

近世代数 (H) 讲义

Author: 吕长乐

Institute: 中国科学技术大学

Date: 2025 年 7 月

本讲义整理于 2020 年网课期间陈小伍老师近世代数 (H) 网课的板书，仅供参考，每年实际授课内容与之有出入

目录

Chapter 1 环论	1
1.1 集合与映射	1
1.2 环的定义	4
1.3 商环与理想	7
1.4 分式域和商域	10
1.5 一元多项式环	13
1.6 添根构造	16
1.7 欧氏整环	19
1.8 Gauss 整数环	22
1.9 唯一因子分解整环	26
1.10 拾遗	30
Chapter 2 域扩张	32
2.1 域扩张和单扩张	32
2.2 域的代数扩张	35
2.3 分裂域	38
2.4 有限域	42
2.5 分圆域	45
Chapter 3 群论	48
3.1 群的基本定义	48
3.2 循环群	50
3.3 正规子群	53
3.4 对称群	56
3.5 群作用	61
3.6 Sylow 子群	65
3.7 群的表现	68
3.8 有限生成 Abel 群	71
Chapter 4 Galois 理论	75
4.1 Galois 扩张	75
4.2 Galois 对应	78

4.3	例子和应用	81
4.4	Galois 大定理	85
附录 A	2024 春近世代数 (H) 期末	89

Chapter 1 环论

1.1 集合与映射

记号：集合 $X, Y, Z \dots$ ，子集 $X \subseteq Y$ ，映射 $f: X \rightarrow Y$ 或 $X \xrightarrow{f} Y, x \mapsto f(x)$.

Example 1.1 恒等映射: $\text{Id}_X: X \rightarrow X, x \mapsto x$.

Example 1.2 包含映射: 对 $S \subseteq X$, 定义 $\text{inc}: S \rightarrow X, s \mapsto s$.

Example 1.3 限制映射: 对映射 $f: X \rightarrow Y$ 和 $S \subseteq X$, 定义 f 在 S 上的限制 $f|_S: S \rightarrow Y, s \mapsto f(s)$.

Definition 1.1

两个映射 $f: X \rightarrow Y$ 和 $f': X' \rightarrow Y'$ 称为**相等**，若 $X = X', Y = Y'$ 且 $f(x) = f'(x)(\forall x \in X)$.

两个映射 $f: X \rightarrow Y$ 和 $g: Y \rightarrow Z$ 的**复合**定义为映射 $g \circ f: X \rightarrow Z, x \mapsto g(f(x))$.

映射 $f: X \rightarrow Y$ 称为**单射**，若 $f(x) = f(x')$, 则 $x = x'$, 此时也记作 $X \xrightarrow{f} Y$.

映射 $f: X \rightarrow Y$ 称为**满射**，若 $\forall y \in Y, \exists x \in X, \text{s.t. } f(x) = y$, 此时也记作 $X \xrightarrow{f} Y$.

若映射 $f: X \rightarrow Y$ 既单又满，则称 f 为**双射**，记为 $X \xrightarrow{f} Y$.



Proposition 1.1

(1) Id_X 为双射， inc 为单射.

(2) 映射的复合满足结合律 $h \circ (g \circ f) = (h \circ g) \circ f$ ，其中 $f: X \rightarrow Y, g: Y \rightarrow Z, h: Z \rightarrow W$.

(3) 有单位元: $\forall f: X \rightarrow Y, f = f \circ \text{Id}_X = \text{Id}_Y \circ f$.



对映射 $f: X \rightarrow Y$ ，我们也可以定义它的像 $\text{Im}(f) = \{f(x) : x \in X\} \subseteq Y$ ，则有如下的交换图表

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

其中 $\bar{f}(x) = f(x)$. 分解 $f = \text{inc} \circ \bar{f}$ 也称为 f 的**典范分解**.

利用已有的集合也可以构造出新的集合，例如无交并 $X \sqcup Y$ ，乘积 $X \times Y$ ，映射集合 $\text{Map}(X, Y) = \{f: X \rightarrow Y\}$ ，所有子集构成的集合 $\mathcal{P}(X) = \{S \subseteq X\}$.

Proposition 1.2

(1) $\text{Map}(X, \{0, 1\}) \xrightarrow{\sim} \mathcal{P}(X), f \mapsto S_f = \{x \in X : f(x) = 1\}$.

(2) $\text{Map}(X \sqcup Y, Z) \xrightarrow{\sim} \text{Map}(X, Z) \times \text{Map}(Y, Z), f \mapsto (f|_X, f|_Y)$.

(3) $\text{Map}(X, Y \times Z) \xrightarrow{\sim} \text{Map}(X, Y) \times \text{Map}(X, Z), g \mapsto (g_1, g_2)$ ，其中 g_1, g_2 为 g 的第一和第二分量.



在集合上我们可以赋予如下的等价关系.

Definition 1.2

集合 X 上的**等价关系**是一个集合 $R \subseteq X \times X$, 满足下面的三个条件:

- (1) 自反性: $(x, x) \in R, \forall x \in X$.
- (2) 对称性: $(x, y) \in R$, 则 $(y, x) \in R$.
- (3) 传递性: $(x, y) \in R, (y, z) \in R$, 则 $(x, z) \in R$.

我们记 $(a, b) \in R$ 作 $a \stackrel{R}{\sim} b$, 语义清晰时也可省略 R .

对 $a \in X$, 定义 a 的**等价类**为集合 $[a] = \{x \in X : x \stackrel{R}{\sim} a\} \subseteq X$, 任意 $x \in [a]$ 称为一个**代表元**.

商集 $X/\stackrel{R}{\sim} \subseteq \mathcal{P}(X)$ 为等价类构成的集合, **商映射**定义为 $\pi_R: X \rightarrow X/\stackrel{R}{\sim}, a \mapsto [a]$.

一个集合 $S \subseteq X$ 称为关于等价关系 R 的**完全代表元系**, 如果 $\forall x \in X, \exists! s \in S, \text{s.t. } s \stackrel{R}{\sim} x$.



Example 1.4 令 $X = \mathbb{Z}$, 定义 $a \sim b$ 当且仅当 $3|(a - b)$, 不难验证这确实是一个等价关系, 此时 $S = \{0, 1, 2\}$ 为一个完全代表元系.

不难注意到等价类满足如下性质:

- (1) 若 $b \sim a$, 则 $[a] = [b]$.
- (2) 若 $[a] \cap [a'] \neq \emptyset$, 则 $[a] = [a']$.

故有

Proposition 1.3

若 $S \subseteq X$ 为完全代表元系, 则

- (1) $S \xrightarrow{\text{inc}} X \xrightarrow{\pi_R} X/\stackrel{R}{\sim}, s \mapsto [s]$ 为双射.
- (2) $X = \sqcup_{s \in S} [s]$ 为无交并.



这自然地给出了分拆的概念

Definition 1.3

集合 X 的一个**分拆**是指一族子集 $\{X_i : i \in I\} \subseteq \mathcal{P}(X)$ 使得

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



根据上面的讨论, 每一个 X 上的等价关系都给出了 X 的一个分拆, 事实上反过来也成立: 给定 X 的分拆 $\{X_i : i \in I\}$, 定义 $x \sim y$ 当且仅当 $\exists i \in I, \text{s.t. } x \in X_i, y \in X_i$. 可以验证 \sim 确实是一个等价关系. 进而 X 上的等价关系和 X 的分拆之间有一一对应.

在本节的最后我们给出一个重要的等价关系的例子.

Theorem 1.1 (映射基本定理)

对任意映射 $f: X \rightarrow Y$, 定义 $x \stackrel{f}{\sim} x'$ 当且仅当 $f(x) = f(x')$, 则 $\stackrel{f}{\sim}$ 是 X 上的一个等价关系, 等价类 $[x] = f^{-1}(f(x))$.

此外 f 诱导了双射 $\bar{f}: X/\stackrel{f}{\sim} \xrightarrow{\sim} \text{Im}(f)$, $[x] \mapsto f(x)$, 并且有如下的交换图表

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



该定理的证明为简单的验证, 在此省略.

1.2 环的定义

Definition 1.4

环 (更精确地说是含么交换环) 是一个非空集合 R 和 R 上的二元运算 $+$ 和 \cdot (通常称为加法和乘法), 满足:

(A1) 加法结合律: $(a + b) + c = a + (b + c)$.

(A2) 加法交换律: $a + b = b + a$.

(A3) 零元: $\exists 0_R \in R, \text{s.t. } a + 0_R = a (\forall a \in R)$.

(A4) 负元: $\forall a \in R, \exists b \in R, \text{s.t. } a + b = 0_R$, 此时记 $b = -a$.

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

(M2) 么元: $\exists 1_R \in R, \text{s.t. } a \cdot 1_R = a (\forall a \in R)$.

(D1) 分配律 1: $(a + b) \cdot c = a \cdot c + b \cdot c$.

(D2) 分配律 2: $a \cdot (b + c) = a \cdot b + a \cdot c$.

借助负元也可以定义环上的减法: $a - b = a + (-b)$,



Example 1.5 整数环 $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$.

Example 1.6 Gauss 整数环 $\mathbb{Z}[i] = \{m + ni : m, n \in \mathbb{Z}\} \subseteq \mathbb{C}$.

Example 1.7 有理系数一元多项式环 $\mathbb{Q}[x]$.

Example 1.8 同余类环 $\mathbb{Z}_n = \{[0], [1], \dots, [n]\}$.

容易验证环有如下的基本性质

Proposition 1.4

对环 R , 有

(1) $\forall a \in R, -(-a) = a$.

(2) $\forall a \in R, n \in \mathbb{Z}$, 可以先对非负的 n 通过累加定义 a 的 n 倍 na , 再通过取负元对负值的 n 定义 na . 则有 $(m + n)a = ma + na$.

(3) 消去: $a + b = a + c$, 则 $b = c$.

(4) $\forall n \in \mathbb{Z}$, 有 $n1_R \in R$, 且 $na = (n1_R) \cdot a$.

(5) 广义分配律: $(\sum_{i=1}^n a_i) \cdot (\sum_{j=1}^m b_j) = \sum_{i=1}^n \sum_{j=1}^m (a_i \cdot b_j)$.

(6) 对 $a \in R, n \in \mathbb{N}$, 可以通过累乘定义 a 的 n 次方 a^n , 则有二项式定理 $(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$.



乘法可逆的元素在环中受到我们的关注.

Definition 1.5

$a \in R$ 称为**乘法可逆元**, 或者称为**单位**, 若 $\exists b \in R, \text{s.t. } a \cdot b = 1_R$. 此时记 $b = a^{-1}$, 称为 a 的逆.

$U(R) = \{a \in R : a \text{ 可逆}\}$ 称为 R 的**单位群**.



Proposition 1.5

$U(R)$ 确实为群 (群会在之后定义), 即:

- (1) $1_R \in U(R)$.
- (2) $a, b \in U(R)$, 则 $a \cdot b \in U(R)$.
- (3) $a \in U(R)$, 则 $a^{-1} \in U(R)$.



证明 (2) $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = 1_R$, 故 $a \cdot b \in U(R)$

(3) $a^{-1} \cdot a = 1_R$, 故 $a^{-1} \in U(R)$. □

Example 1.9 对任意环 R , 0_R 不可逆, 1_R 可逆, -1_R 可逆, 它们的逆都是它们本身.

Example 1.10 对可逆元有乘法消去: $\forall a \in U(R), x, y \in R, a \cdot x = a \cdot y$, 则 $x = y$.

Example 1.11 $U(\mathbb{Z}) = \{1, -1\}, U(\mathbb{Q}) = \mathbb{Q} - \{0\}, U(\mathbb{Z}_n) = \{[m] : (m, n) = 1\}, U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$.

Definition 1.6

环 R 称为**整环**, 若 $a \cdot b = 0_R$, 则必有 $a = 0_R$ 或 $b = 0_R$. 环 R 称为**域**, 若 $R - \{0_R\} = U(R)$.



Proposition 1.6

- (1) 整环上有乘法消去律, 即若 $a \cdot b = a \cdot c, a \neq 0_R$, 则 $b = c$.
- (2) 域为整环, 反之不一定成立. 但有限整环必为域.



证明 (1) 由条件 $a \cdot (b - c) = 0_R$, 再由整环的定义 $b - c = 0_R, b = c$.

(2) 设 R 为域, $a \neq 0_R, b \neq 0_R$, 则只须证 $a \cdot b \neq 0_R$. 这是因为由于 R 为域, 有 $a, b \in U(R)$, 则 $a \cdot b \in U(R) = R - \{0_R\}$, 即 $a \cdot b \neq 0_R$. \mathbb{Z} 是整环但不是域.

现在设 R 是有限整环, 则任何 $x \neq 0_R$, 若任意 $i \neq j \in \mathbb{N}, x^i \neq x^j$, 则 $\{x^k : k \in \mathbb{N}\} \subseteq R$ 是无限集, 矛盾! 故 $\exists i > j \in \mathbb{N}$ 使得 $x^i = x^j$, 由于 R 为整环有消去律 $x \cdot x^{i-j-1} = 1$, 故 $x \in U(R), R$ 是域. □

Example 1.12 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 均为域, \mathbb{Z} 和 $\mathbb{Z}[i]$ 不是域.

Example 1.13 \mathbb{Z}_n 为整环 $\iff n = p$ 为素数 $\iff \mathbb{Z}_n$ 为域, 此时也记 $\mathbb{Z}_n = \mathbb{F}_p$.

Definition 1.7

R 是环, $S \subseteq R$ 是一个包含 1_R 的关于 R 的加法和乘法封闭的子集, 则称 S 为 R 的**子环**, 不难验证 S 关于继承的加法和乘法确实成为一个环.

K 是域, $S \subseteq K$ 是子环, 则 S 称为**子域**, 若 $\forall 0_S \neq a \in S$, 有 $a^{-1} \in S$. 同样不难验证此时 S 确

实是一个域.



Proposition 1.7

$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ 的子域只有 \mathbb{Q} 和 $\mathbb{Q}(i)$ 本身.



证明 设 S 为子域, 则 $1 \in S$, 由于加法封闭可知 $\mathbb{Z} \subseteq S$, 再由于为子域, 故 $\forall n \in \mathbb{Z} - \{0\}, \frac{1}{n} \in S$, 则 $\mathbb{Q} \subseteq S$.

若 $\mathbb{Q} \neq S$, 则存在 $a + bi \in S, a, b \in \mathbb{Q} \subseteq S, b \neq 0$, 则由加法封闭 $bi \in S$, 故 $i = \frac{1}{b} \cdot bi \in S$, 则任何 $a', b' \in \mathbb{Q} \subseteq S$, 有 $a' + b'i \in S$, 即 $S = \mathbb{Q}(i)$. □

1.3 商环与理想

Definition 1.8

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

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

$$(2) \theta(1_R) = 1_S.$$

若环同态 θ 为双射, 则称为**环同构**.



Remark 由定义, 若 $\theta: R \rightarrow S$ 为环同态, 则 $\theta(0_R) = 0_S, \theta(a^m) = \theta(a)^m, \theta(a-b) = \theta(a) - \theta(b)$, 特别地 $\theta(a^{-1}) = \theta(a)^{-1}$, 即 $\theta(U(R)) \subseteq U(S)$.

Example 1.14 任意环 R , 存在同态 $\mathbb{Z} \rightarrow R, n \mapsto n1_R$, 称为 R 的**特征同态**.

Example 1.15 不存在 \mathbb{Q} 到 \mathbb{Z}_8 的环同态: 若存在这样的环同态 θ , 则 $\theta(1) = \bar{1}, \theta(8) = \theta(1) + \theta(1) + \cdots + \theta(1)$ (共 8 个) $= 0$, 又 $8 \in U(\mathbb{Q})$, 故 $0 \in U(\mathbb{Z}_8)$, 矛盾!

Proposition 1.8

若 $\theta: R \rightarrow S$ 为环同构, 则 $\theta^{-1}: S \rightarrow R$ 也为环同构. 特别地, 对环 $R, \text{Aut}(R) = \{\theta: R \rightarrow R \text{ 为同构}\}$ 为一个群, 称为 R 的**自同构群**.



证明 显然 $\theta^{-1}(1_S) = 1_R$. 对 $x, y \in S$, 由于 $\theta(\theta^{-1}(x+y)) = x+y = \theta(\theta^{-1}(x) + \theta^{-1}(y))$ 以及 θ 为双射, 有 $\theta^{-1}(x+y) = \theta^{-1}(x) + \theta^{-1}(y)$.

同理可证 $\theta^{-1}(x \cdot y) = \theta^{-1}(x) \cdot \theta^{-1}(y)$. 同时显然 θ^{-1} 为双射, 故为环同构. □

Example 1.16 $\text{Aut}(\mathbb{Z}) = \{\text{Id}_{\mathbb{Z}}\}, \text{Aut}(\mathbb{Z}[i]) = \{\text{Id}_{\mathbb{Z}[i]}, \sigma\}$, 其中 σ 为取复共轭.

Definition 1.9

对环同态 θ , 定义 θ 的**核**为 $\ker(\theta) = \theta^{-1}(0_S) \subseteq R$.



沿用第一节的记号, 则 $a \stackrel{\theta}{\sim} b$ 当且仅当 $a-b \in \ker(\theta)$. 此外 $[a] = a + \ker(\theta), R / \stackrel{\theta}{\sim} \underset{\theta}{\sim} \text{Im}(\theta)$.

对 $\ker(\theta)$ 我们有如下观察:

- (1) $\ker(\theta)$ 对加法和乘法封闭.
- (2) $\ker(\theta)$ 不是子环, 因为 $1_R \notin \ker(\theta)$.
- (3) $\forall a \in R, r \in \ker(\theta)$, 有 $a \cdot r \in \ker(\theta)$.

这提示我们进行如下的定义

Definition 1.10

非空子集 $I \subseteq R$ 称为**理想**, 记作 $I \triangleleft R$, 若

$$(1) \forall a, b \in I, \text{ 有 } a+b \in I.$$

$$(2) \forall a \in R, r \in I, \text{ 有 } a \cdot r \in I.$$



Remark (1) $R \triangleleft R$, 此外的理想称为真理想, 显然 $I \triangleleft R$ 为真理想等价于 $1_R \notin I$.

(2) $\{0_R\} \triangleleft R$, 它与 R 本身称为 R 的平凡理想.

(3) $\forall a \in R, (a) = aR = \{a \cdot r : r \in R\} \triangleleft R$, 这种理想称为主理想.

(4) I_1, I_2 为 R 的理想, 则 $I_1 + I_2, I_1 I_2, I_1 \cap I_2$ 也为 R 的理想.

Lemma 1.1

R 是域 $\iff R$ 仅有平凡理想.



证明 \Rightarrow : 若存在 $I \triangleleft R$ 且存在 $0_R \neq a \in I$, 则 $1_R = a^{-1} \cdot a \in I$, 则 $I = R$.

\Leftarrow : 任意 $0_R \neq a \in R$, 则由假设 $(a) = R$, 故 $1 \in (a)$, $\exists b, \text{s.t. } a \cdot b = 1_R$, 故 $a \in U(R)$, R 为域. \square

Example 1.17 我们来分类 \mathbb{Z} 的所有理想. 设 $\{0\} \neq I \triangleleft \mathbb{Z}$, 则取 $0 \neq n \in I$ 使得 $|n|$ 最小, 首先有 $n\mathbb{Z} \subseteq I$.

其次任意 $r \in I$, 由带余除法 $r = nq + r', q \in \mathbb{Z}, 0 \leq r' < |n|$, 则 $r' = r - nq \in I$, 由 n 的选取有 $r' = 0$, 故 $n|r, I \subseteq n\mathbb{Z}$. 综上 $I = n\mathbb{Z}$.

故 \mathbb{Z} 的所有理想为 $n\mathbb{Z} (n \in \mathbb{N})$.

Definition 1.11

$I \triangleleft R$, 则定义 $a \equiv b \pmod{I} \iff a - b \in I$, 不难验证这给出了一个等价关系, 则可以定义 $R/I = R/\equiv = \{\bar{a} : a \in R\}$.

R/I 上有自然的运算 $\bar{a} + \bar{b} = \overline{a+b}, \bar{a} \cdot \bar{b} = \overline{a \cdot b}$ (可以验证良定性), 则 R/I 是一个环, 称为商环.

定义 $\text{can} : R \rightarrow R/I, a \mapsto \bar{a}$ 为自然的满同态, 则显然 $\ker(\text{can}) = I$.



Proposition 1.9 (核理想的泛性质)

$\theta : R \rightarrow S$ 为环同态, $I \triangleleft R, \text{can} : R \rightarrow R/I$, 则 $I \subseteq \ker(\theta) \iff \exists \theta' : R/I \rightarrow S$, 使得 $\theta = \theta' \circ \text{can}$.

$$\begin{array}{ccc} R & \xrightarrow{\theta} & S \\ \downarrow \text{can} & \searrow \theta' & \\ R/I & & \end{array}$$



证明 \Rightarrow : 直接定义 $R/I \xrightarrow{\theta'} S, \bar{a} \mapsto \theta(a)$. 还需验证良定性, 即不依赖于代表元的选取: 取 $\bar{a} = \bar{a}'$, 则 $a - a' \in I \subseteq \ker(\theta)$, 故 $\theta(a) = \theta(a')$.

\Leftarrow : $I = \ker(\text{can}) \subseteq \ker(\theta)$. \square

Theorem 1.2 (环同态基本定理)

设 $\theta : R \rightarrow S$ 为环同态, 则存在唯一环同构 $\bar{\theta} : R/\ker(\theta) \xrightarrow{\sim} \text{Im}\theta$, 使得如下图表交换

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



这是映射基本定理的特殊情形.

Example 1.18 $\theta: R \rightarrow S$ 为单的等价于 $\ker(\theta) = \{0_R\}$, 此时有 $\bar{\theta}: R \xrightarrow{\sim} \text{Im}\theta$.

若 θ 是满的, 则 $S \simeq R/\ker(\theta)$.

Example 1.19 考虑之前定义的特征映射 $\phi: \mathbb{Z} \rightarrow R, m \mapsto m1_R$, 则 $\ker(\phi) = n\mathbb{Z}$ ($n = 0$ 或 $n \geq 2$).

$n = 0$ 时 ϕ 是单的; $n \geq 2$ 时 ϕ 不单, 有 $\bar{\phi}: \mathbb{Z}_n \hookrightarrow R$. 两种情况下均称 n 为 R 的特征, 记为 $\text{char}(R)$.

可以证明对整环 R , R 的特征为 0 或素数 p .

Example 1.20 考虑 $I \triangleleft R, J \triangleleft R, I \subseteq J$, 则可定义: $R/I \rightarrow R/J, a + I \mapsto a + J$ (可验证良定性), $\ker = \{a + I : a \in J\} \triangleleft R/I$, 应用同态基本定理, 我们有:

$$(R/I)/(J/I) \xrightarrow{\sim} R/J$$

$$\bar{a} + J/I \mapsto a + J$$

进一步地, 给定 $I \triangleleft R$, 我们有如下的双射:

$$\{J \triangleleft R : I \subseteq J\} \leftrightarrow \{K : K \triangleleft R/I\}$$

$$J \mapsto J/I = \{a + I : a \in J\}$$

练习: 证明上面的对应是一一对应, 并且利用之给出 \mathbb{Z}_n 的所有理想.

1.4 分式域和商域

考虑整环 R , 定义 $R^* = R - \{0\}$, 则定义 $R \times R^*$ 上的关系

$$(a, x) \sim (b, y) \iff a \cdot y = b \cdot x \in R.$$

仍然不难验证这确实是一个等价关系, 则定义**分式** $\frac{a}{x}$ 为 (a, x) 在 $R \times R^*$ 中的等价类, 故

$$\frac{a}{x} = \frac{a'}{x'} \iff ax' = a'x \in R.$$

定义分式的全体为 $\text{Frac}(R) = (R \times R^*) / \sim \subseteq \mathcal{P}(R \times R^*)$. 我们自然定义其上的运算:

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

首先整环告诉我们 $xy \neq 0_R$, 故能定义如上的分式. 其次可以验证上述定义不依赖于代表元的选取:

设 $\frac{a}{x} = \frac{a'}{x'}$, $\frac{b}{y} = \frac{b'}{y'}$, 即 $ax' = a'x$, $by' = b'y$, 则只需 $\frac{ay+bx}{xy} = \frac{a'y'+b'x'}{x'y'}$, $\frac{ab}{xy} = \frac{a'b'}{x'y'}$. 第二个式子是显然的, 第一个式子:

$$(ay + bx)(x'y') - (a'y' + b'x')(xy) = ax'yy' + by'xx' - a'xyy' - b'yxx' = 0, \text{ 故证明了良定性.}$$

Proposition 1.10

(1) $(\text{Frac}(R), +, \cdot)$ 是含么交换环, 并且是域, 称为环 R 的**分式域**.

(2) 可定义单同态 $\text{can}_R : R \hookrightarrow \text{Frac}(R)$, $a \mapsto \frac{a}{1_R}$, 且 can_R 是同构当且仅当 R 是域.

证明 (1) 加法和乘法如上面定义, 可自然定义零元 $\frac{0_R}{1_R}$, 么元 $\frac{1_R}{1_R}$, 负元 $-\frac{a}{x} = \frac{-a}{x}$, 且对 $\forall \frac{a}{x} \neq \frac{0_R}{1_R}$, 有 $\frac{a}{x} \cdot \frac{x}{a} = \frac{1_R}{1_R}$, 故可逆, 则 $\text{Frac}(R)$ 为域.

(2) 不难验证为同态, 且 $\frac{a}{1_R} = \frac{0_R}{1_R}$ 等价于 $a = 0_R \in R$, 故 can_R 为单同态. 若为同构, 则由 $\text{Frac}(R)$ 为域有 R 为域.

反之设 R 为域, 则任意 $\frac{a}{x} \in \text{Frac}(R)$, 有 $\frac{a}{x} = \frac{x^{-1}a}{1_R} \in \text{Im}(\text{can}_R)$, 故为同构. \square

Proposition 1.11 (can_R 的泛性质)

R 整环, K 域, 则 \forall 单同态 $\phi : R \hookrightarrow K$, $\exists! \tilde{\phi} : \text{Frac}(R) \hookrightarrow K$, 使得有下面的交换图表.

$$\begin{array}{ccc} R & \xrightarrow{\text{can}_R} & \text{Frac}(R) \\ \downarrow \phi & \nearrow \exists! \tilde{\phi} & \\ K & & \end{array}$$

证明 唯一性: 若 $\tilde{\phi}$ 存在, 则 $\tilde{\phi}(\frac{a}{1_R}) = \phi(a)$, 故

$$\tilde{\phi}(\frac{a}{x}) = \tilde{\phi}(\frac{a}{1_R} \cdot (\frac{x}{1_R})^{-1}) = \tilde{\phi}(\frac{a}{1_R}) \cdot (\tilde{\phi}(\frac{x}{1_R}))^{-1} = \phi(a) \cdot \phi(x)^{-1}.$$

即 $\tilde{\phi}$ 由上式唯一确定.

存在性: 只用验证 $\tilde{\phi} : \text{Frac}(R) \rightarrow K$, $\frac{a}{x} \mapsto \phi(a) \cdot \phi(x)^{-1}$ 是一个良定的单同态, 并满足上面的交换图表.

良定性: 若 $\frac{a}{x} = \frac{a'}{x'}$, 则 $ax' = a'x$, 只需证 $\phi(a) \cdot \phi(x)^{-1} = \phi(a') \cdot \phi(x')^{-1}$, 这等价于 $\phi(a) \cdot \phi(x') = \phi(a') \cdot \phi(x)$, 由 ϕ 是同态, 这成立.

单同态且满足交换图表: 易验证是单同态, 且 $\tilde{\phi}(\text{can}_R(a)) = \tilde{\phi}(\frac{a}{1_R}) = \phi(a), \forall a \in R$, 故得证. \square

Remark 由上面讨论, $\tilde{\phi}: \text{Frac}(R) \rightarrow K$ 为同构 $\iff \forall w \in K$ 可以表示为 $\phi(a) \cdot \phi(x)^{-1}$ 的形式.

Example 1.21 $\text{Frac}(\mathbb{Z}) = \mathbb{Q}, \text{Frac}(\mathbb{Z}[i]) = \mathbb{Q}(i)$: 由上面的命题, 对单嵌入 $\text{inc}: \mathbb{Z}[i] \hookrightarrow \mathbb{Q}(i)$, 可以得到诱导映射: $\text{Frac}(\mathbb{Z}[i]) \hookrightarrow \mathbb{Q}(i)$.

又对任意 $a + bi \in \mathbb{Q}(i)$, 由于 $a, b \in \mathbb{Q}$, 可以取 $m' \in \mathbb{N} - \{0\}$ 和 $m, n \in \mathbb{Z}$, 使得 $a + bi = \frac{m+ni}{m'} = (m+ni) \cdot (m')^{-1}$, 则由上面的 Remark, 诱导映射给出了同构 $\text{Frac}(\mathbb{Z}[i]) \xrightarrow{\sim} \mathbb{Q}(i)$.

Example 1.22 对域 F , (1) 若 $\text{char} F = 0$, 则有单嵌入 $\mathbb{Z} \hookrightarrow F$, 再由泛性质存在唯一的嵌入 $\mathbb{Q} \xrightarrow{\theta} F, \frac{n}{m} \mapsto (n1_F)(m1_F)^{-1}$.

我们自然地将 \mathbb{Q} 视为 F 的子域, 并且 F 自然成为一个 \mathbb{Q} -线性空间.

(2) 若 $\text{char} F = p > 0$, 类似地可以将 \mathbb{F}_p 嵌入到 F 中, F 成为 \mathbb{F}_p -线性空间.

Remark 在 $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$ 中可以将每个分式化简为既约表达式 $\frac{m}{n}$, 其中 $n > 0, (m, n) = 1$. 但是在一般的分式域 $\text{Frac}(R)$ 中不存在这样的既约表达式!

Definition 1.12

真理想 $P \triangleleft R$ 称为**素理想**, 若 $a \cdot b \in P$, 则 $a \in P$ 或 $b \in P$. 定义 R 的所有素理想构成的集合 $\text{Spec}(R)$ 称为 R 的**素谱**.

真理想 $\mathfrak{m} \triangleleft R$ 称为**极大理想**, 若任意 $\mathfrak{m} \subseteq I \triangleleft R$, 必有 $I = \mathfrak{m}$ 或者 $I = R$. 定义 R 的所有极大理想构成的集合 $\text{Max}(R)$ 称为 R 的**极大谱**.



素理想和极大理想有如下的基本性质.

Proposition 1.12

- (1) $\{0_R\} \triangleleft R$ 是素理想 $\iff R$ 是整环
- (2) 真理想 $P \triangleleft R$ 是素理想 $\iff R/P$ 是整环
- (3) 真理想 $\mathfrak{m} \triangleleft R$ 是极大理想 $\iff R/\mathfrak{m}$ 是域. 特别地, 极大理想均为素理想.
- (4) 对环 $R, \text{Max}(R) \neq \emptyset$.



证明 (1) 是 (2) 的特例, 故只需证 (2). \Rightarrow : 取 $\bar{a}, \bar{b} \in R/P$ 为非零等价类, 则 $a \notin P, b \notin P$, 由于 P 为素理想, 有 $a \cdot b \notin P$, 则 $\bar{a} \cdot \bar{b} = \overline{a \cdot b} \neq \bar{0}$, 故 R/P 为整环.

\Leftarrow : 若 $a \cdot b \in P$, 则 $\bar{a} \cdot \bar{b} = \bar{0} \in R/P$, 则由 R/P 为整环, $\bar{a} = \bar{0}$ 或者 $\bar{b} = \bar{0}$, 则 $a \in P$ 或 $b \in P$, 故 P 为素理想.

