而  $\{1, a^2\} \triangleleft Q_8$ , 由命题 4.9.19,  $(Q_8)_{\text{der}} = \{1, a^2\}$ .

**例 4.9.21** 设  $G$  为非 Abel 单群, 则  $G_{\text{der}} = G$ .

**练习 4.9.22** 对  $n \geqslant 3$ , 有  $(S_n)_{\text{der}} = A_n$ .

**证明** 由命题 4.9.19,  $(S_n)_{\text{der}} \subset A_n$ . 而由例 4.4.7, 当  $n \geqslant 3$  时,  $S_n$  是非 Abel 群, 因此  $(S_n)_{\text{der}} \neq \{\text{Id}\}$ .

- ◊ 若  $n = 3$ , 由例 4.4.31 中  $S_3$  的子群格,  $A_3$  仅有平凡子群, 因此  $(S_3)_{\text{der}} = A_3$ .
- ◊ 若  $n = 4$ , 由表 4.3 可见  $A_4$  的正规子群为  $\{\text{Id}\}, K_4, A_4$ . 由于  $(12)(13)(12)^{-1}(13)^{-1} = (123) \notin K_4$ , 因此  $(S_4)_{\text{der}} = A_4$ .
- ◊ 若  $n \geqslant 5$ , 由定理 4.4.36,  $A_n$  为单群, 因此  $(S_n)_{\text{der}} = A_n$ . □

**定义 4.9.23** 设  $G$  为群, 递归地定义  $G$  的导出列:

$$G^{(0)} = G, \quad G^{(i+1)} = [G^{(i)}, G^{(i)}], \quad i \geqslant 0.$$

**定理 4.9.24** 群  $G$  为可解群当且仅当存在正整数  $n$ , 使得  $G^{(n)} = \{1_G\}$ .

**证明** ( $\Leftarrow$ ) 由于  $G^{(i)}/G^{(i+1)}$  是  $G^{(i)}$  的 Abel 化, 因此正规列  $G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(n)} = \{1_G\}$  的每个子商均为 Abel 群, 从而  $G$  为可解群.

( $\Rightarrow$ ) 设正规列  $G \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1_G\}$  中每个子商均为 Abel 群. 由命题 4.9.19,  $G_1 \supset G^{(1)}, G_2 \supset G_1^{(1)} \supset (G^{(1)})^{(1)} = G^{(2)}, \dots, G_n \supset G^{(n)}$ , 从而  $G^{(n)} = 1_G$ . □

**定理 4.9.25 (Burnside)**  $p^a q^b$  阶群是可解群, 其中  $p, q$  为素数,  $a, b$  为非负整数.

**定理 4.9.26 (Feit-Thompson)** 奇数阶群是可解群.

## 4.10 半直积

**定义 4.10.1** 设  $H, N$  为群, 并给定同态  $\rho : H \rightarrow \text{Aut}(N)$ . 相应的半直积  $N \rtimes_{\rho} H$  为如下定义的群(下标  $\rho$  经常略去):

- ◊ 作为集合,  $N \rtimes H$  无非是积集  $N \times H$ ;
- ◊ 二元运算是  $(n, h)(n', h') = (n\rho(h)(n'), hh')$ , 其中  $n, n' \in N, h, h' \in H$ .

**注记 4.10.2** (1) 若  $\rho(h) = \text{Id}_N, \forall h \in H$ , 则  $N \rtimes_{\rho} H = N \times H$ .

(2) 兮元是  $(1_N, 1_H)$ .

(3)  $(n, h)^{-1} = (\rho(h^{-1})(n^{-1}), h^{-1})$ .

(4) 透过单同态  $h \mapsto (1, h)$  和  $n \mapsto (n, 1)$  可将  $H$  和  $N$  都视为  $N \rtimes H$  的子群. 从二元运算的定义立得  $N \triangleleft (N \rtimes H)$ .

**定理 4.10.3** 设  $G$  为群,  $N \triangleleft G, H \leqslant G, N \cap H = \{1_G\}, NH = G$ . 定义

$$\rho : H \rightarrow \text{Aut}(N), \quad h \mapsto (n \mapsto hnh^{-1}),$$

则有群同构

$$N \rtimes_{\rho} H \xrightarrow{\sim} G, \quad (n, h) \mapsto nh.$$

**例 4.10.4** 考虑  $A_3 \triangleleft S_3, H = ((12)) \leqslant S_3$ , 以及群同态  $\rho : H \rightarrow \text{Aut}(A_3), h \mapsto (n \mapsto hnh^{-1})$  (易验证这是群同态), 由于  $A_3 \cap H = \{\text{Id}\}, A_3 \times H = S_3$ , 由定理 4.10.3,  $S_3 \cong A_3 \rtimes_{\rho} H \cong C_3 \rtimes_{\rho} C_2$ .

**练习 4.10.5** 考虑练习 4.7.20 中的  $Q_8$ , 证明不存在  $Q_8$  的真子群  $H$  与  $N \triangleleft Q_8$ , 使得  $N \cap H = \{1\}$  且  $Q_8 = NH \cong N \times H$ .

**证明** 用反证法, 假设存在, 则  $|N| = 2$  或  $4$ .

- ◊ 若  $|N| = 4$ , 则  $|H| = 2$ , 而  $Q_8$  中只有一个 2 阶元  $a^2$ , 因此  $H = \{1, a^2\}$ . 而此时  $Q_8/N$  为 2 阶群, 即  $Q_8/N \cong C_2$ , 因此  $(aN)^2 = a^2N = N$ , 即  $a^2 \in N$ , 这与  $N \cap H = \{1\}$  矛盾.
- ◊ 若  $|N| = 2$ , 则  $|H| = 4, [Q_8 : H] = 2$ , 由例 4.3.12 知  $H \triangleleft Q_8$ . 又  $N \cap H = \{1\}$ , 由练习 4.3.28 即知  $Q_8 = NH \cong N \times H$  为 Abel 群, 矛盾.  $\square$

## 第五章 Galois 理论

### 5.1 Galois 扩张

设  $K$  为域,  $G \leqslant \text{Aut}(K)$ , 则有  $G^\sim K : (\sigma, v) \mapsto \sigma(v)$ , 其不动点集  $K^G = \{v \in K : \sigma(v) = v, \forall \sigma \in G\}$  称为  $G$ -不动子域. 我们有如下事实:

- ◊  $K^G$  是  $K$  的子域.
- ◊ 若  $H \leqslant G$ , 则有  $K^G \hookrightarrow K^H \hookrightarrow K = K^{\{\text{Id}_K\}}$ . (群越小, 不动子域越大.)
- ◊ 考虑域扩张  $K/k$ , 且  $H \leqslant \text{Gal}(K/k)$ , 则有  $k \hookrightarrow K^H \hookrightarrow K$ . 特别地,  $k \hookrightarrow K^{\text{Gal}(K/k)} \hookrightarrow K$ .
- ◊  $G \leqslant \text{Gal}(K/K^G)$ .

**定理 5.1.1** 若  $G \leqslant \text{Aut}(K)$  是有限子群, 则  $[K : K^G] = |G| < +\infty$  且  $G = \text{Gal}(K/K^G)$ .

**证明** 令  $n = |G|, k = K^G$ , 断言  $[K : k] \leqslant n$ . 若断言已证, 则由

$$n = |G| \leqslant |\text{Gal}(K/k)| \leqslant [K : k] \leqslant n$$

即得欲证. 下面采用反证法证明断言, 假设  $[K : k] \geqslant n + 1$ , 则存在  $\{e_1, \dots, e_{n+1}\} \subset K$  是  $k$ -线性无关的. 设  $G = \{\sigma_0 = \text{Id}, \sigma_1, \dots, \sigma_{n-1}\}$ , 令

$$A = \begin{pmatrix} e_1 & \cdots & e_{n+1} \\ \sigma_1(e_1) & \cdots & \sigma_1(e_{n+1}) \\ \vdots & \ddots & \vdots \\ \sigma_{n-1}(e_1) & \cdots & \sigma_{n-1}(e_{n+1}) \end{pmatrix} \in M_{n \times (n+1)}(K),$$

并记  $V = \{\mathbf{v} \in K^{n+1} : A\mathbf{v} = \mathbf{0}\}$  为  $K^{n+1}$  的线性子空间, 由  $\text{rank}(A) \leqslant n < n + 1$  知  $V \neq \{\mathbf{0}\}$ . 考虑群作用  $G^\sim K^{n+1} : (\sigma, (\lambda_1, \dots, \lambda_{n+1})^\top) \mapsto (\sigma(\lambda_1), \dots, \sigma(\lambda_{n+1}))^\top$ . 对任意  $\mathbf{v} = (\lambda_1, \dots, \lambda_{n+1})^\top \in V$ , 由  $A\mathbf{v} = \mathbf{0}$  可得

$$\sum_{k=1}^{n+1} \lambda_k \sigma_i(e_k) = 0, 0 \leqslant i \leqslant n - 1 \implies \sum_{k=1}^{n+1} \sigma_j(\lambda_k) \sigma_j \circ \sigma_i(e_k) = 0, 0 \leqslant i, j \leqslant n - 1$$

$$\implies \sum_{k=1}^{n+1} \sigma_j(\lambda_k) \sigma_i(e_k) = 0, 0 \leq i, j \leq n-1 \xrightarrow{\tau=\sigma_j} \tau \cdot \mathbf{v} \in V, \forall \tau \in G.$$

取  $\mathbf{v} = (\lambda_1, \dots, \lambda_{n+1})^\top \in V \setminus \{\mathbf{0}\}$  使其非 0 分量最少. 观察到  $\mathbf{v}$  至少有 2 个非 0 分量 (否则, 不妨设仅有  $\lambda_1 \neq 0$ , 则由  $A\mathbf{v} = \mathbf{0}$  得  $\lambda_1 e_1 = 0$ , 但  $\lambda_1, e_1 \neq 0$ , 矛盾). 因此不妨设  $\lambda_1 \lambda_2 \neq 0$ , 进而可不妨设  $\lambda_1 = 1$ , 即  $\mathbf{v} = (1, \lambda_2, \dots, \lambda_{n+1})^\top$ , 其中  $\lambda_2 \neq 0$ . 注意到  $\mathbf{v}$  的分量不全在  $k$  中, 否则由  $A\mathbf{v} = \mathbf{0}$  知  $\lambda_1 e_1 + \dots + \lambda_{n+1} e_{n+1} = 0$ , 与  $e_1, \dots, e_{n+1}$  是  $k$ -线性无关的矛盾. 不妨设  $\lambda_2 \notin k = K^G$ , 则存在  $\tau \in G$  使  $\tau(\lambda_2) \neq \lambda_2$ . 由  $\tau \cdot \mathbf{v} \in V$  知  $\mathbf{v} - \tau \cdot \mathbf{v} \in V$ , 但由  $\tau(0) = 0, \tau(1) = 1$  可见  $\mathbf{v} - \tau \cdot \mathbf{v} \in V$  的非 0 分量比  $\mathbf{v}$  更少, 矛盾.  $\square$

**定义-定理 5.1.2** 设  $K/k$  为有限维域扩张,  $G = \text{Gal}(K/k)$ , 则以下等价:

- (1)  $k = K^G$ .
- (2)  $|G| = [K : k]$ .
- (3) 对任意  $\alpha \in K$ ,  $\alpha$  在  $k$  上的最小多项式无重根, 且在  $K$  上分裂.
- (4) 存在可分多项式  $f(x) \in k[x]$  使得  $K = (k, f(x))$ .

此时称  $K/k$  为有限 Galois 扩张.

**证明** (1)  $\Leftrightarrow$  (2) 由定理 3.2.4 与定理 5.1.1 得

$$[K : k] = [K^G : k][K : K^G] = [K^G : k] \cdot |G|,$$

$$\text{因此 } |G| = [K : k] \iff [K^G : k] = 1 \iff k = K^G.$$

(2)  $\Rightarrow$  (3) 任取  $\alpha \in K$ , 设  $\alpha$  在  $k$  上的最小多项式为  $g(x)$ . 由引理 3.3.1,

$$|G| = |\text{Gal}(K/k)| \leq |\text{Root}_K(g(x))| \cdot [K : k(\alpha)] \leq \deg(g(x)) \cdot [K : k(\alpha)] = [K : k],$$

而由 (2),  $|G| = [K : k]$ , 因此上式中均取等号, 因此  $|\text{Root}_K(g(x))| = \deg(g(x))$ .

(3)  $\Rightarrow$  (4) 由定理 3.2.11, 可设  $K = k(\alpha_1, \dots, \alpha_n)$ , 其中  $\alpha_i \in K$  在  $k$  上的最小多项式为  $g_i(x)$ . 由 (3),  $g_i(x)$  无重根, 且在  $K$  上分裂. 令  $f(x) = g_1(x) \cdots g_n(x) \in k[x]$ , 则  $f(x)$  可分且  $K = (k, f(x))$ .

(4)  $\Rightarrow$  (2) 这是定理 3.3.30.  $\square$

**注记 5.1.3** (1)(2)(4) 是整体性质, (3) 是局部性质.

**例 5.1.4** 考虑  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \omega) = E$ .

- ◊  $E/\mathbb{Q}$  是 Galois 扩张,  $E = (\mathbb{Q}, x^3 - 2)$  (例 3.3.7).
- ◊  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  不是 Galois 扩张 (例 3.3.29).
- ◊  $E/\mathbb{Q}(\sqrt[3]{2})$  是 Galois 扩张 (例 3.2.7).

**定理 5.1.5 (绝对版本的有限 Galois 对应)** 对任意域  $K$ , 存在双射

$$\{\text{有限子群 } G \leq \text{Aut}(K)\} \xleftrightarrow{1:1} \{\text{子域 } k \subset K : K/k \text{ 为有限 Galois 扩张}\}$$

$$G \longleftarrow \longrightarrow K^G$$

$$\text{Gal}(K/k) \longleftarrow \longrightarrow k$$

**证明** 映射的良定性由定义-定理 5.1.2 (1)(2) 可见, 互逆性由定理 5.1.1 与定义-定理 5.1.2 (1) 可见.  $\square$

**定理 5.1.6 (相对版本的有限 Galois 对应)** 设  $K/k$  为有限 Galois 扩张, 则存在双射

$$\{\text{子群 } H \leqslant \text{Gal}(K/k)\} \xleftrightarrow{1:1} \{K/k \text{ 的中间域}\}$$

$$H \longmapsto K^H$$

$$\text{Gal}(K/E) \longleftarrow E$$

**证明** 互逆性在于:

- ◊ 由定理 5.1.1,  $H = \text{Gal}(K/K^H)$ .
- ◊ 若  $E$  是  $K/k$  的中间域, 则由定义-定理 5.1.2 (4),  $K/E$  亦为有限 Galois 扩张, 再由定义-定理 5.1.2 (1) 知  $E = K^{\text{Gal}(K/E)}$ .  $\square$

从例 5.1.4 可见, Galois 扩张的中间域关于底层的域不一定是 Galois 扩张:

$$\begin{array}{ccccc} \mathbb{Q} & \xrightarrow{\text{非 Galois 扩张}} & \mathbb{Q}(\sqrt[3]{2}) & \xrightarrow{\text{Galois 扩张}} & \mathbb{Q}(\sqrt[3]{2}, \omega) \\ & \searrow & & \swarrow & \\ & & \text{Galois 扩张} & & \end{array}$$

关于这一现象, 我们有如下命题.