(3) \Rightarrow : 对 $\forall \bar{0} \neq \bar{x} \in R/\mathfrak{m}$, 则 $x \notin \mathfrak{m}$, 故

$$\mathfrak{m} \subsetneq (x) + \mathfrak{m} = \{ax + y : a \in R, y \in \mathfrak{m}\} \triangleleft R$$

又 \mathfrak{m} 为极大理想, 有 $(x) + \mathfrak{m} = R$, 则存在 $a_0 \in R, y \in \mathfrak{m}$ 使得 $a_0x + y = 1_R \in R$, 即 $\bar{a}_0\bar{x} = \bar{1}$, 故 $\bar{x} \in U(R/\mathfrak{m})$.

\Leftarrow : 若 R/\mathfrak{m} 为域, 则对 $\mathfrak{m} \subsetneq I \triangleleft R$, 有 $\{\bar{0}\} \subsetneq I/\mathfrak{m} \triangleleft R/\mathfrak{m}$. 由域只有平凡理想, $I/\mathfrak{m} = R/\mathfrak{m}$, 则 $I = R$.

(4) 利用集合论中的 Zorn 引理可以证明, 这里省略. □

Example 1.23 $\text{Max}(\mathbb{Z}) = \{(p) : p > 0 \text{ 为素数}\}, \text{Spec}(\mathbb{Z}) = \{(0)\} \cup \text{Max}(\mathbb{Z})$.

Definition 1.13

$0_R \neq a \in R$ 称为**素元**, 若 $(a) \in \text{Spec}(R)$.

$0_R \neq a \in R$ 称为**不可约元**, 若 $a \notin U(R)$, 且若 $a = bc$, 则 b 可逆或者 c 可逆. ♣

Remark (1) 对素元 a , 由于 $(a) \neq R$, 故 a 不可逆.

(2) a 为素元 $\iff \{a|xy \Rightarrow a|x \text{ 或者 } a|y\}$.

(3) \mathbb{Z} 的素元为 $\{\pm p : p = 2, 3, 5, 7 \cdots\}$, 它们也是全体不可约元.

Proposition 1.13

R 为整环, 则素元均为不可约元. ♠

证明 设 a 为素元, 故 $a \neq 0_R$ 且 $a \in U(R)$. 设 $a = bc$, 则 $a|bc \Rightarrow a|b$ 或者 $a|c$.

不妨 $a|b$, 令 $b = ax$, 则 $a = axc \Rightarrow xc = 1_R$, 故 $xc = 1_R, c \in U(R)$. □

Example 1.24 令 $R = \mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} : m, n \in \mathbb{Z}\} \subseteq \mathbb{C}$, 则 $4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$.

2 是不可约元 (模长法): 若 $a = bc$, 则 $2 = |a| = |b||c|$, 则不妨 $|b| = 1$, 设 $b = m + n\sqrt{-3}$, 则 $|b|^2 = m^2 + 3n^2 = 1$, 故 $m = \pm 1, n = 0$, 即 $b = \pm 1 \in U(R)$.

2 不是素元: $2|(1 + \sqrt{-3})(1 - \sqrt{-3})$, 但 $2 \nmid (1 + \sqrt{-3})$ 且 $2 \nmid (1 - \sqrt{-3})$.

1.5 一元多项式环

对环 R , x 为一个符号 (不一定为 R 中元素), 定义 R 上关于 x 的一元多项式为形式和 $f(x) = a_n x^n + \cdots + a_1 x + a_0 = \sum_{i=0}^n a_i x^i$. 其中 $a_i x^i$ 称为单项式, 即多项式为单项式的形式和. 称两个多项式相等是指对应位置的系数均相等. 这里我们特别地约定 $0_R x^i$ 略去, $1_R x^i = x^i$.

对于如上的一个多项式, 若 $a_n \neq 0_R$, 则称 $a_n x^n$ 为 $f(x)$ 的**首项**, a_n 为**首项系数**, **常数项**为 a_0 , 次数 $\deg f(x) = n$. 记 $R[x]$ 为 R 上关于 x 的多项式全体所构成的集合.

$f(x) \in R[x]$ 称为**首一**, 若 $a_n = 1_R$. 定义**零多项式**为 $0_R x + 0_R = 0_R$, 我们不定义 $\deg(0_R)$.

Proposition 1.14

$R[x]$ 自然成为环.



证明 加法: 将对应位置系数相加即可

乘法: $f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{j=0}^m b_j x^j$, 则定义 $f(x) \cdot g(x) = \sum_{l=0}^{m+n} c_l x^l$, 其中 $c_l = \sum i a_i b_{l-i}$.

零元和么元: 零元为零多项式, 也记为 0_R . 么元为取值恒为 1_R 的常值多项式, 也记为 1_R .

负元: $f(x) = \sum_{i=0}^n a_i x^i$, 定义 $-f(x) = \sum_{i=0}^n (-a_i) x^i$. □

Remark 有自然的环嵌入 $R \hookrightarrow R[x], a \mapsto a$, 注意后者的含义是取值恒为 a 的常值多项式.

Proposition 1.15

R 为整环, 则 $R[x]$ 为整环.



证明 若 $f(x)$ 和 $g(x)$ 均非零, 则设 $f(x) = a_n x^n + \text{低次项}$, $g(x) = b_m x^m + \text{低次项}$, 其中 $a_n \neq 0_R, b_m \neq 0_R$.

有 $f(x) \cdot g(x) = a_n b_m x^{n+m} + \text{低次项}$, 由于 R 为整环, $a_n b_m \neq 0$, 故 $f(x) \cdot g(x) \neq 0$. □

Remark 由上面的证明过程, 若 $f(x), g(x)$ 非零, 则 $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

Proposition 1.16 (多项式环的泛性质)

设 R 为环, \forall 环同态 $\psi: R \rightarrow S$ 和 $s \in S$, $\exists!$ 环同态 $\tilde{\psi}: R[x] \rightarrow S$, 使得 $\tilde{\psi}|_R = \psi, \tilde{\psi}(x) = s$.

$$\begin{array}{ccc} R & \xrightarrow{\psi} & S \\ \downarrow & \searrow \exists \tilde{\psi} & \\ R[x] & & \end{array}$$



证明 定义 $\tilde{\psi}(a_n x^n + \cdots + a_1 x + a_0) = \psi(a_n) s^n + \cdots + \psi(a_1) s + \psi(a_0)$, 并验证为同态即可. □

Example 1.25 考虑恒等同态: $\text{Id}_R: R \rightarrow R$, 固定 $a \in R$, 应用上面的命题, 我们可以得到同态 $\text{ev}_a: R[x] \rightarrow R, x \mapsto a$. 该同态也称为 a 处的**赋值同态**.

$\text{ev}_a(f(x)) = a_n a^n + \cdots + a_1 a + a_0 \in R$ 称为 f 在 a 处的值, 记为 $f(a)$ (更严格的写法应为 $f(x)(a)$).

Example 1.26 对 $f(x) \in R[x]$, 利用上面的赋值同态可以定义所谓的多项式函数

$$f : R \rightarrow R, a \mapsto f(a) = \text{ev}_a(f) \in R.$$

故 $f \in \text{Map}(R, R)$. 注意记号 f 和 $f(x)$ 之间的区别!

下面我们来考虑域上的一元多项式. 总设 k 是一个域.

首先我们可以对多项式做首一化: 设 $f(x) = a_n x^n + \cdots + a_0, a_n \neq 0_k$, 则 a_n 可逆, 故 $\bar{f}(x) = x^n + (a_n^{-1} a_{n-1}) x^{n-1} + \cdots + (a_n^{-1} a_0)$ 为首一多项式, $f(x)$ 和 $\bar{f}(x)$ 之间差一个单位 a_n , 称 $f(x)$ 和 $\bar{f}(x)$ 相伴.

此外域上的多项式还可以进行如下的带余除法.

Proposition 1.17

$f(x) \in k[x], 0_k \neq h(x) \in k[x]$, 则存在唯一的 $g(x), r(x) \in k[x]$, 使得 $f(x) = q(x) \cdot h(x) + r(x)$, 且满足 $r(x) = 0_k$ 或者 $\deg r < \deg h$. 我们称 $q(x)$ 为 $f(x)$ 关于 $h(x)$ 的商, $r(x)$ 为余式.



证明 若 $\deg h > \deg f$, 则取 $q(x) = 0, r(x) = h(x)$ 即可.

否则设 $f(x) = b_m x^m + \cdots, h(x) = a_n x^n + \cdots, m \geq n$, 则 $f(x) - \frac{b_m}{a_n} x^{m-n} h(x) = b'_{m-1} x^{m-1} + \cdots$. 则得到了想要的分解. \square

Proposition 1.18

给定 $f(x) \in k[x], a \in k$, 则 $\exists! q(x) \in k[x], \text{s.t. } f(x) = q(x) \cdot (x - a) + f(a)$.



证明 又上面的命题, 存在 $r \in k$ 使得 $f(x) = q(x) \cdot (x - a) + r$. 将 ev_a 作用于两边, 则有 $f(a) = q(a) \cdot (a - a) + r, r = f(a)$. \square

Remark 由该命题 $(x - a) | f(x) \iff f(a) = 0_k$. 所以求解 $f(x)$ 在 k 中的根的问题就转化为了考虑 $x - a$ 是否为 $f(x) \in k[x]$ 的因子.

Definition 1.14

整环 R 称为主理想整环 (PID), 若任意 $I \triangleleft R$ 为主理想.



Theorem 1.3

\mathbb{Z} 和 $k[x]$ 均为 PID.



证明 由之前对 \mathbb{Z} 所有理想的列举可知为 PID.

对 $0 \neq I \triangleleft k[x]$, 取 $h(x) \in I$ 为 I 中次数最小的多项式, 则显然 $(h(x)) \subseteq I$. 另一方面, $\forall f(x) \in I$, 有分解 $f(x) = q(x) \cdot h(x) + r(x)$, 满足 $r(x) = 0_k$ 或者 $\deg r < \deg h$. 由于 $r(x) = f(x) - q(x)h(x) \in I$ 和 $h(x)$ 的选取, 只能 $r(x) = 0$, 则 $h(x) | f(x)$, 故 $I = (h(x))$. \square

PID 有如下的基本性质.

Proposition 1.19

- (1) R 为 PID, 则可以定义所谓的最大公因子: $\forall a, b \in R, \exists d \in R$, 使得 $d|a, d|b$, 且对 $\forall d'|a, d'|b$, 有 $d'|d$. 此时记 $d = \gcd(a, b)$. 它在相伴意义下是唯一的, 且满足 *Bezout* 等式: $\exists u, v \in R$, s.t. $ua + vb = d$.
- (2) R 为 PID, 则素元等价于不可约元.
- (3) R 为 PID, 则 $\text{Spec}(R) = \{(0)\} \cup \text{Max}(R)$.



证明 (1) 由于 R 为 PID, 故存在 $d \in R$ 使得 $(a) + (b) = (d)$. 则 d 为所求, 且显然满足 *Bezout* 等式.

(2) 只需证若 a 为不可约元, 则为素元. 设 $a|bc, a \nmid b$, 则由于 a 不可约 (可以理解为 a 的因子本质上只有 1 和 a 本身), 有 $\gcd(a, b) = 1$. 由 *Bezout* 等式, 存在 $u, v \in R$ 使得 $1 = va + ub, c = vac + ubc$, 右边为 a 的倍数, 故 $a|c$.

(3) 对任意 $0 \neq P$ 为素理想, 只需证其极大. 考虑 $(a) = P \subset I = (b) \subsetneq R$, 则 $b \notin U(R)$, 且 $b|a$. 由于 a 为素元, 则存在单位 u , 使得 $b = ua$. 故 $P = (a) = (b) = I$. \square

我们将上述 PID 的性质应用到 $k[x]$ 上.

对 $f(x), g(x) \in k[x]$, 定义它们的**最大公因式**为首一的多项式 $h(x) \in k[x]$, 使得 $h(x)$ 满足上面最大公因数的定义, 即 $h(x)|f(x), h(x)|g(x)$, 且若 $a(x)|f(x), a(x)|g(x)$, 则 $a(x)|h(x)$.

定义 k 上的**不可约多项式**为 $k[x]$ 中的不可约元 $f(x) (\deg f \geq 1)$, 则 $f(x)$ 和 $(f(x))$ 给出了 k 上首一不可约多项式和 $k[x]$ 的极大理想之间的一一对应. 这也告诉我们对于不可约多项式 $f(x)$, $k[x]/(f(x))$ 是一个域. 这个观点将在之后一直被我们使用.

Proposition 1.20

对 $\lambda \in k, k \rightarrow k[x]/(x - \lambda), a \mapsto a + (x - \lambda)$ 为同构.



而对于 $\deg f \geq 2$ 的情况我们会在下一节开始进行讨论.

1.6 添根构造

k 为域, $k[x]$ 为 PID, 对 $f(x) \in k[x]$, 考虑其解集 $\text{Root}_k(f) = \{\alpha \in k : f(\alpha) = 0_k\} \subseteq k$.

Lemma 1.2

$|\text{Root}_k(f)| \leq \deg f(x)$.



证明 对 $\deg f$ 归纳, $\deg f = 1$ 时显然成立, 设对 $1 \leq \deg g \leq n$ 都成立, 则对 $\deg f = n + 1$, 若 f 在 k 中无根, 则显然成立. 否则取 $\alpha \in \text{Root}_k(f)$, 有 $x - \alpha | f(x)$, 则存在 $g(x) \in k[x]$, $f(x) = (x - \alpha)g(x)$.

则任取 $\beta \neq \alpha \in \text{Root}_k(f)$, 则在 β 处取值有 $f(\beta) = (\beta - \alpha)g(\beta) = 0$, 即 $g(\beta) = 0, \beta \in \text{Root}_k(g)$. 又比较次数有 $\deg g = n$, 由归纳假设 $|\text{Root}_k(g)| \leq n$, 故 $|\text{Root}_k(f)| \leq 1 + n$. \square

再考虑 $k \subset K$ 为更大的域, 则 $f(x) \in k[x] \subseteq K[x]$, 有如下性质.

Proposition 1.21

- (1) $\text{Root}_k(f) \subseteq \text{Root}_K(f)$.
- (2) $f(x)$ 在 K 中为不可约多项式, 则 $f(x)$ 在 k 不可约. 但反之不成立.
- (3) 对 $f(x), g(x) \in k[x]$, 有 $\gcd_k(f, g) = \gcd_K(f, g)$.



证明 (1) 显然. (2) 若 $f(x)$ 在 K 上不可约, 则若 $f(x) = g(x)h(x), g(x), h(x) \in k[x]$, 由 K 上的不可约, 不妨 $g(x) \in U(K[x]) = K - \{0\}$, 则 $g(x) \in k - \{0\} = U(k[x])$, 故 $f(x)$ 在 k 上不可约. 反之不成立: 例如 $k = \mathbb{R}, K = \mathbb{C}, f(x) = x^2 + 1$.

(3) 记 $d(x) = \gcd_K(f, g), d'(x) = \gcd_k(f, g)$, 则由于 $d(x) | f(x), d'(x) | g(x)$ in $k[x] \subseteq K[x]$, 有 $d(x) | d(x)$ in $K[x]$.

同时在 $K[x]$ 上利用 Bezout 等式, 存在 $u(x), v(x) \in K[x]$, 使得 $d(x) = u(x)f(x) + v(x)g(x)$, 由 $d'(x) | f(x), d'(x) | g(x)$, 有 $d'(x) | d(x)$, 故得证. \square

现在我们可以来讨论添根构造. 考虑 $f(x) \in k[x]$ 为首一不可约多项式, $\deg f \geq 2$, 则同上节最后可知 $K = k[x]/(f(x)) \triangleleft k[x]$ 为一个域, 首先有自然的域嵌入: $\theta : k \hookrightarrow K, \lambda \mapsto \bar{\lambda} = \theta(\lambda) = \lambda + (f(x))$. 我们通常把 $\theta(\lambda)$ 也记为 λ .

在此基础上, 对一般的 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x]$, 可以定义 $\theta(f) = x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0} \in K[x]$. 则我们可以讲 $f(x)$ 视为 K 上的多项式. 有如下的关键观察:

Proposition 1.22

- (1) 记 $u = x + (f(x)) \in K$, 则 $u \in \text{Root}_K(\theta(f))$, 即 u 为 " $f(x)$ " 在 K 上的根.
- (2) 自然地将 K 视为 k -向量空间, 则 $\dim_k K = \deg f(x) = n$.



证明 (1)

$$\begin{aligned}\theta(f)(u) &= u^n + \overline{a_{n-1}}u^{n-1} + \cdots + \overline{a_1}u + \overline{a_0} \\ &= \overline{x}^n + \overline{a_{n-1}}\overline{x}^{n-1} + \cdots + \overline{a_1}\overline{x} + \overline{a_0} \\ &= \overline{x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0} = \overline{f(x)} = \overline{0} = 0_K\end{aligned}$$

(2) 我们断言: $\{1_K, u, \dots, u^{n-1}\}$ 构成了 K 的一组 k -基.

首先, 对任意 $\overline{g(x)} \in K[x]$, 在 $k[x]$ 中进行带余除法 $g(x) = f(x)q(x) + r(x)$, 则 $\overline{g(x)} = \overline{r(x)}$, 且 $r(x) = 0$ 或者 $\deg r(x) < n$. 故

$$\begin{aligned}\overline{g(x)} &= \overline{r(x)} = \overline{b_{n-1}x^{n-1} + \cdots + b_1x + b_0} \\ &= \overline{b_{n-1}}\overline{x}^{n-1} + \cdots + \overline{b_1}\overline{x} + \overline{b_0} \\ &= b_{n-1}u^{n-1} + \cdots + b_1u + b_0\end{aligned}$$

故 $\{1_K, u, \dots, u^{n-1}\}$ 一起 k -张成了 K .

则只需证它们 k -线性无关. 设 $c_{n-1}u^{n-1} + \cdots + c_1u + c_0 = 0_K, c_i \in k$, 即 $\overline{c_{n-1}x^{n-1} + \cdots + c_1x + c_0} = \overline{0_K}$, 则 $\overline{f(x)} | \overline{c_{n-1}x^{n-1} + \cdots + c_1x + c_0}$, 由于 $\deg f(x) = n$, 只能 $c_i = 0$. \square

Proposition 1.23 (添根构造的泛性质)

设 $k \xrightarrow{\theta} K = k[x]/(f(x))$ 如上, 任给 $k \xrightarrow{\delta} F$ 以及 $\alpha \in \text{Root}_F(\delta(f))$, 其中 $\delta(f) = x^n + \delta(a_{n-1})x^{n-1} + \cdots + \delta(a_1)x + \delta(a_0)$. 则 $\exists! K \xrightarrow{\delta'} F$, 使得 $\delta' \circ \theta = \delta, \delta'(u) = \alpha$.

$$\begin{array}{ccc} k & \xrightarrow{\delta} & F \\ \downarrow \theta & \searrow \exists \delta' & \\ K & & \end{array}$$

证明 可以定义 $\delta'' : k[x] \rightarrow F, \lambda \in k \mapsto \delta(\lambda), x \mapsto \alpha$. 则由条件 $f(x) \in \ker(\delta''), (f(x)) \subseteq \ker(\delta'')$. 又 $k[x]$ 为 PID, 设 $\ker(\delta'') = (g(x))$, 有 $g(x) | f(x)$, 因为 $f(x)$ 不可约, 只能 $f(x)$ 与 $g(x)$ 相伴, 即 $(f(x)) = (g(x))$.

则由核理想的泛性质存在单同态 $\delta' : K = k[x]/(f(x)) \hookrightarrow F, u = \overline{x} \mapsto \alpha$, 且满足图表交换. \square

Example 1.27 取 $k = \mathbb{R}, f(x) = x^2 + 1$, 则 K 的 \mathbb{R} -基为 $\{1_K, u\}$. 由于 $u \in \text{Root}_K(x^2 + 1)$, 对 $a, b, a', b' \in \mathbb{R}$, 可以计算

$$\begin{aligned}(au + b)(a'u + b') &= aa'u^2 + (ab' + ba')u + bb' \\ &= aa'(-1_K) + (ab' + ba')u + bb' = (ab' + ba')u + (bb' - aa').\end{aligned}$$

这给出了 K 的乘法结构, 以此可以证明 $K \rightarrow \mathbb{C}, u \mapsto i$ 为一个域同构, 即 $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$.

Example 1.28 $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$, 可以验证 $x^2 + x + \bar{1} \in \mathbb{F}_2[x]$ 不可约 (二次, 故只要验证没有 \mathbb{F}_2 的根), 故可以考虑 $\mathbb{F}_2 \hookrightarrow \mathbb{F}_2[x]/(x^2 + x + \bar{1}) = \mathbb{F}_4$. \mathbb{F}_4 的 \mathbb{F}_2 -基为 $\{\bar{1}, u\}$, 故 $|\mathbb{F}_4| = 4, \mathbb{F}_4 = \{\bar{0}, \bar{1}, u, u + \bar{1}\}$. 我们可以在 \mathbb{F}_4 上做基本的计算 (注意 \mathbb{F}_4 和 \mathbb{Z}_4 不同构!).

由于 $u \in \text{Root}_{\mathbb{F}_4}(x^2 + x + \bar{1})$, 则 $u^2 = u + \bar{1}$, 有 $u^{-1} = u^2, u^3 = \bar{1}$. 也立即有 $(u + \bar{1})^{-1} = u$. 并且 $x^2 + x + \bar{1} = (x - u)(x - (u + \bar{1}))$, 故 $\text{Root}_{\mathbb{F}_4}(x^2 + x + \bar{1}) = \{u, u + \bar{1}\}$.

也可以这样求逆: 在 \mathbb{F}_2 中由于 $\gcd(x + \bar{1}, x^2 + x + \bar{1}) = \bar{1}$, 故存在 $a(x)(x + \bar{1}) + b(x)(x^2 + x + \bar{1}) = \bar{1}$. 则提升到 \mathbb{F}_4 中有 $a(u)(u + \bar{1}) = \bar{1}$, 即 $(u + \bar{1})^{-1} = a(u)$. 不难发现 $a(x) = x, b(x) = \bar{1}$ 符合要求, 故 $(u + \bar{1})^{-1} = u$.

Example 1.29 $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, 同样可以验证 $x^2 + \bar{1} \in \mathbb{F}_3[x]$ 中不可约, 则考虑 $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + \bar{1})$, 有 $\{\bar{1}, u\}$ 给出 \mathbb{F}_9 的一组 \mathbb{F}_3 -基.

\mathbb{F}_9 中有 $u^2 + \bar{1} = \bar{0}, u^2 = \bar{2}, u^4 = \bar{1}$. 故 $u^{-1} = u^3 = \bar{2}u$. 故 $x^2 + \bar{1} = (x + u)(x - u) = (x - u)(x - \bar{2}u)$, 即 $\text{Root}_{\mathbb{F}_9}(x^2 + \bar{1}) = \{u, \bar{2}u\}$.

我们可以计算 $(\bar{1} + \bar{2}u)^{-1}$, 仍然是回到 $\mathbb{F}_3[x]$ 中, 有 $\gcd(\bar{1} + \bar{2}x, x^2 + \bar{1}) = \bar{1}$, 注意到 $x^2 + \bar{1} = (\bar{2}x + \bar{2})(\bar{1} + \bar{2}x) + \bar{1}$, 则 $(\bar{2}u + \bar{1})^{-1} = \bar{2}u + \bar{2}$.

1.7 欧氏整环

Definition 1.15

整环 R 称为**欧氏整环 (ED)**, 若存在 $\phi: R^* = R - \{0\} \rightarrow \mathbb{N}$, 满足: $\forall a, b \in R^*, \exists q, r \in R$, 使得 $a = qb + r$, 且 $r = 0_R$ 或者 $\phi(r) < \phi(b)$.



Example 1.30 $R = \mathbb{Z}$, $\phi(a) = |a|$, 则常规的带余除法给出了定义中的分解, 故为 ED. 注意满足定义的分解可能不唯一: 例如 $33 = 3 \cdot 9 + 6 = 4 \cdot 9 + (-3)$.

Example 1.31 k 为域, $R = k[x]$, 则令 $\phi = \deg$, 多项式的带余除法给出了定义中的分解, 故为 ED. 取 $\phi = 2 \deg$ 也符合条件, 故定义中的 ϕ 选取也不唯一.

Proposition 1.24

$ED \Rightarrow PID$.



证明 仿照 $k[x]$ 为 PID 的证明. 任取 $0 \neq I \triangleleft R$, 则取 $0 \neq b \in I$ 使得 $\phi(b)$ 最小, 显然 $(b) \subseteq I$.

另一方面, $\forall a \in I, a = qb + r$ 为定义中的分解, 则 $r = a - qb \in I$, 由 b 的选取只能 $r = 0, b|a$, 故 $a \in (b)$, 则 $I = (b)$. \square

Remark 利用代数数论的知识可以证明 $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ 是 PID, 但不是 ED.

Proposition 1.25

$\mathbb{Z}[i]$ 为 ED.



证明 定义 $N: \mathbb{Q}(i)^* \rightarrow \mathbb{Q}, m + ni \mapsto m^2 + n^2$, 则有 $N(z \cdot w) = N(z)N(w)$. 断言 N 限制在 $\mathbb{Z}[i]^*$ 上符合 ED 的定义.

$\forall x, y \in \mathbb{Z}[i]^*$, 考虑

$$\frac{x}{y} = \frac{x \cdot \bar{y}}{N(y)} = \alpha + \beta i = (m + ni) + ((\alpha - m) + (\beta - n)i)$$

其中 $\alpha, \beta \in \mathbb{Q}, m, n \in \mathbb{Z}$, 使得 $|\alpha - m| \leq \frac{1}{2}, |\beta - n| \leq \frac{1}{2}$.

则令 $q = m + ni, r = x - qy = y \cdot ((\alpha - m) + (\beta - n)i) \in \mathbb{Z}[i]$. 由于

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

故 N 符合定义, 得证. \square

上面定义的 N 有一些小的应用.

Example 1.32 计算 $U(\mathbb{Z}[i])$. 设 $x = m + ni \in U(\mathbb{Z}[i])$, 则 $xy = 1, N(x)N(y) = 1$, 只能有 $N(x) = m^2 + n^2 = 1$, 则 $x = \pm 1, \pm i$, 显然这些数确实也可逆, 故 $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$.

Example 1.33 计算 $\mathbb{Z}[i]$ 中的最大公因数. 例如计算 $\gcd(4 + 7i, 3 + 4i)$, 我们使用辗转相除类似的方法,

由于 $N(4+7i) = 65 > N(3+4i) = 25$, 故用“大”的去比“小”的, 即

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

则 $4+7i = 2 \cdot (3+4i) - (2+i)$, $\gcd(4+7i, 3+4i) = \gcd(3+4i, 2+i)$. 又由于 $\frac{3+4i}{2+i} = 2+i$, 故 $\gcd(4+7i, 3+4i) = 2+i$.

Proposition 1.26

$\mathbb{Z}[\sqrt{-2}] = \{m + b\sqrt{-2} : m, n \in \mathbb{Z}\}$ 为 ED.

证明 定义 $N : \mathbb{Q}(\sqrt{-2})^* \rightarrow \mathbb{Q}$, $m + n\sqrt{-2} \mapsto m^2 + 2n^2$, 则有 $N(z \cdot w) = N(z)N(w)$. 断言 N 限制在 $\mathbb{Z}[\sqrt{-2}]^*$ 上符合 ED 的定义.

$\forall x, y \in \mathbb{Z}[\sqrt{-2}]^*$, 同之前有

$$\frac{x}{y} = q + (\varepsilon + \eta\sqrt{-2}).$$

其中 $\alpha, \beta \in \mathbb{Q}$, $q \in \mathbb{Z}[\sqrt{-2}]$, 使得 $\varepsilon \leq \frac{1}{2}, \eta \leq \frac{1}{2}$.

则令 $r = x - qy = y \cdot (\varepsilon + \eta\sqrt{-2}) \in \mathbb{Z}[\sqrt{-2}]$. 由于

$$N(r) = N(y) \cdot (\varepsilon^2 + 2\eta^2) \leq \frac{3}{4}N(y) < N(y).$$

故 N 符合定义, 得证. □

Remark 类似可以计算 $U(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$.

然而 $\mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} : m, n \in \mathbb{Z}\}$ 不是 ED! 因为它甚至不是 PID: 在 1.4 节的末尾我们证明了 2 是不可约元但不是素元, 又 PID 中不可约元等价于素元, 故它不是 PID.

Proposition 1.27

令 $\omega = \frac{-1+\sqrt{-3}}{2}$ 为三次单位根, $\mathbb{Z}[\omega] = \{m + n\omega : m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-3})$ 称为 *Eisenstein* 整数环, 它是 ED.

证明 仍然对 $z \in \mathbb{Q}(\sqrt{-3})$ 定义模长 $N(z) = N(a+bi) = a^2 + b^2$, 特别有 $N(a+b\omega) = a^2 + b^2 - ab$, 其中 $a, b \in \mathbb{Q}$.

则与之前相同, $\forall x, y \in \mathbb{Z}[\omega]$, 可以有分解

$$\frac{x}{y} = q + (\varepsilon + \eta\omega).$$

其中 $q \in \mathbb{Z}[\omega]$, $|\varepsilon| \leq \frac{1}{2}, |\eta| \leq \frac{1}{2}$, 则 $x = qy + r', r' \in \mathbb{Z}[\omega]$, 且有

$$N(r') = (\eta^2 + \varepsilon^2 - \varepsilon\eta)N(y) \leq \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right)N(y) < N(y).$$

则得到定义中的分解, 故得证. □

Remark 由于 $1+\sqrt{-3}$ 与 2 在 $\mathbb{Z}[\omega]$ 中相伴, 故不能像在 $\mathbb{Z}[\sqrt{-3}]$ 这种那样通过 $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$ 来说明 2 不是素元. 这也和我们这里说明的 $\mathbb{Z}[\omega]$ 是 PID 是符合的.

Example 1.34 $z \in \mathbb{Z}[\omega]$, 则 $N(x) = 1$, 由此不难求出 $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}$.

Proposition 1.28

$\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$ 为 ED.



证明 定义 $N : \mathbb{Q}(\sqrt{2})^* \rightarrow \mathbb{Q}, a + b\sqrt{2} \mapsto |a^2 - 2b^2|$. 仍然重复上面的步骤, 对任意 $x, y \in \mathbb{Z}[\sqrt{2}]$, 有分解

$$x = qy + r', q \in \mathbb{Z}[\sqrt{2}], r' = (a + b\sqrt{2})y.$$

其中 $a, b \in \mathbb{Q}, |a| \leq \frac{1}{2}, |b| \leq \frac{1}{2}$, 故 $N(r') = |a^2 - 2b^2|N(y) \leq \frac{3}{4}N(y) < N(y)$. □

Example 1.35 利用同样的方法可以证明 $\mathbb{Z}[\sqrt{3}]$ 为 ED, 但需要取的更精细一些.

最后还有一个抽象的判断一个环不是 PID 的方法, 进而可以初步判断一个环是否为 ED.

Definition 1.16

对包含 \mathbb{Q} 的域 F , 称 $\alpha \in F$ 为**代数整数**, 若存在 $f(x) \in \mathbb{Z}[x]$ 首一, 使得 $f(\alpha) = 0$. 记 $\mathcal{O}_F = \{\alpha \in F \mid \alpha \text{ 为代数整数}\}$.

**Proposition 1.29**

(1) \mathcal{O}_F 是 F 的子环, 且 $\text{Frac}(\mathcal{O}_F) = F$.

(2) 设环 $R \subseteq \mathcal{O}_F$, 则若 R 为 PID (事实上对后面将要定义的 UFD 也对), 则 $R = \mathcal{O}_F$. ♠

证明超出本课范围, 故略去.

Example 1.36 令 $F = \mathbb{Q}(\sqrt{-3})$, 则显然 $\mathbb{Z}[\sqrt{-3}] \subsetneq \mathbb{Z}[\omega] \subseteq \mathcal{O}_F$. 则又上面的命题, $\mathbb{Z}[\sqrt{-3}]$ 不是 PID, 故不是 ED.