**命题 5.1.7** 设  $K/k$  是有限 Galois 扩张,  $E$  是  $K/k$  的中间域, 则  $E/k$  是 Galois 扩张当且仅当  $\sigma(E) = E, \forall \sigma \in \text{Gal}(K/k)$ .

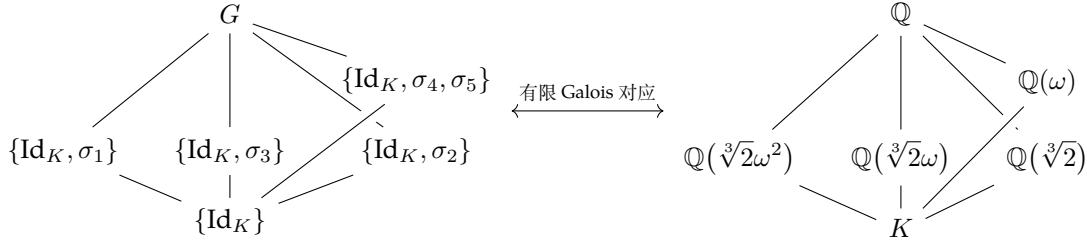
**证明** ( $\Rightarrow$ ) 由定义-定理 5.1.2 (4), 可设  $E = k(\beta_1, \dots, \beta_n)$ ,  $g(x) = (x - \beta_1) \cdots (x - \beta_n) \in k[x]$ . 对任意  $\sigma \in \text{Gal}(K/k)$ , 有  $\sigma(E) = k(\sigma(\beta_1), \dots, \sigma(\beta_n))$ , 而由  $g(x) \in k[x]$  知  $\sigma(\beta_i)_E \in \{\beta_1, \dots, \beta_n\}$  ( $1 \leq i \leq n$ ), 因此  $\sigma(E) \subset E$ . 同理可得  $\sigma^{-1}(E) \subset E$ , 即  $E \subset \sigma(E)$ . 故  $\sigma(E) = E$ .

( $\Leftarrow$ ) 任取  $b \in E$ , 设  $b$  在  $k$  上的最小多项式为  $g(x) \in k[x]$ . 由于  $K/k$  是有限 Galois 扩张, 由定义-定理 5.1.2 (3), 可设  $g(x) = (x - \beta_1) \cdots (x - \beta_n)$ , 其中  $\beta_1 = b, \beta_2, \dots, \beta_n \in K$  两两不同. 由引理 3.3.1, 对  $1 \leq i \leq n$ , 存在域同构  $\sigma_i : k(b) \xrightarrow{\sim} k(\beta_i)$  使得  $\sigma_i(b) = \beta_i$ . 再由定理 3.3.13,  $\sigma_i$  可进一步延拓为  $\delta : K \xrightarrow{\sim} K$ , 即  $\delta \in \text{Gal}(K/k)$ . 由条件,  $\beta_i = \delta(b) \in \delta(E) = E$ , 从而  $g(x)$  无重根且在  $E$  上分裂, 由定义-定理 5.1.2 (3),  $E/k$  是 Galois 扩张.  $\square$

**例 5.1.8** 考虑  $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[3]{2}, \omega) = (\mathbb{Q}, x^3 - 2)$ , 记  $G = \text{Gal}(K/\mathbb{Q})$ , 例 3.2.7 已得  $[K : \mathbb{Q}] = 6$ , 因此  $|G| = 6$ . 考虑  $G \cap \text{Root}_K(x^3 - 2)$ , 由练习 4.5.8, 存在群的单同态  $G \hookrightarrow S(\text{Root}_K(x^3 - 2)) \cong S_3$ , 而  $|S_3| = 6 = |G|$ , 因此这是群同构. 记  $a = \sqrt[3]{2}, b = \sqrt[3]{2}\omega, c = \sqrt[3]{2}\omega^2$ , 利用  $S_3$  可得  $G$  中元素:

$S_3$	$G$
Id	$\text{Id}_K$
$(ab)$	$\sigma_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}, \sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}\omega^2$
$(bc)$	$\sigma_2 : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega^2, \sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}\omega$
$(ca)$	$\sigma_3 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}$
$(abc)$	$\sigma_4 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega^2, \sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}$
$(acb)$	$\sigma_5 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}, \sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}\omega$

结合例 4.4.31, 可得  $G$  的子群格, 并由定理 5.1.6 得到  $K$  的子域格:



现重述定理 3.4.21 如下.

**例 5.1.9 (有限域的 Galois 对应)** 设  $E$  为有限域,  $|E| = p^n$ . 由注记 3.4.16 知  $E/\mathbb{F}_p$  是 Galois 扩张. 再由注记 3.4.20 可知  $\text{Gal}(E/\mathbb{F}_p)$  子群的形式. 故存在双射

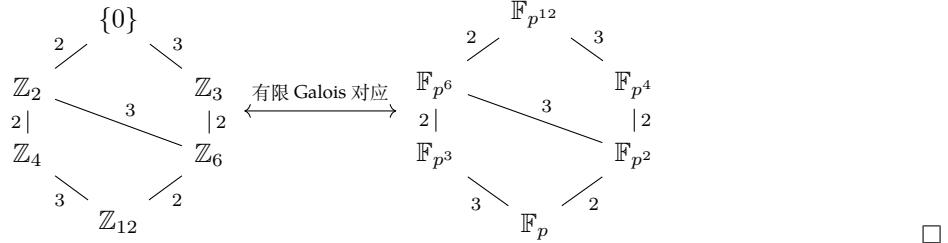
$$\{\text{子群 } H \leq \text{Gal}(E/\mathbb{F}_p)\} \xleftrightarrow{1:1} \{E/\mathbb{F}_p \text{ 的中间域}\}$$

$$(\sigma^d) \longleftrightarrow \text{Root}_E(x^{p^d} - x)$$

由于  $\text{Gal}(E/\mathbb{F}_p) = \text{Aut}(E)$ , 对于有限域, 定理 5.1.5 与定理 5.1.6 两个版本的 Galois 对应是统一的.

**练习 5.1.10** 画出  $\mathbb{F}_{p^{12}}/\mathbb{F}_p$  的 Hasse 图, 这里  $p$  为素数.

**解答** 由定理 3.4.19,  $\text{Gal}(\mathbb{F}_{p^{12}}/\mathbb{F}_p) = \{\text{Id}, \sigma, \sigma^2, \dots, \sigma^{11}\} \cong \mathbb{Z}_{12}$ .



□

**例 5.1.11 (任何有限群均可视为 Galois 扩张的 Galois 群)** 对任意有限群  $G$ , 由定理 4.5.13, 存在正整数  $n$  使得  $G$  同构于  $S_n$  的子群, 考虑  $S_n \cap K = k(t_1, \dots, t_n), (\sigma, t_i) \mapsto t_{\sigma(i)}$ , 则  $G$  可视为  $\text{Aut}(K)$  的子群. 由定理 5.1.1,  $G \cong \text{Gal}(K/K^G)$ . 故任何有限群(在同构意义下)都是某一 Galois 扩张的 Galois 群.

## 5.2 Galois 对应

**定义 5.2.1** 偏序集意指资料  $(L, \leq)$ , 其中  $L$  是集合而  $\leq$  是  $L$  上的二元关系(偏序), 满足

- ▷ **反身性**  $x \leq x, \forall x \in L$ ;
- ▷ **传递性**  $(x \leq y) \wedge (y \leq z) \implies x \leq z$ ;
- ▷ **反称性**  $(x \leq y) \wedge (y \leq x) \implies x = y$ .

**例 5.2.2** 记  $\mathbb{N}_+ = \{1, 2, 3, \dots\}$ , 有如下两个偏序集:

(1)  $(\mathbb{N}_+, \leq)$ , 其中  $\leq$  为自然数间的正常大小关系.

(2)  $(\mathbb{N}_+, \preccurlyeq)$ , 其中  $a \preccurlyeq b \iff a | b$ .

**例 5.2.3** 设  $G$  为群, 则  $\text{Sub}(G) := \{H : H \leq G\}$  在集合的包含关系下构成偏序集.

**例 5.2.4** 对于域扩张  $K/k$ ,  $\text{Lat}(K/k) := \{K/k \text{ 的中间域}\}$  在集合的包含关系下构成偏序集.

**例 5.2.5 (反偏序集)** 设  $(L, \leq)$  为偏序集, 则称  $L^{\text{op}} = (L, \leq^{\text{op}})$  为  $L$  的反偏序集, 其中  $a \leq^{\text{op}} b \iff b \leq a$ .

**定义 5.2.6** 设  $(L, \leq)$  为偏序集.

(1) 对任意  $a, b \in L$ , 称  $a \vee b \in L$  为  $a, b$  的最小上界, 若

- ◊  $a \leq (a \vee b)$  且  $b \leq (a \vee b)$ .
- ◊ 若  $c \in L$  使得  $a \leq c$  且  $b \leq c$ , 则  $(a \vee b) \leq c$ .

(2) 对任意  $a, b \in L$ , 称  $a \wedge b \in L$  为  $a, b$  的最大下界, 若

- ◊  $(a \wedge b) \leq a$  且  $(a \wedge b) \leq b$ .
- ◊ 若  $c \in L$  使得  $c \leq a$  且  $c \leq b$ , 则  $c \leq (a \wedge b)$ .

**注记 5.2.7** 最小上界与最大下界若存在, 则唯一.

**定义 5.2.8** 偏序集  $(L, \leq)$  称为格, 若对任意  $a, b \in L$ ,  $a \vee b$  与  $a \wedge b$  均存在.

**例 5.2.9** 集合  $\{1, 2, 3, 4, 5\}$  在整除关系下构成偏序集, 但不构成格, 例如  $2 \vee 3$  不存在.

**例 5.2.10** 设  $G$  为群, 则  $\text{Sub}(G)$  是格.

- ◊ 若  $H_1, H_2 \leq G$ , 则  $H_1 \vee H_2 = (H_1 \cup H_2), H_1 \wedge H_2 = H_1 \cap H_2$ .
- ◊ 若  $H \leq G, N \triangleleft G$ , 则  $H \vee N = HN = NH$ .

**例 5.2.11** 考虑域扩张  $K/k$ , 则  $\text{Lat}(K/k)$  是格. 若  $E, F$  均为  $K/k$  的中间域, 则  $E \wedge F = E \cap F, E \vee F$  即由  $E \cup F$  生成的域.

**例 5.2.12** 设  $L$  是格, 则其反格  $L^{\text{op}}$  也是格, 因为  $a \vee^{\text{op}} b = a \wedge b, a \wedge^{\text{op}} b = a \vee b$ .

**定义 5.2.13** 设  $L, L'$  为偏序集, 称  $f : L \rightarrow L'$  为(偏序集)同态, 若  $f(a) \leq f(b), \forall a \leq b$ . 若  $f : L \rightarrow L'$  为同态, 且为双射,  $f^{-1}$  亦为同态, 则称  $f$  为(偏序集)同构.

**注记 5.2.14** 偏序集同态即“保序映射”.

**例 5.2.15** 记  $[5] = \{1, 2, 3, 4, 5\}, \text{Id} : ([5], \preceq) \rightarrow ([5], \leq)$  是同态, 且是双射, 但不是同构. 这里  $\preceq$  表示整除关系,  $\leq$  表示正常大小关系.

**引理 5.2.16** 设  $L, L'$  是格,  $f : L \rightarrow L'$  为同构, 则

$$f(a \vee b) = f(a) \vee f(b), \quad f(a \wedge b) = f(a) \wedge f(b), \quad \forall a, b \in L.$$

**例 5.2.17** 对正整数  $n$ ,  $L_n = \{n \text{ 的正因子}\}$  在整除关系下构成格. 对  $d_1, d_2 \in L_n$ ,  $d_1 \vee d_2 = \text{lcm}(d_1, d_2)$ ,  $d_1 \wedge d_2 = \text{gcd}(d_1, d_2)$ . 考虑  $n$  阶循环群  $C_n = \langle g \mid g^n = 1 \rangle = \{1, g, \dots, g^{n-1}\}$ , 有格同构

$$L_n \xrightarrow{\sim} \text{Sub}(C_n), \quad d \mapsto (g^{\frac{n}{d}}).$$

**定理 5.2.18 (Galois 理论基本定理)** 设  $K/k$  为有限 Galois 扩张,  $G = \text{Gal}(K/k)$ , 则存在格同构

$$\text{Sub}(G) \xrightarrow{\sim} \text{Lat}(K/k)^{\text{op}}$$

$$H \longmapsto K^H$$

$$\text{Gal}(K/E) \longleftrightarrow E$$

**证明** 在定理 5.1.6 的基础上, 再注意到

$$H \leqslant H' \implies K^{H'} \subset K^H, \quad E \subset F \implies \text{Gal}(K/F) \subset \text{Gal}(K/E).$$

□

**注记 5.2.19** 对任意  $H \leqslant G$ , 由定理 4.1.18,  $|G| = |H|[G : H]$ ; 由定理 3.2.4,  $[K : k] = [K : K^H][K^H : k]$ ; 由定义-定理 5.1.2 (2),  $|G| = [K : k]$ ; 由定理 5.1.1,  $|H| = [K : K^H]$ , 因此  $[G : H] = [K^H : k]$ .

**推论 5.2.20** 设  $K/k$  为有限 Galois 扩张,  $G = \text{Gal}(K/k)$ , 则

(1) 若  $H_1, H_2 \leqslant G$ , 则  $K^{H_1 \vee H_2} = K^{H_1} \cap K^{H_2}$ ,  $K^{H_1 \wedge H_2} = K^{H_1} \vee K^{H_2}$ .

(2) 若  $E_1, E_2$  均为  $K/k$  的中间域, 则  $\text{Gal}(K/E_1 \vee E_2) = \text{Gal}(K/E_1) \cap \text{Gal}(K/E_2)$ ,  $\text{Gal}(K/E_1 \wedge E_2) = \text{Gal}(K/E_1) \vee \text{Gal}(K/E_2)$ .

(3) 有限 Galois 扩张  $K/k$  仅有有限个中间域.

**格结构上的群作用** 在定理 5.2.18 中同构的两个格上, 各存在如下群作用:

◊  $G^\curvearrowright \text{Sub}(G), (\sigma, H) \mapsto \sigma H \sigma^{-1}$ .

◊  $G^\curvearrowright \text{Lat}(K/k), (\sigma, E) \mapsto \sigma(E)$ .

事实上, 这两个作用是相容的, 我们有如下命题.

**命题 5.2.21** 定理 5.2.18 的 Galois 对应保持上述  $G$ -作用, 即对任意  $\sigma \in G, H \leqslant G$ , 以及  $K/k$  的中间域  $E$ , 有

$$K^{\sigma H \sigma^{-1}} = \sigma(K^H), \quad \sigma \text{Gal}(K/E)\sigma^{-1} = \text{Gal}(K/\sigma(E)).$$

**证明** 我们有

$$\begin{aligned} K^{\sigma H \sigma^{-1}} &= \{\lambda \in K : \sigma h \sigma^{-1}(\lambda) = \lambda, \forall h \in H\} = \{\lambda \in K : h \sigma^{-1}(\lambda) = \sigma^{-1}(\lambda), \forall h \in H\} \\ &= \{\lambda \in K : \sigma^{-1}(\lambda) \in K^H\} = \sigma(K^H), \end{aligned}$$

及

$$\begin{aligned} \text{Gal}(K/\sigma(E)) &= \{\delta \in \text{Aut}(K) : \delta \circ \sigma(e) = \sigma(e), \forall e \in E\} = \{\delta \in \text{Aut}(K) : \sigma^{-1} \circ \delta \circ \delta|_E = \text{Id}_E\} \\ &= \sigma \text{Gal}(K/E)\sigma^{-1}. \end{aligned}$$

□

**注记 5.2.22**  $\text{Sub}(G)$  与  $\text{Lat}(K/k)$  在  $G$ -作用下的不动点集是相对应的, 它们分别为

$$\text{Sub}(G)^G = \{H \leqslant G : \sigma H \sigma^{-1} = H\} = \{H \triangleleft G\},$$

与

$$\begin{aligned} \text{Lat}(K/k)^G &= \{K/k \text{ 的中间域 } E : \sigma(E) = E, \forall \sigma \in G\} \\ &\stackrel{\text{命题 5.1.7}}{=} \{K/k \text{ 的中间域 } E : E/k \text{ 为有限 Galois 扩张}\}. \end{aligned}$$

我们将注记 5.2.22 表述为如下命题.

**命题 5.2.23** 设  $K/k$  为有限 Galois 扩张,  $E$  为  $K/k$  的中间域, 则  $E/k$  为有限 Galois 扩张当且仅当  $\text{Gal}(K/E) \triangleleft G$ . 此时, 存在群同构  $G/\text{Gal}(K/E) \simeq \text{Gal}(E/k)$ .

**证明** 仅需证明最后的断言. 由命题 5.1.7,  $\sigma(E) = E, \forall \sigma \in \text{Gal}(K/k)$ , 因此有群同态

$$G \rightarrow \text{Gal}(E/k), \quad \sigma \mapsto \sigma|_E,$$

满性在于  $\text{Gal}(E/k) \leq \text{Gal}(K/k)$  (利用引理 3.3.1 进行延拓), 而其核为  $\text{Gal}(K/E)$ , 由定理 4.1.18 即得  $G/\text{Gal}(K/E) \simeq \text{Gal}(E/k)$ .  $\square$

**例 5.2.24** 在例 4.4.31 的 Hasse 图中,  $\{\{\text{Id}, (12)\}, \{\text{Id}, (13)\}, \{\text{Id}, (23)\}\}$  是  $S_3$ -作用下的一个轨道,  $A_3$  是  $S_3$  作用下的不动点. 在例 5.1.8 中的 Hasse 图中,  $\{\mathbb{Q}(\sqrt[3]{2}\omega^2), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2})\}$  是  $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ -作用下的一个轨道,  $\mathbb{Q}(\omega)/\mathbb{Q}$  为有限 Galois 扩张.

**定理 5.2.25 (Steinitz)** 设  $K/k$  为有限维域扩张, 则  $K/k$  为单扩张当且仅当  $K/k$  仅有有限个中间域.

**证明** ( $\Rightarrow$ ) 设  $K = k(\alpha)$ ,  $\alpha$  在  $k$  上的最小多项式为  $f(x) \in k[x]$ . 对任意  $K/k$  的中间域  $E$ , 设  $\alpha$  在  $E$  上的最小多项式为  $g(x) = x^m + c_1x^{m-1} + \cdots + c_m \in E[x]$ . 记  $B = k(c_1, \dots, c_m) \subset E$ , 则  $g(x)$  在  $E$  上亦不可约, 因此  $g(x)$  是  $\alpha$  在  $B$  上的最小多项式. 由定理 3.2.4,  $[K : E] = \deg(g(x)) = [K : B]$ , 因此  $B = E$ . 故  $K/k$  的中间域  $E$  被  $g(x)$  完全确定, 但  $f(x)$  仅有有限个因式, 因此  $K/k$  仅有有限个中间域.

( $\Leftarrow$ ) 若  $k$  为有限域, 由命题 3.4.13 即得  $K/k$  为单扩张. 下设  $|k| = +\infty$ ,  $K = k(\alpha_1, \dots, \alpha_n)$ . 由归纳法, 只需证  $K = k(\alpha, \beta)$  是单扩张. 对任意  $\lambda \in k$ , 考虑  $E_\lambda = k(\alpha + \lambda\beta)$ , 由于  $K/k$  仅有有限个中间域, 必存在互异的  $\lambda_1, \lambda_2 \in k$  使得  $E_{\lambda_1} = E_{\lambda_2}$ , 于是  $(\alpha + \lambda_1\beta) - (\alpha + \lambda_2\beta) = (\lambda_1 - \lambda_2)\beta \in E_{\lambda_1}$ , 由  $\lambda_1 - \lambda_2 \in k^\times$  即得  $\beta \in E_{\lambda_1}$ , 进而  $\alpha = (\alpha + \lambda_1\beta) - \beta \in E_{\lambda_1}$ ,  $k(\alpha, \beta) \subset E_{\lambda_1}$ . 故  $K = k(\alpha, \beta) = k(\alpha + \lambda_1\beta)$  为单扩张.  $\square$

**推论 5.2.26** (1) 若  $K/k$  为有限维单扩张,  $E$  是  $K/k$  的中间域, 则  $E/k$  为单扩张.

(2) 有限 Galois 扩张是单扩张.

**练习 5.2.27**  $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2} + \omega)$ . [提示] 由例 5.1.8 的 Hasse 图可见, 包含  $\sqrt[3]{2} + \omega$  的最小子域只能为  $\mathbb{Q}(\sqrt[3]{2}, \omega)$ .

**定义 5.2.28** 称代数扩张  $K/k$  为可分扩张, 若  $K$  中每个元素在  $k$  上的最小多项式均可分.

**定义 5.2.29** 设  $K/k$  为有限维域扩张, 若  $u \in K$  满足  $K = k(u)$ , 则称  $u$  为  $K/k$  的本原元.

**定理 5.2.30 (本原元定理)** 设  $K/k$  为有限维可分扩张, 则  $K/k$  为单扩张.

**证明** 设  $K = k(\alpha_1, \dots, \alpha_n)$ ,  $\alpha_i$  在  $k$  上的最小多项式为  $g_i(x)$ , 则  $g_1(x), \dots, g_n(x)$  均可分. 设  $g(x) = g_1(x) \cdots g_n(x) \in k[x]$ , 则  $g(x)$  亦可分. 考虑  $k \subset K \subset (K, g(x)) = E$ , 由定义-定理 5.1.2 (3),  $E/k$  为有限 Galois 扩张, 再由推论 5.2.26 (2) 与 (1) 知  $K/k$  为单扩张.  $\square$

作为 Galois 理论的应用, 我们证明代数基本定理.

**定理 3.2.20**  $\mathbb{C}$  是代数闭域.

**证明** 在假定分析中的中值定理成立的前提下, 我们有如下事实:

- (1) 每个正实数  $r$  有实平方根. (设  $f(x) = x^2 - r$ , 则  $f(1 + r) > 0$  且  $f(0) < 0$ .)
- (2) 任意 2 次多项式  $g(x) \in \mathbb{C}[x]$  有复根. (我们有求根公式.)
- (3)  $\mathbb{C}$  无二次扩张, 即若有域扩张  $\mathbb{C} \subset K$ , 则  $[K : \mathbb{C}] \neq 2$ . (否则  $K$  中有元素在  $\mathbb{C}$  上的最小多项式为 2 次, 与 (2) 矛盾.)
- (4) 奇数次多项式  $f(x) \in \mathbb{R}[x]$  必有实根. ( $f(-\infty) = -\infty, f(+\infty) = +\infty$ .)
- (5) 若有域扩张  $\mathbb{R} \subsetneq K$ , 则  $[K : \mathbb{R}]$  非奇数. (由 (4), 对任意  $\alpha \in K \setminus \mathbb{R}$ ,  $[\mathbb{R}(\alpha) : \mathbb{R}]$  为偶数.)

下面证明任意非常值多项式  $f(x) \in \mathbb{C}[x]$  有复根. 对  $f(x) = \sum a_i x^i \in \mathbb{C}[x]$ , 定义  $\bar{f}(x) = \sum \bar{a}_i x^i$ . 设  $f(x)\bar{f}(x) = \sum c_k x^k$ , 则  $c_k = \sum_{i+j=k} a_i \bar{a}_j$ , 由此可见  $\bar{c}_k = c_k$  即  $c_k \in \mathbb{R}$ , 因此  $f(x)\bar{f}(x) \in \mathbb{R}[x]$ . 由于  $f(x)$  有复根当且仅当  $f(x)\bar{f}(x)$  有复根, 只需证每个实多项式有复根.

设  $p(x) \in \mathbb{R}[x]$  不可约, 并设  $E/\mathbb{R}$  为  $(x^2 + 1)p(x)$  的分裂域, 则  $E \supset \mathbb{C}$ . 由  $\text{char}(R) = 0$  知  $E/\mathbb{R}$  为有限 Galois 扩张, 记  $G = \text{Gal}(E/\mathbb{R})$ . 若  $|G| = 2^m k$ , 其中  $k$  为奇数, 则由定理 4.6.2 (1),  $G$  有  $2^m$  阶子群  $H$ , 令  $B = E^H$ . 由注记 5.2.19,  $[B : \mathbb{R}] = [G : H] = k$ , 这与前述事实 (3) 矛盾. 故  $k = 1$  即  $G$  为 2-群. 假设  $E \supsetneq \mathbb{C}$ , 则  $\text{Gal}(E/\mathbb{C}) \leq G$  为非平凡 2-群, 由定理 4.5.55, 存在  $F \leq \text{Gal}(E/\mathbb{C})$  使得  $[\text{Gal}(E/\mathbb{C}) : F] = 2$ . 由注记 5.2.19,  $[E^F : \mathbb{C}] = 2$ , 这与前述事实 (3) 矛盾. 故  $E = \mathbb{C}$ , 即  $p(x)$  在  $\mathbb{C}$  中有根.  $\square$

## 5.3 根式扩张

**定义 5.3.1** 称域扩张  $E/k$  为  $m$  型根式扩张, 若  $E = k(\alpha)$ , 其中  $\alpha^m \in k$ , 这里  $m$  为正整数.

**定义 5.3.2** 称域扩张塔  $k = E_0 \subset E_1 \subset \cdots \subset E_n$  为根式扩张塔, 若每个  $E_{i+1}/E_i$  均为根式扩张.

**定义 5.3.3** 称  $f(x) \in k[x]$  为根式可解的, 若存在根式扩张塔  $k = E_0 \subset E_1 \subset \cdots \subset E_n$ , 使得  $f(x)$  在  $E_n$  中分裂, 即  $E_n \supset (k, f(x))$ .

**例 5.3.4** 设  $f(x) = x^2 + bx + c \in \mathbb{C}[x]$ ,  $k = \mathbb{Q}(b, c)$ ,  $E = k(\sqrt{b^2 - 4c})$ , 则  $E/k$  为 2-型根式扩张, 且  $E = (k, f(x))$ , 因此  $f(x)$  为根式可解的.

**讨论一** 当根式扩张不是 Galois 扩张时略显棘手, 我们先讨论如下情形. 设  $E = k(\alpha)$ ,  $\alpha^m = a \in k$ .

- ◊ 若  $k$  中有  $m$  次本原单位根  $\omega$ , 则由  $x^m - a = (x - \alpha)(x - \omega\alpha) \cdots (x - \omega^{m-1}\alpha)$  知  $E = (k, x^m - a)$  是  $k$  上可分多项式的分裂域, 因此  $E/k$  为 Galois 扩张, 且有群嵌入

$$\text{Gal}(E/k) \hookrightarrow (\mathbb{Z}_m, +), \quad \sigma_i \mapsto \bar{i},$$

其中  $\sigma_i(\alpha) = \alpha\omega^i$  ( $0 \leq i \leq m-1$ ), 因此  $\text{Gal}(E/k)$  为 Abel 群.