Example 1.37 同样的方法可以说明 $\mathbb{Z}[\sqrt{5}]$ 不是 ED.

Remark 对任意上面的域 F , 代数整数环 \mathcal{O}_F 是 **Dedekind 整环**, 见代数数论.

1.8 Gauss 整数环

首先再次强调一下相伴的概念.

Definition 1.17

整环 R 中非零元素 a, b 称为**相伴**, 若 $\exists u \in U(R)$ 使得 $a = ub$, 这也等价于说 $(a) = (b)$.



不难验证相伴关系式 R^* 上的相伴关系. 且对于 PID, 可以看出素元集合在相伴关系下和极大理想有一一对应.

我们本节的目标是讨论 Gauss 整数环 $\mathbb{Z}[i]$ 的素元 (称为 Gauss 素数), 又回忆 $\mathbb{Z}[i] = \{\pm 1, \pm i\}$, 故 $\mathbb{Z}[i]$ 上的相伴关系是简单的 ($m + ni$ 相伴于 $-m - ni, -n + mi, n - mi$), 则可以借此得到 Gauss 整数环的所有素理想.

Example 1.38 通过之前定义的模长可以验证 $1 + i$ 是 Gauss 素数, 则 $2 = (-i)(1 + i)^2$ 不为 Gauss 素数.

Proposition 1.30

有环同构 $\mathbb{Z}[i]/(1 + i) \xrightarrow{\sim} \mathbb{F}_2$.



证明 记 $I = (1 + i)$. 先证 $\{0, 1\}$ 构成了模 I 的完全代表系.

$\forall z = m + ni \in \mathbb{Z}[i]$, 则 $z \equiv (m - n) \pmod{I}$, 故显然 $z \equiv 0 \text{ or } 1 \pmod{I}$. 又由于 $1 \notin I$, 故 $0 \not\equiv 1 \pmod{I}$. 故为完全代表系.

则 $\mathbb{Z}[i]/(1 + i) = \{0 + I, 1 + I\}$, 又 $(1 + I) + (1 + I) = 2 + I = 0 + I$ (因为 $2 = (1 + i)(1 - i) \in I$), 故商环同构于 \mathbb{F}_2 . □

Example 1.39 练习: 讨论 $\mathbb{Z}[i]/(2)$ 的性质.

先把之前利用模长来处理素性的方法一般化:

Lemma 1.3

$z \in \mathbb{Z}[i]$, 若 $N(z) = p$ 为素数, 则 z 为 Gauss 素数.



证明 若 $z = x \cdot y \in \mathbb{Z}[i]$, 则 $N(z) = N(x)N(y) = p$, 只能 $N(x) = 1$ 或者 $N(y) = 1$, 则 x 或者 y 可逆, z 不可约, 则由 PID 为素元. □

Lemma 1.4

设 p 为 $4k + 3$ 型素数, 则 p 也为 Gauss 素数.



证明 设 $p = x \cdot y$ 为非平凡的分解, 则 $p^2 = N(x)N(y)$, 只能 $N(x) = N(y) = p$. 设 $x = m + ni$, 则 $m^2 + n^2 \equiv 3 \pmod{4}$, 矛盾! 故得证. □

再考虑 $4k+1$ 型素数.

Example 1.40 对 $4k+1$ 型素数 5, 它不是 Gauss 素数: $5 = (1+2i)(1-2i)$, 则 $1+2i$ 和 $1-2i$ 为 Gauss 素数且不相伴. 对 $13 = (2+3i)(2-3i)$, $17 = (1+4i)(1-4i)$ 有类似的讨论.

上面的例子具有一般性:

Theorem 1.4 (Fermat 二平方和)

p 为奇素数, 则 $p = 4k+1 \iff \exists a, b \in \mathbb{N}, p = a^2 + b^2$. 且这样的 a, b 是唯一的, 进而 p 唯一地给出两个互不相伴的 Gauss 素数 $a+bi, a-bi$.



证明 只需证 \Rightarrow . 唯一性的证明是初等的, 在此省略. 证明存在性只需证 p 在 $\mathbb{Z}[i]$ 中有非平凡分解, 等价于证明 $\mathbb{Z}[i]/(p)$ 不是整环.

又由于 $4|p-1$, -1 是模 p 的二次剩余, 则 $x^2 + \bar{1} = \bar{0}$ 在 \mathbb{F}_p 中有解, 故 $\mathbb{F}_p[x]/(x^2 + \bar{1})$ 不是整环. 我们断言: 有环同构 $\mathbb{Z}[i]/(p) \xrightarrow{\sim} \mathbb{F}_p[x]/(x^2 + \bar{1})$. 则存在性得证. 剩下的工作就是证明这个环同构.

第一步: 定义 $\mathbb{Z}[x] \hookrightarrow \mathbb{Z}[i], n \mapsto n \in \mathbb{Z}, x \mapsto i$, 由同态基本定理有 $\mathbb{Z}[x]/(x^2 + 1) \xrightarrow{\theta} \mathbb{Z}[i]$.

第二步: 考虑 θ 也给出了 $\mathbb{Z}[x]/(x^2 + 1)$ 的理想 $(p, x^2 + 1)/(x^2 + 1)$ 和 $\mathbb{Z}[i]$ 的理想 (p) 之间的一一对应, 则 θ 诱导了

$$\mathbb{Z}[x]/(x^2 + 1) / (p, x^2 + 1)/(x^2 + 1) \xrightarrow{\sim} \mathbb{Z}[i]/(p).$$

反复使用 $(R/I)/(J/I) \xrightarrow{\sim} R/J$, 我们有

$$\mathbb{Z}[x]/(x^2 + 1) / (p, x^2 + 1)/(x^2 + 1) \xrightarrow{\sim} \mathbb{Z}[x]/(p, x^2 + 1) \xrightarrow{\sim} \mathbb{Z}[x]/(p) / (p, x^2 + 1)/(p).$$

第三步: 考虑自然的同构 $\mathbb{Z}[x]/(p) \xrightarrow{\sim} \mathbb{F}_p[x]$, 它也给出了 $\mathbb{Z}[x]/(p)$ 的理想 $(p, x^2 + 1)/(p)$ 到 $\mathbb{F}_p[x]$ 的理想 $(x^2 + \bar{1})$ 之间的一一对应, 故诱导了同构

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

综上得证. □

这样我们完全得到了所有的 Gauss 素数

Theorem 1.5 (相伴意义下 Gauss 素数分类)

在相伴意义下, Gauss 素数有如下类: (1) $1+i$, (2) $p = 4k+3$ 素数, (3) $a \pm bi, 0 < a < b$, 其中 $a^2 + b^2 = p$ 为 $4k+1$ 型素数.



证明 显然这些为互不相伴的 Gauss 素数, 现在任取 z 为 Gauss 素数, 则有 $z|N(z) = p_1^{t_1} \cdots p_s^{t_s}$, 后者为素因数分解, 则 $N(z) = z_1 \cdots z_m, z_i$ 为定理中的 Gauss 素数. 由于 z 素, 只能对某个 $i, z|z_i$, 故 z 与

z_i 相伴. □

现在我们可以 $\mathbb{Z}[i]$ 中进行素分解.

Lemma 1.5

$p = a^2 + b^2 = 4k + 1$ 素, 则 $p \mid N(z) \Rightarrow (a + bi) \mid z$ or $(a - bi) \mid z$. ♡

证明 由条件 $(a + bi)(a - bi) = p \mid z \cdot \bar{z}$, 则 $(a + bi) \mid z \cdot \bar{z}$, 即 $(a + bi) \mid z$ 或 $(a + bi) \mid \bar{z}$, 后者显然等价于 $(a - bi) \mid z$. □

Example 1.41 $z = 29 - 2i$, 则 $N(z) = 845 = 5 \times 13^2$, 由上面引理 $(1 + 2i) \mid (29 - 2i)$ 或 $(1 - 2i) \mid (29 - 2i)$. 不难算得 $29 - 2i = (1 + 2i)(5 - 12i)$. 同理 $(2 + 3i) \mid (5 - 12i)$ 或 $(2 - 3i) \mid (5 - 12i)$, 算得 $-(2 + 3i)^2 = 5 - 12i$, 故最终有 $29 - 2i = -(2 + 3i)^2(1 + 2i)$.

Remark 利用同样的方法可以对 Gauss 整环中任何元素进行素分解, 事实上可以证明: 对任意 ED 都可以进行素分解 (利用对 $\phi(r)$ 归纳).

通过 $\mathbb{Z}[i]$ 上的素分解可以解决如下初等数论中的问题.

Theorem 1.6 (二平方定理)

$n \geq 2$, 则 n 可以写成二平方和 $\iff n = 2^l p_1^{m_1} \cdots p_t^{m_t}$, 其中若 $p_i = 4k + 3$ 型素数, 则 m_i 为偶数. ♡

证明 \Leftarrow : $n = (1^2 + 1^2)^l \prod_i (p_i^2)^{\frac{m_i}{2}} \prod_j (a_j^2 + b_j^2)^{m_j}$, 其中下标 i 对应 $4k + 3$ 型素数, j 对应 $4k + 1$ 型素数, a_j, b_j 为二平方和定理中的分解.

\Rightarrow : 由条件存在 $z \in \mathbb{Z}[i], n = N(z)$, 对 z 进行素分解 $z = z_1 \cdots z_t$, 则 $n = N(z_1) \cdots N(z_t)$, 其中 $N(z_i)$ 只能为 $2, p(4k + 1 \text{ 型})$ 和 $p^2(p \text{ 为 } 4k + 3 \text{ 型})$, □

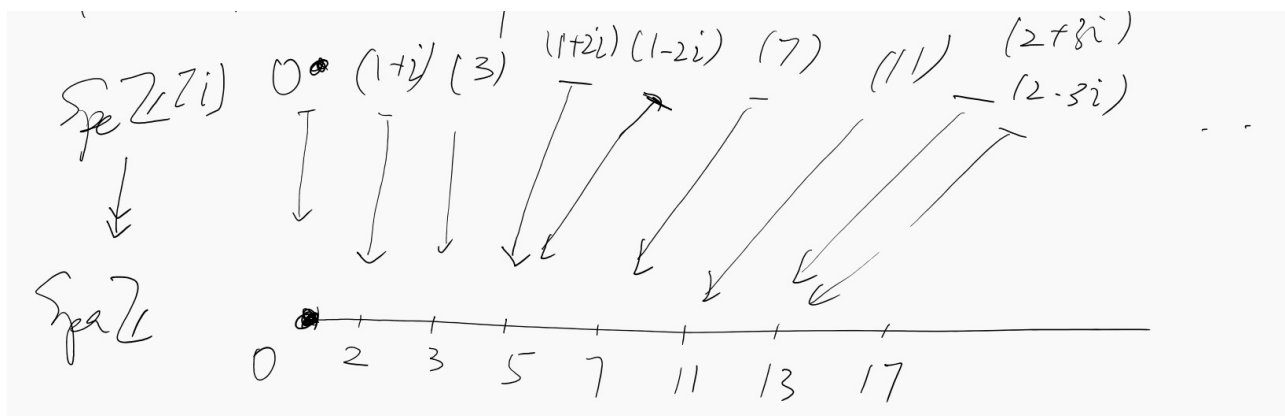
最后来考察 $\mathbb{Z}[i]$ 的素理想. 首先考虑一般的环嵌入 $R \xrightarrow{\theta} S$, 对 $q \in \text{Spec} S$, 则 $q \cap R \triangleleft R$ 为素理想 (这里 $q \cap R$ 中的 q 是通过 θ 拉回而视作 R 中的理想), 故有诱导映射 $\theta^*: \text{Spec} S \rightarrow \text{Spec} R$.

再考虑 $\mathbb{Z} \xrightarrow{\theta} \mathbb{Z}[i]$ 以及诱导映射 $\text{Spec} \mathbb{Z}[i] \xrightarrow{\theta^*} \text{Spec} \mathbb{Z}$. 不难有对应 $(0) \mapsto (0), (1 + i) \mapsto 2\mathbb{Z}, (p) \mapsto p\mathbb{Z} (p = 4k + 3), (a \pm bi) \mapsto p\mathbb{Z} (p = a^2 + b^2 = 4k + 1)$. 则有 $|(\theta^*)^{-1}(p\mathbb{Z})| = 1 \text{ or } 2$.

每个 $I \in \text{Spec}(\mathbb{Z})$ 的原像称为纤维. 下图直观表现了 $\mathbb{Z}[i]$ 的素理想到 \mathbb{Z} 的素理想的具体对应 (摘自陈小伍老师板书).

Remark 上面所用到的 “ $q \cap R \triangleleft R$ 为素理想” : 考虑 $\theta: R \hookrightarrow S \twoheadrightarrow S/q, \ker \theta = q \cap R$, 则有嵌入 $R / \theta^{-1}(q) \hookrightarrow S/q$, 后者为整环, 故前者为整环, 即 $q \cap R$ 为素理想.

用范畴论的语言来说 Spec 具有函子性, 但 Max 没有!

图 1.1: $\text{Spec} \mathbb{Z}[i]$ 到 $\text{Spec} \mathbb{Z}$ 的对应

Example 1.42 $\mathbb{Z}[i]/(3)$ 为域, 不难验证模 (3) 的完全代表元系为 $\{a+bi : a, b = 0, 1, 2\}$, 则为九元域. 或者利用 Fermat 二平方定理中的同构 $\mathbb{Z}[i]/(3) \xrightarrow{\sim} \mathbb{F}_3[x]/(x^2 + 1)$, 结合例 1.29 同样得到这个域为九元域.

Example 1.43 考虑 $\mathbb{Z}[i]/(1+2i)$, $\{0, 1, 2, 3, 4\}$ 为模 $I = (1+2i)$ 的完全代表元系: 由于 $i-2$ 和 $1+2i$ 相伴, 对任意 $m+ni$, 有

$$m+ni = (m+2n) + n(i-2) \equiv m+2n \pmod{I}.$$

不难验证 $0, 1, 2, 3, 4$ 模 I 不等价, 且 $5k+j \equiv j \pmod{I}$, 故有 $\mathbb{Z}[i]/(1+2i)$ 为五元域.

上面的结果可以一般化, 证明留作练习.

Proposition 1.31

- (1) 若 $p = a^2 + b^2 (a < b)$ 为 $4k+1$ 型素数, 则 $\mathbb{Z}[i]/(a+bi) \xrightarrow{\sim} \mathbb{F}_p$.
- (2) 若 $p = 4k+3$ 型素数, 则 $\mathbb{Z}[i]/(p)$ 是大小为 p^2 的域.



1.9 唯一因子分解整环

Definition 1.18

整环 R 称为**唯一因子分解整环 (UFD)**, 若它满足

- (1) 存在不可约分解: $\forall 0 \neq a \in R - U(R), \exists c_1, \dots, c_r$ 不可约, 使得 $a = c_1 \cdots c_r$.
- (2) 不可约分解唯一: 若 $a = c_1 \cdots c_r = c'_1 \cdots c'_t$ 如上, 则 $r = t$ 且存在置换 π 使得 c_i 和 $c'_{\pi(i)}$ 相伴 ($\forall 1 \leq i \leq r$).



Proposition 1.32

设 R 为 UFD, 则 (1) R 中不可约元等价于素元.

(2) $\forall a \in R$ 有标准分解: $\exists u \in U(R), p_1, \dots, p_r$ 不可约且互不相伴, $n_i \geq 1$, 使得 $a = up_1^{n_1} \cdots p_r^{n_r}$. 此时 a 的因子形如 $vp_1^{m_1} \cdots p_r^{m_r}, v \in U(R), 0 \leq m_i \leq n_i$, 故共有 $(n_1 + 1) \cdots (n_r + 1)$ 个互不相伴的因子.

(3) 总可以定义最大公约元、最小公倍元.

(4) 令 $K = \text{Frac}(R)$, 则任意 $\frac{a}{b} \in K$ 可以化为相伴意义下唯一既约形式 $\frac{a'}{b'}, \gcd(a', b') \sim 1$.



证明 (1) 只需证不可约元 a 为素元, 设 $a|bc$, 则

$$S = b_1 \cdots b_r c_1 \cdots c_t = b \cdot c = a \cdot d = ad_1 \cdots d_s.$$

其中 $b_1, \dots, b_r; c_1, \dots, c_t; d_1, \dots, d_s$ 为 b, c, d 的不可约分解. 又由于 S 的不可约分解的唯一性, 必须存在 b_i 或者 c_j 使得 $a \sim b_i$ 或 c_j , 则 $a|b$ 或 $a|c$, a 为素元.

(2) 若 $a \in U(R)$, 则 $a = a$ 为所求分解. 否则取 $a = c_1 \cdots c_r$ 为不可约分解, 再将所有相伴的不可约元合并在一起即可. 对 $b|a$, 设 $up_1^{n_1} \cdots p_r^{n_r} = a = bc$, 设 b 的标准分解为 $b = vuq_1^{s_1} \cdots q_t^{s_t}$, 由 a 的不可约分解的唯一性, 只能 $q_i \in \{p_1, \dots, p_r\}, s_i \leq$ 对应的 n_j .

(3) 对 $a = up_1^{n_1} \cdots p_r^{n_r}, b = vp_1^{m_1} \cdots p_r^{m_r}$, 其中 $n_j, m_i \geq 0$, 则 $\gcd(a, b) \sim p_1^{\min(n_1, m_1)} \cdots p_r^{\min(n_r, m_r)}$, 最小公倍元取次数的 \max 即可.

(4) 将 a, b 同时消掉 $\gcd(a, b)$ 则得到既约形式, 唯一性: 若 $\frac{a}{b} = \frac{c}{d}, \gcd(a, b) \sim 1 \sim \gcd(c, d)$, 则 $ad = bc$, 则只能 $a|c, c|a$, 故 $a \sim c$, 同理 $b \sim d$. □

Noether 整环也是一种存在不可约分解的例子.

Definition 1.19

(1) 对环 R 和 $X \subseteq R$, 包含 X 的最理想为 $(X) = RX = \{\sum a_i x_i : a_i \in R, x_i \in X\}$, 其中求和为有限求和. 理想 $I \triangleleft R$ 称为**有限生成**, 若存在有限集合 X , 使得 $I = (X)$, 此时 X 称为 I 的生成元集.

(2) 环 R 称为 **Noether** 的, 若 $\forall I \triangleleft R$ 有限生成.



Proposition 1.33

- (1) 显然 PID 均为 Noether 环.
- (2) Hilbert 基定理: 若 R 为 Noether 环, 则 $R[x_1, \dots, x_n]$ 及其商环也为 Noether 环.
- (3) R 为 Noether 环, 则 R 中不存在真理想的无限真升链.



证明 只证 (3). 若存在真理想的无限真升链 $I_1 \subsetneq I_2 \subsetneq \dots$, 考虑 $I = \cup_i I_i \triangleleft R$, 则取 I 的生成元集 $X = \{x_1, \dots, x_r\}$. 由于 x_i 属于 I_j 的并, 存在 m_i 使得 $x_i \in I_{m_i}$, 令 $N = \max_{1 \leq i \leq r} m_i$, 有 $I_N = I_{N+1} = \dots$, 矛盾. \square

Theorem 1.7

R 为 Noether 整环, 则 $\forall a \in R$ 有不可约分解.



证明 否则 $\exists a \in R$ 无不可约分解, 则 a 可约, 设 $a = a_1 \cdot a_2$, 则不妨 a_1 没有不可约分解, 继续设 $a_1 = a_{11}a_{12}$, 且 a_{11} 没有不可约分解, 则该过程可以一直进行下去, 进而得到真理想的无限真升链 $(a) \subsetneq (a_1) \subsetneq (a_{11}) \subsetneq \dots$, 矛盾! \square

下面的命题给出了素分解和不可约分解之间的关系.

Proposition 1.34

- (1) 设 R 为整环, a 有素分解, 则 a 的不可约分解唯一.
- (2) 若整环 R 有不可约分解 (例如 R 是 Noether 的), 则 R 为 UFD $\iff R$ 中不可约元均为素元. 特别地, PID 均为 UFD.



证明 (1) 设素分解为 $a = p_1 \cdots p_r$, 再任取不可约分解 $a = c_1 \cdots c_t$, 有 $p_1 | c_1 \cdots c_t$, 通过调整下标不妨 $p_1 | c_1$, 由 c_1 不可约只能 $p_1 \sim c_1$, 再依次对后面的元素进行同样操作, 则在调整下标后 $t = r, p_i \sim c_i$.

(2) \Rightarrow : 由命题 1.32 已知

\Leftarrow : 只需证不可约分解唯一, 由于不可约元均为素元, 故存在素分解, 由 (1) 得证. \square

Example 1.44 利用命题 1.29 和例 1.36 中的论证, 可知 $\mathbb{Z}[\sqrt{-3}]$ 不是 UFD.

Remark UFD 不一定为 PID, 例如 $\mathbb{C}[x, y], \mathbb{Z}[x]$. 它们为 UFD 直接来自于下面的 Gauss 定理, 同时也很容易看出它们不为 PID.

本节的最后来讨论多项式环是否是 UFD. 有如下的定理

Theorem 1.8 (Gauss)

R 为 UFD, 则 $R[x_1, \dots, x_n]$ 为 UFD.



下面均假设 R 为 UFD., 因为这种情况下多项式不再能直接首一化, 我们要先引入本原多项式的概念.

Definition 1.20

对 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, 定义 $f(x)$ 的容量为 $c(f) = \gcd(a_0, \cdots, a_n) \in R$. 若 $c(f) \gcd 1$, 则称 $f(x)$ 为本原多项式.

**Lemma 1.6 (Gauss 引理)**

$f(x), g(x) \in R[x]$ 本原, 则 $f(x) \cdot g(x)$ 本原.



证明 这里提供两种证法, 分别对应具体和抽象的语言.

法一: 设 $f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{j=0}^m b_j x^j$, 则 $f(x)g(x) = \sum_{l=0}^{n+m} c_l x^l, c_l = \sum_{i+j=l} a_i b_j$. 若 $f(x)g(x)$ 不本原, 则存在 p 素, 使得 $p|c_l (\forall l)$.

同时由于 f, g 本原, 存在唯一 $0 \leq i_0 \leq n, 0 \leq j_0 \leq m$, 使得 $p|a_0, \cdots, p|a_{i_0-1}, p \nmid a_{i_0}, p|b_0, \cdots, p|b_{j_0-1}, p \nmid b_{j_0}$, 则

$$c_{i_0+j_0} = (a_0 b_{i_0+j_0} + \cdots + a_{i_0-1} b_{j_0+1}) + a_{i_0} b_{j_0} + (a_{i_0+1} b_{j_0-1} + \cdots + a_{i_0+j_0} b_0).$$

第一个和第三个括号都是 p 的倍数, 但 $p \nmid a_{i_0} b_{j_0}$, 则 $p \nmid c_{i_0+j_0}$, 矛盾!

法二: 仍然设 $f(x)g(x)$ 不本原, 则取素元 $p|c_l (\forall l)$, 并定义 $\pi: R \rightarrow R/(p), r \mapsto \bar{r}$, 自然诱导同态 $\pi: R[x] \rightarrow (R/(p))[x]$.

则 $\ker \pi = p \cdot R[x], \pi(f(x)g(x)) = \pi(f(x))\pi(g(x)) = \bar{0}$. 由于 $R/(p)$ 为整环, 故 $(R/(p))[x]$ 也为整环, 则不妨 $\pi(f(x)) = 0, f \in \ker \pi = p \cdot R[x]$, 与 f 本原矛盾! \square

现在来证明 Gauss 定理.

证明 记 $K = \text{Frac}(R)$, 则 $f(x) \in R[x] \subseteq K[x]$, 后者为 PID, 进而为 UFD. 在 $R[x]$ 中 $f(x) = c(f) \cdot f_0(x) = c_1 \cdots c_r f_0(x)$, 其中 c_i 不可约 (从而为素元), f_0 本原.

构造类似上面法二中的同态 $\pi: R[x] \rightarrow (R/(c_i))[x], \ker \pi = c_i \cdot R[x]$, 故由同态基本定理 $R[x]/(c_i) \xrightarrow{\sim} R/(c_i)[x]$ 为整环, 则 $c_i \in R[x]$ 也为素元.

由于 $K[x]$ 为 UFD, 考虑不可约分解 $f_0(x) = f_1(x) \cdots f_s(x), f_i(x) \in K[x]$ 不可约. 通分有 $f_i(x) = \frac{1}{a} \tilde{f}_i(x) = \frac{c(\tilde{f}_i)}{a} \cdot \bar{f}_i(x)$.

故可以写成 $f_0 = h \bar{f}_1 \cdots \bar{f}_s$, 其中 $h \in K$, 不妨设为 $h = \frac{a}{b}, \bar{f}_i(x)$ 为 $R[x]$ 中的本原多项式. 则 $b f_0 = a \bar{f}_1 \cdots \bar{f}_s$.

由 Gauss 引理 $\bar{f}_1 \cdots \bar{f}_s$ 也为 $R[x]$ 中本原多项式, 则对两边同时取容量, 有 $a \sim b$, 则得到分解 $f_0 = \bar{f}_1 \cdots \bar{f}_s$. 由 $f_i(x)$ 在 $K[x]$ 不可约可知 $\bar{f}_i(x)$ 在 $K[x]$ 中不可约.

若 $\bar{f}_i(x) = g(x)h(x), g(x), h(x) \in k[x]$, 由 $\bar{f}_i(x)$ 在 $K[x]$ 中不可约, 不妨 $g(x) \in U(K[x]) = K - \{0\}$, 则 $g(x) = a \in R - \{0\}$, 则 $a | \bar{f}_i(x)$ in $R[x]$, 又由于 $\bar{f}_i(x)$ 在 $R[x]$ 中本原, 只能 $a \in U(R[x])$, 故 $\bar{f}_i(x)$ 在

$R[x]$ 中不可约. 则我们得到了 $f(x)$ 在 $R[x]$ 中的不可约分解.

下面只需证 $\overline{f_i}(x)$ 在 $R[x]$ 中还是素元, 则得到了素分解, 由命题 1.34, $f(x) \in R[x]$ 的不可约分解唯一, 则得证.

首先证明 $\overline{f_i}(x) \cdot R[x] = (\overline{f_i}(x) \cdot K[x]) \cap R[x]$, 左边包含于右边显然, 则任取 $g(x) = \overline{f_i}(x) \cdot h(x) \in R[x], h(x) \in K[x]$, 通分并提出容量有 $h(x) = \frac{a}{b}h_0(x)$, 其中 $h_0(x)$ 在 $R[x]$ 中本原, 则 $bg(x) = a\overline{f_i}(x)h_0(x)$, 再次使用 Gauss 引理并两边取容量有 $bc(g) = a, \frac{a}{b} \in R$, 故 $h(x) \in R[x], g(x) \in \overline{f_i}(x) \cdot R[x]$. 右边包含于左边.

则考虑 $\phi : R[x] \hookrightarrow K[x] \rightarrow K[x]/(\overline{f_i}(x)) = L$, 有 $\ker \phi = (\overline{f_i}(x) \cdot K[x]) \cap R[x] = \overline{f_i}(x) \cdot R[x]$, 则 $R[x]/(\overline{f_i}(x) \cdot R[x]) \hookrightarrow L$, 由 L 为整环, 有 $R[x]/(\overline{f_i}(x) \cdot R[x])$ 为整环, 则 $\overline{f_i}(x)$ 在 $R[x]$ 中是素元. \square

1.10 拾遗

Theorem 1.9 (中国剩余定理, CRT)

设 $I_1, \dots, I_n \triangleleft R$ 且 $I_i + I_j = R (\forall i, j)$ (即两两互素), 则环同态

$$R \xrightarrow{\theta} \prod_{i=1}^n (R/I_i)$$

$$r \mapsto (r + I_1, \dots, r + I_n)$$

诱导了同构

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



证明 首先由于 $I_1 + I_2 = I_1 + I_3 = R$, 有

$$R = RR = (I_1 + I_2)(I_1 + I_3) = I_1^2 + I_2I_1 + I_1I_3 + I_2I_3 \subseteq I_1 + I_2I_3 \subseteq R.$$

故 $R = I_1 + I_2I_3$, 以此类推有 $I_1 + I_2 \dots I_n = R$, 由对称性 $\forall 1 \leq i \leq n, I_i + \prod_{j \neq i} I_j = R$.

显然 $\ker \theta = I_1 \cap I_2 \cap \dots \cap I_n$, 故只需证 θ 是满射.

$\forall a_1, \dots, a_n \in R, \forall 1 \leq i \leq n$, 由上面所证 $I_i + \prod_{j \neq i} I_j = R$, 存在 $b_i \in I_i, c_i \in \prod_{j \neq i} I_j$, s.t. $b_i + c_i = 1$. 令 $b = a_1b_1 + \dots + a_nb_n$, 可知 $\theta(b) = (a_1 + I_1, \dots, a_n + I_n)$. 故满射得证. \square

Example 1.45 对于 $(m, n) = 1$, 有 $\mathbb{Z}_{mn} = \mathbb{Z} / (m) \cap (n) \xrightarrow{\sim} \mathbb{Z}_m \times \mathbb{Z}_n$. 可以验证 $U(\mathbb{Z}_{mn}) = U(\mathbb{Z}_m \times \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$.

在 Gauss 定理的证明中, 我们证明了对 $\overline{f_i(x)}$ 本原, 若它在 $K[x]$ 中不可约 ($K = \text{Frac}(R)$), 则在 $R[x]$ 中不可约. 事实上反过来也成立.

Proposition 1.35

R 为 UFD, $K = \text{Frac}(R)$, $f(x) \in R[x]$ 本原多项式, 则 $f(x)$ 在 $R[x]$ 中不可约 $\iff f(x)$ 在 $K[x]$ 中不可约.



证明 只需证 \Rightarrow : 设在 $K[x]$ 中 $f(x) = h_1(x)h_2(x)$, 其中 $\deg h_i < \deg f$, 通分并提出容量有 $bf(x) = a\tilde{h}_1(x)\tilde{h}_2(x)$, $\tilde{h}_i(x) \in R[x]$ 本原, 由 Gauss 引理 $\tilde{h}_1(x)\tilde{h}_2(x)$ 本原, 故两边取容量有 $a \sim b$, 即 $f(x) = \tilde{h}_1(x)\tilde{h}_2(x)$, 与在 $R[x]$ 中不可约矛盾. \square

Example 1.46 显然在 $R[x]$ 中的不可约性更容易判断, 故在 $K[x]$ 中的不可约性问题可以得到简化. 例如 $f(x) = x^3 + 3x - 2 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, 不难验证 $f(x)$ 无整根, 则 \mathbb{Z} 中不可约, 由上面的命题它在 $\mathbb{Q}[x]$ 中也不可约.

Example 1.47 考虑 $k[x, y] = (k[x])[y]$, $y^3 - x^2$ 在 $k[x, y]$ 中不可约: 设 $y^3 - x^2 = (y - a(x))(y^2 + b(x, y))$, 则 $a(x)|x^2$ in $k[x]$, 只能 $a(x) = \lambda, \lambda x, \lambda x^2$, 对每种情况讨论可知不可能. 进而 $y^3 - x^2$ 在 $k(x)[y]$ 中不可

约.

练习: 令 $A = k[x, y] / (y^3 - x^2)$ 为整环, 找出 A 的一组 k -基. 并判断 A 是否为 UFD (Hint: 考虑 $\overline{y^3}$ 的不可约分解).

上面将问题划归为了 $R[x]$ 中的不可约性判定, Eisenstein 判别法是一个重要的工具.

Theorem 1.10 (Eisenstein 判别法)

R 为 UFD, $f(x) = c_n x^n + \cdots + c_1 x + c_0 \in R[x]$ 本原多项式, 设存在 $p \in R$ 为素元使得 $p \nmid c_n, p | c_{n-1}, \cdots, p | c_1, p | c_0, p^2 \nmid c_0$, 则 $f(x)$ 在 $R[x]$ 中不可约.



证明 依然提供对应具体和抽象语言的两种证明方法, 总设 $f(x) = g(x)h(x)$ 为非平凡分解, $g(x) =$

$$\sum_{0 \leq i \leq m} a_i x^i, h(x) = \sum_{0 \leq j \leq n-m} b_j x^j.$$

法一: 由于 $p | c_0, p^2 \nmid c_0 = a_0 b_0$, 不妨设 $p \nmid b_0, p | a_0$. 则存在 $1 \leq i_0 \leq \deg g < n = \deg f$ 使得 $p | a_0, \cdots, p | a_{i_0-1}, p \nmid a_{i_0}$, 则

$$c_{i_0} = a_{i_0} b_0 + (a_{i_0-1} b_1 + \cdots + a_0 b_{i_0}).$$

括号内为 p 的倍数, $p \nmid a_{i_0} b_0$, 则 $p \nmid c_{i_0}$. 矛盾!

法二: 考虑满同态: $R[x] \xrightarrow{\pi} (R/(p))[x]$, 将 $R/(p)$ 嵌入到域 K' 中, 则 $\pi(g \cdot h) = \pi(g) \cdot \pi(h) = \bar{c}_n x^n \in K'[x]$, 由于 $K'[x]$ 为 UFD, 则只能 $\pi(g) = \bar{\xi} x^m, \pi(h) = \bar{\eta} x^{n-m}$, 则 $p | a_0, p | b_0$, 有 $p^2 | c_0 = a_0 b_0$, 矛盾! □


Example 1.48 对 $n \geq 1, x^n - 2$ 在 $\mathbb{Q}[x]$ 中不可约: 取 $p = 2$, 则由 Eisenstein 判别法有 $\mathbb{Z}[x]$ 中不可约, 由命题 1.35 得证.

Example 1.49 p 素, $f(x) = \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1}$, 则令 $g(x) = f(x+1) = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p$, 对 p 使用 Eisenstein 判别法有 $g(x)$ 在 $\mathbb{Z}[x]$ 不可约. 故 $f(x)$ 在 $\mathbb{Z}[x]$ 不可约 (为什么?), 进而 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

Chapter 2 域扩张

2.1 域扩张和单扩张

Definition 2.1

域扩张是指单域的域同态 $\theta: k \hookrightarrow K$, 记为 K/k (不是商!). 此时 k 通过 $\theta(k)$ 自然地视为 K 的子域. 

Example 2.1 考虑 $k[x]$ 中的 $d \geq 2$ 次不可约多项式 $f(x)$, 则 $K = k[x]/(f(x))$ 为域, 有自然的嵌入 $k \hookrightarrow K, \lambda \mapsto \bar{\lambda} = \lambda + (f(x))$.

回忆 $u = x + (f(x)) \in K$, 有 $u \in \text{Root}_K(f)$, 且 $\{1, u, \dots, u^{d-1}\}$ 构成 K 的一组 k -基.


Example 2.2 考虑 $k[x]$ 的分式域 $k(x) = \{\frac{f(x)}{g(x)} : g(x) \neq 0\} = \{\frac{f(x)}{g(x)} : g(x) \neq 0, \gcd(f, g) = 1, g \text{ 首一}\}$, 称为 k 上的**有理函数域**, 显然有嵌入 $k \hookrightarrow k[x] \subseteq k(x), \lambda \mapsto \lambda \mapsto \frac{\lambda}{1}$. 故 $k(x)/k$ 是域扩张.

Remark \forall 域扩张 $\theta: k \hookrightarrow K$, 则 K 有 k -线性空间的结构 $(K, +, \cdot)$, 其中加法自然定义, 数乘定义为 $\lambda \cdot v = \theta(\lambda) \cdot v, \lambda \in k, v \in K$. 这个线性空间依赖于 θ .

Definition 2.2

对域扩张 $\theta: k \hookrightarrow K, \theta': k \hookrightarrow K'$, 则称 θ 和 θ' 同构, 若存在域同构 $\phi: K \rightarrow K'$, 使得 $\phi \circ \theta = \theta'$. 称 ϕ 为 θ 到 θ' 的**域扩张同构**.

$$\begin{array}{ccc} k & \xrightarrow{\theta} & K \\ & \searrow \theta' & \swarrow \phi \\ & & K' \end{array}$$

当 $\theta' = \theta, K' = K$ 时, 从 θ 到 θ 的域同构称为 θ 的**自同构**, 所有这样的自同构的集合称为域扩张 K/k 的自同构群, 记作 $\text{Aut}(K/k)$. 

Remark 域扩张同构 ϕ 同时也是 k -线性空间同构: $\forall \lambda \in k, v \in K, \phi(\lambda \cdot v) = \phi(\theta(\lambda) \cdot v) = \phi(\theta(\lambda)) \cdot \phi(v) = \theta'(\lambda) \cdot \phi(v) = \lambda \cdot \phi(v) \in K'$.

在进一步讨论所谓的单扩张之前要引入如下的记号: 对 $R \subseteq S$ 为子环, 固定 $\alpha \in S$, 定义 $R[\alpha] = \{\sum r_i \alpha^i : r \in R\} \subseteq S$ 为 S 中包含 R 和 α 的最小子环, 其中求和为有限和. 注意这里 $R[\alpha]$ 和之前的多项式环 $R[x]$ 不一样! 更一般地, 考虑环嵌入 $\theta: R \hookrightarrow S, \alpha \in S$, 则定义 $R[\alpha]$ 为同时包含 $\theta(R)$ 和 s 的最小子环.

对域而言, 考虑 $k \subseteq K$ 为子域, $\alpha \in K$, 记 $k(\alpha) = \{(\sum r_i \alpha^i)(\sum r'_j \alpha^j)^{-1} : r_i, r'_j \in k, \sum r'_j \alpha^j \neq 0_k\}$ 为 K 中包含 k 和 α 的最小子域, 求和为有限和. 更一般地对域扩张 $\theta: k \hookrightarrow K$ 和 $\alpha \in K$, 定义 $k(\alpha) = \theta(k)(\alpha)$ 为 K 的子域.

Example 2.3 对 $\mathbb{Q} \subseteq \mathbb{C}$, 有 $\mathbb{Q}[i] = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

现在可以定义单扩张.

Definition 2.3

域扩张 K/k 称为**单扩张**, 若 $\exists \alpha \in K$, 使得 $K = k(\alpha)$. 此时称 α 为 K 的**域生成元**.



Example 2.4 $k \hookrightarrow K = k[x]/(f(x))$, $u = x + (f(x)) \in K$, 则 $K = k(u) = k[u]$.

Example 2.5 $k \hookrightarrow k(x)$, $x = \frac{x}{1}$, 则 $k \hookrightarrow k[x] \subsetneq k(x)$.

Example 2.6 $\mathbb{R} \subseteq \mathbb{C}$, 有 $\mathbb{C} = \mathbb{R}(i)$.

Definition 2.4

对域扩张 K/k , $\alpha \in K$ 称为 k 上的**代数元**, 若存在 $f(x) \in k[x]$, 使得 $f(\alpha) = 0_K$. 否则称 α 为 k 上**超越元**.



Example 2.7 对 \mathbb{C}/\mathbb{Q} , $\sqrt{2}$ 和 $\omega = e^{\frac{2\pi i}{3}}$ 为 \mathbb{Q} 上代数元.

Example 2.8 对 $k(x)/k$, x 为 k 上超越元.

Theorem 2.1

对 K/k , $\alpha \in K$, 设 α 为 k 上代数元, 则存在唯一首一不可约多项式 $f(x) \in k[x]$ 使得 $f(\alpha) = 0_K$, 且若 $g(x) \in k[x]$ 使得 $g(\alpha) = 0_K$, 则有 $f(x)|g(x)$. 这样的 $f(x)$ 称为 α 关于 k 的**最小多项式**.



证明 考虑 $\text{ev}_\alpha : k[x] \rightarrow K, g(x) \mapsto g(\alpha)$, 则由于 $k[x]$ 为 PID, 有 $\ker(\text{ev}_\alpha) = (f(x))$, 其中 $f(x)$ 首一且 $f(\alpha) = 0_K$. 又 $k[x]/(f(x)) \hookrightarrow K$, 后者为整环, 故前者为整环, $f(x)$ 不可约.

则若对 $g(x) \in k[x]$ 有 $g(\alpha) = 0$, 则 $g(x) \in (f(x))$, 有 $f(x)|g(x)$, 故 $f(x)$ 即为所求, 得证. \square

Example 2.9 对 \mathbb{C}/\mathbb{Q} , $x^3 - 2$ 为 $\sqrt[3]{2}$ 的最小多项式. 练习: 求 $\sqrt{2} + \sqrt{3}$ 的最小多项式.

Example 2.10 对 $\theta : k \hookrightarrow K$ 和 $\theta' : k \hookrightarrow K'$, 设 $\phi : K \rightarrow K'$ 为域扩张同构, 则 α 为 k 上代数 $\iff \phi(\alpha)$ 在 k 上代数, 且此时它们有一样的最小多项式.

下面的定理明确了单扩张的结构.

Theorem 2.2 (单扩张的结构定理)

设 $\theta : k \hookrightarrow K$ 和 $\alpha \in K$ 使得 $K = k(\alpha)$.

(1) 若 α 代数, 设 α 的最小多项式为 $f(x)$, $\deg f(x) = d$, 则 $\dim_k K = d < \infty$, 且 K 有 k -基 $\{1, \alpha, \dots, \alpha^{d-1}\}$, $K = k[\alpha]$, 进一步有 $\theta : k \rightarrow K$ 和 $k \rightarrow k[x]/(f(x))$ 同构.

(2) 若 α 超越, 则 $\dim_k K = \infty$, $k[\alpha] \subsetneq K$, 且有域扩张 θ 和 $k \rightarrow k(x)$ 之间的同构.



证明 (1) 若 α 代数, 考虑 $\text{ev}_\alpha : k[x] \rightarrow K$, 则由核理想的泛性质有同构 $k[x]/(f(x)) \xrightarrow{\xi} K, u \mapsto \alpha, \bar{\lambda} \mapsto \theta(\lambda)$. 则 $\text{Im} \xi = K$ 为包含 α 和 k 最小子环, 即 $k[\alpha]$, 且有 k -基 $\{1, \alpha, \dots, \alpha^{d-1}\}$. 同时显然有如下的交

换图表

$$\begin{array}{ccc} k[x]/(f(x)) & \xrightarrow{\xi} & K \\ & \searrow \theta' \nearrow & \\ & k & \end{array}$$

(2) 不难反证来验证 $\{1, \alpha, \dots, \alpha^n, \dots\}$ 在 k 上线性无关, 则 $\dim_k K = \infty$. 又由于 $\text{ev}_\alpha : k[x] \rightarrow K$ 为单射, 由分式域的泛性质, 有

$$\begin{array}{ccc} k[x] & \xrightarrow{\text{ev}_\alpha} & K \\ & \searrow \exists! \xi \nearrow & \\ & k(x) & \end{array}$$

则 $\xi : k(x) \rightarrow K, \lambda \in k \rightarrow \theta(\lambda), x \mapsto \alpha$, 故为 θ 和 $k \rightarrow k(x)$ 之间的域同构. 同时由 $k[x] \subsetneq k(x)$ 和图表的交换性, 有 $k[\alpha] \subsetneq K$. \square

Example 2.11 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 有 \mathbb{Q} -基 $1, \sqrt[3]{2}, \sqrt[3]{4}$. 特别地 $1, \sqrt[3]{2}, \sqrt[3]{4}$ 是 \mathbb{Q} -线性无关的. 对应的结果对 $n \geq 2$ 都成立.

Example 2.12 练习: 有域扩张的同构 $\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q} \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, 但 $\mathbb{Q}(\sqrt[3]{2}\omega)$ 和 $\mathbb{Q}(\sqrt[3]{2})$ 作为 \mathbb{C} 的子域不相等.

2.2 域的代数扩张

Definition 2.5

K/k 称为**代数扩张**, 若 $\forall \alpha \in K$ 为 k 上的代数元.



Lemma 2.1

有限维 (f.d.) 扩张 K/k (即 $\dim_k K < \infty$) 均为代数扩张.



证明 对 $\alpha \in K$, 有 $k \subseteq k(\alpha) \subseteq K$, 由于 K/k 有限维, 有 $\dim_k k(\alpha) < \infty$, 则由单扩张结构定理有 α 代数.

或者由 $\{1, \alpha, \dots, \alpha^n, \dots\}$ 是 k -线性无关的可以找到 α 在 $k[x]$ 中的零化多项式, 故 α 代数. \square

Proposition 2.1 (维数公式)

$k \subseteq E \subseteq K$ 为域扩张链, 若 E/k 和 F/E 均 f.d., 则 K/k 也 f.d., 且 $\dim_k K = \dim_k E \cdot \dim_E K$.



证明 线性代数练习. 取 E 的 k -基 $\{u_1, \dots, u_n\}$ 和 K 的 E -基 $\{v_1, \dots, v_m\}$, 则 $\{u_i v_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ 为 K 的 k -基:

(1) k -线性张成: $\forall \alpha \in K$, 有

$$\alpha = \sum_j y_j v_j = \sum_j \left(\sum_i \lambda_{ij} u_i \right) v_j = \sum_{i,j} \lambda_{ij} u_i v_j, y_j \in E, \lambda_{ij} \in k.$$

(2) k -线性无关: $\forall \lambda_{ij} \in k$ 且 $\sum_{i,j} \lambda_{ij} u_i v_j = 0$, 则 $\sum_j \left(\sum_i \lambda_{ij} u_i \right) v_j = 0$, 由 $\{v_j\}$ 的 E -无关性有 $\sum_i \lambda_{ij} u_i = 0 (\forall j)$, 再次由 $\{u_i\}$ 的 k -无关性有 $\lambda_{ij} = 0$. \square

Example 2.13 计算 $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 的 \mathbb{Q} -维数. 首先 $\sqrt{2}$ 在 \mathbb{Q} 的最小多项式为 $x^2 - 2$, $\{1, \sqrt{2}\}$ 为 $\mathbb{Q}(\sqrt{2})$ 的 \mathbb{Q} -基.

再考虑 $\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的最小多项式. 显然 $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ 首一且零化 $\sqrt{3}$, 且在 $\mathbb{Q}(\sqrt{2})[x]$ 中不可约: 只需证 $x^2 - 3$ 在 $\mathbb{Q}(\sqrt{2})$ 中无根. 设 $(a + b\sqrt{2})^2 = 3$, 则 $a^2 + 2b^2 = 3, 2ab = 0$, 故只能 $a = b = 0$. 则 $x^2 - 3$ 为所求的最小多项式, 故 $\{1, \sqrt{3}\}$ 为 K 的 $\mathbb{Q}(\sqrt{2})$ -基.

则 $\dim_{\mathbb{Q}} K = 2 \cdot 2 = 4$, 且 K 的一组 \mathbb{Q} -基为 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

Example 2.14 ω 为三次单位根, $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. 已知 $\mathbb{Q}(\sqrt[3]{2})$ 的 \mathbb{Q} -维数为 3, 一组基为 $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. 再求 ω 在 $\mathbb{Q}(\sqrt[3]{2})$ 上的最小多项式.

注意到 $x^2 + x + 1$ 首一且化零 ω , 故只需证 $x^2 + x + 1$ 在 $\mathbb{Q}(\sqrt[3]{2})$ 上不可约, 则只需证无根. 这是显然的, 因为 $x^2 + x + 1$ 无实根, 而 $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

故 K 的 \mathbb{Q} 维数为 $2 \cdot 3 = 6$, 一组基为 $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega\}$.

以 $\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ 的顺序考虑也可以, 则第二步需要证明 $x^3 - 2$ 在 $\mathbb{Q}(\omega)$ 上不可约, 作为练习.

Example 2.15 K/k 为 f.d. 扩张, $\alpha \in K$ 的最小多项式为 $f(x)$, 则 $\deg f \mid \dim_k K$.

回顾: K/k 称为有限生成, 若 $\exists \alpha_1, \dots, \alpha_n \in K$ 使得 $K = k(\alpha_1, \dots, \alpha_n)$.

Theorem 2.3

K/k 为 f.d. 扩张 $\iff K/k$ 为代数且有限生成的.



证明 \Rightarrow : 取 K 的 k -基 u_1, \dots, u_n , 有 $K = k(u_1, \dots, u_n)$.

\Leftarrow : 设 $K = k(\alpha_1, \dots, \alpha_n)$, 则 $k \subseteq k(\alpha_1) \subseteq k(\alpha_1, \alpha_2) \cdots \subseteq K$. 由 $k(\alpha_1)$ 在 k 上代数, 故由单扩张结构定理有 $k(\alpha_1)/k$ 为 f.d. 扩张, 依次类推任意 i 有 $k(\alpha_1, \dots, \alpha_i)/k(\alpha_1, \dots, \alpha_{i-1})$ 为 f.d. 扩张, 故由维数公式有 K/k 也 f.d. \square

Proposition 2.2

$k \subseteq E \subseteq K$, 则 K/k 代数 $\iff K/E$ 和 E/k 都代数.



证明 \Rightarrow : 显然

\Leftarrow : 任取 $\alpha \in K$, 取 $\alpha^n + u_{n-1}\alpha^{n-1} + \cdots + u_1\alpha + u_0 = 0, u_i \in E$, 则 α 在 $k(u_0, u_1, \dots, u_{n-1}) \subseteq E$ 上代数. 考虑 $k \subseteq k(u_0, \dots, u_{n-1}) \subseteq k(u_0, \dots, u_{n-1}, \alpha)$, 第一个扩张有限生成且代数, 第二个为代数的单扩张, 故 $k(u_0, \dots, u_{n-1}, \alpha)/k$ 有限维, 则代数. 进而 α 在 k 上代数. \square

下面我们讨论代数闭域的概念.

Definition 2.6

对 K/k , 定义 E 为 K 中 α 上代数元的集合, 称为 k 在 K 中的**代数闭包**. 域 K 称为**代数闭域**, 若任意代数扩张 $K \subseteq E$, 有 $K \simeq E$.



Proposition 2.3

- (1) 对域扩张 K/k , E 为如上的代数闭包, 则 E 是 K 的子域, 且 $\forall u \in K - E$, 有 u 在 E 上超越.
- (2) K 为代数闭域 \iff 任意 $K[x]$ 中不可约多项式都是一次的 \iff 任意多项式 $f(x) \in K[x]$ 完全分裂.
- (3) (代数基本定理) \mathbb{C} 为代数闭域.
- (4) 任意域 k , 存在代数扩张 $k \hookrightarrow \bar{k}$ 且 \bar{k} 代数闭域, 称 \bar{k} 为 k 的**代数闭包**.



证明 在当下我们只证明 (1). 首先证明 E 是子域: 对 $\alpha, \beta \in E$, 考虑 $k \subseteq k(\alpha) \subseteq k(\alpha, \beta)$, 两个扩张均为代数的单扩张, 故 $k(\alpha, \beta)/k$ 为代数扩张, 有 $\alpha \pm \beta, \alpha \cdot \beta, \alpha^{-1}$ 在 k 上代数.

再考虑 $\forall u \in K - E$, 若 u 在 E 上代数, 则 $k \subset E \subseteq E(u)$ 的两个扩张均代数, 有 $E(u)/k$ 代数, 则 $u \in E$, 矛盾! \square

Example 2.16 对 \mathbb{C}/\mathbb{Q} , 定义 $\overline{\mathbb{Q}}$ 为 \mathbb{Q} 在 \mathbb{C} 中的代数闭包. 可以证明 $\overline{\mathbb{Q}}$ 为可数的代数闭域. $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) =$

$\text{Aut}(\overline{\mathbb{Q}})$ 称为绝对 Galois 群.

分裂域和 Galois 群会在后面重点研究.

本节的最后来讨论延拓同态的问题: 对域同构 $\sigma: k \xrightarrow{\sim} k'$ 以及域扩张 $E/k, E'/k'$, 如何将 σ 延拓到 E 上? 即寻找 $\tilde{\sigma}: E \rightarrow E', \tilde{\sigma}|_k = \sigma$.

$$\begin{array}{ccc} E & \xrightarrow{\quad \tilde{\sigma} \quad} & E' \\ \uparrow & & \uparrow \\ k & \xrightarrow{\quad \sigma \quad} & k' \end{array}$$

处理这种问题的工具是如下的关键引理.

Lemma 2.2 (关键引理)

$\sigma: k \rightarrow k'$ 为域同构, $E/k, E'/k'$ 为域扩张, 设 $\alpha \in E$ 有最小多项式 $f(x) \in k[x]$, 则设 $\beta \in \text{Root}_{E'}(\sigma(f))$, 存在唯一 σ 的延拓 $\tilde{\sigma}: k(\alpha) \xrightarrow{\sim} k'(\beta) \subseteq E', \alpha \mapsto \beta$.

特别地, 共有 $|\text{Root}_{E'}(\sigma(f))|$ 个延拓 $\tilde{\sigma}: k(\alpha) \rightarrow E'$.

$$\begin{array}{ccc} E & & E' \\ \uparrow & & \uparrow \\ k(\alpha) & \xrightarrow{\quad \tilde{\sigma} \quad} & k'(\beta) \\ \uparrow & & \uparrow \\ k & \xrightarrow{\quad \sigma \quad} & k' \end{array}$$



证明 定义 $\tilde{\sigma}(\lambda) = \lambda \in k, \tilde{\sigma}(\alpha) = \beta$, 则只需证这么定义的 $\tilde{\sigma}$ 为域同构. 这由如下的交换图表立得:

$$\begin{array}{ccc} k(\alpha) & \xleftarrow{\quad \sim \quad} & k[x]/(f(x)) \\ \downarrow \exists! \tilde{\sigma} & & \downarrow \sigma \\ k'(\beta) & \xleftarrow{\quad \sim \quad} & k'[x]/(\sigma(f)(x)) \end{array}$$

同时若有延拓 $\tilde{\sigma}: k(\alpha) \rightarrow E'$, 必有 $\tilde{\sigma}(\alpha) \in \text{Root}_{E'}(\sigma(f))$, 故得证. □

2.3 分裂域

Definition 2.7

$f(x) \in k[x]$ 的**分裂域**是指 E/k 使得

(1) $f(x)$ 在 E 上分裂, 即 $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n), \alpha_i \in E$.

(2) $E = k(\alpha_1, \cdots, \alpha_n)$.



Remark 易见 E/k 为有限生成且代数的扩张, 故 $\dim_k E < \infty$.

Remark 分裂域确实存在: 设 $f(x) = f_1(x)\tilde{f}(x)$, $f_1(x)$ 不可约且 $\deg f_1 \geq 2$, 则令 $u_1 = \bar{x} \in K_1 = k[x]/(f_1(x))$. 在 $K_1[x]$ 中有分解 $f(x) = (x - u_1)f_{11}(x)\tilde{f}(x)$. 再对 $g(x) = f_{11}(x)\tilde{f}(x)$ 做同样的操作, 由于多项式次数一直降低, 故设在域 K 时终止, 有 $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ in $K[x]$, 则取 $E = k(\alpha_1, \cdots, \alpha_n)$ 即可.

下面是求分裂域的例子.

Example 2.17 $f(x) = \mathbb{Q}[x]$, 则有 $f(x) = (x - z_1) \cdots (x - z_n) \in \mathbb{C}[x], z_i \in \mathbb{C}$, 则 $E = \mathbb{Q}(z_1, \cdots, z_n), E/\mathbb{Q}$ 为分裂域.

例如 $x^3 - 2 \in \mathbb{Q}[x]$ 的分裂域为 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$, $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ 的分裂域为 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

Example 2.18 $f(x) = x^2 + x + \bar{1} \in \mathbb{F}_2[x]$, 则考虑嵌入 $\mathbb{F}_2 \hookrightarrow \mathbb{F}_2[x]/(x^2 + x + \bar{1}) = \mathbb{F}_4$ 以及 $u = x + (x^2 + x + \bar{1})$. 回忆 $x^2 + x + \bar{1} = (x + u)(x + u + \bar{1})$ in $\mathbb{F}_4[x]$, 故分裂域为 $\mathbb{F}_2(u, u + \bar{1})/\mathbb{F}_2 = \mathbb{F}_4/\mathbb{F}_2$.

Example 2.19 $f(x) = x^2 + \bar{1} \in \mathbb{F}_3[x]$, 则考虑嵌入 $\mathbb{F}_3 \hookrightarrow \mathbb{F}_3[x]/(x^2 + \bar{1}) = \mathbb{F}_9$ 以及 $v = x + (x^2 + \bar{1})$. 回忆 $x^2 + \bar{1} = (x + v)(x - v)$ in $\mathbb{F}_3[x]$, 故分裂域为 $\mathbb{F}_9/\mathbb{F}_3$.

可以计算分解 $x^2 - x - \bar{1} = (x - v + \bar{1})(x + v + \bar{1})$, 故 $\mathbb{F}_9/\mathbb{F}_3$ 也是 $x^2 - x - \bar{1}$ 的分裂域.

下面的定理进一步回答了之前的延拓同态问题.

Theorem 2.4

给定域同构 $\sigma: k \rightarrow k'$, 对 $f(x) \in k[x]$ 有分裂域 E/k , $\sigma(f) \in k'[x]$ 有分裂域 E'/k' , 则 σ 可以延拓为域同构 $\delta: E \rightarrow E'$, 且这样的延拓至多有 $\dim_k E = \dim_{k'} E' < \infty$ 个.



证明 对 $\dim_k E$ 归纳, $\dim_k E = 1$ 时 $k \xrightarrow{\sim} E$, 则 $f(x)$ 在 k 上分裂, 故 $\sigma(f)$ 在 k' 上分裂, 有 $k' = E'$, 则只能 $\delta = \sigma$.

再设 $\dim_k E > 1$ 且结论对 $\dim_k E$ 更小的时候均成立, 则对 $f(x) = (x - \alpha_1) \cdots (x - \alpha_n), \alpha_i \in E$, 设 $\alpha_1 \notin k$, 则 α_1 在 k 有最小多项式 $g(x), \deg g \geq 2$, 故 $g(x)|f(x)$, 记 $f(x) = g(x)h(x)$, 则 $\sigma(f) = (x - \beta_1) \cdots (x - \beta_n) = \sigma(g)\sigma(h), \beta_i \in E'$, 故 $\sigma(g)$ 在 E' 中有根.

$$\begin{array}{ccc}
E & \xrightarrow{\delta} & E' \\
\uparrow & & \uparrow \\
k(\alpha_1) & \xrightarrow{\sigma'} & k'(\beta_1) \\
\uparrow & & \uparrow \\
k & \xrightarrow{\sigma} & k'
\end{array}$$

不妨取 $\beta_1 \in E'$ 使得 $\sigma(g)(\beta_1) = 0$, 则由关键引理, 有延拓 $\sigma' : k(\alpha_1) \rightarrow k'(\beta_1), \alpha_1 \mapsto \beta_1$, 这样的延拓有 $|\text{Root}_{E'}(\sigma(g))| \leq \deg \sigma(g) = \deg g = \dim_k k(\alpha_1)$ 个.

又由于 $\dim_{k(\alpha_1)} E < \dim_k E$, 由归纳假设, 存在 σ' 的延拓 $\delta : E \rightarrow E'$, 且至多有 $\dim_{k(\alpha_1)} E$ 个. 综上 σ 的延拓 δ 存在, 且数量至多为 $\dim_k k(\alpha_1) \cdot \dim_{k(\alpha_1)} E = \dim_k E$ 个. \square

Example 2.20 考虑 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, 分裂域 $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$, 我们想计算 $\text{Aut}(E/\mathbb{Q}) = \text{Aut}(\mathbb{Q})$. 只需要找 $\text{Id}_{\mathbb{Q}}$ 的所有延拓 δ .

这种题的解决方法在上面的定理证明过程中也体现出来了, 即逐步延拓. 对 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq E$, 先考虑延拓到 $\mathbb{Q}(\sqrt[3]{2})$ 上. 对应上面证明中的记号, 则 $g(x) = x^3 - 2, \alpha_1 = \sqrt[3]{2}$, 需要找 $\beta_1 \in E = E'$ 为 $\sigma(g) = g$ 的根, 有 3 个: $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$, 对应了 3 个到 $\mathbb{Q}(\sqrt[3]{2})$ 上的延拓 σ' , 将 $\sqrt[3]{2}$ 打到 β_1 .

$$\begin{array}{ccc}
E & \xrightarrow{\delta: \omega \mapsto \beta'_1} & E \\
\uparrow & & \uparrow \\
\mathbb{Q}(\sqrt[3]{2}) & \xrightarrow{\sigma': \sqrt[3]{2} \mapsto \beta_1} & \mathbb{Q}(\beta_1) \\
\uparrow & & \uparrow \\
\mathbb{Q} & \xrightarrow{\text{Id}} & \mathbb{Q}
\end{array}$$

固定 β_1 , 再考虑 ω 在 $\mathbb{Q}(\sqrt[3]{2})$ 上的最小多项式为 $g'(x) = x^2 + x + 1 = 0$, 在 $E = E'$ 上 $\sigma'(g') = g'$ 找根 β'_1 , 有两个: ω, ω^2 , 对应 $E = \mathbb{Q}(\sqrt[3]{2})(\omega)$ 上的两个延拓 δ , 把 ω 打到对应的 β'_1 .

则总共有 6 种延拓, $|\text{Aut}(E)| = 6$, 每个延拓由它在 $\sqrt[3]{2}$ 和 ω 上的取值决定.

Example 2.21 考虑 $\mathbb{F}_2 \hookrightarrow \mathbb{F}_4 = \mathbb{F}_2[x] / (x^2 + x + \bar{1})$, 欲求 $\text{Aut}(\mathbb{F}_4) = \text{Aut}(\mathbb{F}_4/\mathbb{F}_2)$.

令 $u = x + (x^2 + x + \bar{1})$, 则 $\mathbb{F}_4 = \mathbb{F}_2(u)$, 考虑 u 在 \mathbb{F}_2 上的最小多项式 $x^2 + x + \bar{1}$, 它在 \mathbb{F}_4 上有根 $u, u + \bar{1}$, 故有两个到 \mathbb{F}_4 的延拓, 分别将 u 打到 u 和 $u + \bar{1}$.

$$\begin{array}{ccc}
\mathbb{F}_4 & \xrightarrow{\delta: u \mapsto u, u + \bar{1}} & \mathbb{F}_4 \\
\uparrow & & \uparrow \\
\mathbb{Q} & \xrightarrow{\text{Id}} & \mathbb{Q}
\end{array}$$

在上面的证明过程中也看到多项式重根的存在性会影响延拓的数量, 所以需要对重根进行研究.

Definition 2.8

称 $0 \neq f(x) \in k[x]$ 有重根, 若存在 E/k 和 $a \in E$, 使得 $(x-a)^2 \mid f(x)$.

对 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in k[x]$, 定义其形式微分为 $f'(x) = (na_n)x^{n-1} + \cdots + 2a_2 x + a_1 \in k[x]$.



Example 2.22 $(x^2 + 1)^2 \in \mathbb{R}[x]$ 无实根, 但有重根.

Remark 可以验证 $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$, 且 $\deg f' \leq \deg f - 1$, 可以取到严格的小于: 例如 $n1_k = 0_k$ 时.

Lemma 2.3

$f(x) \in k[x]$ 无重根 $\iff \gcd_k(f, f') = 1$.



证明 \Leftarrow : 若存在 E/k 使得 $(x-a)^2 \mid f(x)$, 则 $1 = \gcd_k(f, f') = \gcd_E(f, f')$. 又 $(x-a)^2 \mid f(x)$, 有 $(x-a) \mid f'(x)$, 故 $(x-a) \mid \gcd_E(f, f')$, 矛盾!