- ◊ 若  $\text{char}(k) = 0$ , 取  $E' = (E, x^m - 1)$ . 由定理 4.2.14,  $\text{Root}_{E'}(x^n - 1) \leqslant (E')^\times$  为循环群, 且由  $\text{char}(k) = 0$  知其阶恰为  $m$  (参考引理 3.3.25 的证明), 故  $E'$  中存在  $m$  次本原单位根  $\omega$ .

$$\begin{array}{ccc} k & \xrightarrow{\text{m型根式扩张}} & E = k(\alpha) \\ \downarrow x^{m-1} \text{的分裂域} & & \downarrow x^{m-1} \text{的分裂域} \\ k' = k(\omega) & \xrightarrow{\text{m型根式扩张}} & E' = k'(\alpha) \end{array}$$

由上一种情形知  $\text{Gal}(E'/k') \hookrightarrow (\mathbb{Z}_m, +)$  为 Abel 群. 而由  $k' = (k, x^m - 1)$  知  $\text{Gal}(k'/k) \hookrightarrow U(\mathbb{Z}_m)$  亦为 Abel 群. 注意到  $E' = (k, x^m - 1)$ , 因此  $E'/k$  为 Galois 扩张, 又  $k'/k$  亦为 Galois 扩张, 由命题 5.2.23 知  $\text{Gal}(E'/k') \triangleleft \text{Gal}(E'/k)$ , 且  $\text{Gal}(E'/k)/\text{Gal}(E'/k') \simeq \text{Gal}(k'/k)$ .

$$\begin{array}{ccccc} & & \text{Abel 群} & & \\ & \swarrow & & \searrow & \\ \text{Gal}(E'/k') & \xleftarrow{\text{正规子群}} & \text{Gal}(E'/k) & \longrightarrow & \text{Gal}(k'/k) \\ & & \uparrow & & \\ & & \{\sigma \in \text{Gal}(E'/k) : \sigma(E) = E\} & & \\ & & \downarrow & & \\ & & \text{Gal}(E/k) & & \end{array}$$

**讨论二** 我们再进行如下观察.

- ◊ 若  $\text{char}(k) = 0$ , 则从  $k$  出发的任何根式扩张塔  $k = E_0 \subset E_1 \subset \cdots \subset E_n$  均可扩充为新的根式扩张塔  $k = E_0 \subset E_1 \subset \cdots \subset E_n \subset \cdots \subset E_m$ , 使得  $E_m/E_0$  为 Galois 扩张.

**证明** 设  $E_n = k(\alpha_1, \dots, \alpha_l)$ , 其中  $\alpha_i$  在  $k$  上的最小多项式为  $f_i(x)$ . 令  $f(x) = f_1(x) \cdots f_l(x) \in k[x] \subset E_n[x]$ , 取  $K = (E_n, f(x))$ . 由根式扩张定义可知  $f(x)$  为  $E_n$  上的可分多项式, 因此  $K/E_n$  为 Galois 扩张, 设  $\text{Gal}(K/E_n) = \{\sigma_0 = \text{Id}_K, \sigma_1, \dots, \sigma_p\}$ , 则有根式扩张塔

$$\begin{aligned} k &\subset [E_n \subset E_n \vee \sigma_1(E_n)] \subset E_n \vee \sigma_1(E_n) \vee \sigma_2(E_n) \subset \cdots \\ &\subset E_n \vee \sigma_1(E_n) \vee \cdots \vee \sigma_p(E_n) = K =: E_m. \end{aligned}$$

以框中部分为例说明这是根式扩张:

$$[E_n] \stackrel{\textcircled{1}}{\subset} E_n \vee \sigma_1(E_1) \stackrel{\textcircled{2}}{\subset} E_n \vee \sigma_1(E_2) \subset \cdots \subset [E_n \vee \sigma_1(E_n)],$$

由  $k \subset E_1$  为根式扩张知 ① 为根式扩张, 由  $E_1 \subset E_2$  为根式扩张知 ② 为根式扩张, 以此类推. □

- ◊ 现假设  $k$  有充分多的单位根. 根据上一点, 可设根式扩张塔  $k = E_0 \subset \cdots \subset E_{n-1} \subset E_n$  满足  $E_n/k$  为 Galois 扩张, 且由于  $k$  有充分多的单位根, 根据讨论一的第一点, 每个  $E_i/E_{i-1}$  均为 Galois 扩张, 每个  $\text{Gal}(E_i/E_{i-1})$  均为 Abel 群. 结合定理 5.1.6 与命题 5.2.23 即得

$$\begin{array}{cccccccccc} \text{Gal}(E_n/E_0) & \triangleleft & \text{Gal}(E_n/E_1) & \triangleleft & \text{Gal}(E_n/E_2) & \triangleleft & \cdots & \triangleleft & \text{Gal}(E_n/E_{n-1}) \text{ 为 Abel 群} \\ \text{Gal}(E_1/E_0) \text{ 为 Abel 群} & & \text{Gal}(E_2/E_1) \text{ 为 Abel 群} & & & & & & \end{array}$$

若  $f(x)$  根式可解,  $(k, f(x)) \subset E_n$ , 则有满射  $\text{Gal}(E_n/k) \twoheadrightarrow \text{Gal}((k, f(x))/k) = \text{Gal}_k(f)$ .

◇ 下面解释上一点 “ $k$  有充分多的单位根” 这一技术性条件并不难达成. 设  $\text{char}(k) = 0$ , 且有根式扩张塔  $k = E_0 \subset \cdots \subset E_{n-1} \subset E_n$ , 其中  $E_n/k$  为 Galois 扩张. 设  $E_i/E_{i-1}$  为  $m_i$  型根式扩张 ( $1 \leq i \leq n$ ), 令  $M = \text{lcm}(m_1, \dots, m_n)$ , 取  $E' = (E, x^M - 1)$ . 同讨论一的第二点可知  $E'$  中存在  $M$  次本原单位根  $\omega$ , 进而  $E'$  中有  $m_1, \dots, m_n$  次本原单位根, 这就实现了“有充分多的单位根”.

$$\begin{array}{ccccc} & & \text{Abel 群} & & \\ & \swarrow & & \searrow & \\ \text{Gal}(E'_n/k') & \xleftarrow{\text{正规子群}} & \text{Gal}(E'_n/k) & \twoheadrightarrow & \text{Gal}(k'/k) \\ & & \downarrow * & & \\ & & \text{Gal}(E_n/k) = \text{Gal}_k(f) & & \end{array}$$

\* 处满射得自  $E_n/k$  为 Galois 扩张, 由命题 5.1.7,  $\sigma(E_n) = E_n, \forall \sigma \in \text{Gal}(E'_n/k)$ .

**定义 5.3.5** 设  $G$  为群, 若存在正规列  $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1_G\}$  使得每个子商均为 Abel 群, 则称  $G$  为可解群.

**例 5.3.6** (1) 若  $G_1 \triangleleft G$ ,  $G_1$  与  $G/G_1$  均为 Abel 群, 则  $G$  为可解群, 因为  $G \supset G_1 \supset \{1_G\}$ .

(2) Abel 群  $G$  是可解群, 因为  $G \supset \{1_G\}$ .

(3) 若  $G$  是可解群, 则  $H \leq G$  也是可解群.

**证明** 由  $G$  是可解群, 存在正规列  $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1_G\}$ , 使得每个子商均为 Abel 群, 由定理 4.3.23 (2) 知  $H \supset H \cap G_1 \supset H \cap G_2 \supset \cdots \supset H \cap G_n$  是正规列, 且每个子商均为 Abel 群.  $\square$

(4) 设  $N \triangleleft G$ , 则  $G$  是可解群当且仅当  $N$  与  $G/N$  均为可解群. 故可解群的子群和商群均为可解群.

**证明** ( $\Rightarrow$ ) 由 (3), 仅需证  $G/N$  为可解群. 由  $G$  是可解群, 存在正规列  $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1_G\}$ , 使得每个子商均为 Abel 群. 由  $N \triangleleft G$  可得正规列  $G/N \supset G_1N/N \supset G_2N/N \supset \cdots \supset G_nN/N$ , 且由定理 4.3.22,  $(G_iN/N)/(G_{i+1}N/N) \cong G_iN/G_{i+1}N$  为 Abel 群.

( $\Leftarrow$ ) 设正规列  $G/N = G^* = G_0^* \supset G_1^* \supset \cdots \supset G_n^* = \{1_{G^*}\}$  满足每个子商均为 Abel 群, 由定理 4.3.21, 存在正规列  $G = G_0 \supset G_1 \supset \cdots \supset G_m = N$  满足每个子商均为 Abel 群. 由于  $N$  是可解群, 存在正规列  $H = H_0 \supset H_1 \supset \cdots \supset H_m = \{1_H\}$  满足每个子商均为 Abel 群. 将这两个正规列相接即得  $G$  为可解群.  $\square$

(5)  $p$ -群  $G$  是可解群.

**证明** 对  $|G|$  归纳. 若  $|G| \neq 1$ , 由命题 4.5.53,  $Z(G) \neq \{1_G\}$ . 若  $Z(G) = G$ , 则  $G$  是 Abel 群, 由 (2) 知  $G$  是可解群. 若  $Z(G) \neq G$ , 则  $G/Z(G)$  是阶  $< |G|$  的  $p$  群, 由归纳假设知其为可解群. 由于  $Z(G) \triangleleft G$ ,  $Z(G)$  与  $G/Z(G)$  均为可解群, 由 (4) 即得  $G$  为可解群.  $\square$

(6)  $S_3$  是可解群, 因为  $S_3 \supset A_3 \supset \{\text{Id}\}$ .

(7)  $S_4$  是可解群, 因为  $S_4 \supset A_4 \supset K_4 \supset \{\text{Id}\}$  (例 4.4.33).

(8)  $S_n$  ( $n \geq 5$ ) 不是可解群, 否则由 (3),  $A_n \triangleleft S_n$  亦为可解群, 但由定理 4.4.36,  $A_n$  ( $n \geq 5$ ) 是单群, 而  $A_n$  非 Abel 群, 矛盾.

**引理 5.3.7** 设  $A$  为 Abel 群, 素数  $p \mid |A|$ , 则存在  $A' \leq A$  使得  $A/A' \simeq C_p$ .

**证明** 由练习 4.8.37, 存在  $A' \leq A$  使得  $|A/A'| = p$ , 再由推论 4.2.12 即得证.  $\square$

**引理 5.3.8** 设  $K/k$  为有限 Galois 扩张,  $\text{Gal}(K/k) \simeq C_p = (\sigma)$ , 其中  $p$  为素数. 若  $k$  中有  $p$  次本原单位根, 则  $K/k$  为  $p$  型根式扩张.

**证明** 如练习 3.1.7,  $\sigma : K \rightarrow K$  可视为  $k$ -线性自同构. 由  $(\sigma) = C_p$  可知  $x^p - 1$  是  $\sigma$  的最小多项式, 而  $[K : k] = |\text{Gal}(K/k)| = p$ , 因此  $x^p - 1$  是  $\sigma$  的特征多项式. 由于  $p$  次本原单位根  $\omega \in k$  满足  $\omega^p - 1 = 0$ , 因此  $\omega$  是  $\sigma$  的特征值, 设  $\beta$  是  $\omega$  对应的特征向量, 则  $\sigma(\beta) = \omega\beta$ , 因此  $\beta \notin k$  且  $\sigma(\beta^p) = [\sigma(\beta)]^p = (\omega\beta)^p = \beta^p$ , 由命题 5.1.7 即知  $\beta^p \in k$ . 考虑域扩张塔  $k \subsetneq k(\beta) \subset K$ , 由定理 3.2.4,  $[k(\beta) : k] \mid [K : k]$ , 而  $[k(\beta) : k] > 1$ ,  $[K : k] = p$ , 因此  $K = k(\beta)$ . 故  $K/k$  为  $p$  型根式扩张.  $\square$

**定理 5.3.9 (Galois 大定理)** 设  $k$  为域,  $\text{char}(k) = 0$ ,  $f(x) \in k[x]$ , 则  $f(x)$  根式可解当且仅当  $\text{Gal}_k(f)$  为可解群.

**证明** ( $\Rightarrow$ ) 在前面讨论二的第二点中已经看到, 若  $f(x)$  根式可解, 则  $\text{Gal}(E'_n/k)$  的正规子群  $\text{Gal}(E'_n/k')$  与相应的商群  $\text{Gal}(k'/k)$  均为 Abel 群, 从而为可解群, 由例 5.3.6 (4) 知  $\text{Gal}(E'_n/k)$  为可解群. 而  $\text{Gal}_k(f)$  同构于可解群  $\text{Gal}(E'_n/k)$  的商群, 由例 5.3.6 (4) 即知  $\text{Gal}_k(f)$  为可解群.

( $\Leftarrow$ ) 若  $G = \text{Gal}_k(f)$  为可解群, 取  $G_1 \trianglelefteq G$  使得  $G/G_1$  为 Abel 群. 设素数  $p \mid |G|$ , 则由引理 5.3.7, 存在  $G/G_1$  的子群  $H/G_1$ , 使得  $(G/G_1)/(H/G_1) \simeq C_p$ , 进而由定理 4.3.22 知  $H \triangleleft G$  且  $G/H \simeq C_p$ . 令  $K = (k, f(x))$ , 由于  $\text{Gal}(K/K^H) = H \triangleleft G$ , 由命题 5.2.23,  $K^H/k$  为 Galois 扩张, 且  $\text{Gal}(K^H/k) \simeq G/H \simeq C_p$ . 而由例 5.3.6 (4),  $\text{Gal}(K/K^H) = H \triangleleft G$  为可解群, 如上操作可得  $H' \triangleleft H$ , 使得  $H/H' \simeq C_{p'}$ , 其中  $p' \mid |H|$  为素数.

$$\begin{array}{ccccccc} k & \xrightarrow{\text{Galois 扩张}} & K^H & \xrightarrow{\text{Galois 扩张}} & K^{H'} & \cdots & \xrightarrow{\text{如前}} K \\ \parallel & & \parallel & & \parallel & & \nearrow \\ E_0 & \xrightarrow{\text{Gal}(E_1/E_0) \simeq C_p} & E_1 & \xrightarrow{\text{Gal}(E_2/E_1) \simeq C_{p'}} & E_2 & \cdots & \end{array}$$

- ◊ 若  $k$  有  $|G|$  次本原单位根 (存在性由  $\text{char}(k) = 0$  确保), 则对任意素数  $p \mid |G|$ ,  $k$  亦有  $p$  次本原单位根. 由引理 5.3.8, 上图中每个  $E_{i+1}/E_i$  均为根式扩张, 最终便得到根式扩张塔  $k = E_0 \subset E_1 \subset E_2 \subset \cdots \subset K = (k, f(x))$ , 即  $f(x)$  根式可解.
- ◊ 对于一般情形, 记  $\omega$  为  $|G|$  次本原单位根, 令  $k^* = k(\omega)$ ,  $K^* = K(\omega)$ , 其中  $\omega$  为  $|G|$  次本原单位根. 由  $K = (k, f(x))$  知  $K^* = (k, (x^{|G|} - 1)f(x))$ , 因此  $K^*/k$  为 Galois 扩张, 进而  $K^*/k^*$  亦为 Galois 扩张. 令  $G^* = \text{Gal}(K^*/k^*)$ , 考虑群同态的复合

$$\rho : G^* = \text{Gal}(K^*/k^*) \hookrightarrow \text{Gal}(K^*/k) \twoheadrightarrow G = \text{Gal}(K/k),$$