\Rightarrow : 若 $\gcd_k(f, f') = g(x)$, 则取 K 使得 $g(x)$ 在 K 上分裂, 则取 $a \in K$ 使得 $(x-a) \mid g(x)$, 故 $(x-a) \mid f'$, 则 $(x-a)^2 \mid f$: 否则 $f(x) = (x-a)h(x)$, $h(a) \neq 0$, 求微分并在 a 取值有 $f'(a) = h(a) \neq 0$, 与 $(x-a) \mid f'$ 矛盾, 故 f 有重根. \square

Definition 2.9

$0 \neq f(x) \in k[x]$ 称为 k 上可分的, 若 $f(x)$ 的不可约因子均无重根.

**Lemma 2.4**

若 $\text{char } k = 0$, 则任意 $f(x) \in k[x]$ 均可分.



证明 任取 $g(x) \in k[x]$ 不可约, 由 $\text{char } k = 0$ 有 $\deg g' = \deg g - 1$, $g' \neq 0$, 则 $\gcd(g, g') = 1$, 无重根. \square

Example 2.23 取 $k = \mathbb{F}_p(t)$, 则 $|k| = \infty$, 且 $\text{char } k = p$, 可以验证 $x^p - t \in k[x]$ 不可约, 但有重根.

结合定理 2.4 的证明过程和可分的定义, 则有

Theorem 2.5

条件同定理 2.4, 则 $f(x) \in k[x]$ 可分 \iff 这样的延拓 δ 恰有 $\dim_k E$ 个. 即此时 $|\text{Aut}(E/k)| = \dim_k E$.



Remark 可分多项式 $f(x) \in k[x]$ 的分裂域 E , 则记 $\text{Aut}(E/k) = \text{Gal}(E/k)$ 称为 E/k 的 Galois 群, 也记作 $\text{Gal}_k(f)$. 课程最后将会更系统地学习 Galois 理论, 其核心在于将 $\text{Gal}(E/k)$ 的子群和 E 的子域建立对应. 下面先给出一个例子.

Theorem 2.6 (Galois 对应)

对有限维域扩张 E/k , 对每个子群 $H \leq \text{Aut}(E/k)$, 其固定子域定义为 $E^H = \{z \in E : \sigma(z) = z, \forall \sigma \in H\} \subseteq E$. 对每个中间域 $k \subseteq K \subseteq E$, 定义 $\text{Aut}(E/K) = \{\sigma \in \text{Aut}(E) : \sigma|_K = \text{Id}|_K\}$. 则有对应 $\{H \leq \text{Aut}(E/K)\} \xrightleftharpoons[\text{Aut}(E/K) \leftarrow K]{H \rightarrow E^H} \{k \subseteq K \subseteq E : K \text{ 为中间域}\}$. 当 E/k 为某个可分多项式的分裂域时, 该对应为一一对应, 且上述为互逆映射.



Example 2.24 令 $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 为 $x^3 - 2 \in \mathbb{Q}[x]$ 的分裂域, 则 $\dim_{\mathbb{Q}} E = 6$. $X = \text{Root}_E(x^3 - 2) = \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$, 则令 $S(X)$ 为 X 上的置换全体, 显然 $|S(X)| = 3! = 6$. 则 $\text{Aut}(E)$ 和 $S(X)$ 之间有一一对应.

Example 2.25 练习: 验证 $x^4 + x + \bar{1} \in \mathbb{F}_2[x]$ 不可约, 进而 $\mathbb{F}_{2^4} = \mathbb{F}_2[x] / (x^4 + x + \bar{1})$, 求 \mathbb{F}_{2^4} 的所有子域, 并求 $x^4 + x + \bar{1}$ 在 $\mathbb{F}_{2^4}[x]$ 中的分解.

2.4 有限域

现在设 E 是有限域, 设 $\text{char} E = p > 0$, 则有嵌入 $\mathbb{F}_p \hookrightarrow E$, 且 E 上有 \mathbb{F}_p -线性空间结构, 故 $\dim_{\mathbb{F}_p} E = n \iff E \simeq \mathbb{F}_p \times \cdots \times \mathbb{F}_p$, 此时有 $|E| = p^n$.

Definition 2.10

$\sigma: E \xrightarrow{\sim} E, a \mapsto a^p$ 是一个域同构, 称为 **Frobenius 自同构**.



Remark σ 确实是同态: $\sigma(a+b) = a^p + pa^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + pab^{p-1} + b^p = a^p + b^p$, 且显然是单的, 故为域同构. 此外, 由 Fermat 小定理可知 $\sigma|_{\mathbb{F}_p} = \text{Id}$.

Example 2.26 对 $\mathbb{F}_4 = \mathbb{F}_2[x] / (x^2 + x + \bar{1})$, 则 $\mathbb{F}_4 = \{\bar{0}, \bar{1}, u, u + \bar{1}\}$, 且 $u^2 = u + \bar{1}$, 则 Frobenius 自同构 $\sigma(u) = u + \bar{1}, \sigma(u + \bar{1}) = u^2 + \bar{1} = u$, 故 $\sigma \neq \text{Id}_{\mathbb{F}_4}$, 且显然有 $\sigma^2 = \text{Id}_{\mathbb{F}_4}$.

Lemma 2.5

$\forall a \in E^* = E - \{0\}$, 有 $a^{p^n-1} = 1$, 故 $\forall b \in E$, 有 $b^{p^n} - b = \bar{0}$.



证明 固定 $a \in E^*$, 由于 E 有限, 必然存在 $i < j$ 使得 $a^i = a^j, a^{j-i} = \bar{1}$, 取 d 为最小的满足 $a^d = \bar{1}$ 的正整数, 则 $H = \{\bar{1}, a, \dots, a^{d-1}\}$ 两两不同, 且为 E^* 的子群, 由后面群论将要证明的 Lagrange 定理, 有 $d|(p^n - 1)$, 故 $a^{p^n-1} = \bar{0}$. \square

下面来证明 p^n 阶的有限域是存在唯一的.

Theorem 2.7

$\forall n \in \mathbb{N}$ 和 p 素, 存在唯一 p^n 阶有限域, 记为 \mathbb{F}_{p^n} .



证明 唯一性: 若 E 是 p^n 阶域, 则由上面的引理, $\forall a \in E$ 是 $x^{p^n} - x$ 的根, 故有 $x^{p^n} - x = \prod_{a \in E} (x - a)$, E/\mathbb{F}_p 为 $x^{p^n} - x$ 的分裂域. 则唯一确定.

存在性: 再反过来取 E 是如上的分裂域, 则 E/\mathbb{F}_p 为有限维扩张, $|E| < \infty$. 再定义 $K = \{a \in E : a^{p^n} = a\} \subseteq E$. 不难验证 K 是子域, 且由于 $x^{p^n} - x$ 无重根 (验证 $\gcd(f, f') = 1$), 有 $|K| = p^n$. 又由于 E 是分裂域, 有 $K = E$, 故 $|E| = p^n$. \square

Remark 我们实际上也证明了在 \mathbb{F}_{p^n} 中有 $x^{p^n} - x = \prod_{a \in \mathbb{F}_{p^n}} (x - a)$.

Proposition 2.4

$\mathbb{F}_p[x]$ 中有分解 $x^{p^n} - x = \prod_{d|n} \prod_{f \in M_d} f(x)$, 其中 $M_d = \{f(x) : \deg f = d, \text{且 } f \text{ 首一不可约}\}$.



证明 设 $f(x)|x^{p^n} - x$ 且首一不可约 in $\mathbb{F}_p[x]$, 取 $a \in \mathbb{F}_{p^n}$ 使得 $f(a) = 0$, 则考虑域扩张 $\mathbb{F}_p \subseteq \mathbb{F}_p(a) \subseteq \mathbb{F}_{p^n}$, 第一个扩张的维数为 $\deg f$, 则由维数公式必有 $\deg f | n$.

另一方面 $\forall g(x) \in \mathbb{F}_p[x]$ 首一不可约, 设 $\deg g = d|n$, 则考虑 $\mathbb{F}_p \hookrightarrow K = \mathbb{F}_p[x] / (g(x))$, 有

$\dim_{\mathbb{F}_p} K = d$, 故由引理 2.5 有 $u = x + (g(x))$ 满足 $u^{p^d} - u = 0$. 则 $g(x)|(x^{p^d} - x)|(x^{p^n} - x)$, 最后一步用到 $(p^d - 1)|(p^n - 1)$. 故得证. \square

Example 2.27 $p = 2$ 时, 有 $x^4 - x = x(x + \bar{1})(x^2 + x + \bar{1})$, $x^8 - x = x(x + \bar{1})(x^3 + x^2 + \bar{1})(x^3 + x + \bar{1})$.

练习: 给出 $x^{16} - x$ 在 $\mathbb{F}_2[x]$ 的分解和 $x^9 - x$ 在 $\mathbb{F}_3[x]$ 中的分解.

下面来讨论有限域的子域.

Proposition 2.5

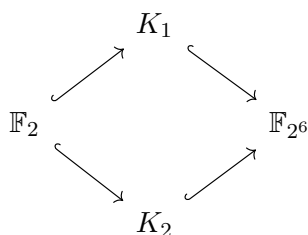
E 为 p^n 阶有限域, 则 (1) 若 $K \subseteq E$ 为子域, 则 $|K| = p^d$, d 满足 $d|n$

(2) $\forall d|n$, 存在唯一子域 $K \subseteq E$ 使得 $|K| = p^d$. 

证明 (1) 考虑 $\mathbb{F}_p \subseteq K \subseteq E$, 利用维数公式即可.

(2) 设 $|K| = p^d$, 同定理 2.7 可以证明 $K = \{a \in E : a^{p^d} - a = \bar{0}\} \subseteq E$, 且不难验证 K 确实是 E 的子域. \square

Example 2.28 对 \mathbb{F}_{2^6} , 它有三个真子域 $\mathbb{F}_2, \mathbb{F}_{2^2} = K_1, \mathbb{F}_{2^3} = K_2$.




设 $b \in K_1 \cap K_2$, 则 $\sigma^2(b) = \sigma^3(b) = b$, 故 $\sigma(b) = \sigma(\sigma^2(b)) = b$, 故 $b \in \mathbb{F}_2$, 即 $K_1 \cap K_2 = \mathbb{F}_2$.

进一步, 由于 $|K_1| = 4, |K_2| = 8, |K_1 \cap K_2| = 2$, 有 $|K_1 \cup K_2| = 10$, 则有 54 个 $u \in E - (K_1 \cup K_2)$. 对任意一个这样的 u , 均有 $\mathbb{F}_2(u)$ 既不包含于 K_1 也不包含于 K_2 , 则只能 $\mathbb{F}_2(u) = E$.

下面的命题说明上面的这种 u 的存在性是普遍的.

Proposition 2.6

对任意 n , 存在次数为 n 的 $\mathbb{F}_p[x]$ 上的不可约多项式 $f(x)$. 

证明 对 $n = q_1^{n_1} \cdots q_s^{n_s}$ 为素分解, 则 E 恰有 s 个极大真子域 $K_i, |K_i| = p^{\frac{n}{q_i}}$. 不难验证 $\sum_{i=1}^s p^{\frac{n}{q_i}} \leq s \cdot p^{\frac{n}{2}} < p^n$, 故这些极大子域不能覆盖 E .

即存在 $u \in E$ 且 $u \notin K_i (\forall 1 \leq i \leq s)$. 此时有 $\mathbb{F}_p(u) = E$, 则 E/\mathbb{F}_p 为单扩张, u 的最小多项式 $f(x)$ 的次数为 n . 则 $f(x)$ 为所求. \square

Remark (1) $\forall 1 \leq i \leq n-1$, 有 $\sigma^i(u) \neq u$: 显然 $\sigma^n(u) = u$, 则取最小的 d 使得 $\sigma^d(u) = u$, 有 $d|n$. 否则

设 $n = dq' + d'$, $d' < d$, 有 $u = \sigma^n(u) = \sigma^{d'}(u)$, 与 d 的定义矛盾! 则有命题 2.5 的证明有 u 落在某个 p^d 阶子域中, 与 u 的选取矛盾!

(2) 进而 $\forall 1 \leq i \neq j \leq n-1$, 有 $\sigma^i(u) = \sigma^j(u)$.

(3) $f(x)$ 为 u 的最小多项式, 则由于 $f(u) = 0$, 有 $0 = \sigma(f(u)) = f(\sigma(u))$, 则 u 和 $\sigma(u), \dots, \sigma^{n-1}(u)$ 都有一样的最小多项式, 进而 $f(x) = \prod_{i=1}^n (x - \sigma^i(u))$.

Theorem 2.8

$$\text{Aut}(E) = \{\text{Id}, \sigma, \dots, \sigma^{n-1}\}.$$



证明 设 $\delta: E \rightarrow E$ 为自同构, $\delta|_{\mathbb{F}_p} = \text{Id}|_{\mathbb{F}_p}$, 仍然取 u 如上, 则若 $g(\delta(u)) = 0$, 有 $\delta(g(u)) = g(\delta(u)) = 0$, 即 $g(u) = 0$, 同理则有 $g(u) = 0$ 等价于 $g(\delta(u)) = 0$. 故 u 与 $\delta(u)$ 有相同的最小多项式. 则存在 i 使得 $\delta(u) = \sigma^i(u)$.

又 $E = \mathbb{F}_p(u)$, 则容易验证 $\forall w \in E$, 有 $\delta(w) = \sigma^i(w)$, 即 $\delta = \sigma^i$. 又由于 $\sigma^i(u) \neq \sigma^j(u) (i \neq j)$, 故 $\sigma^i \neq \sigma^j (i \neq j)$. 故得证. \square

对任意 $d|n$, $H_d = \{\text{Id}, \sigma^d, \dots, \sigma^{d \cdot \frac{n}{d}}\} \leq \text{Aut}(E)$ 为子群, 它们构成了 $\text{Aut}(E)$ 的所有子群. 更进一步地有如下的 Galois 对应.

Theorem 2.9 (有限群的 Galois 对应)

$|E| = p^n$ 为有限域, 则存在一一对应 $\{K \subseteq E \text{ 为子域}\} \iff \{H \leq \text{Aut}(E) \text{ 为子群}\}$.

其中任意 $K \subseteq E$ 对应了 $\text{Aut}(E/K) = \{\delta \in \text{Aut}(E) : \delta(a) = a (\forall a \in K)\}$,

$H_d \leq \text{Aut}(E)$ 对应了 $K_d = \{a \in E : \sigma^d(a) = a\}$.

可以验证两边的对应是互逆的, 所有子域以及所有自同构群的子群都分别与 $\{1 \leq d \leq n : d | n\}$ 一一对应.



2.5 分圆域

在域 k 中, ω 称为 n 次单位根, 若 $\omega^n = 1_k$. 若 d 为最小的满足 $\omega^d = 1_k$ 的正整数, 则称 ω 为本原 d 次单位根, 记 $\text{ord}(\omega) = d$ 为 ω 的阶.

Lemma 2.6

设 $\text{ord}(\omega) = d$, 则 $\omega^n = 1 \iff d|n$.



证明 \Leftarrow : 显然.

\Rightarrow : 若 $n = dq + r, r < d$, 则 $\omega^n = 1 = \omega^{dq+r} = \omega^r$, 由 d 的定义有 $r = 0, d|n$. \square

Remark 若 $\text{char} k = p > 0, \text{ord}(\omega) = d$, 则 $p \nmid d$. 否则设 $d = d_1 p$, 则有 $\omega^d - 1 = (\omega^{d_1})^p - 1 = (\omega^{d_1} - 1)^p = 0$, 故 $\omega^{d_1} = 1$, 与 d 的定义矛盾.

Example 2.29 $|E| = p^n$ 为有限域, 则 $\omega \in E^*$, 有 $\text{ord}(\omega) | (p^n - 1)$.

Proposition 2.7

k 为域, $\omega \in k$ 为 d 次本原单位根, 则 $\text{Root}_k(x^d - 1) = \{1, \omega, \dots, \omega^{d-1}\} \leq k^*$ 为 d 阶子群.

反之, 对任意 $H \leq k^*$ 为 d 阶子群, 存在 d 次本原单位根 ω 使得 $H = \{1, \omega, \dots, \omega^{d-1}\}$, 且这样的 H 是唯一的.



在此暂时不给出证明.

下面我们重点关注复数域上的单位根. $\forall n \geq 2$, 定义 $\xi = \xi_n = e^{\frac{2\pi i}{n}}$, 则 $x^n - 1 = (x - 1)(x - \xi) \cdots (x - \xi^{n-1})$, $\{1, \xi, \dots, \xi^{n-1}\} \leq \mathbb{C}^*$ 为 n 阶子群.

Proposition 2.8

所有 n 次本原单位根为 $\{\xi^m : 1 \leq m \leq n, (m, n) = 1\}$, 共有 $\phi(n)$ 个.



证明 设 $\gcd(m, n) = d$, 则 $(\xi^m)^{\frac{n}{d}} = 1$. 另一方面若 $(\xi^m)^k = 1$, 则由引理 2.6 有 $n|mk$, 则 $\frac{n}{d}|k$. 故 $\text{ord}(\xi^m) = \frac{n}{(m, n)}$, 即 ξ^m 本原 n 次当且仅当 $(m, n) = 1$. \square

Definition 2.11

n 次分圆域定义为 $\mathbb{Q}(\xi_n)$, 也恰为 $x^n - 1 \in \mathbb{Q}[x]$ 的分裂域.

n 次分圆多项式定义为 $\Phi_n(x) = \prod_{1 \leq m \leq n-1, (m, n)=1} (x - \xi^m) \in \mathbb{C}[x]$. 显然有 $\deg \Phi_n(x) = \phi(n)$.



Example 2.30 $\mathbb{Q}(\xi_2) = \mathbb{Q}, \mathbb{Q}(\xi_3) = \mathbb{Q}(\frac{-1+\sqrt{3}i}{2}), \mathbb{Q}(\xi_4) = \mathbb{Q}(i)$.

$\Phi_1(x) = x - 1, \Phi_2(x) = x + 1, \Phi_3(x) = x^2 + x + 1$.

Lemma 2.7

$x^n - 1 = \prod_{d|n} \Phi_d(x)$, 进而 $\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d < n} \Phi_d(x)} \in \mathbb{Z}[x]$.



证明 $\forall d|n$, 由 $\text{ord}(\xi^m) = \frac{n}{(m, n)}$, d 次本原单位根全体为 $\mu_d = \{\xi^{m' \cdot \frac{n}{d}} : 1 \leq m' \leq d-1, (m', \frac{n}{d}) = 1\}$.

进而 $\{1, \xi, \dots, \xi^{n-1}\} = \sqcup_{d|n} \mu_d = \sqcup_{d|n} \mu_d = \{\xi^{m' \cdot \frac{n}{d}} : 1 \leq m' \leq d-1, (m', \frac{n}{d}) = 1\}$. 故

$$x^n - 1 = (x - 1)(x - \xi) \cdots (x - \xi^{n-1}) = \prod_{d|n} \prod_{\text{ord}(\omega)=d} (x - \omega) = \prod_{d|n} \Phi_d(x).$$

我们归纳证明 $\Phi_n(x) \in \mathbb{Z}[x]$. 设对 $d < n$ 都成立, 则考虑 $\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d < n} \Phi_d(x)}$, 由归纳假设分母为首一的整系数多项式. 则问题转化为 $f(x) = g(x)h(x)$, 其中 $f(x), g(x) \in \mathbb{Z}[x], h(x) \in \mathbb{C}[x]$, 且 $g(x)$ 首一, 要证明 $h(x) \in \mathbb{Z}[x]$.

在 $\mathbb{Z}[x]$ 上做带余除法 $f(x) = g(x)q(x) + r(x)$, 其中 $q(x), r(x) \in \mathbb{Z}[x]$ 且 $r = 0$ 或 $\deg r < \deg g$, 则 $g(q - h) = r$, 比较次数只能有 $r = 0, q = h$, 故 $h(x) \in \mathbb{Z}[x]$. \square

Example 2.31 由此可以更方便地计算出分圆多项式, 例如 $\Phi_4(x) = x^2 + 1, \Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ 等.

最后讨论域扩张 $\mathbb{Q}(\xi_n)/\mathbb{Q}$ 的性质.

Theorem 2.10 (Gauss, 1801)

$\Phi_n(x) \in \mathbb{Z}[x]$ 不可约.



进而直接有

Theorem 2.11

(1) $\xi = \xi_n$ 在 \mathbb{Q} 上的最小多项式为 $\Phi_n(x)$.

(2) $\dim_{\mathbb{Q}} \mathbb{Q}(\xi_n) = \phi(n)$.

(3) 有一一对应 $\text{Aut}(\mathbb{Q}(\xi_n)/\mathbb{Q}) = \text{Aut}(\mathbb{Q}(\xi_n)) \xrightarrow{\sim} U(\mathbb{Z}_n), \sigma \mapsto \bar{k}$, 其中 σ 由 $\sigma(\xi) = \xi^k$ 决定.

事实上这是一个群同构, 特别地 $|\text{Aut}(\mathbb{Q}(\xi_n))| = \phi(n)$.



下面来证明定理 2.10, 即 $\Phi_n(x)$ 不可约. 首先是 $n = p$ 为素数的情况, 此时 $\Phi_p(x) = \frac{x^p - 1}{x - 1}$, 之前利用 Eisenstein 判别法证明过它不可约.

对一般的 $\xi = \xi_n$, 取其 \mathbb{Z} 上最小多项式 $f(x)$, 则 $f(x) | \Phi_n(x)$. 我们断言: 若 p 素且 $p \nmid n, z$ 为 n 次本原单位根, 则 $f(z) = 0$ 能推出 $f(z^p) = 0$.

对任何与 n 互素的 $k \leq n-1$, 做素分解 $k = p_1 \cdots p_s$, 则 $p_1, p_2 \nmid n$, 则由断言 $f(\xi^{p_1}) = 0$, 进一步由 ξ^{p_1} 也为 n 次本原单位根, 再次用断言有 $f(\xi^{p_1 p_2}) = f((\xi^{p_1})^{p_2}) = 0$. 依次类推有 $f(\xi^k) = 0$, 从而任何 n 次本原多项式均为 f 的根, 则只能 $\Phi_n(x) | f(x)$, 则 $\Phi_n(x) = f(x) \in \mathbb{Z}[x]$ 为最小多项式, 不可约.

则只需证明断言. 若断言不成立, 则 z^p 的最小多项式为 $g(x) \in \mathbb{Z}[x]$, 设 $g(x)$ 本原 (为什么?),

则 $f(x)|g(x^p), f(x) \neq g(x)$ 且 $g(x)|(x^n - 1)$. 则利用引理 2.7 中的论证可知存在 $h(x) \in \mathbb{Z}[x]$ 使得 $x^n - 1 = f(x)g(x)h(x)$.

考虑 $\mathbb{Z}[x] \rightarrow \mathbb{F}_p[x], f(x) \mapsto \bar{f}(x)$. 设 $g(x) = x^m + b_{m-1}x^{m-1} + \dots + b_0$, 则

$$\bar{g}(x^p) = (x^m)^p + (\overline{b_{m-1}}x^{m-1})^p + \dots + \bar{b}_0 = (x^m + \overline{b_{m-1}}x^{m-1} + \dots + b_0)^p = (\bar{g}(x))^p$$

注意到第一个等号使用了 Fermat 小定理, 第二个等号利用了 $\mathbb{F}_p[x]$ 中 $(a+b)^p = a^p + b^p$. 则 $\bar{f}(x)|(\bar{g}(x))^p$. 考虑 $x^n - \bar{1} = \bar{f}(x)\bar{g}(x)\bar{h}(x)$ in $\mathbb{F}_p[x]$. 由于 $\bar{f}(x)$ 和 $\bar{g}(x)$ 有共同的不可约因子 (这里用到 $\mathbb{F}_p[x]$ 是 UFD, 这也是放在 \mathbb{F}_p 中考虑的原因!), 故 $x^n - \bar{1}$ 有重根.

另一方面 $\gcd(x^n - \bar{1}, nx^{n-1}) = \bar{1}$, 与引理 2.3 矛盾! 故原命题得证. \square

下面是一个综合运用 Galois 对应和分圆理论的例子.

Example 2.32 令 $E = \mathbb{Q}(\xi_8 = \xi) = \mathbb{Q}(\frac{\sqrt{2}+\sqrt{2}i}{2}) = \mathbb{Q}(\sqrt{2}, i)$. 有一一对应 $\text{Aut}(E) \xrightarrow{\sim} U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

其中 $\bar{1}$ 对应 Id_E , $\bar{3}$ 对应 $\tau: \xi \mapsto \xi^3, i = \xi^2 \mapsto \xi^6 = -i, \xi^3 \mapsto \xi, \bar{5}$ 对应 $\delta: \xi \mapsto -\xi, \xi^2 = i \mapsto \xi^{10} = i$, $\bar{7}$ 对应 $\sigma: \xi \mapsto \xi^7 = \bar{\xi}$, 即取复共轭.

现在我们要求 \mathbb{Q} 和 E 的中间域, 由 Galois 对应, 只需考虑 $H \leq \text{Aut}(E)$ 的固定子域. 又由于同构 $\text{Aut}(E) \xrightarrow{\sim} U(\mathbb{Z}_8)$, 转化为考虑 $U(\mathbb{Z}_8)$ 的子群, 只有平凡子群和 $\{\bar{1}, \bar{3}\}, \{\bar{1}, \bar{5}\}, \{\bar{1}, \bar{7}\}$, 则对应 $\text{Aut}(E)$ 的平凡子群和子群 $H_1 = \{\text{Id}_E, \tau\}, H_2 = \{\text{Id}_E, \delta\}, H_3 = \{\text{Id}_E, \sigma\}$. 平凡子群对应平凡中间域.

可以验证: $E^{H_1} = E^\tau = \mathbb{Q}(\sqrt{2}i), E^{H_2} = E^\delta = \mathbb{Q}(i), E^{H_3} = E^\sigma = \mathbb{Q}(\sqrt{2})$. 故有三个非平凡的中间域 $\mathbb{Q}(\sqrt{2}i), \mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$. 它们都是 2 维的.

事实上后面我们将会看到固定子域的维数等于自同构群的指数, 这也与我们这里的结果相吻合.

Chapter 3 群论

3.1 群的基本定义

Definition 3.1

一个群 G 是指一个非空集合及其上面的二元运算 (G, \cdot) , 其中 \cdot 称为乘法, 满足如下条件:

(G1) 结合律: $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(G2) 有么元: $\exists 1_G \in G, \text{s.t. } a \cdot 1_G = a = 1_G \cdot a (\forall a \in G)$.

(G3) 有逆元: $\forall a \in G, \exists b \in G, \text{s.t. } a \cdot b = 1_G = b \cdot a$. 这样的 b 唯一, 称为 a 的逆, 记为 a^{-1} .

此外, 若 G 还满足 $a \cdot b = b \cdot a (\forall a, b \in G)$, 则称 G 为 **Abel 群**.



群有如下的基本性质, 其验证是初等的, 在此省略.

Proposition 3.1

(1) 乘法消去律: $a \cdot b = a \cdot c \Rightarrow b = c, b \cdot a = c \cdot a \Rightarrow b = c$.

(2) $\forall a, b \in G, (a^{-1})^{-1} = a, (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

(3) $(\cdot)^{-1} : G \rightarrow G, a \mapsto a^{-1}$ 为双射.

(4) $\forall a \in G, n \in \mathbb{Z}$, 可以定义 $a^n \in G$, 且满足 $a^{m+n} = a^m \cdot a^n$.



Definition 3.2

非空子集 $H \subseteq G$ 称为**子群**, 若它对乘法和求逆封闭, 即 $\forall a, b \in H$, 有 $a \cdot b \in H, a^{-1} \in H$. 记 $H \leq G$.



Remark 由定义易知 H 自然也称为群, $1_G \in H$ 也是 H 的么元. $\{1_G\}$ 和 G 本身是 G 的平凡子群.

Example 3.1 对环 $(R, +, \cdot)$, $(R, +)$ 自然成为一个 Abel 群, 该群的么元是 0_R , $a \in R$ 的逆元是 $-a$. 它称为 R 的加法群.

Example 3.2 环 R , 则其单位群 $U(R)$ 和自同构群 $\text{Aut}(R)$ 为群.

Example 3.3 域扩张 K/k , 其自同构群 $\text{Aut}(K/k)$ 为群.

Example 3.4 线性群: $GL_n(\mathbb{R}) \leq GL_n(\mathbb{C}), SL_n(\mathbb{C}), SO(n), O(n)$.

Example 3.5 对 $P \subseteq \mathbb{R}^n$, 定义其对称群为 $\Sigma(P) = \{g \in O(n) : g(P) = P\} \leq O_n$. 例如 $\Sigma(S^1) = O_2$, $\Sigma(S)$ 由四个旋转 90 度和四个沿对称轴反射组成, 其中 S 是正方形.

Example 3.6 X 是一个集合, 一个 X 上的置换是指双射 $\sigma : X \rightarrow X$, 则 X 的对称群 $S(X)$ 是由 X 上所有置换构成的群.

Cayley 定理: 任何群都本质上是一个对称群的子群.

Theorem 3.1 (Lagrange)

有限群 G 的子群为 H , 则 $|G|$ 是 $|H|$ 的倍数.



证明 定义 $a \sim b$ 若 $ab^{-1} \in H$, 即 $Ha = Hb$. 显然 $a \sim a$, 且若 $a \sim b$, 有 $ba^{-1} = (ab^{-1})^{-1} \in H$, 故 $b \sim a$. 此外若 $a \sim b, b \sim c$, 故 $ac^{-1} = ab^{-1}bc^{-1} \in H$, 则 $a \sim c$. 故 \sim 是 G 上的等价关系.

\sim 的等价类 $[a]$ 为 $Ha = \{ha : h \in H\}$ 称为 H 的右陪集, 则有左陪集分解 $G = \sqcup_{i \in I} Ha_i$, 其中 $\{a_i\}_{i \in I}$ 为 H 的右陪集完全代表元系. 又 $H \rightarrow Ha, h \mapsto ha$ 为双射, 故 $|H| = |Ha|$, 则 $|G| = |H||I|$. \square

Remark (1) 记 $|I| = [G : H]$ 为 H 的指数, 则 $|G| = |H|[G : H]$.

(2) 可以类似定义左陪集 $aH = \{ah : h \in H\}$, 它是等价关系 \sim' 的等价类, 其中 $a \sim' b \iff aH = bH$. 可证若 $\{a_i\}$ 为 H 的右陪集完全代表元系, 则 $\{a_i^{-1}\}$ 为 H 的左陪集代表元系.

Definition 3.3

$a \in G$ 的阶定义为满足 $a^d = 1$ 的最小正整数 d , 记作 $\text{ord}(a)$. 若不存在正整数 d 使得 $a^d = 1$, 则记 $\text{ord}(a) = \infty$.

**Proposition 3.2**

(1) G 为有限群, 则任意 $a \in G$ 是有限阶的, 进一步地有 $\text{ord}(a) \mid |G|$.

(2) 若 $\text{ord}(a) = d < \infty$, 则 $a^n = 1 \iff d \mid n$.



证明 (1) 由于 G 有限, 故必然存在 $i < j$, 使得 $a^i = a^j$, 则 $a^{i-j} = 1$, 故有限阶, 记 $\text{ord}(a) = d$, 则 $H = \{1, a, \dots, a^{d-1}\}$ 为 G 的大小为 d 的子群, 则由 Lagrange 定理即得.

(2) \Rightarrow : 设 $n = dq + r, r = 0$ 或 $r < d$, 则 $1 = a^n = (a^d)^q \cdot a^r = a^r$, 由 d 的定义有 $r = 0$, 则 $d \mid n$.

\Leftarrow : 显然. \square

3.2 循环群

Definition 3.4

G, G' 为群, 则映射 $f: G \rightarrow G'$ 称为**群同态**, 若 $\forall a, b \in G, f(a \cdot b) = f(a) \cdot f(b)$. 若 f 还是双射, 则称为**群同构**.