其中第二个箭头的良定性来自命题 5.1.7: 由于  $K^*/k$  为 Galois 扩张,  $K/k$  亦为 Galois 扩张, 因此  $\sigma(K) = K, \forall \sigma \in \text{Gal}(K^*/k)$ . 由于

$$\begin{aligned} \text{Ker } \rho &= \{\sigma \in \text{Aut}(K^*) : \sigma|_K = \text{Id}_K, \sigma|_{k^*} = \text{Id}_{k^*}\} \\ &= \{\sigma \in \text{Aut}(K^*) : \sigma|_K = \text{Id}_K, \sigma|_{k^*} = \text{Id}_{k^*}, \sigma(\omega) = \omega\} \\ &= \{\sigma \in \text{Aut}(K^*) : \sigma|_{K(\omega)} = \text{Id}_{K(\omega)}\} = \{\text{Id}_{K^*}\}, \end{aligned}$$

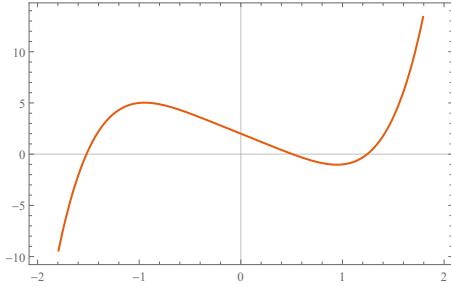
由定理 4.3.16,  $G^*$  同构于可解群  $G$  的子群, 由例 5.3.6 (3),  $G^*$  为可解群. 由于  $|G^*| \mid |G|$ ,  $k^*$  中有

$|G^*|$  次本原单位根, 根据上一类情形, 结合  $k^*/k$  为根式扩张, 可得根式扩张塔

$$k \subset k^* = E_0^* \subset E_1^* \subset E_2^* \subset \cdots \subset K^*.$$

由于  $K^* \supset K = (k, f(x))$ ,  $f(x)$  根式可解.  $\square$

**例 5.3.10** 考虑  $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ , 易知  $f(x)$  有 3 个实根, 2 个虚根.



记  $\text{Root}_{\mathbb{C}}(f) = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ , 其中  $\alpha_1, \alpha_2 \notin \mathbb{R}$ . 由练习 4.5.8 可得群的单同态  $\theta : \text{Gal}_{\mathbb{Q}}(f) \hookrightarrow S_5$ . 由于  $f$  恰有 2 个虚根, 复共轭  $\sigma \in \text{Gal}_{\mathbb{Q}}(f)$ , 因此  $(12) \in \text{Im } \theta$ . 由 Eisenstein 判别法知  $f(x) \in \mathbb{Q}[x]$  不可约, 因此  $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \deg(f) = 5$ , 从而由定理 3.2.4 与定义-定理 5.1.2 (2) 知  $5 \mid [(\mathbb{Q}, f) : \mathbb{Q}] = |\text{Gal}_{\mathbb{Q}}(f)|$ . 由定理 4.6.11 即知  $\text{Gal}_{\mathbb{Q}}(f)$  中有 5 阶元, 即  $\text{Im } \theta$  中有 5 轮换. 故由练习 5.3.11 知  $\text{Im } \theta = S_5$ , 即  $\text{Gal}_{\mathbb{Q}}(f) \cong S_5$  非可解群.

**练习 5.3.11** 设  $p$  为素数, 则  $S_p$  可由 (12) 与任一  $p$ -轮换生成.

**证明** 这等价于证明  $S_p$  可由  $\tau = (1a)$  与  $c = (12 \cdots p)$  生成, 其中  $a \in \{2, \dots, p\}$ . 首先, 由引理 4.4.12,

$$c\tau c^{-1} = (c(1)c(a)) = (2, a+1) \quad (\text{这里 } a+1 \text{ 在模 } p \text{ 意义下考虑}),$$

重复此操作可得所有形如  $(k, k+a)$  的对换, 因此可以生成  $(p, a), (a, 2a), (2a, 3a), \dots, ((a^{-1}-1)a, 1)$ , 这里  $a^{-1}$  在模  $p$  意义下考虑. 再次利用引理 4.4.12 可得

$$\begin{aligned} (a, 2a)(p, a)(a, 2a) &= (p, 2a), \\ (2a, 3a)(p, 2a)(2a, 3a) &= (p, 3a), \\ &\vdots \\ ((a^{-1}-1)a, 1)(p, (a^{-1}-1)a)((a^{-1}-1)a, 1) &= (p, 1), \\ c(p, 1)c^{-1} &= (c(p)c(1)) = (12), \\ c(12)c^{-1} &= (c(1)c(2)) = (23), \\ &\vdots \\ c(p-2, p-1)c^{-1} &= (c(p-2)c(p-1)) = (p-1, p). \end{aligned}$$

由引理 4.4.27,  $(12), (23), \dots, (p-1, p)$  可生成  $S_p$ .  $\square$

**定理 5.3.12 (Abel-Ruffini)** 考虑域  $k$  上的  $n$  元有理函数域  $F = k(t_1, \dots, t_n)$ , 则多项式

$$f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} + \cdots + (-1)^n t_n \in F[x]$$

不可约, 且  $\text{Gal}_F(f) \simeq S_n$ . 特别地, 当  $n \geq 5$  时  $f$  无法用根式求解.

**注记 5.3.13** 这里取系数  $t_1, \dots, t_n$  为独立变元, 意蕴在于考虑  $F$  上“一般的” $n$  次首一多项式. 在这个意义上, “一般的”五次以上多项式方程无根式解.

**证明** 考虑  $n$  元多项式环  $k[x_1, \dots, x_n]$ , 其上有左  $S_n$ -作用:  $(\sigma, f) \mapsto f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ . 由 Vieta 定理,  $n$  元初等对称多项式

$$e_k := \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \cdots x_{i_k}, \quad 1 \leq k \leq n$$

由

$$\prod_{i=1}^n (X - x_i) = X^n - e_1 X^{n-1} + \cdots + (-1)^n e_n$$

刻画, 这里  $X$  为变元. 对称多项式基本定理给出同构

$$F = k(t_1, \dots, t_n) \xrightarrow{\sim} k(x_1, \dots, x_n)^{S_n} = k(e_1, \dots, e_n), \quad t_i \mapsto e_i.$$

借此视  $k(x_1, \dots, x_n)$  为  $k(t_1, \dots, t_n)$  的扩张. 由  $k(x_1, \dots, x_n)^{S_n} = F$  及定义-定理 5.1.2(1) 知  $k(x_1, \dots, x_n)/F$  为 Galois 扩张, Galois 群实现为  $S_n$  在  $\{x_1, \dots, x_n\}$  上的自然作用. 而  $\{x_1, \dots, x_n\}$  恰为  $f$  的根集, 因此  $k(x_1, \dots, x_n)$  是  $f$  的分裂域,  $\text{Gal}_F(f) \simeq S_n$ , 再结合引理 4.5.22 即知  $f$  不可约. 当  $n \geq 5$  时, 由例 5.3.6(8) 知  $f$  无法用根式求解.  $\square$

## 5.4 判别式

**定义 5.4.1** 设  $\text{char}(k) = 0$ ,  $f(x) \in k[x]$ ,  $\deg(f) = n$ . 若  $f(x)$  在  $K = (k, f(x))$  上分裂为

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n),$$

定义其判别式

$$D(f) = \Delta^2 := \left( \prod_{i < j} (\alpha_i - \alpha_j) \right)^2 \in k.$$

**注记 5.4.2** (1)  $D(f) = \frac{(-1)^{\frac{n(n-1)}{2}}}{c} \text{Res}(f, f')$ .

(2)  $D(f) \neq 0 \iff f$  无重根.

**例 5.4.3** 若  $f(x) = ax^2 + bx + c$  ( $a \neq 0$ ), 则  $D(f) = -\frac{1}{a} \begin{vmatrix} a & b & c \\ 2a & b & \\ & 2a & b \end{vmatrix}^2 = b^2 - 4ac$ .

**例 5.4.4** 若  $f(x) = x^3 + qx + r$ , 则

$$D(f) = - \begin{vmatrix} 1 & 0 & q & r \\ & 1 & 0 & q & r \\ 3 & 0 & q & \\ & 3 & 0 & q \\ & & 3 & 0 & q \end{vmatrix} = -4q^3 - 27r^2.$$

**引理 5.4.5** 设  $f(x) \in \mathbb{Q}[x]$  无重根,  $\deg(f) = n$ ,  $E = (\mathbb{Q}, f(x))$ ,  $G = \text{Gal}(E/\mathbb{Q})$ , 由练习 4.5.8,  $G \hookrightarrow S_n$ . 令  $H = G \cap A_n$ , 由定理 4.3.23 (2),  $H \triangleleft G$  且  $G/H \hookrightarrow S_n/A_n \cong C_2$ . 我们有以下结论:

- (1)  $E^H = \mathbb{Q}(\Delta)$ , 这里  $\Delta = \sqrt{D}$ .
- (2)  $\Delta = \sqrt{D} \in \mathbb{Q}$  当且仅当  $H = G$  (即  $G \hookrightarrow A_n$ ,  $G$  中元素均为偶置换).

**证明** 对任意  $\sigma \in S_n$ ,  $\sigma(\Delta) = \text{sgn}(\sigma)\Delta$ , 而  $H \leqslant A_n$ , 因此  $\Delta \in E^H$ , 进而  $\mathbb{Q}(\Delta) \subset E^H$ ,  $[E^H : \mathbb{Q}] = [G : H] \leqslant 2$ .

- ◊ 若  $[G : H] = 1$ , 则  $G = H$ ,  $\mathbb{Q}(\Delta) \subset E^H = E^G = \mathbb{Q}$ , 因此  $\Delta \in \mathbb{Q}$ ,  $E^H = \mathbb{Q}(\Delta)$ .
- ◊ 若  $[G : H] = 2$ , 则存在  $\sigma \in G \setminus A_n$ , 使得  $\sigma(\Delta) = -\Delta$ . 由  $\sigma|_{\mathbb{Q}} = \text{Id}_{\mathbb{Q}}$  即知  $\Delta \notin \mathbb{Q}$ , 考虑  $\mathbb{Q} \subsetneq \mathbb{Q}(\Delta) \subset E^H$ , 由  $[E^H : \mathbb{Q}] \leqslant 2$  与  $[\mathbb{Q}(\Delta) : \mathbb{Q}] \geqslant 2$  即知  $E^H = \mathbb{Q}(\Delta)$ .  $\square$

**定理 5.4.6** 设  $f(x) \in \mathbb{Q}[x]$  不可约,  $\deg(f) = 3$ ,  $G = \text{Gal}_{\mathbb{Q}}(f)$ ,  $D = D(f) \neq 0$ , 则

- (1)  $f(x)$  恰有 1 个实根当且仅当  $D(f) < 0$ , 此时  $G \cong S_3$ .
- (2)  $f(x)$  恰有 3 个实根当且仅当  $D(f) > 0$ , 此时若  $\sqrt{D} \in \mathbb{Q}$ , 则  $G \cong A_3 \cong \mathbb{Z}_3$ , 若  $\sqrt{D} \notin \mathbb{Q}$ , 则  $G \cong S_3$ .

**证明** 令  $E = (\mathbb{Q}, f(x))$ . 由  $f(x) \in \mathbb{Q}[x]$  不可约即知  $D \neq 0$ . 由练习 4.5.8,  $G \hookrightarrow S_3$ , 再设  $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ , 则由  $\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset E$  可知  $3 = \deg(f) = [\mathbb{Q}(\alpha_1) : \mathbb{Q}] \mid [E : \mathbb{Q}] = |G|$ , 因此  $G \cong A_3$  或  $S_3$ .

- (1) 若  $f(x)$  恰有 1 个实根  $\alpha$  与两个虚根  $\beta = u + iv, \bar{\beta} = u - iv$ , 则

$$\Delta = (\alpha - \beta)(\alpha - \bar{\beta})(\beta - \bar{\beta}) = (\alpha - \beta)(\overline{\alpha - \beta})(\beta - \bar{\beta}) = 2iv|\alpha - \beta|^2,$$

从而  $D = \Delta^2 = -4v^2|\alpha - \beta|^4 < 0$ . 此时  $E \neq \mathbb{Q}(\alpha)$ , 因此  $|G| > 3$ , 即  $G \cong S_3$ .

- (2) 若  $f(x)$  有 3 个实根, 则  $\Delta \in \mathbb{R}$ , 从而  $D = \Delta^2 > 0$ ,  $\sqrt{D} \in \mathbb{R}$ . 由引理 5.4.5, 若  $\sqrt{D} \in \mathbb{Q}$ , 则  $G \hookrightarrow A_3$ , 即  $G \cong A_3 \cong \mathbb{Z}_3$ ; 若  $\sqrt{D} \notin \mathbb{Q}$ , 则  $G \cong S_3$ .  $\square$

**例 5.4.7** (1)  $\text{Gal}_{\mathbb{Q}}(x^3 - 2) \cong S_3$ .

(2)  $\text{Gal}_{\mathbb{Q}}(x^3 - 4x + 2) \cong S_3$ .

(3)  $\text{Gal}_{\mathbb{Q}}(x^3 - x + \frac{1}{3}) \cong A_3 \cong \mathbb{Z}_3$ .

## 第二部分

## 往年真题



## 第六章 期中考试题目

### 6.1 2020 春期中考试

1. 考虑 Gauss 整数环  $R = \mathbb{Z}[i]$ .

- (1) 设  $p$  为奇素数. 试证明:  $x^n - p \in R[x]$  总是不可约的.
- (2) 在  $R$  中将  $81 + 8i$  分解为不可约元的乘积.
- (3) 求不定方程  $x^2 + y^2 = 585$  的所有整数解.
- (4) 考虑商环  $R_1 = R/(3)$  以及  $R_2 = R/(5)$ . 计算  $\text{Aut}(R_1)$  与  $\text{Aut}(R_2)$  的阶.

2. 考虑多项式环  $\mathbb{Q}[x]$ , 设  $S$  为其包含  $\mathbb{Q}$  以及  $x^2, x^3$  的最小子环.

- (1) 证明:  $S \simeq \mathbb{Q}[y, z]/(y^2 - z^3)$ .
- (2) 证明:  $S \not\simeq \mathbb{Q}[x]$ .
- (3) 证明:  $\text{Frac}(S) \simeq \mathbb{Q}(x)$ .

3. 设  $E$  为  $f(x) = x^4 - 2 \in \mathbb{Q}[x]$  在  $\mathbb{Q}$  上的分裂域.

- (1) 计算  $[E : \mathbb{Q}]$ .
- (2) 列出  $\text{Aut}(E)$  中的元素.
- (3) 设  $K = \mathbb{Q}(\sqrt[4]{2})$ . 试给出  $\text{Aut}(K)$  中的元素, 并给出  $K$  的所有非平凡子域.
- (4) 设  $u = \sqrt[4]{2} + i$ . 试求  $u$  在  $\mathbb{Q}$  上的最小多项式.

4. 设  $(R, \phi)$  的 Euclid 整环,  $a \in R$  是  $R$  中所有非零非单位元素中  $\phi(a)$  取值最小的.

- (1) 试证明:  $R/(a) = \{\bar{r} : r = 0 \text{ 或 } r \in U(R)\}$ , 这里  $\bar{r} = r + (a)$  表示其模  $(a)$  同余类.
- (2) 试证明:  $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$  不是 Euclid 整环.

## 6.2 2022 春期中考试

1. 设  $R = \mathbb{Z}[\mathbf{i}]$ ,  $K = \mathbb{Q}(\mathbf{i})$ , 域扩张  $E/K$  使得  $E$  为  $x^4 + x^3 + x^2 + x + 1 \in K[x]$  的分裂域.

- (1) 证明:  $K \simeq \text{Frac}(R)$ .
- (2) 列出  $R$  的所有子环, 并指出哪些是 UFD.
- (3) 在  $R$  中计算  $\gcd(4 + 7\mathbf{i}, 4 - 3\mathbf{i})$ .
- (4) 计算商环  $R/(4 + 7\mathbf{i}, 4 - 3\mathbf{i})$  的阶.
- (5) 分类商环  $R/(4 - 3\mathbf{i})$  的所有理想, 并指出哪些是素理想.
- (6) 判断并论证  $x^4 + x^3 + x^2 + x + 1 \in K[x]$  的可约性.
- (7) 计算  $[E : \mathbb{Q}]$ .
- (8) 判断并论证  $\text{Aut}(E)$  是否为 Abel 群.

**解答** (1) 由  $R \subset \mathbb{Q}(\mathbf{i}) \subset \text{Frac}(R)$  再取分式域即得  $K \simeq \text{Frac}(R)$ .

- (2) 由练习 2.2.34,  $R$  的子环恰为  $\mathbb{Z}$  和  $\mathbb{Z}[n\mathbf{i}]$ , 其中  $n$  为正整数. 由于  $\mathbb{Z}$  与  $\mathbb{Z}[\mathbf{i}]$  均为 ED, 它们都是 UFD. 对  $n \geq 2$ , 注意到  $\text{Frac}(\mathbb{Z}[n\mathbf{i}]) = \mathbb{Q}(\mathbf{i})$ ,  $\mathbf{i} \in \mathbb{Q}(\mathbf{i})$  是首一整系数方程  $x^2 + 1 = 0$  的解, 但  $\mathbf{i} \notin \mathbb{Z}[n\mathbf{i}]$ , 由命题 2.5.16, UFD 是整闭环, 因此  $\mathbb{Z}[n\mathbf{i}] (n \geq 2)$  不是 UFD.
- (3) 有素分解  $4 + 7\mathbf{i} = -(1 - 2\mathbf{i})(2 - 3\mathbf{i})$ ,  $4 - 3\mathbf{i} = \mathbf{i}(1 - 2\mathbf{i})^2$ , 因此  $\gcd(4 + 7\mathbf{i}, 4 - 3\mathbf{i})$  相伴于  $1 - 2\mathbf{i}$ .
- (4) 由 (3),  $R/(4 + 7\mathbf{i}, 4 - 3\mathbf{i}) = R/(1 - 2\mathbf{i})$ . 由练习 2.6.26,  $R/(1 - 2\mathbf{i}) \simeq \mathbb{F}_5$ , 故其阶为 5.
- (5) 由例 2.2.27 对应定理,  $\{R/(4 - 3\mathbf{i}) \text{ 的理想}\} \xleftrightarrow{1:1} R$  中包含  $(4 - 3\mathbf{i})$  的理想, 而  $R$  为 PID, 若  $(4 - 3\mathbf{i}) \subset (a)$ , 则  $a \mid (4 - 3\mathbf{i})$ . 由素分解  $4 - 3\mathbf{i} = \mathbf{i}(1 - 2\mathbf{i})^2$  即知  $R$  中包含  $(4 - 3\mathbf{i})$  的理想恰为  $(\mathbf{i}) = R, (1 - 2\mathbf{i}), (4 - 3\mathbf{i})$ . 故  $R/(4 - 3\mathbf{i})$  的理想恰为  $R/(4 - 3\mathbf{i}), (1 - 2\mathbf{i})/(4 - 3\mathbf{i}), \{0\}$ . 由练习 2.3.35 (3), 其中素理想为  $(1 - 2\mathbf{i})/(4 - 3\mathbf{i})$ .
- (6) 由练习 2.7.46 (2) 与命题 2.7.34, 等价于判定

$$(x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1 = x^4 + 5x^3 + 10x^2 + 5x \in R[x]$$

的可约性. 利用 Gauss 素数  $1 - 2\mathbf{i}$  的 Eisenstein 判别法即知其不可约.

- (7) 由于  $E = K(\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4) = K(\zeta_5)$ , 由定理 3.1.23 (1),  $[E : K] = 4$ . 由定理 3.2.4,  $[E : \mathbb{Q}] = [E : K][K : \mathbb{Q}] = 4 \cdot 2 = 8$ .
- (8)  $E = \mathbb{Q}(\mathbf{i}, \zeta_5) = \mathbb{Q}(\zeta_{\text{lcm}(4, 5)}) = \mathbb{Q}(\zeta_{20})$ . 由定理 3.5.21,  $\text{Aut}(E) = \text{Aut}(\mathbb{Q}(\zeta_{20})) \simeq U(\mathbb{Z}_{20})$  是 Abel 群.  
□

2. 考虑八元域  $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + \bar{1})$ , 记  $u = \bar{x}$ . 于是  $\mathbb{F}_8$  中元素均形如  $a + bu + cu^2$ , 其中  $a, b, c \in \mathbb{F}_2$ . 自然视  $\mathbb{F}_2$  为  $\mathbb{F}_8$  的子域.

- (1) 分类  $\mathbb{F}_8$  的所有子环.
- (2)  $\mathbb{F}_8$  中共有多少个首一 2 次不可约多项式?
- (3) 将多项式  $x^3 + x + \bar{1}$  在  $\mathbb{F}_8[x]$  中进行不可约分解.
- (4) 将多项式  $x^{16} + x$  在  $\mathbb{F}_8[x]$  中进行不可约分解.
- (5) 计算  $(u^2 + \bar{1})^{-1}$ .

(6) 考虑商环  $R = \mathbb{F}_2[y]/(y^3 + y^2 + \bar{1})$ , 论证并具体构造环同构  $R \simeq \mathbb{F}_8$ .

**解答** (1) 由练习 2.1.26,  $\mathbb{F}_8$  的子环即  $\mathbb{F}_8$  的子域. 由命题 3.4.10,  $\mathbb{F}_8$  的子域即  $\mathbb{F}_2$  与  $\mathbb{F}_8$ .

(2)  $\mathbb{F}_8[x]$  中首一 2 次多项式共有  $8 \cdot 8 = 64$  个, 其中可约多项式形如  $(x - \alpha)(x - \beta)$ , 共有  $\binom{8}{2} + 8 = 36$  个. 因此  $\mathbb{F}_8$  中首一不可约 2 次多项式共有  $64 - 36 = 28$  个.

(3) 由于  $u$  是根, 由命题 3.4.15,  $x^3 + x + \bar{1} = (x - u)(x - u^2)(x - u^4) = (x + u)(x + u^2)(x + u^2 + u)$ .

(4)

(5) 待定系数得  $u(u^2 + \bar{1}) = \bar{1} \implies (u^2 + \bar{1})^{-1} = u$ .

(6) 由于  $y^3 + y^2 + \bar{1} \in \mathbb{F}_2[y]$  不可约, 因此  $E$  是八元域. 记  $v = \bar{y}$ , 则  $R = \mathbb{F}_2(v)$ . 设  $\theta : R \rightarrow \mathbb{F}_8$  为环同态, 则  $\theta$  由  $\theta(v)$  唯一决定. 由于  $v \in R$  是  $x^3 + x^2 + \bar{1} \in R[x]$  的根, 因此  $\theta(v) \in \mathbb{F}_8$  是  $x^3 + x^2 + \bar{1}$  的根, 从而  $\theta(v) = u + \bar{1}$  或  $u^2 + \bar{1}$  或  $u^2 + u + \bar{1}$ . 考虑赋值同态

$$\text{ev}_{u+\bar{1}} : \mathbb{F}_2[y] \rightarrow \mathbb{F}_8, \quad f(y) \mapsto f(u + \bar{1}).$$

由于  $(y^3 + y^2 + \bar{1}) \subset \text{Ker}(\text{ev}_{u+\bar{1}})$ . 因此  $\text{ev}_{u+\bar{1}}$  诱导环嵌入  $\theta : R \hookrightarrow \mathbb{F}_8$  使得  $v \mapsto u + \bar{1}$ . 又因为  $|R| = |\mathbb{F}_8|$ ,  $\theta$  为环同构.  $\square$

3. 设  $K = \mathbb{Q}(t)$ ,  $E = \mathbb{Q}(t^4)$  为  $K$  中包含  $t^4$  的最小子域.

- (1) 证明  $E \simeq K$ .
- (2) 计算  $[K : E]$ .
- (3) 计算  $\text{Aut}(K/E)$  的阶.
- (4) 判断并论证  $\mathbb{Q}(t^2)$  上的任何自同构是否均可延拓为  $K$  上的自同构.

4. 设  $R$  为整环, 记  $R^\times = R \setminus \{0_R\}$ . 试证明以下等价:

- (1) 环  $R$  为 PID.
- (2) 存在映射  $\phi : R^\times \rightarrow \mathbb{N}$  满足如下条件: 对任意  $a, b \in R^\times$ , 要么  $b \mid a$ , 要么存在适当的  $\delta, \gamma \in R$  使得  $\phi(a\delta - b\gamma) < \phi(b)$ . (注: 两种情况可能同时发生.)

## 6.3 2023 春期中考试

1. 设  $R = \mathbb{Z}[i]$ ,  $S = \mathbb{Z}[2i]$ ,  $K = \mathbb{Q}(i)$ .

- (1) 求不定方程  $x^2 + y^2 = 325$  的所有整数解.
- (2) 在  $R$  中计算  $\text{gcd}(9 + 2i, 15 - 20i)$ .
- (3) 判定并论证  $x^4 - 2 \in K[x]$  的可约性.
- (4) 分类商环  $R/5R$  的所有子环与所有理想. 这里  $5R$  表示元素 5 在  $R$  中生成的主理想.
- (5) 计算  $\text{Aut}(R/5R)$  的阶.
- (6) 计算商环  $S/(3 + 2i)$  的阶, 判定其是否为域.
- (7) 判断商环  $S/2S$ ,  $\mathbb{Z}_4$  与  $\mathbb{F}_2[y]/(y^2 + \bar{1})$  三者之间是否有环同构.
- (8) 判断整环  $S$  是否为 UFD.

**解答** (1)  $(\pm 1, \pm 18), (\pm 6, \pm 17), (\pm 10, \pm 15)$ .

(2) 有素分解  $9 + 2i = (1 - 2i)(1 + 4i)$ ,  $15 - 20i = -5(1 + 2i)^2$ , 因此  $\gcd(9 + 2i, 15 - 20i)$  相伴于 1.

(3) 由于  $K = \text{Frac}(R)$ ,  $x^4 - 2 \in K[x]$  本原, 由命题 2.7.34, 这等价于判断  $x^4 - 2 \in R[x]$  的可约性.

**(法一)** 由于  $x^4 - 2$  在  $R$  中无根, 若它可约, 只能分解为两个 2 次多项式乘积, 设为  $x^4 - 2 = (x^2 + ax + b)(x^2 + cx + d)$ , 其中  $a, b, c, d \in \mathbb{Z}[i]$ . 整理得

$$\begin{cases} a + c = 0, \\ b + ac + d = 0, \\ ad + bc = 0, \\ bd = 2. \end{cases} \implies \begin{cases} c = -a, \\ a^2 = b + d, \\ a(d - b) = 0, \\ bd = 2. \end{cases}$$

若  $a = 0$ , 则  $d = -b, b^2 = -2$ , 无解; 若  $a \neq 0$ , 则  $b = d, b^2 = 2$ , 无解. 故  $x^4 - 2 \in R[x]$  不可约, 从而在  $K[x]$  中也不可约.

**(法二)** 由练习 2.6.26,  $R/(1+2i) \simeq \mathbb{F}_5$ . 由模  $p$  约化, 为证  $x^4 - 2 \in R[x]$  不可约, 只需证  $x^4 - \bar{2} \in \mathbb{F}_5[x]$  不可约. 再由命题 3.4.8, 只需证  $\gcd_{\mathbb{F}_5[x]}(x^{5^2} - x, x^4 - \bar{2}) = \bar{1}$ , 这来自

$$\begin{aligned} (x^4 - \bar{2}, x^{25} - x) &= (x^4 - \bar{2}, \bar{2}x^{21} - x) = (x^4 - \bar{2}, \bar{4}x^{17} - x) = (x^4 - \bar{2}, \bar{3}x^{13} - x) \\ &= (x^4 - \bar{2}, x^9 - x) = (x^4 - \bar{2}, \bar{2}x^5 - \bar{2}) = (x^4 - \bar{2}, \bar{4}x - \bar{2}) \\ &= (x^4 - \bar{2}, x + \bar{2}) = \bar{1}. \end{aligned}$$

(4) ① 由练习 2.2.30,  $\{R/5R\}$  的子环  $\xleftarrow{1:1} \{R\}$  中包含  $5R$  的子环, 而由练习 2.2.34 (2),  $R$  中包含  $5R$  的子环即  $R$  与  $\mathbb{Z}[5i]$ , 故  $R/5R$  的所有子环恰为  $R/5R$  与  $\mathbb{Z}[5i]/5R$ . ② 由例 2.2.27 对应定理,  $\{R/5R\}$  的理想  $\xleftarrow{1:1} \{R\}$  中包含  $5R$  的理想, 而  $R$  为 PID, 若  $5R \subset (a)$ , 则  $a \mid 5$ . 由素分解  $5 = (1 + 2i)(1 - 2i)$  即知  $R$  中包含  $5R$  的理想恰为  $(1) = R, (1 + 2i), (1 - 2i), (5) = 5R$ . 故  $R/5R$  的理想恰为  $R/5R, (1 + 2i)/5R, (1 - 2i)/5R, \{0\}$ .