Remark (1) 若 $f: G \rightarrow G'$ 为群同态, 则 $f(1_G) = f(1_G \cdot 1_G) = f(1_G) \cdot f(1_G)$, 则 $f(1_G) = 1_{G'}$. 此外 $\forall a \in G, f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(1_G) = 1_{G'}$, 故 $f(a^{-1}) = (f(a))^{-1}$.

(2) 若 $f: G \xrightarrow{\sim} G'$ 为同构, 则 $\forall a \in G, \text{ord}(f(a)) = \text{ord}(a)$.

(3) $G \xrightarrow{I} G, g \mapsto g^{-1}$ 为同构 $\iff G$ 是 Abel 群.

Example 3.7 $H \leq G$ 为子群, 则 $\text{inc}: H \hookrightarrow G, h \mapsto h$ 为单同态.

Example 3.8 $\det: GL(n, \mathbb{C}) \rightarrow \mathbb{C}^*, A \mapsto \det(A)$ 为群同态.

Example 3.9 令 n 次单位根的集合为 $M_n = \{z \in \mathbb{C} : z^n = 1\} \leq \mathbb{C}^*$, 则 $M_n \xrightarrow{\sim} (\mathbb{Z}_n, +), e^{\frac{2\pi ki}{n}} \mapsto \bar{k}$ 为群同构.

Definition 3.5

对群 G, H , 定义它们的**直积**为群 $G \times H = \{(g, h) : g \in G, h \in H\}$ 其乘法定义为 $(g, h) \cdot (g', h') = (g \cdot g', h \cdot h')$, 么元 $1_{G \times H} = (1_G, 1_H)$, 逆元 $(g, h)^{-1} = (g^{-1}, h^{-1})$.



Remark (1) 显然有恒等映射的分解 $G \hookrightarrow G \times H \rightarrow G, g \mapsto (g, 1_H) \mapsto (g)$.

(2) $(g, h) = (1_G, h) \cdot (g, 1_H)$.

(3) $\text{ord}(g, h) = \text{lcm}(\text{ord}(g), \text{ord}(h))$.

Example 3.10 Klein 四元群定义为 $V_4 = M_2 \times M_2$, 其中 $M_2 = \{1, -1\}$. 则 $\text{ord}(1, 1) = 1, \text{ord}(1, -1) = \text{ord}(-1, 1) = \text{ord}(-1, -1) = 2$, 通过比较阶可知 V_4 不与 \mathbb{Z}_4 同构. 事实上 $V_4 \simeq U(\mathbb{Z}_8)$.

Definition 3.6

对群 G 和子集 $X \subseteq G$, 记 $\langle X \rangle = \{x_1 x_2 \cdots x_n : x_i \in X \text{ or } x_i^{-1} \in X, n \geq 1\}$. 可以验证它为 G 的子群, 为包含 X 的最小子群, 称为集合 X 生成的子群.

若 $\langle X \rangle = G$, 则称 X 为 G 的生成元集, 特别地, 若 $\exists a \in G$ 使得 $G = \langle a \rangle$, 则称 G 为**循环群**, a 为 G 的生成元.



Example 3.11 $(\mathbb{Z}, +)$ 为循环群, ± 1 均为生成元.

Example 3.12 $(\mathbb{Z}_n, +)$ 为循环群, $\bar{1}$ 为生成元.

Example 3.13 若 G 和 G' 同构, 则 G 循环当且仅当 G' 循环. 此外显然循环群为 Abel 群.

Proposition 3.3

若 G 为循环群, 则 G 同构于 \mathbb{Z} 或者 \mathbb{Z}_n .



证明 若 $\text{ord}(a) = n < \infty$, 则可以验证 $(a) = \{1, a, a^2, \dots, a^{n-1}\} \xrightarrow{\sim} \mathbb{Z}_n, a^l \mapsto \bar{l}$ 为同构

若 $\text{ord}(a) = \infty$, 则 $\forall n \neq m \in \mathbb{Z}, a^n \neq a^m$, 则 $(\mathbb{Z}, +) \xrightarrow{\sim} (a), n \mapsto a^n$ 为同构. \square

更精细地, 我们有

Proposition 3.4

设 $G = (a)$ 为循环群, 则

(1) 若 $|G| = \infty$, 则 G 恰有两个生成元 a, a^{-1} , G 的子群只有 $\{1_G\}$ 和 (a^d) , 其中 $d \geq 1$. 且 (a^d) 和 G 同构.

(2) 若 $|G| = n$, 则 G 恰有 $\phi(n)$ 个生成元 $\{a^k : (k, n) = 1, 1 \leq k \leq n-1\}$, 且对任意 $d|n$, 存在唯一的 d 阶子群 $H_d = (a^{\frac{n}{d}}) \leq G$. 进一步地, G 的子群和 $\{d : 1 \leq d \leq n, d|n\}$ 形成一一对应.



本节的最后我们讨论循环群的抽象刻画.

Proposition 3.5

设群 G 满足 $|G| = n < \infty$, 则 G 为循环群 $\iff G$ 中有 n 阶元.



证明 \Rightarrow : 设 $G = (a)$, 则 $\text{ord}(a) = n$.

\Leftarrow : 设 $g \in G$ 且 $\text{ord}(g) = n$, 则 $(g) = \{1, g, \dots, g^{n-1}\} \subseteq G$, 比较集合大小, 只能有 $G = (g)$, 故循环. \square

Example 3.14 Klein 四元群 V_4 不是循环群.

Example 3.15 M_d 为 d 次单位根的集合, 则有 $M_2 \times M_3 \simeq M_6$: 因为有 6 阶元 $(1, \omega)$.

Example 3.16 由中国剩余定理, 有环同构 $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$, 则有对应的加法群同构.

Example 3.17 若 $|G| = p$ 素数, 则 G 为 p 阶循环群.

Theorem 3.2

设 $|G| = n < \infty$, 则 G 是循环群 $\iff \forall d|n$, 至多存在唯一一个 d 阶子群.



证明 \Rightarrow : 由命题 3.4(2) 立得

\Leftarrow : 对任意 $d|n$, 定义 $S_d = \{g \in G : \text{ord}(g) = d\}$, 则 $G = \sqcup_{d|n} S_d$. 由命题 3.5, 只需要证 $S_n \neq \emptyset$.

首先若 $g \in S_d$, 则 (g) 为 G 的 d 阶子群, 记为 H_d , 又至多只有一个 d 阶子群 M_d , 故 g 为 M_d 的生成元, 由命题 3.4(2), M_d 有 $\phi(d)$ 个生成元, 故 $|S_d| \leq \phi(d)$.

另一方面, $n = |G| = \sum_{d|n} |S_d| \leq \sum_{d|n} \phi(d) = n$, 故只能 $|S_d| = \phi(d)$. 特别地有 $S_n \neq \emptyset$. \square

Example 3.18 Klein 四元群有三个 2 阶子群, 分别由 $(1, -1), (-1, -1)$ 和 $(-1, 1)$ 生成, 故它不是循环群.

Theorem 3.3

设 k 为域, 且 $G \leq k^*$ 为有限子群, 则 G 为循环群.



证明 记 $|G| = n < \infty$, 若 $d|n$, 则设 $H_d \leq G$ 为 d 阶子群, 则若 $h \in H_d$, 有 $h^d = 1_G = 1_k$, 即 $H_d \subseteq \text{Root}_k(x^d - 1_k)$. 比较集合大小有 $|H_d| = |\text{Root}_k(x^d - 1_k)|$. 故至多只有一个 d 阶子群, 故由定理 3.2 得证. \square

Example 3.19 设 E/\mathbb{F}_p 为域扩张, 且 $|E| < \infty$, 则由上述定理, E^* 为循环群, 设 $E^* = \langle v \rangle$, 故 $E = \mathbb{F}_p(v)$.

Example 3.20 回忆 $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + \bar{1})$, $u = x + (x^2 + \bar{1})$. 则 \mathbb{F}_9^* 同构于 \mathbb{Z}_8 . 不难验证 u 为四阶元, $\langle u \rangle = \{\bar{1}, u, \bar{2}, \bar{2}u\}$.

练习: \mathbb{F}_9 中有 4 个八阶元, 分别为 $u + \bar{1}, u + \bar{2}, \bar{2}u + \bar{1}, \bar{2}u + \bar{2}$. 它们均为 \mathbb{F}_9 的生成元.

Example 3.21 \mathbb{C}^* 的有限子群恰为 n 次单位根的集合 M_n . 但 \mathbb{C}^* 本身不是循环群.

3.3 正规子群

对群同态 $f: G \rightarrow G'$, 与环同态类似地可以定义像 $\text{Im}(f) = \{f(g) : g \in G\}$, 核 $\ker(f) = \{h \in G : f(h) = 1_{G'}\}$, 显然它们都是 G' 的子群.

记 $N = \ker(f) \leq G$, 则 $f(a) = f(b) \iff ab^{-1} \in N \iff Na = Nb$, 同理也等价于 $Nb = Na$.

同时我们注意到, 对任意的 $a \in G$, 若 $b \in aN$, 则 $a^{-1}b \in N$, 故 $ba^{-1} \in N$, 即 $b \in Na$, $aN \subseteq Na$. 同理反向的包含关系也成立, 故 $aN = Na$. 这启示我们定义如下:

Definition 3.7

子群 $N \leq G$ 称为**正规子群**, 记作 $N \triangleleft G$, 若 $\forall a \in G$, 有 $aN = Na$.



Example 3.22 由上面的讨论, 若 $f: G \rightarrow G'$ 为群同态, 则 $\ker(f) \triangleleft G$.

Example 3.23 对环同态 $f: R \rightarrow R'$, $\ker(f) \triangleleft R$ 为理想, 但不是子环!

Example 3.24 G 为 Abel 群, 则任何子群为正规子群.

Example 3.25 群 G 的中心 $Z(G) = \{g \in G : gh = hg, \forall h \in G\}$ 是 G 的正规子群.

Example 3.26 若 $H \leq G$, 且 $[G : H] = 2$, 则有 $H \triangleleft G$.

定义子群 N 的共轭为 $aNa^{-1} = \{ana^{-1} : n \in N\}$, 不难验证它也是 G 的子群. 则由定义 $N \triangleleft G \iff N = aNa^{-1}, \forall a \in G$.

Example 3.27 令 $G = GL_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{F}_2, ad - bc \neq 0 \right\}$. (a, b) 有 3 个选择, 固定 (a, b) 后 (c, d) 有 2 个选择, 故 $|G| = 6$.

不难验证 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 的阶为 2. 它生成了子群 $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$.

可以验证 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} H \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\} \neq H$, 故 H 不是 G 的正规子群.

令 $h = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, 同样可以验证 $\text{ord}(h) = 3$, 故 $N = \langle h \rangle$ 为 G 的指数为 2 的子群, 进而为正规子群.

Example 3.28 $\det: GL_n(\mathbb{C}) \rightarrow \mathbb{C}^*, A \mapsto \det A$, 其核 $SL_n(\mathbb{C}) \triangleleft GL_n(\mathbb{C})$.

Definition 3.8

对 $N \triangleleft G$, 定义**商群** $G/N = \{aN : a \in G\}$, 定义乘法为 $\bar{a} \cdot \bar{b} = a \cdot b$. 幺元 $1_{G/N} = \bar{1} = N$.

此时有典范同态 $\text{can}: G \rightarrow G/N, a \mapsto \bar{a}$. 显然有 $\ker(\text{can}) = N$.



Remark 上面的乘法定义是合理的: 若 $\bar{a} = \bar{a'}, \bar{b} = \bar{b'}$, 则 $a'^{-1}a \in N, b'^{-1}b \in N$. 故 $(a'b')^{-1}ab = b'^{-1}a'^{-1}ab \in b'^{-1}Nb = b'^{-1}bN \in N$, 则 $\overline{a \cdot b} = \overline{a' \cdot b'}$.

与之前一样地我们有如下的群同态基本定理.

Theorem 3.4 (群同态基本定理)

设 $f: G \rightarrow H$ 为群同态, 则 f 诱导唯一环同构 $\bar{f}: G/\ker(f) \xrightarrow{\sim} \text{Im} f$, 使得如下图表交换

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow \text{can} & & \uparrow \text{inc} \\ G/\ker(f) & \xrightarrow{\bar{f}} & \text{Im} f \end{array}$$



Example 3.29 考虑 \mathbb{R}^2 中的正方形 \square , 其顶点为 $A(1, 1), B(-1, 1), C(-1, -1), D(1, -1)$. 设 $g = \Sigma(\square) = \{g \in O(2) : g(\square) = \square\} \leq O(2)$. 则显然有群同态: $\Sigma(\square) \xrightarrow{\phi} S(V), g \mapsto \phi(g) = g|_V$, 其中 $V = \{A, B, C, D\}$ 为正方形的顶点集.

ϕ 是单射: 若 $g|_V = \text{Id}|_V$, 则 $g(A) = A, g(B) = B$, 即 $g(\overrightarrow{OA}) = \overrightarrow{OA}, g(\overrightarrow{OB}) = \overrightarrow{OB}$. 由 $g \in O(2)$ 可知 $g = \text{Id}_{\mathbb{R}^2}$.

又熟知 $O(2) = SO(2) \sqcup \{g \in O(2) : \det(g) = -1\}$, 前面的部分为旋转, 则在 ϕ 下对应于正方形的 $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ 四个角度的旋转. 后面的部分为镜像对称, 则在 ϕ 下对应正方形关于四条对称轴的镜像对称.

特别地, $|\Sigma(\square)| = 8$, 则 $S(V) \simeq S_4$ 有 8 阶子群.

Example 3.30 对 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, 考虑其分裂域 $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$. 则由于 $f(x)$ 可分, 有 $|\text{Aut}(E/\mathbb{Q})| = |\text{Aut}(E)| = \dim_{\mathbb{Q}} E = 6$. 记 $X = \text{Root}_E(x^3 - 2)$, 它是一个三元集.

对每个 $\sigma \in \text{Aut}(E)$ 和 $a \in X$, 有 $\sigma(a)^3 = \sigma(a^3) = 2$, 故 $\sigma(a) \in X$, 进而有群同态 $\phi: \text{Aut}(E) \rightarrow S(X), \sigma \mapsto \sigma|_X$.

同样有 ϕ 是单的: 若 $\sigma|_X = \text{Id}_X$, 则 $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}, \sigma(\omega) = \omega$, 有 $\sigma|_E = \text{Id}_E$. 则由于 $|\text{Aut}(E)| = |S(X)|$, 只能 ϕ 为双射, 进而为群同构.

上面的情形用更一般的语言描述, 即为可分多项式的分裂域的同构诱导根集上的置换.

最后再看几个群同态基本定理的抽象应用.

Theorem 3.5 (对应定理)

设 $N \triangleleft G$, 则有一一对应 $\{K : N \leq K \leq G\} \leftrightarrow \{H : H \leq G/N\}, K \mapsto K/N$. 且 $K \triangleleft G \iff (K/N) \triangleleft (G/N)$, 此时有同构 $(G/N)/(K/N) \simeq G/K$.



证明 设 $K' \leq G/N$, 则定义 $K = \{g \in G : \bar{g} \in K'\}$, 有 $N \leq K \leq G$, 此时 $K' = K/N$.

另一方面, 若 $K \triangleleft G$, 考虑 $G/N \twoheadrightarrow G/K, gN \mapsto gK$, 它是良定的, 且核为 K/N , 则由同态基本定理, $(K/N) \triangleleft (G/N)$, 且 $(G/N)/(K/N) \simeq G/K$. \square

练习: 补充上面证明的细节.

Theorem 3.6 (同构定理)

设 $N \triangleleft G, H \leq G$, 则

(1) $NH = HN$, 且 $N \leq NH \leq G$.

(2) $(N \cap H) \triangleleft H$, 且 $H / (N \cap H) \xrightarrow{\sim} NH / N$.



证明 (1) 是直接的验证.

(2) 思路是考虑 $H \rightarrow NH / N \hookrightarrow G / N, h \mapsto \bar{h}$, 其像为 NH / N , 核为 $N \cap H$, 则由同态基本定理即得. □

3.4 对称群

回忆对抽象的集合 X , 定义其对称群 $S(X) = \{\sigma : X \xrightarrow{1:1} X\}$ 为 X 上置换所构成的集合. 它关于映射的复合成群.

Proposition 3.6

若存在双射 $\delta : X \rightarrow Y$, 则有群同构: $\Phi : S(X) \rightarrow S(Y), \sigma \mapsto \delta \circ \sigma \circ \delta^{-1}$.

特别地, 定义 $S_n = S(\underline{n})$, 其中 $\underline{n} = \{1, 2, \dots, n\}$, 则若 $|X| = n$, 有 $S(X) \cong S_n$.



故下面我们主要研究 S_n . 定义如下的记号: 若 $\sigma \in S_n$, 则将 σ 记为 $(\begin{smallmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{smallmatrix})$, 则自然地有 $\sigma^{-1} = (\begin{smallmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{smallmatrix})$.

首先 S_1 平凡, S_2 为二阶循环群, 它们均为 Abel 群.

再考察 S_3 , 设 $\sigma = (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$, 则 $\sigma^{-1} = (\begin{smallmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{smallmatrix}) = \sigma$, 即 $\sigma^2 = \text{Id}$. 再设 $\delta = (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$, 则 $\delta^{-1} = (\begin{smallmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{smallmatrix}) = \delta^2$, 故 $\delta^3 = \text{Id}$.

再令 $\tau = (\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$, 有 $\sigma \circ \tau = (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) = \delta, \tau \circ \sigma = (\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}) \neq \sigma \circ \tau$, 故 S_3 不是 Abel 群!

事实上这对更一般的对称群也正确.

Proposition 3.7

若 $n \geq 3$, 则 S_n 不是 Abel 群.



证明 对任意的 n , $S_n \hookrightarrow S_{n+1}, \sigma \mapsto \bar{\sigma}$, 其中 $\bar{\sigma} : \underline{n+1} \rightarrow \underline{n+1}, i \mapsto \sigma(i) (1 \leq i \leq n), n+1 \mapsto n+1$. 则特别地对 $n \geq 3, S_3 \hookrightarrow S_n$, 故由 S_3 非 Abel, 有 S_n 非 Abel. \square

下面再用轮换表述置换. 对 $i_1, i_2, \dots, i_t \in \underline{n}, t \geq 2$ 两两不同, 令 $(i_1 i_2 \dots i_t) \in S_n$ 表示 $i_1 \mapsto i_2 \mapsto \dots \mapsto i_{t-1} \mapsto i_t \mapsto i_1$, 而保持其它位置不动的置换, 它也被称为 t -轮换. 当 $t = 2$ 时称之为对换. 不难验证轮换有如下性质:

Lemma 3.1

对 t -轮换 $c = (i_1 i_2 \dots i_t)$, 有

(1) $\text{ord}(c) = t$, 且 $c^{-1} = (i_t i_{t-1} \dots i_1)$.

(2) 它可以表示成 $\frac{n(n-1)}{2}$ 个对换的积 (即复合).



Example 3.31 用轮换的语言, 有 $S_2 = \{\text{Id}, (12)\}, S_3 = \{\text{Id}, (12), (13), (23), (123), (132)\}$.

Lemma 3.2

对任意的置换 σ , 有 $\sigma \circ (i_1 i_2 \dots i_t) \circ \sigma^{-1} = (\sigma(i_1) \sigma(i_2) \dots \sigma(i_t))$.

特别地, 若轮换 $\sigma, \tau \in S_n$ 不相交, 则 $\sigma\tau = \tau\sigma$.



证明 显然 $\sigma \circ (i_1 i_2 \cdots i_t) = (\sigma(i_1) \sigma(i_2) \cdots \sigma(i_t)) \circ \sigma$, 故 $\sigma \circ (i_1 i_2 \cdots i_t) \circ \sigma^{-1} = (\sigma(i_1) \sigma(i_2) \cdots \sigma(i_t))$!
再由不交的条件, 有 $\sigma(i_j) = i_j (1 \leq j \leq t)$, 则结果显然成立. \square

Example 3.32 S_3 中, $(12)(23)(12) = (\sigma(2)\sigma(3)) = (13) \neq (23)$, 其中 $\sigma = (12)$. 再次有 S_3 非 Abel.

$(23)(12)(23) = (\tau(1)\tau(2)) = (13) = (12)(23)(12)$, 其中 $\tau = (23)$. 这种等式在更一般的情况下也成立, 称为辫关系.

Proposition 3.8

对任意 $\sigma \in S_n$, 存在唯一的表达式 $\sigma = c_1 c_2 \cdots c_l$, 其中 c_i 为互不相交的轮换.



证明 取最小的 t 使得 $\sigma^t(1) = 1$, 则令 $c_1 = (1\sigma(1)\cdots\sigma^{t-1}(1))$, 再取 $j \neq \{1, \sigma(1), \cdots, \sigma^{t-1}(1)\}$, 对 j 做同样的操作得到 c_2 , 再以此类推即可. \square

Example 3.33 在 S_7 中, 令 $\sigma = (456)(567)(761)$, 则可以写为 $\sigma = (16)(45)$.

Definition 3.9

对 $\sigma \in S_n$, 将 $\sigma = c_1 c_2 \cdots c_t$ 唯一写为不相交的轮换, 记 λ_i 为表达式中长度为 i 的轮换个数, 则显然 $\sum i\lambda_i = n$, 定义 $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$ 为 σ 的型.



Theorem 3.7

S_n 中的元素共轭 \iff 它们同型.



证明 \Rightarrow : 设 $\sigma = c_1 c_2 \cdots c_t$ 为不交轮换之积, 则 $h\sigma h^{-1} = (hc_1 h^{-1})(hc_2 h^{-1}) \cdots (hc_t h^{-1})$, 由引理 3.2, 同样为不交轮换之积, 且对应轮换的长度不变, 则 σ 和 $h\sigma h^{-1}$ 同型.

\Leftarrow : 若 σ 和 σ' 同型, 则设 $\sigma = (ab \cdots c) \cdots (\alpha\beta \cdots \gamma)$ 为不交分解, 长度与之对应地有 $\sigma' = (a'b' \cdots c') \cdots (\alpha'\beta' \cdots \gamma')$, 则定义 τ 为 $a \mapsto a', \cdots, c \mapsto c', \cdots, \alpha \mapsto \alpha', \cdots, \gamma \mapsto \gamma'$. 有 $\tau\sigma\tau^{-1} = \sigma'$. \square

Example 3.34 在 S_3 中根据型有如下的共轭分类:

型	共轭类
1^3	Id
$1^1 2^1$	$(12), (13), (23)$
3^1	$(123), (132)$

Example 3.35 在 S_4 中根据型有如下的共轭分类:

型	共轭类
1^4	Id
$1^2 2^1$	$(12), (13), (14), (23), (24), (34)$
2^2	$(12)(34), (13)(24), (14)(23)$
$1^1 3^1$	$(123), (124), (132), (134), (142), (143), (234), (243)$
4^1	$(1234), (1243), (1324), (1342), (1423), (1432)$

特别地注意到 $S_3 \hookrightarrow S_4$ 对共轭不封闭, 故不为正规子群.

Example 3.36 回忆在例 3.29 中我们将正方形的对称群嵌入为 S_4 中的 8 阶子群 H . 我们将正方形的顶点逆时针标为 1234.

$(1234) \in H$, 它对应逆时针旋转 90 度, 且 $(13) \in H$, 它对应沿连接 24 的对角线镜像对称, 故 $H' = (1234), (13) \subseteq H$,

又 $(13) \notin ((1234))$, 故 $|H'| > 4$, 又 $H' \subseteq H$ 且为 S_4 的子群, 结合 Lagrange 定理只能有 $|H'| = 8$, 即 $H = H' = ((1234), (13))$.

练习: 将正方形的顶点逆时针标为 1324 和 1243, 分别计算对应的 S_4 的 8 阶子群.

Lemma 3.3

$\forall \sigma \in S_n$ 可以写成若干个对换之积.



证明 只需把轮换写成对换之积, 这是容易的: $(i_1 i_2 \cdots i_t) = (i_{t-1} i_t) \cdots (i_2 i_t)(i_1 i_t)$. □

Proposition 3.9

记 $s_i = (i, i+1)$, 则 S_n 可由 s_1, \cdots, s_{n-1} 生成, 且 s_i 满足:

- (1) $s_i^2 = 1$ $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$.
- (2) $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$. 这一关系被称为辫关系 (braid relation).
- (3) $s_i s_j = s_j s_i (\forall |i - j| \geq 2)$.



证明 由引理 3.3, 只需证任意的对换 (ij) 可以用这些 s_k 生成. 不妨 $i < j$, 对 $j - i$ 归纳. 当 $j - i = 1$ 时显然成立, 若 $j - i < m$ 时成立, 当 $j - i = m$ 时, 由于

$$(ij) = (i+1, j)(i, i+1)(i+1, j)^{-1} = (i+1, j)(i, i+1)(i+1, j)$$

由归纳假设, $(i+1, j)$ 和 $(i, i+1)$ 均可以由这些 s_k 所生成, 故得证. 最后的几个等式容易验证. □

最后再来讨论奇偶置换的概念. 首先注意到有嵌入 $S_n \hookrightarrow GL_n(\mathbb{R}), \sigma \mapsto P_\sigma$, P_σ 是对应的置换矩阵, 它将 e_i 打为 $e_{\sigma(i)}$, 不难验证这是一个单同态.

再复合 $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$, 并注意到置换方阵的行列式为 ± 1 , 故有同态 $\text{sign} : S_n \rightarrow \{\pm 1\}$. 则 $\text{sign}(\sigma) = -1$ 等价于它可以被写成奇数个对换之积, 此时称之为奇置换, 否则称为偶置换.

Definition 3.10

$A_n = \ker(\text{sign}) \triangleleft S_n$ 是偶置换的集合, 称为 n 阶交错群.



Remark 由于 $S_n/A_n = \{\pm 1\}$, 故 $|A_n| = \frac{1}{2}n!$.

Example 3.37 $A_3 = \{\text{Id}, (123), (132)\} \triangleleft S_3$. 考虑 S_3 的非平凡子群, 由 Lagrange 定理, 必须为 2 阶或者 3 阶的.

找 2 阶子群只用找 2 阶元, 故有 3 个, 对应 $\{\text{Id}, (12)\}, \{\text{Id}, (13)\}, \{\text{Id}, (23)\}$, 由例 3.34 中的表格, 它们都不是共轭封闭的, 即不为正规子群.

找 3 阶子群只用找 3 阶元, 有 2 个三阶元, 故只有一个 3 阶子群, 就是 A_3 , 它是正规子群.

Example 3.38 考虑 S_4 的所有非平凡正规子群. 一个子群 $N \leq S_4$ 是正规的当且仅当它是共轭类的并. 回忆例 3.35 中给出 S_4 的共轭类, 类的大小分别为 1, 6, 3, 8, 6.

由于 Lagrange 定理, $|N|$ 只能为 12, 8, 6, 4, 3, 2. 且子群必须包含恒等元所在的类, 故只可能 $|N|$ 为 $12 = 1 + 3 + 8$ 或 $4 = 1 + 3$. 前者对应 A_4 , 后者为 $K_4 = \{\text{Id}, (12)(34), (13)(24), (14)(23)\} \triangleleft S_4$, 由于 $(12)(34) \cdot (13)(24) = (14)(23)$, 有 $K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$, 即为 Klein 四元群. 综上 S_4 的非平凡正规子群为 A_4, K_4 .

下面解决了 $n \geq 5$ 的情形.

Definition 3.11

若群 G 没有非平凡的正规子群, 则称之为单群.



Example 3.39 若 G 为有限 Abel 群, 则 G 是单群等价于 G 为素数阶循环群. 证明作为练习.

Theorem 3.8

$n \geq 5$, 则 A_n 为单群.



证明 首先注意到 A_n 可以由 3-轮换生成. 这是因为对 $i \neq j, r \neq s$, 若 $j = r$, 则 $(ij)(rs) = (jsi)$, 否则 $(ij)(rs) = (ris)(ijr)$.

进一步地, 任取两个 3-轮换 $(ijk), (i'j'k')$, 它们同型, 故 S_n 中共轭, 即取 $\gamma \in S_n$, 使得 $\gamma(ijk)\gamma^{-1} = (i'j'k')$, 若 $\gamma \notin A_n$, 则取 $r \neq s$ 且 $r, s \notin \{i', j', k'\}$ (注意到这里用到了 $n \geq 5$!), 则令 $\gamma' = (rs)\gamma \in A_n$, 且

$$\gamma'(ijk)\gamma'^{-1} = (rs)(i'j'k')(rs)^{-1} = (i'j'k')$$

故 (ijk) 和 $(i'j'k')$ 在 A_n 中共轭.

对 $\{1\} \neq N \triangleleft A_n$, 可以证明 N 必然包含一个 3-轮换 (参考课本), 则所有的 3-轮换都在 N 中, 又由于 A_n 由 3-轮换生成, 故 $N = A_n$. \square

下面是一个直接的推论.

Proposition 3.10

$n \geq 5$, 则 A_n 是 S_n 的唯一非平凡正规子群



证明 若 $N \triangleleft S_n$ 是非平凡正规子群, 则考虑 $A_n \hookrightarrow S_n \twoheadrightarrow S_n/N$, 其核为 $N \cap A_n \triangleleft A_n$, 由 A_n 为单群, 只能 $A_n = \{1\}$ 或 A_n 本身.

若 $N \cap A_n = A_n$, 则 $A_n \subseteq N$, 由 Lagrange 定理只能 $N = A_n$.

若 $N \cap A_n = \{1\}$, 则 $A_n \hookrightarrow S_n/N$, 比较集合的大小只能 $|N| = 2$. 由于 $N - \{\text{Id}\}$ 只能为奇置换, 则只能 $N = \{\text{Id}, (ij)\}$, 它不对共轭封闭, 则不为 S_n 的正规子群, 矛盾. 综上非平凡正规子群只有 A_n . \square

Example 3.40 A_4 不是单群! 在 A_4 中, 有 $(143)(12)(34)(143)^{-1} = (13)(24)$, 故 $(12)(34)$ 和 $(13)(24)$ 共轭, 同理与 $(14)(23)$ 也共轭, 故 $K_4 \triangleleft A_4$.

	大小	共轭类
	1	Id
利用后面将要提到的轨道-稳定化子公式可以计算出 A_4 的共轭类表格	3	$(12)(34), (13)(24), (14)(23)$
	4	$(123), (134), (142), (243)$
	4	$(124), (132), (143), (234)$

进而 A_4 没有 6 阶子群: 若存在指数为 2, 故正规子群, 由共轭类的大小可知不可能.

3.5 群作用

Definition 3.12

称群 G 左作用于集合 X , 记作 $G \curvearrowright X$, 是指存在映射 $\psi : G \times X \rightarrow X, (g, x) \mapsto \psi(g, x) = g.x$, 满足

$$(1) 1_G.x = x, \forall x \in X.$$

$$(2) h.(g.x) = (hg).x, \forall h, g \in G, x \in X \text{ 此时称 } X \text{ 为 } G\text{-集合}.$$



Example 3.41 $S(X)$ 自然作用在 X 上: 定义 $\psi : S(X) \times X \rightarrow X, (\sigma, x) \mapsto \sigma(x)$. 即 X 为 $S(X)$ -集合.

Example 3.42 若 $G \curvearrowright X$, 则 $G \curvearrowright \mathcal{P}(X) = \{Y : Y \subseteq X\}$.

设 (X, ψ) 为 G -集, 则 $\rho : G \rightarrow S(X), g \mapsto \rho(g)$ 为群同态, 其中 $\rho(g) : X \rightarrow X, x \mapsto g.x$. 首先该映射良定: 由于 $g.(g^{-1}.x) = x$, 故 $\rho(g)$ 为满射, 且若 $g.x = g.y$, 则 $x = g^{-1}.(g.x) = y$, 故 $\rho(g)$ 为单射, 即 $\rho(g)$ 确实是 $S(X)$ 中的元素. 其次由群作用定义中的 (2) 可以验证为同态.