(5) 有环同构 (参考练习 2.6.9)

$$\begin{aligned} \mathbb{Z}[i]/(5) &\simeq (\mathbb{Z}[x]/(x^2 + 1))/(\bar{5}) \simeq \mathbb{Z}[x]/(5, x^2 + 1) \simeq (\mathbb{Z}[x]/(5))/(\overline{x^2 + 1}) \\ &\simeq (\mathbb{Z}/(5))[x]/(x^2 + \bar{1}) \simeq \mathbb{F}_5[x]/(x^2 + \bar{1}) \simeq \mathbb{F}_5[x]/((x - 2)(x - 3)) \\ &\stackrel{*}{\simeq} (\mathbb{F}_5[x]/(x - 2)) \times (\mathbb{F}_5[x]/(x - 3)) \simeq \mathbb{F}_5 \times \mathbb{F}_5, \end{aligned}$$

其中  $*$  处的同构来自定理 2.8.4. 由注记 2.2.10 (3),  $\text{Aut}(R/5R) \simeq \text{Aut}(\mathbb{F}_5 \times \mathbb{F}_5)$ . 设  $\theta \in \text{Aut}(\mathbb{F}_5 \times \mathbb{F}_5)$ ,  $\theta((1, 0)) = (a, b)$ , 则

$$(a^2, b^2) = \theta((1, 0))^2 = \theta((1, 0)) = (a, b) \implies a = 0 \text{ 或 } 1, b = 0 \text{ 或 } 1.$$

若  $(a, b) = (0, 0)$  或  $(1, 1)$ ,  $\theta$  均非单射, 排除. 而  $\phi: \mathbb{F}_5 \times \mathbb{F}_5 \rightarrow \mathbb{F}_5 \times \mathbb{F}_5, (x, y) \mapsto (y, x)$  与  $\text{Id}_{\mathbb{F}_5 \times \mathbb{F}_5}$  均为同构, 因此  $|\text{Aut}(\mathbb{F}_5 \times \mathbb{F}_5)| = 2$ , 即  $|\text{Aut}(R/5R)| = 2$ .

(6) 有环同构

$$\begin{aligned} \mathbb{Z}[2i]/(3 + 2i) &\simeq (\mathbb{Z}[x]/(x^2 + 4))/(\overline{3 + x}) \simeq \mathbb{Z}[x]/(3 + x, x^2 + 4) \\ &\stackrel{*}{\simeq} (\mathbb{Z}[x]/(13))/((3 + x, x^2 + 4)/(13)) \simeq \mathbb{F}_{13}[x]/(x + \bar{3}, x^2 + \bar{4}), \end{aligned}$$

其中  $\star$  处的同构来自例 2.2.27, 这里用到了  $(13) \subset (3 + x, x^2 + 4)$ , 这是因为

$$x(x+3) - (x^2 + 4) = 3x - 4, \quad 3(x+3) - (3x - 4) = 13.$$

而  $x^2 + \bar{4} = (x + \bar{3})(x + \bar{10})$ , 由练习 2.4.26,  $(x + \bar{3}, x^2 + \bar{4}) = (x + \bar{3})$ , 进而

$$S/(3 + 2i) \simeq \mathbb{F}_{13}[x]/(x + \bar{3}, x^2 + \bar{4}) \simeq \mathbb{F}_{13}[x]/(x + \bar{3}) \simeq \mathbb{F}_{13}.$$

故  $S/(3 + 2i)$  为域, 其阶为 13.

(7) 有环同构

$$\begin{aligned} S/2S &\simeq (\mathbb{Z}[x]/(x^2 + 4))/\bar{2}(\mathbb{Z}[x]/(x^2 + 4)) \simeq \mathbb{Z}[x]/(2, x^2 + 4) \simeq \mathbb{Z}[x]/(2, x^2) \\ &\simeq \mathbb{F}_2[x]/(x^2) \xrightarrow[y=x+\bar{1}]{} \mathbb{F}_2[y]/(y^2 + \bar{1}). \end{aligned}$$

由此可知  $\text{char}(S/2S) = 2 \neq 4$ , 故  $S/2S \not\simeq \mathbb{Z}_4$ .

(8) 假设  $S$  是 UFD, 由命题 2.5.16,  $S$  是整闭环. 注意到  $\text{Frac}(S) = \mathbb{Q}(i)$ ,  $i \in \mathbb{Q}(i)$  是首一整系数方程  $x^2 + 1 = 0$  的解, 由整闭环性,  $i \in S$ , 矛盾. 故  $S$  不是 UFD.  $\square$

2. 考虑商域  $K = \mathbb{F}_2[y]/(y^3 + y + \bar{1})$ , 记  $u = \bar{y}$ , 则  $K$  中元素均形如  $a + bu + cu^2$ , 其中  $a, b, c \in \mathbb{F}_2$ . 自然视  $\mathbb{F}_2$  为  $K$  的子域.

- (1) 将多项式  $x^3 + x^2 + \bar{1}$  在  $K[x]$  中进行不可约分解.
- (2) 在  $K$  中, 计算  $(u^4 + \bar{1})^{-1}$ .
- (3) 分类  $K$  的所有子环.
- (4) 判断  $K[x]/(x^2 + (u + \bar{1})x + u^2)$  是否为域.
- (5) 考虑域  $E = \mathbb{F}_2[z]/(z^3 + z^2 + \bar{1})$ . 试具体建立从  $E$  到  $K$  的环同构.
- (6) 分别求从  $\mathbb{Z}_8$  到  $K$ , 以及从  $K$  到  $\mathbb{Z}_8$  的(保单位的)环同态的个数.

**解答** (1)  $x^3 + x^2 + \bar{1} = (x + u^2 + \bar{1})(x + u + \bar{1})(x + u^2 + u + \bar{1})$ .

(2) 待定系数得  $u^2(u^4 + \bar{1}) = (u^3)^2 + u^2 = (u + \bar{1})^2 + u^2 = \bar{1} \implies (u^4 + \bar{1})^{-1} = u^2$ .

(3) 由于  $K$  的子环必包含  $\mathbb{F}_2$ , 而域上的有限维整环是域,  $K$  的子环即  $K$  的子域. 由命题 3.4.10,  $K$  的子域即  $\mathbb{F}_2$  与  $K$ .

- (4) 是. 只需证  $x^2 + (u + \bar{1})x + u^2 \in K[x]$  不可约, 这由 Vieta 定理及表 6.1 易得.
- (5) 由(1)知  $z^3 + z^2 + \bar{1} \in \mathbb{F}_2[z]$  不可约, 因此  $E$  是八元域. 记  $v = \bar{z}$ , 则  $E = \mathbb{F}_2(v)$ . 设  $\theta : E \rightarrow K$  为环同态, 则  $\theta$  由  $\theta(v)$  唯一决定. 由于  $v \in E$  是  $x^3 + x^2 + \bar{1} \in E[x]$  的根, 因此  $\theta(v) \in K$  是  $x^3 + x^2 + \bar{1}$  的根, 由(1),  $\theta(v) = u + \bar{1}$  或  $u^2 + \bar{1}$  或  $u^2 + u + \bar{1}$ . 考虑赋值同态

$$\text{ev}_{u+\bar{1}} : \mathbb{F}_2[z] \rightarrow K, \quad f(z) \mapsto f(u + \bar{1}).$$

由(1)知  $(z^3 + z^2 + \bar{1}) \subset \text{Ker}(\text{ev}_{u+\bar{1}})$ . 因此  $\text{ev}_{u+\bar{1}}$  诱导环嵌入  $\theta : E \hookrightarrow K$  使得  $v \mapsto u + \bar{1}$ . 又因为  $|E| = |K|$ ,  $\theta$  为环同构.

- (6) ① 从  $\mathbb{Z}_8$  到  $K$  的环同态(若存在), 只能为

$$\mathbb{Z}_8 \rightarrow K, \quad \bar{0}, \bar{2}, \bar{4}, \bar{6} \mapsto \bar{0}, \quad \bar{1}, \bar{3}, \bar{5}, \bar{7} \mapsto \bar{1}.$$

可验证这的确是环同态. ② 为求从  $K$  到  $\mathbb{Z}_8$  的环同态  $\phi$ , 只需确定  $u \in K$  的像. 由于  $\phi(u)$  是方程  $x^3 + x + \bar{1}$  的解, 但计算可知此方程在  $\mathbb{Z}_8$  中无解, 故不存在从  $K$  到  $\mathbb{Z}_8$  的环同态.  $\square$

表 6.1:  $\mathbb{F}_8 = \mathbb{F}_2[y]/(y^3 + y + \bar{1})$  的乘法表

$\times$	$\bar{0}$	$\bar{1}$	$u$	$u + \bar{1}$	$u^2$	$u^2 + \bar{1}$	$u^2 + u$	$u^2 + u + \bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$u$	$u + \bar{1}$	$u^2$	$u^2 + \bar{1}$	$u^2 + u$	$u^2 + u + \bar{1}$
$u$	$\bar{0}$	$u$	$u^2$	$u^2 + u$	$u + \bar{1}$	$\bar{1}$	$u^2 + u + \bar{1}$	$u^2 + \bar{1}$
$u + \bar{1}$	$\bar{0}$	$u + \bar{1}$	$u^2 + u$	$u^2 + \bar{1}$	$u^2 + u + \bar{1}$	$u^2$	$\bar{1}$	$u$
$u^2$	$\bar{0}$	$u^2$	$u + \bar{1}$	$u^2 + u + \bar{1}$	$u^2 + u$	$u$	$u^2 + \bar{1}$	$\bar{1}$
$u^2 + \bar{1}$	$\bar{0}$	$u^2 + \bar{1}$	$\bar{1}$	$u^2$	$u$	$u^2 + u + \bar{1}$	$u + \bar{1}$	$u^2 + u$
$u^2 + u$	$\bar{0}$	$u^2 + u$	$u^2 + u + \bar{1}$	$\bar{1}$	$u^2 + \bar{1}$	$u + \bar{1}$	$u$	$u^2$
$u^2 + u + \bar{1}$	$\bar{0}$	$u^2 + u + \bar{1}$	$u^2 + \bar{1}$	$u$	$\bar{1}$	$u^2 + u$	$u^2$	$u + \bar{1}$

3. 考虑商域  $F = \mathbb{Q}[y]/(y^3 + y + 1)$ , 记  $u = \bar{y}$ . 自然视  $\mathbb{Q}$  为  $F$  的子域.

- (1) 将  $x^3 + x + 1$  在  $F[x]$  上进行不可约分解.
- (2) 计算  $\text{Aut}(F)$  的阶.
- (3) 将  $x^3 + x^2 + 1$  在  $F[x]$  上进行不可约分解.
- (4) 设  $R$  为  $F$  的子环, 且  $\mathbb{Q} \subset R$ . 证明:  $R = \mathbb{Q}$  或  $R = F$ .
- (5) 是否存在正整数  $n$ , 使得  $u^n = 1_F$ ?
- (6) 考虑  $E = F[x]/(x^2 + 5)$ . 判断  $E$  是否为域. 求  $\text{Aut}(E)$  的阶.

解答 (1)  $x^3 + x + 1 = (x - u)(x^2 + ux + u^2 + 1)$ . 下证  $x^2 + ux + u^2 + 1 \in F[x]$  不可约.

- ◊ 由于  $(y^3 + y + 1)' = 3y^2 + 1 > 0, \forall y \in \mathbb{R}, y^3 + y + 1$  在  $\mathbb{R}$  上有且仅有一个根  $y_0$ . 由命题 2.4.13, 存在环同态  $\theta : \mathbb{Q}[y] \rightarrow \mathbb{Q}[y_0]$  使  $\theta(y) = y_0$  而  $\theta|_{\mathbb{Q}} = \text{Id}_{\mathbb{Q}}$ . 由于  $y_0$  在  $\mathbb{Q}$  上代数,  $\mathbb{Q}[y_0] = \mathbb{Q}(y_0)$ . 又  $y^3 + y + 1$  在  $\mathbb{Z}$  上无根, 即在  $\mathbb{Q}$  上不可约,  $(y^3 + y + 1) \subset \text{Ker } \theta$ , 而由命题 2.4.23,  $\mathbb{Q}[y]$  是 PID, 因此  $\text{Ker } \theta = (y^3 + y + 1)$ . 由定理 2.2.20,  $F = \mathbb{Q}[y]/(y^3 + y + 1) \simeq \mathbb{Q}(y_0)$ .
- ◊ 假设  $x^2 + ux + u^2 + 1 \in F[x]$  可约, 则其根可表为  $u$  的多项式, 即存在  $P, Q \in \mathbb{Q}[x]$ , 使得  $x^2 + ux + u^2 + 1 = [x - P(u)][x - Q(u)]$ . 在上述环同构下, 此等式化为

$$x^2 + y_0x + y_0^2 + 1 = [x - P(y_0)][x - Q(y_0)],$$

从而在  $\mathbb{R}[x]$  中成立等式

$$x^3 + x + 1 = (x - y_0)[x - P(y_0)][x - Q(y_0)],$$

但这与  $x^3 + x + 1$  在  $\mathbb{R}$  上有且仅有一个根矛盾. 故  $x^2 + ux + u^2 + 1 \in F[x]$  不可约.

- (2) 由注记 2.2.10 (3),  $\text{Aut}(F) \simeq \text{Aut}(\mathbb{Q}(y_0))$ . 由引理 3.3.1,  $|\text{Aut}(F)| = |\text{Root}_F(y^3 + y + 1)| \stackrel{(1)}{=} 1$ .
- (3) 作替换  $t = \frac{1}{x}$ , 则  $t^3(x^3 + x^2 + 1) = t^3 + t + 1 \stackrel{(1)}{=} (t - u)(t^2 + ut + u^2 + 1)$ , 因此

$$\begin{aligned} x^3 + x^2 + 1 &= x^3(t - u)(t^2 + ut + u^2 + 1) = (1 - ux)[1 + ux + (u^2 + 1)x^2] \\ &= (u^{-1} - x)[u + u^2x + (u^3 + u)x^2] = (x + u^2 + 1)(x^2 - u^2x - u). \end{aligned}$$

(4) 由  $R \subset F$  知  $R$  为整环, 而域上的有限维整环是域, 即  $R$  为域. 由定理 3.2.4,

$$[F : R][R : \mathbb{Q}] = [F : \mathbb{Q}] = 3.$$

因此  $[F : R] = 3, [R : \mathbb{Q}] = 1$  或  $[F : R] = 1, [R : \mathbb{Q}] = 3$ , 即  $R = \mathbb{Q}$  或  $R = F$ .

(5) 不存在. 用反证法, 假设存在正整数  $n$  使得  $u^n = 1_F$ , 由引理 3.5.14,  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ , 因此存在  $d | n$ , 使得  $\Phi_d(u) = 0$ . 由于  $\Phi_d(x) \in \mathbb{Q}[x]$  首一不可约,  $y^3 + y + 1 \in \mathbb{Q}[x]$  亦首一不可约且零化  $u$ , 因此  $\Phi_d(x) = x^3 + x + 1$ . 但  $\phi(d) = \begin{cases} 1, & d = 2, \\ \text{偶数}, & d \geq 3, \end{cases}$  因此  $\deg(\Phi_d(x)) \neq 3$ , 矛盾.

(6) ① 为证  $E$  为域, 只需证  $x^2 + 5 \in F[x]$  不可约. 用反证法, 假设  $x^2 + 5 \in F[x]$  可约, 则有域扩张塔

$$\mathbb{Q} \subset \mathbb{Q}[x]/(x^2 + 5) \subset F,$$

由定理 3.2.4,  $3 = [F : \mathbb{Q}] = [F : \mathbb{Q}[x]/(x^2 + 5)][\mathbb{Q}[x]/(x^2 + 5) : \mathbb{Q}] = 2$ , 矛盾. ② 先证明对任意  $\sigma \in \text{Aut}(E)$ , 均有  $\sigma|_F = \text{Id}_F$ . 由于  $\sigma_F$  被  $\sigma(u)$  唯一确定, 只需证  $\sigma(u) = u$ , 进而只需证  $y^3 + y + 1$  在  $E$  上仅有  $u$  一个根. 假设  $y^3 + y + 1$  在  $E$  上的根多于 1 个, 则它在  $E$  上恰有 3 个根, 设为  $\alpha, \beta, \gamma$ . 由于

$$\Delta^2 = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = -4 \cdot 1^3 - 27 \cdot 1^2 = -31,$$

必有  $\sqrt{-31} \in E$ , 进而有域扩张塔

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{-5}, \sqrt{-31}) \subset E.$$

由定理 3.2.4,  $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{-5}, \sqrt{-31})][\mathbb{Q}(\sqrt{-5}, \sqrt{-31}) : \mathbb{Q}]$ . 但  $[E : \mathbb{Q}] = 2 \cdot 3 = 6$ ,  $[\mathbb{Q}(\sqrt{-5}, \sqrt{-31}) : \mathbb{Q}] = 4, 4 \nmid 6$ , 矛盾. 故  $\sigma|_F = \text{Id}_F$  得证, 从而

$$|\text{Aut}(E)| = |\text{Aut}(E/F)| = |\text{Root}_E(x^2 + 5)| = 2.$$

□

## 6.4 2024 春期中考试

- 考虑  $\mathbb{C}$  的子域  $E = \mathbb{Q}(i, \xi)$ , 其中  $i = \sqrt{-1}$  且  $\xi = e^{\frac{2\pi i}{5}}$ . 回顾  $\cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$ .
  - 证明  $E/\mathbb{Q}$  是多项式  $x^9 - x^5 - x^4 + 1 \in \mathbb{Q}[x]$  的分裂域.
  - 计算  $\xi$  在  $\mathbb{Q}(\sqrt{5})$  上的最小多项式, 计算  $\xi$  在  $\mathbb{Q}(i)$  上的最小多项式.
  - 将多项式  $x^4 + 6x^2 + 5 \in \mathbb{Q}(\xi)[x]$  分解成不可约多项式之积, 给出充分论证.
  - 计算维数  $\dim_{\mathbb{Q}} E$ , 计算维数  $\dim_{\mathbb{Q}}(E \cap \mathbb{R})$ , 给出充分论证.
  - 简要论证并具体构造  $\text{Aut}(E)$  中的全部元素, 判断其是否为 Abel 群.
- 考虑域  $K = \mathbb{F}_3[y]/(y^2 + 1)$ . 记  $u = \bar{y}$ . 于是,  $K$  中元素均形如  $a + bu$ , 其中  $a, b \in \mathbb{F}_3$ . 自然视  $\mathbb{F}_3$  为  $K$  的子域. 同理, 考虑域  $L = \mathbb{F}_3[z]/(z^2 + z - 1)$ , 记  $v = \bar{z}$ . 请论证并给出全部的环同态  $K \rightarrow L$ .
- 考虑主理想整环  $R$  以及 (非零) 极大理想  $\mathfrak{m}$ . 假设有环同构  $R/\mathfrak{m} \simeq \mathbb{F}_p$ . 试计算商环  $R/\mathfrak{m}^2$  的阶数 (大小), 计算环自同构群  $\text{Aut}(R/\mathfrak{m}^2)$  的阶数 (大小).
- 考虑 Gauss 整数环  $R = \mathbb{Z}[i]$ . 对于任何正素数  $p$ , 我们定义  $R$  的子环  $S_p = \{m + (pn)i : m, n \in \mathbb{Z}\}$ .

- (1) 在  $R$  中将  $17 - 7i$  进行不可约分解.
- (2) 考虑商环  $\bar{R} = R/(17 - 7i)$ . 计算该环的阶数, 计算环自同构群  $\text{Aut}(\bar{R})$  的阶数, 充分论证.
- (3) 判断并论证: 商环  $S_5/(5)$  和  $S_5/(5i)$  是否同构? 对于不同的正素数  $p, q$ , 环  $S_p$  与  $S_q$  是否同构?

## 第七章 期末考试题目

### 7.1 2020 春期末考试

1. 考虑  $S_4$  中的共轭类  $C = \{(12)(34), (13)(24), (14)(23)\}$  以及  $S_4$  在  $C$  上的共轭作用.

- (1) 计算  $C$  中三个元素的稳定化子及其交集.
- (2) 记  $\text{SHom}(S_4, S_3)$  为所有  $S_4 \rightarrow S_3$  的满同态, 计算  $\text{SHom}(S_4, S_3)$  和  $\text{Hom}(S_4, S_3)$  的阶数.
- (3) 是否存在单同态  $S_3 \hookrightarrow \text{SL}(2, \mathbb{C})$ ,  $S_3 \hookrightarrow \text{GL}(2, \mathbb{C})$ ?

2. 考虑  $R = \mathbb{Z}[i]$ ,  $K = \mathbb{Q}(i)$ .

- (1) 计算  $\gcd(4 + 7i, 3 + 4i)$ .
- (2) 把  $81 + 8i$  分解成  $R$  中不可约元的乘积.
- (3) 求  $u^2 + v^2 = 585$  的所有整数解.
- (4) 计算  $\text{Aut}(R/(13))$ .
- (5)  $x^5 - 5$  和  $x^4 + x^3 + x^2 + x + 1$  是否为  $K$  中的不可约多项式?
- (6) 分类  $R$  的子环, 并指出哪些是 UFD.
- (7) 设  $K'$  是  $x^5 - 5$  在  $\mathbb{Q}(i)$  上的分裂域. 计算  $[K' : K]$ , 并判断  $\text{Gal}(K'/K)$  是否为 Abel 群.

3. 设  $f(x) = x^4 + x + \bar{2} \in \mathbb{F}_3[x]$ , 考虑  $\mathbb{F}_{81} = \mathbb{F}_3[x]/(f(x))$ , 记  $u = x + (f(x))$ .

- (1) 证明  $f(x)$  在  $\mathbb{F}_3$  上不可约.
- (2) 在  $\mathbb{F}_{81}$  中分解  $f(x)$ .
- (3) 求  $\mathbb{F}_{81}$  的九元子域.
- (4) 计算  $(u^2 + u + \bar{1})^{-1}$ .
- (5) 求  $u^2 + u + \bar{1}$  在  $\mathbb{F}_3$  上的最小多项式.
- (6) 计算  $u^2 + u + \bar{1}$  在  $\mathbb{F}_{81}^\times$  中的阶数.

## 7.2 2021 春期末考试

1. 考虑  $A_4$  在 (123) 上的共轭作用, 记  $C$  为其轨道.
  - (1) 求 (123) 的稳定化子及  $|C|$ .
  - (2) 求  $C$ . 判断此作用在  $C$  上是否忠实.
  - (3) 计算  $|\mathrm{Hom}(A_4, S_3)|$ .
  - (4) 是否存在群的单同态  $A_4 \hookrightarrow \mathrm{SL}(2, \mathbb{C}), A_4 \hookrightarrow \mathrm{GL}(2, \mathbb{C})$ ?
2. 考虑  $E = \mathbb{Q}(\sqrt[4]{2}, i)$ ,  $K = E \cap \mathbb{R}$ .
  - (1) 判断  $x^4 - 2 \in \mathbb{Q}[x]$  是否可约,  $x^4 - 2 \in \mathbb{Q}(i)[x]$  是否可约.
  - (2) 计算  $[E : \mathbb{Q}]$  和  $[E : K]$ .
  - (3)  $\mathrm{Gal}(E/\mathbb{Q})$  在集合
 
$$\mathfrak{X} = \left\{ a = \sqrt[4]{2}, b = i\sqrt[4]{2}, c = -\sqrt[4]{2}, d = -i\sqrt[4]{2} \right\}$$
 上有一自然作用, 它诱导群同态  $\rho : \mathrm{Gal}(E/\mathbb{Q}) \rightarrow S(\mathfrak{X})$ , 求  $\mathrm{Ker} \rho$  与  $\mathrm{Im} \rho$ .
  - (4) 求  $\mathrm{Gal}(E/\mathbb{Q}(i))$  和  $\mathrm{Gal}(E/K)$  在  $\rho$  下的像.
3. 考虑  $E = (\sqrt{2}, \sqrt{5})$ , 求所有的  $u \in E$ , 使得  $E = \mathbb{Q}(u)$ . 提示 求  $E$  的线性基和所有域扩张的中间域.
4. 考虑  $A = \mathbb{Q}^\times \setminus \{1\}$  和  $A$  上的双射  $\sigma(a) = \frac{1}{a}, \tau(a) = \frac{1}{1-a}$ . 设  $G$  为由  $\sigma$  和  $\tau$  生成的群, 乘法为映射的复合. 判断  $G$  是否为有限群. 若有限, 求  $|G|$ .

## 7.3 2023 春期末考试

1. 考虑  $K = \mathbb{Q}(\sqrt[4]{3}, i)$  以及  $E = K \cap \mathbb{R}$ . 以下, 维数均指  $\mathbb{Q}$  上的维数.
  - (1) 计算域  $E$  的维数与  $|\mathrm{Aut}(E)|$ .
  - (2) 求  $\sqrt[4]{3} + i$  在  $\mathbb{Q}$  上的最小多项式.
  - (3) 考虑  $F = \mathbb{Q}(\sqrt{2}, i)$ . 证明:  $x^4 - 3 \in F[x]$  不可约.
  - (4) 考虑  $x^4 - 3$  的根集  $\mathfrak{X} = \left\{ a = \sqrt[4]{3}, b = \sqrt[4]{3}i, c = -\sqrt[4]{3}, d = -\sqrt[4]{3}i \right\}$  以及群作用  $\mathrm{Aut}(K) \curvearrowright K$  诱导的群同态  $\rho : \mathrm{Aut}(K) \rightarrow S(\mathfrak{X})$ , 计算并描述  $\rho$  的像.
  - (5) 分类  $K$  的全体维数为 4 的子域.
2. 考虑  $n$  元集合  $\{1, \dots, n\}$  的对称群  $S_n$ .
  - (1) 证明:  $S_n$  可由 (12) 和  $(12 \cdots n)$  生成.
  - (2) 对 2, 3, 4 的任一排列  $a, b, c$ , 定义  $H_{(a,b,c)} = ((12), (1abc)) \leqslant S_4$ , 试分类所有的排列  $a, b, c$  使得  $H_{(a,b,c)} = S_4$ .
  - (3) 设  $H \leqslant S_5$  满足  $(12) \in H$  且  $5 \mid |H|$ . 证明:  $H = S_5$ .
  - (4) 考虑  $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ , 证明:  $\mathrm{Gal}_{\mathbb{Q}}(f) \simeq S_5$ .
3. 将  $\mathbb{Z}^3$  中的元素写成行向量, 考虑由  $(4, -6, 0)$  和  $(0, 6, -4)$  生成的子群  $H$ .
  - (1) 在同构意义下, 计算商群  $\mathbb{Z}^3/H$  的扭子群.
  - (2) 证明: 不存在群同态  $f : \mathbb{Z}^3 \rightarrow \mathbb{Z}$  使得  $\mathrm{Ker} f = H$ .

## 7.4 2024 春期末考试

1. 考虑  $E = \mathbb{Q}(\sqrt[4]{18}, i)$ , 以及  $K = E \cap \mathbb{Q}(\sqrt{3} + \sqrt{2})$ . 以下, 维数均指  $\mathbb{Q}$  上维数.
  - (1) 计算域  $E$  的维数, 给出充分论证.
  - (2) 判断并论证: 多项式  $x^4 - 18 \in \mathbb{Q}(i)[x]$  是否可约?
  - (3) 计算域  $K$  的维数, 给出充分论证.
  - (4) 考虑  $x^4 - 18$  的根集  $\mathcal{X} = \{a = \sqrt[4]{18}, b = \sqrt[4]{18}i, c = -\sqrt[4]{18}, d = -\sqrt[4]{18}i\}$ , 以及群作用  $\text{Aut}(E) \curvearrowright \mathcal{X}$  诱导的群同态  $\rho : \text{Aut}(E) \rightarrow S(\mathcal{X})$ . 试给出  $\rho$  像中的全部元素.
  - (5) 试分类  $E$  的全部子域, 给出充分论证.
2. 考虑一元有理函数域  $E = \mathbb{C}(x)$ . 对于任意正整数  $n$ , 考虑其子域  $L_n = \mathbb{C}(x^n + x^{-n})$ .
  - (1) 计算域扩张  $E/L_n$  的维数, 给出充分论证.
  - (2) 判断并论证: 断言 " $L_n \subset L_m$  当且仅当  $m|n$ ", 是否成立?
  - (3) 试给出域扩张  $E/L_4$  的所有中间域, 给出充分论证.
3. 设  $G$  为有限群,  $H \leq G$  为真子群. 试证明:  $G \neq \bigcup_{g \in G} gHg^{-1}$ . 试问: 该结论对于无限群  $G$  是否也成立?
4. 设  $A$  为有限生成 Abel 群, 秩为 2. 设有群的满同态  $\theta : A \rightarrow \mathbb{Z} \oplus \mathbb{Z}$ . 证明:  $\text{Ker } \theta$  恰等于  $A$  的扭 (torsion) 子群.