反之任意群同态 $\rho : G \rightarrow S(X)$, 给出了 X 的一个 G -集结构: 定义 $\psi : G \times X \rightarrow X, (g, x) \mapsto \rho(g)(x) = g.x$, 则 $1_G.x = \rho(1_G)(x) = \text{Id}(x) = x$, 且

$$\rho(h)(\rho(g)(x)) = (\rho(h) \circ \rho(g))(x) = \rho(hg)(x) = (hg).x.$$

则 ψ 给出了 X 的 G -集结构.


则综上 G 在 X 上的作用可以等价地通过群同态 $\rho : G \rightarrow S(X)$ 来理解. 此时每个元素 $g \in G$ 可以表示为具体的 $\rho(g) \in S(X)$.

Definition 3.13

设 $G \curvearrowright X, x \in X$, 则定义

$$(1) x \text{ 的 } G\text{-轨道为 } \mathcal{O}_x = \{g.x : g \in G\} \subseteq X.$$

$$(2) x \text{ 的稳定化子为 } G_x = \{g \in G : g.x = x\} \leq G.$$

(3) 称该 G -作用为可迁的, 或者称为传递的, 若只有一个轨道, 即 $\forall x, y \in X, \exists g \in G, \text{s.t. } x = g.y$. 

Remark 在 X 上定义关系 $x \sim y \iff \exists g \in G, \text{s.t. } y = g.x$, 可以验证这是一个等价关系, 且等价类即为轨道 \mathcal{O}_x . 则由等价类的分解 $X = \sqcup_{x \in I} \mathcal{O}_x$, 也称为 X 的 G -轨道分解.

Lemma 3.4

设 $x = h.y, h \in G$, 则 $G_x = hG_yh^{-1}$.



证明 若 $g \in G_y$, 则 $(hgh^{-1}).x = (hg).y = h.(g.y) = h.y = x$, 即 $hG_yh^{-1} \subseteq G_x$.

另一方面若 $g \in G_x$, 则同理 $(h^{-1}gh).y = h^{-1}.(g.x) = y$, 则 $G_x \subseteq hG_yh^{-1}$. □

Example 3.43 设 $H \leq G$, 则有 $G \curvearrowright G/H, g.aH = gaH$, 该作用称之为左陪集作用, 它是可迁的. 不难验证 $G_aH = aHa^{-1}$, 特别地 $G_H = H$.

若 $H = \{1_G\}$, 则变为 $G \curvearrowright G, g.x = gx$, 称为左正则作用.

Example 3.44 自然作用 $S(X) \curvearrowright X$ 是可迁的.

Example 3.45 再次考察例 3.30 的例子. 考虑域扩张 K/k , 则有自然作用 $\text{Aut}(K/k) \curvearrowright K, \sigma.\mu = \sigma(\mu) \in K$. 设 $f(x) \in k[x]$, 根集为 $\text{Root}_K(f) = \{\mu \in K : f(\mu) = 0\}$, 对 $\sigma \in \text{Aut}(K/k)$ 和 $f(\mu) = 0$, 有 $\sigma(f(\mu)) = f(\sigma(\mu)) = 0$, 进而有作用 $\text{Aut}(K/k) \curvearrowright \text{Root}_K(f)$.

更进一步地设 K 是 $f(x) \in k[x]$ 的分裂域, 则 $\text{Root}_K(f) = \{\mu_1, \dots, \mu_n\} \subseteq K$, 记该集合为 R , 则有 $\text{Aut}(K/k) \curvearrowright R$. 若 $\sigma(\mu_i) = \mu_i (\forall 1 \leq i \leq n)$, 则由于 $K = k(\mu_1, \dots, \mu_n)$, 有 $\sigma|_K = \text{Id}_K$, 故 $\text{Aut}(K/k) \hookrightarrow S(R) = S_n$.

Example 3.46 回忆 $GL_2(\mathbb{F}_2)$, 定义 $V = \mathbb{F}_2 \oplus \mathbb{F}_2$, 则有 $GL_2(\mathbb{F}_2) \curvearrowright V^* = V - \{(\bar{0}, \bar{0})^T\}$, 且 $GL_2(\mathbb{F}_2) \hookrightarrow S(V^*) = S_3$. 又由于 $|GL_2(\mathbb{F}_2)| = 6$, 只能为同构.

Theorem 3.9 (轨道-稳定化子公式)

设 $G \curvearrowright X, x \in X$, 则有一一对应 $f: G/G_x = \{gG_x : g \in G\} \xrightarrow{1:1} \mathcal{O}_x, gG_x \mapsto g.x$.

进而结合 Lagrange 定理有 $|\mathcal{O}_x| = [G : G_x] \mid |G|$.



证明 f 良定: 若 $gG_x = g'G_x$, 则 $g = g'h, h \in G_x$, 进而 $g.x = (g'h).x = g'.x$.

f 单射: 若 $g.x = g'.x$, 则 $(g^{-1}g').x = x$, 故 $g^{-1}g' \in G_x, gG_x = g'G_x$.

满射显然, 故得证. □

Definition 3.14

对 $G \curvearrowright X$, 诱导了群同态 $\rho: G \rightarrow S(X)$, 则 $\ker \rho = \cap_{x \in X} G_x$ 称为作用的核. 若 $\ker \rho = \{1_G\}$, 则称为**忠实**作用.

若 $\forall x \in X, G_x = \{1_G\}$, 则称为**自由**作用. 显然自由作用是忠实的.



Remark 若 $G \curvearrowright X$ 自由, 则由轨道-稳定化子公式, 有 $|\mathcal{O}_x| = |G|$, 此时 $|G| \mid |X|$, 因为 $X = \sqcup_{x \in I} \mathcal{O}_x$.

Example 3.47 左正则作用 $G \curvearrowright G, g.x = gx$ 是自由作用. 则有嵌入 $G \hookrightarrow S(G)$.

同理右正则作用 $G \curvearrowright G, g.x = xg^{-1}$ 也自由.

Example 3.48 $H \leq G$, 则 $H \curvearrowright G, h.x = hx$, 它是自由的, 且轨道为左陪集.

Example 3.49 对 $G \curvearrowright X$, 定义不动点集 $X^G = \{x \in X : g.x = x, \forall g \in G\} = \{x \in X : G_x = G\}$, 则若 $X^G \neq \emptyset$, 有 $G \curvearrowright X^G$ 是平凡作用.

考虑共轭作用 $G \curvearrowright X = G, g.x = gxg^{-1}$, 若 G 为 Abel 群, 则这显然为平凡作用.

对 $x \in X$, 其轨道为 $C_x = \{gxg^{-1} : g \in G\}$, 即 x 所在的共轭类. 特别地, 若 $C_x = \{x\}$, 则 $x \in Z(G)$.

x 的稳定化子为 $Z(x) = \{g \in G : gx = xg\} \leq G$, 则 $Z(G) \subseteq Z(X)$, 且由轨道-稳定化子公式, 有 $|C_x| \cdot |Z(x)| = |G|$, 特别地 $|C_x| \mid |G|$.

进一步地有所谓的类等式

$$|G| = |Z(G)| + \sum_{|C_x| > 1} |C_x| = |Z(G)| + \sum_{|C_x| > 1} \frac{|G|}{|Z(x)|}.$$

Example 3.50 A_4 中, $Z(123) = \{\sigma \in A_4 : \sigma(123)\sigma^{-1} = (123)\} = \{\sigma \in A_4 : (\sigma(1)\sigma(2)\sigma(3)) = (123)\} = \{\text{Id}, (123), (132)\}$. 则由 $|C_{(123)}||Z(123)| = |A_4| = 12$, 有 $|C_{(123)}| = 4$. 可以验证 $(134), (142), (243)$ 均与 (123) 共轭, 则它们恰好组成 (123) 的共轭类. 类似可以计算其他共轭类.

Example 3.51 对正则作用 $G \curvearrowright G$, 可以考虑共轭作用 $G \curvearrowright C_x$.

特别地, 考虑 $S_4 \curvearrowright X = \{(12)(34), (13)(24), (14)(23)\}$, 分别令 $(12)(34), (13)(24), (14)(23)$ 为 A, B, C , 则有共轭作用 $S_4 \curvearrowright S(X) = S_3, g \mapsto (x \in X \mapsto gxg^{-1})$. 可以验证核为 $K_4 = X \cup \{\text{Id}\}$, 故比较集合大小为满射, 则 $S_4/K_4 \xrightarrow{\sim} S_3$.

Example 3.52 对 $H \leq G$, G 共轭作用于 $X_H = \{H' \leq G : H' \text{ 共轭于 } H\}$, $g.H' = gH'g^{-1} \in X_H$. 正规化子定义为 $N_G(H) = \{g \in G : gHg^{-1} = H\} \leq G$, 由轨道-稳定化子公式, 有 $|G| = |N_G(H)||X_H|$.

则 $H \triangleleft G \iff |X_H| = 1 \iff N_G(H) = G$.

Definition 3.15

p 素数, 群 G 称为 p -群, 若 $|G| = p^n$.



Proposition 3.11

p -群有非平凡的中心, 进而不是单群.



证明 设 $|G| = p^n$, 则只能 $|Z(G)| = p^r$, 若 $r = 0$, 则由类等式

$$p^n = 1 + \sum_{|C_x| > 1} |C_x| = 1 + \sum_{|C_x| > 1} \frac{p^n}{|Z(x)|}.$$

又中心非平凡, $|Z(x)| < p^n$, 则 $|C_x| = p^k (k \geq 1)$, 两边模 p 可知矛盾. □

Proposition 3.12

p^2 阶群是 Abel 群, 同构于 \mathbb{Z}_{p^2} 或者 $\mathbb{Z}_p \times \mathbb{Z}_p$.



证明 由中心平凡, 取 $1 \neq g \in Z(G)$, 若为循环群, 则 $\text{ord}(g) = p^2$, G 同构于 \mathbb{Z}_{p^2} .

若不为循环群, $\text{ord}(g) = p$, 则令 $H = \langle g \rangle \subseteq Z(G)$. 取 $1 \neq g' \notin H$, 则 $\text{ord}(g') = p$, 考虑 $1 \leq i, j, k, l \leq p-1, g^i g'^j = g^k g'^l$, 则由于 $g' \notin \langle g \rangle$, 只能 $i = k, j = l$, 即 $\{g^i g'^j : 1 \leq i, j \leq p-1\}$ 为大小为 $p^2 - 2p + 1$ 的集合.

则比较集合大小有 $\langle g, g' \rangle = G$. 且 $\{g^i g'^j : 1 \leq i, j \leq p-1\} = \{g'^i g^j : 1 \leq i, j \leq p-1\}$, 又 $g^k \in Z(G), \forall 1 \leq k \leq p-1$, 故 $(g^k g'^l)(g^x g'^y) = g^{k+x} g'^{l+y} = (g^x g'^y)(g^k g'^l)$, 故 G 为 Abel 群.

令 $K = \langle g' \rangle$, 此时可以验证 $H \times K \rightarrow G, (g^i, g'^j) \mapsto g^i g'^j$ 为同构, 故 $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. \square

最后看一个利用正则表示的例子.

Theorem 3.10

若 G 为有限群, 且 $|G| = 4k + 2 \geq 6$, 则 G 不是单群.



证明 记 $|G| = 2n$, 考虑左正则表示 $\rho: G \rightarrow S(G) = S_{2n}$, 则由于 ρ 忠实, 有 $G \simeq \rho(G)$. 故不妨 G 是一个置换群. 注意到 G 中必有二阶元素 g , 从而 $\rho(g)$ 为一些对换 $(a, \rho(g)a)$ 的积, 即为 n 个对换之积, 由条件 ρ 为奇置换, 则 $\rho(G)$ 包含奇置换, 故 $\rho(G)$ 中的偶置换构成了 $\rho(G)$ 的指数 2 的子群, 则为正规子群. \square

3.6 Sylow 子群

Definition 3.16

若 $|G| = p^r m, p \nmid m, p$ 为素数, 则子群 $P \leq G$ 称为 **Sylow p -子群**, 若 $|P| = p^r$.



我们的主定理是如下的 Sylow 定理.

Theorem 3.11 (Sylow 定理)

设 $|G| = p^r m, p \nmid m$, 则

- (1) 总存在 Sylow p -子群, 且它们之间互相共轭.
- (2) Sylow p -子群的个数是 m 的因子, 且形如 $kp + 1$.
- (3) 任意 p -子群 $B \leq G$, 存在 Sylow p -子群 P 使得 $B \leq P \leq G$.



证明 这里只证明存在 Sylow p -子群, 剩余命题的证明参照课本.

$|G| = p^r m, p \nmid m$, 令 $X = \{U \subseteq G : |U| = p^r\} \subseteq \mathcal{P}(G)$, 由于 $G \curvearrowright \mathcal{P}(G), g.U = gU$, 则 $G \curvearrowright X$.

又 $|X| = \binom{p^r m}{p^r} = \frac{n(n-1)\cdots(n-p^r+1)}{p^r(p^r-1)\cdots 1}$, 比较分子分母 p 的次数可以验证 $p \nmid |X|$.

进行轨道分解 $X = \sqcup_U \mathcal{O}_U$, 则存在 $U \in X$, 使得 $p \nmid |\mathcal{O}_U|$. 此时 $G_U = \{g \in G : gU = u\} \leq G$, 则 $|G_U||\mathcal{O}_U| = p^r m$, 即 $|G_U| = p^r m', m' | m$.

另一方面, 存在自由作用 $G_U \curvearrowright U, g.u = gu \in U$, 则 $|G_U| \mid |U|, |G_U| = p^r$, 只能 $|G_U| = p^r$. 则存在 Sylow p -子群. \square

Example 3.53 $|S_4| = 3^1 \cdot 2^3$, 则 Sylow 3-子群为三阶子群, 只需要找三阶元, 有 8 个三阶元, 故有 4 个三阶子群 $\{\text{Id}, (123), (132)\}, \{\text{Id}, (124), (142)\}, \{\text{Id}, (134), (143)\}, \{\text{Id}, (234), (243)\}$.

Sylow 2-子群为 8 阶子群, 且个数为 3 的因子, 形如 $2k+1$, 则只能为 1 个或 3 个. 若只有 1 个 Sylow 2-子群, 则它为正规子群 (为什么?), 但回忆 S_4 没有 8 阶正规子群, 则只能为 3 个 Sylow 2-子群.

回忆例 3.36 中通过正方形的对称群找到了 S_4 的 8 阶子群, 且通过对正方形的顶点重新编号, 总共可以得到 3 个 8 阶子群, 则得到了所有的 Sylow 2-子群, 分别为 $H_2 = (K_4, (12)), H_3 = (K_4, (13)), H_4 = (K_4, (14))$.

Example 3.54 $|A_4| = 3^1 \cdot 2^2$, 则 Sylow 3-子群为 3 阶子群, 有 8 个三阶元, 故有 4 个三阶子群, 同 S_4 的情形.

Sylow 2-子群为 4 阶子群, 又 $K_4 \triangleleft A_4$ 为四阶正规子群, 则由于 Sylow 2-子群互相共轭, 只有 K_4 这一个 Sylow 2-子群.

Sylow 定理可以帮助我们确定某些特定群的结构.

Theorem 3.12 (Cauchy)

设 p 为 $|G|$ 的素因子, 则 G 含有 p 阶元.



证明 考虑 G 的 Sylow p -子群 $P \leq G$, 则取 $1 \neq g \in P$, 有 $\text{ord}(g) = p^{r'}, 1 \leq r' \leq r$, 则取 $g' = g^{p^{r'}-1}$, 有 $\text{ord}(g') = p$. □

Proposition 3.13

35 阶群必然同构于 $\mathbb{Z}_5 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{35}$.



证明 若 $|G| = 35 = 5 \times 7$, 则 Sylow 5-子群的个数为 7 的因子且形如 $5k+1$, 只能为 1 个, 记为 $\mathbb{Z}_5 \simeq P \triangleleft G$, 同理有唯一的 7 阶子群 $\mathbb{Z}_7 \simeq Q \triangleleft G$.

$P - \{1\}$ 为 5 阶元, $Q - \{1\}$ 为 7 阶元, 则 $P \cap Q = \{1\}$. 且任意 $g \in P, h \in Q, (ghg^{-1})h^{-1} = g(hg^{-1}h^{-1}) \in P \cap Q$, 故只能 $gh = hg$.

从而 $\Phi : P \times Q \rightarrow G, (h, g) \mapsto hg$ 为同态: $\Phi((h_1, g_1) \cdot (h_2, g_2)) = \Phi(h_1h_2, g_1g_2) = h_1h_2g_1g_2 = h_1g_1h_2g_2 = \Phi(h_1, g_1) \cdot \Phi(h_2, g_2)$, 倒数第二步用到了可交换性. 且显然为单同态, 则比较集合大小有 Φ 为同构. 故由中国剩余定理 $G \simeq \mathbb{Z}_5 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{35}$. □

更一般地有

Proposition 3.14

设 G 为 *Abel* 群, 且有素因数分解 $|G| = p_1^{s_1} \cdots p_r^{s_r}$, 则存在唯一的 Sylow p_i -子群, 且有典范同构 $P_1 \times P_2 \cdots \times P_r \xrightarrow{\sim} G, (g_1, g_2, \dots, g_r) \mapsto g_1g_2 \cdots g_r$.



Sylow 定理可以帮助我们找到正规子群, 进而说明某些群不是单群.

Proposition 3.15

(1) 108 阶群不为单群 (2) 56 阶群不是单群.



证明 (1) $|G| = 108 = 2^2 \cdot 3^3$, 则同上, Sylow 3-子群只能有 1 个, 记为 $P \triangleleft G$. 则考虑左诱导作用 $G \curvearrowright G/P, g \cdot (hP) = ghP$, 它是可迁作用, 对应了 $\rho : G \rightarrow S(G/P) = S_4$. 它的像不是平凡的, 故 $\ker \rho \neq G$, 且由于 $[G : \ker \rho] \leq 24$, 只能 $\ker \rho \triangleleft G$ 是非平凡的 G 的正规子群.

(2) 设 $|G| = 56 = 7 \times 8$, 则 7 阶子群个数为 8 的因子且形如 $7k+1$. 若只有 1 个, 则为正规子群, 得证. 下设有 8 个 7 阶子群 H_1, \dots, H_8 .

则 $H_i - \{1\}$ 为 7 阶元, 且 $H_i \cap H_j = \{1_G\}, \forall i \neq j$, 则

$$\cup_{1 \leq i \leq 8} H_i = \{1_G\} \cup \cup_{1 \leq i \leq 8} (H_i - \{1_G\}).$$

则左边的元素个数为 $1 + (7 - 1) \cdot 8 = 49$, 考虑 Sylow 2-子群 Q , 它的大小为 8, 且 $Q - \{1_G\}$ 中的元

素阶只能为 2,4,8, 则 $Q - \{1_G\} \subseteq (\cup_{1 \leq i \leq 8} H_i)^c$, 则比较元素个数只能这两个集合相等, 则 Q 唯一确定, 即只有一个 Sylow 2-子群, 为正规子群. \square

更多的例子可以参考课本例定理 3 和定理 4, 它们分别指出了 pq 阶和 p^2q 阶的群不是单群, 这里 p, q 为素数. 则它们结合定理 3.10 以及命题 3.11, 可以对大部分小阶群进行排除, 再单独排除少数没有筛掉的情形可以得到

Theorem 3.13

若 G 为非 *Abel* 单群, 则 $|G| \geq 60$, 且取等当且仅当 $G \simeq A_5$.



3.7 群的表现

对非空抽象集合 X , 则定义 $X^{-1} = \{x^{-1} : x \in X\}$, 其中 x^{-1} 称为**形式逆**. 则 $X \sqcup X^{-1}$ 称为**字母集**. 我们约定 $(x^{-1})^{-1} = x$.

定义**字 (word)** 为 $w = x_1x_2 \cdots x_n, x_i \in X \sqcup X^{-1}$, 字 w 称为**既约的**, 若不存在 $x_i = x_{i+1}^{-1}$. 约定长度为 0 的字为**空字**, 记为 1.

Proposition 3.16

任何字可以约化为唯一的既约字.



证明 留作练习.



Definition 3.17

对非空抽象集合 X , X 上的**自由群**为 $F(X) = \{X \text{ 上既约字全体}\}$, 上面的乘法定义为两个字的连接并约化, 么元为空字 1. 若 $|X| < \infty$, 称 $F(X)$ 为有限生成自由群.



Example 3.55 $X = \{a\}$, 则 $F(X) = \{a^n : n \in \mathbb{Z}\}$ 为无限循环群.

Example 3.56 $X = \{x, y\}$, 则 $F(X) = \{1, x, y, x^{-1}, y^{-1}, x^2, xy, xy^{-1}, yx, y^2, yx^{-1}, \dots\}$.

Proposition 3.17 (自由群的泛性质)

设 G 为群, 则对任何映射 $f : X \rightarrow G$, f 可以唯一延拓为群同态 $\tilde{f} : F(X) \rightarrow G$.

$$\begin{array}{ccc} X & \xrightarrow{f} & G \\ \downarrow & \searrow \exists! \tilde{f} & \\ F(X) & & \end{array}$$



证明 至多唯一性: 若 \tilde{f} 存在, 则只能 $\tilde{f}(x^{-1}) = f(x)^{-1}$, 进而 $\tilde{f}(x_1x_2 \cdots x_n) = \tilde{f}(x_1)\tilde{f}(x_2) \cdots \tilde{f}(x_n)$.

存在性: $\forall x \in X$, 定义 $\tilde{f}(x) = f(x), \tilde{f}(x^{-1}) = f(x)^{-1}$, 对一般的 $w = x_1x_2 \cdots x_n \in F(X)$, 定义 $\tilde{f}(w) = \tilde{f}(x_1)\tilde{f}(x_2) \cdots \tilde{f}(x_n)$. 可以验证这是满足条件的延拓同态. \square

Proposition 3.18

任意群 G 均为某个自由群的商群.



证明 设 $X \subseteq G$ 为 G 的生成元集, 则对 $X \hookrightarrow G$ 包含映射使用泛性质, 有延拓 $\tilde{f} : F(X) \twoheadrightarrow G$, 则由同态基本定理有 $G \simeq F(X) / \ker \tilde{f}$. \square

Definition 3.18

群 G 的有限表现是指 $G = \langle x_1, \dots, x_n \mid r_1, r_2, \dots, r_m \rangle, m, n < \infty$, 其中 x_i 为生成元, $r_i \in F(x_1, \dots, x_n)$ 为关系. 也可以记为 $G = \langle x_1, \dots, x_n \mid r_1 = 1, r_2 = 1, \dots, r_m = 1 \rangle$.
这也同义于 $F(x_1, x_2, \dots, x_n) / N(r_1, \dots, r_m)$, 其中 $N(r_1, \dots, r_m)$ 为 $F(x_1, \dots, x_n)$ 中包含 r_1, \dots, r_m 的最小正规子群.



Remark 不难验证 $N(r_1, \dots, r_m)$ 为 $\{wr_iw^{-1} : w \in F, 1 \leq i \leq m\}$ 生成的子群.

Proposition 3.19 (有限表现的泛性质)

$G = \langle x_1, \dots, x_n \mid r_1, r_2, \dots, r_m \rangle$, H 为群, 对映射 $f : X = \{x_1, \dots, x_n\} \rightarrow H$, 则 f 可以延拓为群同态 $G \rightarrow H \iff f(x_1), \dots, f(x_n)$ 在 H 中满足关系 $r_i, 1 \leq i \leq m$.



证明 \Rightarrow : 显然.

\Leftarrow : 利用自由群的泛性质, 有延拓 $\tilde{f} : F(X) \rightarrow H$, 则 $f(x_1), \dots, f(x_n)$ 在 H 中满足关系 $r_i, 1 \leq i \leq m$ 说明 $r_1, \dots, r_m \in \ker \tilde{f}$, 进而 $N(r_1, \dots, r_m) \subseteq \ker \tilde{f}$. 由核的泛性质, 诱导了唯一的同态 $\bar{f} = F(X) / N(r_1, \dots, r_m) \rightarrow H, x_i \mapsto f(x_i)$. \square

Example 3.57 考虑 $M_n = \{1, \omega, \dots, \omega^{n-1}\} \subseteq \mathbb{C}^*, \omega = e^{\frac{2\pi i}{n}}$. 我们来说明 $M_n = \langle g \mid g^n = 1 \rangle$.

考虑单元素集合上的映射 $f : \{g\} \rightarrow M_n, g \mapsto \omega$, 则由自由群的泛性质, 存在延拓 $\tilde{f} : F(\{g\}) \rightarrow M_n, g^l \mapsto \omega^l (l \in \mathbb{Z})$. 则 $g^n \in \ker \tilde{f}$, 进而 $N(g^n) \subseteq \ker \tilde{f}$. 故由核的泛性质有诱导映射 $\bar{f} : \langle g \mid g^n = 1 \rangle \rightarrow M_n, g \mapsto \omega$. 比较两边集合大小可知为同构.

Example 3.58 回忆 S_3 可以由 (12) 和 (23) 生成, 考虑二元集合上的映射 $f : X = \{a, b\} \hookrightarrow S_3, a \mapsto (12), b \mapsto (23)$. 则有延拓 $\tilde{f} : F(X) \twoheadrightarrow S_3$. 则 $N(a^2, b^2, (ab)^3) \subseteq \ker \tilde{f}$, 进而有诱导映射 $\bar{f} : F/N = \langle a, b \mid a^2 = b^2 = (ab)^3 = 1 \rangle \twoheadrightarrow S_3$.

通过 $\bar{a} = \bar{a}^{-1}, \bar{b} = \bar{b}^{-1}$ 可以避免 $\bar{a}^{-1}, \bar{b}^{-1}$ 的出现, 且利用 $\overline{aba} = \overline{bab}$, 可以验证任意 F/N 中元素可以约化为 $\bar{1}, \bar{a}, \bar{b}, \overline{ab}, \overline{ba}, \overline{aba}$, 则 $|F/N| \leq 6$. 比较集合大小有 \bar{f} 为同构.

故 $S_3 = \langle a, b \mid a^2 = b^2 = (ab)^3 = 1 \rangle = \langle a, b \mid a^2 = b^2 = 1, aba = bab \rangle$.

Example 3.59 考虑 n 个顶点的正多边形, 定义 D_n 为它在 \mathbb{R}^2 中的对称群, 即 $O(2)$ 中保持该多边形的元素的集合. 则记 a 为逆时针转 $\frac{2\pi}{n}$, b 为关于一个对称轴的对称, 则 $a^n = 1, b^2 = 1, D_n = \langle a, b \rangle$. 特别地有 $|D_n| = 2n$.

不难发现 a, b 满足 $(ab)^2 = 1$, 进而我们希望验证 $D_n = \langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle$. 过程同上面一样地, 定义 $N = N(x^n, y^2, xyxy)$, 利用泛性质我们直接考虑延拓的诱导映射 $\phi : F(x, y) / N \twoheadrightarrow D_n, \bar{x} \mapsto a, \bar{y} \mapsto b$.

考虑任意 F/N 中的字 w , $\bar{w} = \overline{x_1 x_2 \cdots x_n}$, $x_i \in \{x^{\pm 1}, y^{\pm 1}\}$, 则通过 $\bar{y}^{-1} = \bar{y}$ 保证 \bar{y}^{-1} 不出现, $\bar{x}^{-1} = \bar{x}^{n-1}$ 保证 \bar{x}^{-1} 不出现, 并利用 $\bar{y}\bar{x} = \bar{x}^{n-1}\bar{y}$ 将所有 \bar{y} 移到右边, 最终可以化为 $\bar{w} = \bar{x}^s \bar{y}^t$ ($0 \leq s \leq n-1, 0 \leq t \leq 1$), 进而 $|F/N| \leq 2n$. 故比较集合大小有 ϕ 为同构.

还可以验证 $D_n = \langle s, t \mid s^2 = t^2 = (st)^n = 1 \rangle$, 则考虑延拓映射 $F(s, t) \twoheadrightarrow D_n, s \mapsto ab, t \mapsto b$, 则 $s^2, t^2, (st)^n$ 均包含在核中, 故有诱导映射 $\psi: F(s, t) / N(s^2, t^2, (st)^n) \twoheadrightarrow D_n$. 同样可以保证 $\bar{s}^{-1}, \bar{t}^{-1}$ 不出现, 且 $\bar{ts} = \overline{st}^{n-1}$, 则可以化为 $(\overline{st})^k$ 或者 $(\overline{st})^k \bar{s}, 0 \leq k \leq n-1$, 则 $|F/N| \leq 2n$, 同理有 ψ 为同构.

进一步也可以定义无限的多面体群 $D_\infty = \langle s, t \mid s^2 = t^2 = 1 \rangle$, 它是一个无限的群, 且可以作用在 \mathbb{R}^2 上.

Example 3.60 考虑四元数群 \mathbb{Q}_8 , 可以证明 $\mathbb{Q}_8 = \langle x, y \mid x^4 = 1, x^2 = y^2, yx = x^3y \rangle$. 证明过程与上面相似, 在此省略.

3.8 有限生成 Abel 群

对加法群 A, B (自然是 Abel 的), 定义它们的直和为 $A \oplus B = A \times B = \{(a, b) : a \in A, b \in B\}$, 加法定义为 $(a, b) + (a', b') = (a + a', b + b')$, 则 $A \oplus B$ 也是 Abel 群.


Example 3.61 对 $n \geq 1$, 记 $\mathbb{Z}^n = \mathbb{Z} \oplus \mathbb{Z} \cdots \oplus \mathbb{Z}$ (n 个). 它由 e_1, \dots, e_n , 其中 $e_i = (0, \dots, 1, 0, \dots, 0)$, 只有第 i 位为 1 其余为 0.

我们称 \mathbb{Z}^n 为秩为 n 的自由 Abel 群. 可以验证 \mathbb{Z}^n 有群表现 $\langle x_1, \dots, x_n \mid x_i x_j = x_j x_i, i \neq j \rangle$.

Definition 3.19

对 Abel 群 A , 有限子集 $S \subseteq A$ 称为有限基, 若


(1) S 生成 A : $\forall a \in A, \exists n_i \in \mathbb{Z}, s_i \in S, a = n_1 s_1 + \cdots + n_l s_l$.

(2) S 是 \mathbb{Z} -线性无关的: $\forall s_1, \dots, s_l \in S$ 两两不同, 若 $n_1 s_1 + \cdots + n_l s_l = 0_A, n_i \in \mathbb{Z}$, 则 $n_i = 0$. 

Example 3.62 $\{e_1, \dots, e_n\}$ 为 \mathbb{Z}^n 的有限基.

Proposition 3.20

(1) 有限生成的 Abel 群存在有限基 $\iff A \simeq \mathbb{Z}^n$.

(2) 设 A 为有限生成 Abel 群, 则存在 n 和 $K \leq \mathbb{Z}^n$ 使得 $A \simeq \mathbb{Z}^n / K$. 

证明 (1) \Leftarrow : 已知.

\Rightarrow : 设 A 有有限基 $S = \{v_1, \dots, v_n\}$, 则定义同态: $\mathbb{Z}^n \rightarrow A, e_i \mapsto v_i$. 由定义中条件 (1) 可知为满射, 条件 (2) 可知为单射, 则有同构 $A \simeq \mathbb{Z}^n$.

(2) 取 A 的生成元集 $\{v_1, \dots, v_n\}$, 仍然考虑满同态 $\phi: \mathbb{Z}^n \rightarrow A, e_i \mapsto v_i$, 则有 $A \simeq \mathbb{Z}^n / \ker \phi$. \square

Theorem 3.14

若 $K \leq \mathbb{Z}^n$, 则 K 有限生成. 

证明 $n = 1$ 时, K 只能为 0 或者 $d\mathbb{Z}$, 则显然有限生成.

$n = 2$ 时, $K \leq (\mathbb{Z}e_1) \oplus (\mathbb{Z}e_2)$. 则考虑 $(K \cap \mathbb{Z}e_1) \leq \mathbb{Z}e_1 \simeq \mathbb{Z}$ 有限生成. 有同构

$$K / K \cap \mathbb{Z}e_1 \rightarrow K + \mathbb{Z}e_1 / \mathbb{Z}e_1, x + (K \cap \mathbb{Z}e_1) \mapsto x + \mathbb{Z}e_1.$$

进而 $K / K \cap \mathbb{Z}e_1 \subseteq \mathbb{Z}^2 / \mathbb{Z}e_1 \simeq \mathbb{Z}e_2$, 则有限生成.

练习: 若 $N \triangleleft G, N$ 和 G/N 都有限生成, 则 G 有限生成.

则使用该结论有 K 有限生成. $n > 2$ 的情形类似, 在此省略. \square

下面我们引入矩阵的语言. 记 $M_{n \times m}(\mathbb{Z})$ 为 n 行 m 列的整数矩阵的全体, 对 $A \in M_{n \times m}(\mathbb{Z})$, 可以定义群同态 $\phi_A: \mathbb{Z}^m \rightarrow \mathbb{Z}^n, \vec{v} \mapsto A\vec{v}$.

进一步地任意群同态 $f: \mathbb{Z}^m \rightarrow \mathbb{Z}^n$, 取 A 为以 $f(e_1), \dots, f(e_m)$ 为列向量拼成的 $n \times m$ 矩阵, 则有 $f = \phi_A$. 即有

Proposition 3.21

$M_{n \times m}(\mathbb{Z})$ 中的矩阵与 $\mathbb{Z}^n \rightarrow \mathbb{Z}^m$ 的群同态一一对应, 且矩阵乘法对应群同态的复合, 即若 $A \in M_{n \times m}(\mathbb{Z}), B \in M_{p \times n}(\mathbb{Z})$, 有 $\phi_B \circ \phi_A = \phi_{BA}: \mathbb{Z}^m \rightarrow \mathbb{Z}^p$.



Example 3.63 利用这个结论我们可以证明: 若 $\mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}^m$, 则 $n = m$.

Definition 3.20

对 $A \in M_{n \times m}(\mathbb{Z})$, 则定义 $\phi_A: \mathbb{Z}^m \rightarrow \mathbb{Z}^n$ 的余核为 $\text{Cok}(\phi_A) = \mathbb{Z}^n / \text{Im}(\phi_A)$.

**Proposition 3.22**

任意有限生成 Abel 群均同构与某个 $\text{Cok}(\phi_A)$.



证明 由命题 3.20(2), 设 $G \simeq \mathbb{Z}^n / K$, 由定理 3.14, K 有限生成, 设 $K = \langle v_1, \dots, v_m \rangle$, 则定义 $\phi_A: \mathbb{Z}^m \rightarrow \mathbb{Z}^n, e_i \rightarrow v_i$, 则有 $G \simeq \text{Cok}(\phi_A)$. \square

故有限生成 Abel 群的考察转化为 $\text{Cok}(\phi_A)$ 的考察.

考虑 $GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \exists B \in M_n(\mathbb{Z}), AB = BA = I_n\} = \{A \in M_n(\mathbb{Z}) : \det A = \pm 1\}$. 则显然 $A \in GL_n(\mathbb{Z})$ 当且仅当 $\phi_A: \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ 为群同构.

与线性代数中一样地可以定义整数矩阵的相抵: 对 $A, B \in M_{n \times m}(\mathbb{Z})$, 称他们 \mathbb{Z} -相抵, 若存在 $P \in GL_n(\mathbb{Z}), Q \in GL_m(\mathbb{Z})$ 使得 $B = PAQ$. 注意相抵是一个等价关系.

Proposition 3.23

若 A, B 是 \mathbb{Z} -相抵, 则 $\text{Cok}(\phi_A) \simeq \text{Cok}(\phi_B)$.



证明 设 $B = PAQ$, 其中 $\phi_P: \mathbb{Z}^n \rightarrow \mathbb{Z}^n, \phi_Q: \mathbb{Z}^m \rightarrow \mathbb{Z}^m$ 为同构, 考察如下的交换图表

$$\begin{array}{ccccc} \mathbb{Z}^m & \xrightarrow{\phi_A} & \mathbb{Z}^n & \xrightarrow{\text{can}_A} & \text{Cok}(\phi_A) \\ \uparrow \tilde{\phi}_Q & & \uparrow \tilde{\phi}_P & & \uparrow \overline{\phi_P} \\ \mathbb{Z}^m & \xrightarrow{\phi_B} & \mathbb{Z}^n & \xrightarrow{\text{can}_B} & \text{Cok}(\phi_B) \end{array}$$

可以验证 $\overline{\phi_P}$ 为同构, 细节留作练习. \square

则有限生成 Abel 群的结构问题可以通过找矩阵的相抵标准型来简化. 我们通过整数矩阵的行列变换来进行相抵简化: 可以行列互换, 行列乘以 ± 1 , 将某行(列)的若干倍加到另一行(列)上(也即“打洞”). 可以获得如下的 Smith 标准型.

Theorem 3.15 (Smith 标准型)

任意 $A \in M_{n \times m}(\mathbb{Z})$ 可以相抵为 $B = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r & \\ & & & 0 \end{pmatrix}$, 其中 $1 \leq d_1 \mid d_2 \cdots \mid d_r$.



证明 线性代数习题, 略. □

Example 3.64 $A = \begin{pmatrix} 2 & 4 \\ 6 & 5 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 \\ 0 & -7 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & -7 \end{pmatrix} \sim \begin{pmatrix} 2 & -7 \\ 0 & -7 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 \\ 0 & -7 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 \\ -7 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 \\ 0 & 14 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix} = B$, 进而 $\mathbb{Z}^2 / ((2, 6)^T, (4, 5)^T) = \text{Cok}(\phi_A) \simeq \text{Cok}(\phi_B) = \mathbb{Z}_{14}$.

注意到我们使用了如下结论 (可以自行证明): 若 $N_1 \triangleleft G_1, N_2 \triangleleft G_2, N_1 \times N_2 \triangleleft G_1 \times G_2$, 则 $G_1 \times G_2 / N_1 \times N_2 \simeq (G_1/N_1) \times (G_2/N_2)$.

总而言之, 对一般的有限生成 Abel 群 G , 则由命题 3.22, G 同构于 $\text{Cok}(\phi_A)$, 又 A 可以相抵于 Smith 标准型 B , 则由命题 3.23, 有 $G \simeq \text{Cok}(\phi_B)$.

这里 $\phi_B: \mathbb{Z}^m \rightarrow \mathbb{Z}^n, e_i \mapsto d_i e_i (i \leq r) \text{ 或 } 0 (i > r)$. 则 $\text{Im} \phi_B = \mathbb{Z}(d_1 e_1) \oplus \cdots \oplus \mathbb{Z}(d_r e_r)$. 故由定义有 $\text{Cok}(\phi_B) \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z}^{n-r}$. 于是我们有下面的结构定理.

Theorem 3.16 (有限生成 Abel 群结构定理)

任意有限生成 Abel 群 G , 存在 $s \geq 0, 1 \leq d_1 \mid \cdots \mid d_r$ 使得

$$G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z}^s.$$

特别地, 若 G 有限, 则 $G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n}$.



有一些简单的情形:

Proposition 3.24

(1) 若 $A \in M_n(\mathbb{Z})$, 且 $\det A \neq 0$, 则 $|\text{Cok}(\phi_A)| < \infty$, 且 $|\text{Cok}(\phi_A)| = |\det A|$.

(2) 若 $K \leq \mathbb{Z}^n$, 则存在 \mathbb{Z}^n 的基 e_1, \dots, e_n 和 $d_1 \mid \cdots \mid d_r (r \leq n)$, 使得 K 恰好以 $d_1 e_1, \dots, d_r e_r$ 为基.



证明 (1) $\det A \neq 0$, 则 Smith 标准型 B 的对角元为 d_1, \dots, d_n 均非 0, 则

$$\text{Cok}(\phi_A) \simeq \text{Cok}(\phi_B) \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n}$$

则 $|\text{Cok}(\phi_A)| = |\text{Cok}(\phi_B)| = d_1 \cdots d_n = |\det A|$.

(2) 设 $K = \text{Im} \phi_A$, A 的 Smith 标准型为 B , 则有交换图表

$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{\phi_A} & \mathbb{Z}^n \\ \tilde{\phi}_Q \uparrow & & \uparrow \tilde{\phi}_P \\ \mathbb{Z}^m & \xrightarrow{\phi_B} & \mathbb{Z}^n \end{array}$$

则 $K = \phi_P(\text{Im} \phi_B)$, 特别地 K 以 $\phi_P(d_1 e_1), \dots, \phi_P(d_r e_r)$ 为基, 其中 e_1, \dots, e_n 为 \mathbb{Z}^n 的标准基. □

Definition 3.21

Abel 群 G 的扭子群为 $t(G) = \{g \in G : \text{ord}(g) < \infty\} \leq G$.

**Theorem 3.17**

设 G 为有限生成 Abel 群, 则存在内直和 $G = t(G) \oplus F$, 其中 F 是有限生成自由 Abel 群, 被称为 $t(G)$ 的补 (注意 $F \leq G$ 不唯一!). 且 $|t(G)| < \infty$, 同构于 $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$.



证明 由结构定理有同构 $\theta : G \rightarrow \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z}^s$, 将有限部分记为 A , 自由部分记为 B , 则 $G = \theta(A) \oplus \theta(B)$.

只需要说明 $\theta(A) = t(G)$. 首先显然有 $A \simeq \theta(A) \leq t(G)$, 另一方面若 $g \in t(G)$, $\text{ord}(g) = k$, 则设分解 $g = a + b$, 其中 $a \in \theta(A)$, $b \in \theta(B)$, 则 a 有限阶, 设 $\text{ord}(a) = l$, 则 $kla + klb = klg = 0$, 即 $klb = 0$, 由 b 自由只能有 $b = 0$, 进而 $t(G) \subseteq \theta(A)$. 故得证. \square

Example 3.65 $G = \mathbb{Z}_2 \oplus \mathbb{Z}$, 则 $t(G) = \mathbb{Z}_2 \oplus 0$, 可以验证 $0 \oplus \mathbb{Z}$ 和 $\mathbb{Z}(-1, 1)$ 均为 $t(G)$ 的补.

下面将扭子群进一步约化. 首先回忆中国剩余定理给出若 p_1, \dots, p_r 为不同的素数, 则有

$$\mathbb{Z}_{p_1^{i_1} \cdots p_r^{i_r}} \simeq \mathbb{Z}_{p_1^{i_1}} \times \cdots \times \mathbb{Z}_{p_r^{i_r}}.$$

则 $t(G)$ 可以写成 Sylow p -子群的积.

Proposition 3.25

G 为有限 Abel 群, 则 $G \simeq (\mathbb{Z}_{p_1^{s_{11}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{s_{1t_1}}}) \oplus \cdots \oplus (\mathbb{Z}_{p_r^{s_{r1}}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{s_{rt_r}}})$. 称 $p_i^{s_{ij}}$ 为 G 的初等因子.



Example 3.66 设 $|G| = 1500 = 2^2 \times 3^1 \times 5^3$ 且 G 为 Abel 群, 则 2^2 可以对应 $\mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2$ 共两种, 3^1 对应 \mathbb{Z}_3 共 1 种, 5^3 对应 $\mathbb{Z}_{125}, \mathbb{Z}_{25} \oplus \mathbb{Z}_5, \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ 共 3 种, 则 G 有六种结构.

Chapter 4 Galois 理论

4.1 Galois 扩张

对域扩张 K/k , 记 $\text{Gal}(K/k) = \text{Aut} K/k$ 为域扩张 K/k 的 Galois 群.

Lemma 4.1

若 $\dim_k K < \infty$, 则 $|\text{Gal}(K/k)| \leq \dim_k K < \infty$. 特别地当 $K = (k, f(x))$ 为某个可分多项式 $f(x) \in k[x]$ 的分裂域时, 有 $|\text{Gal}(K/k)| = \dim_k K$.



证明 与定理 2.4 的证明思路一致, 这里再回忆一遍. 仍然对 $\dim_k K$ 归纳. 当 $\dim_k K = 1$ 时显然成立.

若 $\dim_k K > 1$ 且对 $\dim_k K$ 更小的时候成立, 则取 $\alpha \in K - k$. 由于 $\dim_k K < \infty$, 则 α 在 k 上代数. 则取最小多项式 $f(x) \in k[x]$. 设有 $\text{Id} : k \rightarrow k$ 到 $k(\alpha)$ 上的延拓 δ , 则 $0 = \delta(f(\alpha)) = f(\delta(\alpha))$, 即 $\delta(\alpha) \in \text{Root}_k(f)$.

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K \\ \uparrow & & \uparrow \\ k(\alpha) & \xrightarrow{\delta} & k(\beta) \\ \uparrow & & \uparrow \\ k & \xrightarrow{\text{Id}} & k \end{array}$$

由于延拓 $\delta : k(\alpha) \rightarrow K$ 由 $\delta(\alpha)$ 确定, 故 $k(\alpha)$ 上的延拓 δ 的个数为 $|\text{Root}_k(f)| \leq \deg f(x) = \dim_k k(\alpha)$.

再由归纳假设, δ 到 K 上的延拓个数小于等于 $\dim_{k(\alpha)} K$, 故 $\text{Id} : k \rightarrow k$ 到 K 上的延拓至多有 $\dim_k k(\alpha) \dim_{k(\alpha)} K = \dim_k K$ 个. 当 K 为可分多项式的分裂域时上面的不等号都能取到等号, 则得证. \square

进一步考虑 $G \leq \text{Aut}(K)$, 则 $G \curvearrowright K, \sigma.v = \sigma(v)$, 考虑不变子域 $K^G = \{v \in K : \sigma(v) = v, \forall \sigma \in G\} \subseteq K$. 我们有如下观察:

- (1) 若 $H \leq G$, 则有 $K^G \subseteq K^H \subseteq K$, 特别地有 $K^{\text{Id}_K} = K$.
- (2) 若 $G \leq \text{Aut}(K/k)$, 则 $k \subseteq K^G \subseteq K$. 特别地有 $k \subseteq K^{\text{Gal}(K/k)}$.
- (3) 取 $G \leq \text{Aut}(K)$, 则 $G \leq \text{Aut}(K/K^G)$.

关于 K^G 有如下更精确的刻画:

Theorem 4.1

若 $G \leq \text{Aut}(K/k)$ 为有限子群, 则

- (1) $[K : K^G] = |G|$.
- (2) $G = \text{Gal}(K/K^G)$.



证明 设 $|G| = n, k = K^G$, 则 $n = |G| \leq \dim_k K$, 则我们只需证 $\dim_k K \leq n$.

若不然, 则存在 $e_1, \dots, e_{n+1} \subseteq K$ 是 k -线性无关的, 则考虑 $n \times (n+1)$ 的 K 矩阵 $A = (\sigma_i(e_j))_{i,j}$, 其中 $G = \{\sigma_1 = 1, \dots, \sigma_n\}$.

取 $V = \{v \in K^{n+1} : Av = 0\}$ 为 A 的零空间, 则它是非空的 (这里给出了本质区别). 我们有如下的重要观察: 若 $v \in V, \tau \in G$, 则 $\tau(v) \in V$. 下面证明之.

设 $v = (\lambda_1, \dots, \lambda_{n+1})^T$, 则由 $v \in V$, 有 $\forall \sigma \in G, 0 = \sum_{i=1}^{n+1} \lambda_i \sigma(e_i)$. 则两边作用 τ 有

$$0 = \sum_{i=1}^{n+1} \tau(\lambda_i) \cdot \tau\sigma(e_i), \forall \sigma \in G.$$

又所有的 $\tau\sigma (\sigma \in G)$ 也取遍了所有的 G 中元素, 即有

$$0 = \sum_{i=1}^{n+1} \tau(\lambda_i) \cdot \sigma(e_i), \forall \sigma \in G.$$

故 $\sigma(v) \in V$.

现在取非零的 $v = (\lambda_1, \dots, \lambda_{n+1})^T \in V$ 使得其非零分量数最少, 由于 $\sum \lambda_i e_i = 0$, 显然至少有两个非零分量, 则不妨设 $v = (1, \lambda_2, \dots, 0)$. 再次由于 $\sum \lambda_i e_i = 0$ 以及 e_i 是 k -线性无关的, 故 v 中的分量不会都在 K 中, 则不妨设 $\lambda_2 \notin k = K^G$.

则存在 $\sigma \in G$ 使得 $\sigma(\lambda_2) \neq \lambda_2$, 又由上面的观察有 $v - \sigma(v) \in V$. 另一方面 $0 \neq v - \sigma(v) = (0, \lambda_2 - \sigma(\lambda_2), \dots, 0)^T$ 的非零分量个数比 v 更少, 与 v 的选取矛盾! 则矛盾. \square

现在考虑有限维域扩张 K/k , 记 $G = \text{Gal}(K/k)$, 则引理 4.1 给出 $|G| \leq \dim_k K < \infty$. 下面的定理给出了这里取等的等价刻画.

Theorem 4.2

以下命题等价:

(1) $k = K^G$.

(2) $|G| = \dim_k K$.

(3) $\forall \alpha \in K$, 则 α 在 k 上的最小多项式无重根且在 K 上分裂.

(4) $K = (k, f(x))$ 为可分多项式 $f(x) \in k[x]$ 的分裂域.

此时称 K/k 为有限 **Galois 扩张**.



证明 定理 4.1 给出了 $(1) \iff (2)$, 此外已知 $(4) \Rightarrow (2)$, 则只需证明 $(2) \Rightarrow (3) \Rightarrow (4)$.

$(2) \Rightarrow (3)$: 对任意 $\alpha \in K$, k 上最小多项式为 $g(x)$, 则仍然考虑如下的扩张

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K \\ \uparrow & & \uparrow \\ k(\alpha) & \xrightarrow{\delta} & k(\beta) \\ \uparrow & & \uparrow \\ k & \xrightarrow{\text{Id}} & k \end{array}$$

则延拓 δ 的个数为 $|\text{Root}_K g(x)| \leq \deg g(x) = \dim_k k(\alpha)$. 由 (2) 的条件这里必须取等, 则 $|\text{Root}_K g(x)| = \deg g(x)$, 即 $g(x)$ 在 K 上分裂且无重根.

(3) \Rightarrow (4): 设 $K = k(\alpha_1, \dots, \alpha_n)$, 则设 α_i 的最小多项式为 $g_i(x)$, 定义 $f(x) = g_1(x) \cdots g_n(x)$, 则 $f(x)$ 在 K 上分裂且可分, $K = (k, f(x))$. \square

Remark 若 K/k 为有限 Galois, 且 $k \subseteq E \subseteq K$ 为中间域, 则 K/E 为有限 Galois 扩张, 因为 $K = (k, f(x)) = (E, f(x))$.

Example 4.1 考虑 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq (\mathbb{Q}, x^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. 后面的域扩张为 Galois 的, 但第一个域扩张 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是 (见例 4.2).

Example 4.2 对 Galois 扩张 K/k , 设 $H \leq G = \text{Gal}(K/k)$, 则 $H = \text{Gal}(K/K^H)$, $|H| = [K : K^H]$.

由 Galois 扩张有 $|G| = \dim_k K$, 则由 Lagrange 定理 $|G| = [G : H]|H|$, 即 $\dim_k K = [G : H][K : K^H]$, 则 $[G : H] = \dim_k K^H$. 这是一个非常有用的结论!

下面给出了 E/k 是 Galois 扩张的条件.

Proposition 4.1

设 K/k 有限 Galois 扩张, $k \subseteq E \subseteq K$ 为中间域, 则

E/k 是 Galois 的 $\iff \forall \sigma \in \text{Gal}(K/k), \sigma(E) = E$.



证明 \Rightarrow : 若 E/k 为 Galois 扩张, 设 $E = (k, g(x)) = k(\beta_1, \dots, \beta_m)$, 其中 $g(x) = (x - \beta_1) \cdots (x - \beta_m) \in k[x]$. 则对 $\sigma \in G = \text{Gal}(K/k)$, 有 $\sigma(E) = k(\sigma(\beta_1), \dots, \sigma(\beta_m))$.

由于 $g(\beta_i) = 0$, 则 $g(\sigma(\beta_i)) = \sigma(g(\beta_i)) = 0$, 故 $\sigma(\beta_i) \in \{\beta_1, \dots, \beta_m\}$. 从而 $\sigma(E) = E$.

\Leftarrow : $\forall b \in E \subseteq K$, 考虑其 k 上最小多项式 $g(x) \in k[x]$, 则又 K/k 是 Galois 扩张可知 $g(x)$ 可分且在 K 上分裂, 则设 $g(x) = (x - \beta_1) \cdots (x - \beta_m) \in k[x]$, 其中 $\beta_i \in K$.

不妨设 $\beta_1 = b$, 则对任意 $i \geq 2$, 仍然考虑

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K \\ \uparrow & & \uparrow \\ k(\beta_1) & \xrightarrow{\delta} & k(\beta_i) \\ \uparrow & & \uparrow \\ k & \xrightarrow{\text{Id}} & k \end{array}$$

则 $\sigma \in \text{Gal}(K/k)$, 且 $\sigma(\beta_1) = \beta_i$, 由条件 $\beta_i \in E$, 故最终 $g(x)$ 在 E 上分裂且可分, 则 E/k 为 Galois 扩张. \square

4.2 Galois 对应

对有限 Galois 扩张有如下的 Galois 对应.

Proposition 4.2 (绝对 Galois 对应)

任意域 K , 有一一对应

$$\{G \leq \text{Aut}(K)\} \xrightleftharpoons[\text{Gal}(K/k) \leftarrow k]{G \rightarrow K^G} \{k \subseteq K : K/k \text{ 为有限 Galois 扩张}\}$$



Proposition 4.3 (相对 Galois 对应)

设 K/k 为有限 Galois 扩张, 则有一一对应

$$\{G \leq \text{Gal}(K/k)\} \xrightleftharpoons[\text{Gal}(K/E) \leftarrow E]{H \rightarrow K^H} \{k \subseteq E \subseteq K : E \text{ 为中间域}\}$$



Example 4.3 考虑 $\mathbb{Q} \subseteq K = (\mathbb{Q}, x^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$, 则 K/\mathbb{Q} 为有限 Galois 扩张, 且 $\dim_{\mathbb{Q}} K = 6$.

则 $G \curvearrowright K$ 且保持 $x^3 - 2$ 的根, 故 $G \curvearrowright X = \text{Root}_K(x^3 - 2) = \{a = \sqrt[3]{2}, b = \sqrt[3]{2}\omega, c = \sqrt[3]{2}\omega^2\}$. 这是一个忠实作用, 则有嵌入 $G \hookrightarrow S(X) = S_3$. 比较集合大小可知有同构 $G \simeq S(X) = S_3$.

设 $(ab) \in S(X)$ 对应 σ_1 , 则 $\sigma : \sqrt[3]{2} \leftrightarrow \sqrt[3]{2}\omega$ 且保持 $\sqrt[3]{2}\omega^2$ 不动. 此时有 $\sigma(\omega) = \sigma(\frac{\sqrt[3]{2}\omega}{\sqrt[3]{2}}) = \frac{\sqrt[3]{2}}{\sqrt[3]{2}\omega} = \omega^2$.

注意到由于 $\sigma(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\sqrt[3]{2}\omega) \neq \mathbb{Q}(\sqrt[3]{2})$, 则有上一节的命题 4.1, 可知 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是 Galois 扩张.

考虑 G 的子群 $H = \{\sigma, \text{Id}\}$, 我们来求 K^H .

首先有 $[K : K^H] = |H| = 2$, 则 $\dim_{\mathbb{Q}} K^H = 3$. 同时又知道 $\sqrt[3]{2}\omega^2$ 在 σ_1 下保持不动, 则 $\mathbb{Q}(\sqrt[3]{2}\omega^2) \subseteq K^H$. 比较两边维数可知 $K^H = \mathbb{Q}(\sqrt[3]{2}\omega^2)$. 它是 K 的子域.

Example 4.4 考虑定理 2.9 中的有限域 Galois 对应. 设 $\dim_{\mathbb{F}_p} K = n$, 即 $K = (\mathbb{F}_p, x^{p^n} - x)$, 则 K/\mathbb{F}_p 是 Galois 扩张. 且熟知 $\text{Gal}(K/\mathbb{F}_p) = \{1, \sigma, \dots, \sigma^{n-1}\} \simeq (\mathbb{Z}_n, +)$, 其中 σ 为 Frobenius 同构.

则 K 的子域对应于 $\text{Gal}(K/\mathbb{F}_p)$ 的子群, 即为 $\langle \sigma^d \rangle$ (其中 $d|n$), 它的不动子域为 $\{a \in K : \sigma^d(a) = a\} = \text{Root}_K(x^{p^d} - x)$.

Example 4.5 对有限群 G , 则设 $G \leq S_n$, 显然 $S_n \curvearrowright k(t_1, \dots, t_n) = K$, 即 n 元有理函数域, 其中 $\sigma(t_i) = t_{\sigma(i)}$, 则 $G \curvearrowright K, G \leq \text{Aut}(K)$, 进而由绝对 Galois 对应, $G \simeq \text{Gal}(K/K^G)$.

下面用偏序集和格的语言描述 Galois 对应.

Definition 4.1

给定非空集合 L , L 上的**偏序**是 L 上的一个二元关系 \leq , 满足

- (1) 自反性: $\forall a \in L, a \leq a$.
- (2) 反对称性: 若 $a \leq b, b \leq a$, 则 $a = b$.
- (3) 传递性: 若 $a \leq b, b \leq c$, 则 $a \leq c$.

此时称 (L, \leq) 是一个**偏序集**.



Example 4.6 对群 G , 则 G 的子群构成的集合 $\text{Sub}(G) = \{H : H \leq G\}$ 关于集合的包含关系成为一个偏序集.

Definition 4.2

设 (L, \leq) 为偏序集.

(1) 设 $a, b \in L$, 定义 $a \vee b \in L$ 为 a, b 的**最小上界** (若存在则唯一) 满足

- (i) $a \leq (a \vee b), b \leq (a \vee b)$.
- (ii) $a \leq c, b \leq c$, 则 $a \vee b \leq c$.

(2) 设 $a, b \in L$, 定义 $a \wedge b \in L$ 为 a, b 的**最大下界** (若存在则唯一) 满足

- (i) $(a \wedge b) \leq a, (a \wedge b) \leq b$.
- (ii) $c \leq a, c \leq b$, 则 $c \leq a \wedge b$.

若 L 满足 $\forall a, b \in L, a \vee b$ 和 $a \wedge b$ 都存在, 则称偏序集 (L, \leq) 为**格**.



Example 4.7 G 是群, 则 $\text{Sub}(G)$ 是一个格: 对 $H, U \leq G$, 则 $H \vee U = \langle H, U \rangle = \{s_1 \cdots s_n : n \geq 1, s_i \in H \cup U\}, H \wedge U = H \cap U$.

Example 4.8 对域扩张 K/k , 定义格 $\text{Lat}(K/k)$ 为中间域的集合, 集合的包含关系作为偏序关系.

对 E, F 为中间域, 有 $E \wedge F = E \cap F, E \vee F$ 为 E, F 生成的子域, 即 $\{(\sum e_j f_j)(\sum e_i f_i)^{-1} : e_i, e_j \in E, f_i, f_j \in F\}$.

Example 4.9 对格 (L, \leq) , 可以定义反格 (L^{op}, \leq^{op}) , 其中 $a \leq^{op} b \iff b \leq a$, 则 $a \wedge^{op} b = a \vee b, a \vee^{op} b = a \wedge b$.

Example 4.10 对 $n \geq 1$, 定义 $L_n = \{d : 1 \leq d \leq n, d|n\}$, 定义 $d \leq d' \iff d|d'$, 则 (L_n, \leq) 为偏序集. 且 $d_1 \vee d_2 = \text{lcm}(d_1, d_2), d_1 \wedge d_2 = \text{gcd}(d_1, d_2)$. 故 (L_n, \leq) 为格.

取 $C_n = \langle g \mid g^n = 1 \rangle = \{1, g, \dots, g^{n-1}\}$, 则有格同构 $\text{Sub}(C_n) \xrightarrow{\sim} L_n, \langle g^{\frac{n}{d}} \rangle \mapsto d$.

Lemma 4.2

若 L, L' 为格, 且 $f : L \rightarrow L'$ 为偏序集的同构, 即 f 为双射且 f, f^{-1} 均保持偏序关系, 则 f 保持 \wedge 以及 \vee .



证明 $a \leq a \vee b, b \leq a \vee b$, 则 $f(a) \leq f(a \vee b), f(b) \leq f(a \vee b)$, 则 $f(a) \vee f(b) \leq f(a \vee b)$.

记 $d = f^{-1}(f(a) \vee f(b))$, 则 $f(a) \leq f(d), f(b) \leq f(d)$, 则 $a \leq d, b \leq d$, 故 $a \vee b \leq d$. 则 $f(a \vee b) \leq f(d) = f(a) \vee f(b)$.

综上有 $f(a) \vee f(b) = f(a \vee b)$, 对 \wedge 同理. □

则我们可以利用上面的语言叙述如下的 Galois 理论基本定理.

Theorem 4.3 (Galois 理论基本定理)

设 K/k 为有限 Galois 扩张, 令 $G = \text{Gal}(K/k)$, 则有格同构

$$\text{Sub}(G) \xrightleftharpoons[\text{Gal}(K/E) \leftarrow E]{H \rightarrow K^H} \text{Lat}(K/k)^{op}$$



则立即有如下推论

Proposition 4.4

(1) 若 $H, U \leq G$, 则 $K^{H \vee U} = K^H \cap K^U, K^{H \cap U} = K^H \vee K^U$.

(2) 若 $k \subseteq B, E \subseteq K$, 则 $\text{Gal}(K/B \vee E) = \text{Gal}(K/B) \cap \text{Gal}(K/E), \text{Gal}(K/B \cap E) = \text{Gal}(K/B) \vee \text{Gal}(K/E)$.



4.3 例子和应用

首先观察 $G \curvearrowright \text{Sub}(G) = \{H : H \leq G\}$, $\sigma.H = \sigma H \sigma^{-1}$, 则 H 在该作用下不动等价于 $H \triangleleft G$.

类似地考虑 $G \curvearrowright \text{Lat}(K/k)$, $\sigma.E = \sigma(E) \subseteq K$. 则由命题 3.1, 有 E 在该作用下不动等价于 E/k 是 Galois 扩张. 这提示我们进行下面的论断

Theorem 4.4

$k \subseteq E \subseteq K$, 则 E/k 是 Galois 扩张 $\iff \text{Gal}(K/E) \triangleleft G$, 且此时有 $G/\text{Gal}(K/E) \xrightarrow{\sim} \text{Gal}(K/k)$. ♥

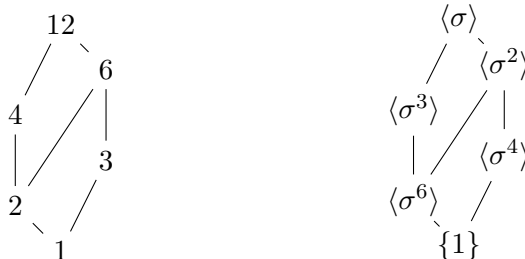
证明 若证第一个命题, 由命题 4.1 和 Galois 对应, 只需要证明 $\sigma \text{Gal}(K/E) \sigma^{-1} = \text{Gal}(K/\sigma(E))$, 并直接设 $E = K^H$, 则只需证明 $K^{\sigma H \sigma^{-1}} = \sigma(K^H)$. 这是因为

$$\begin{aligned} K^{\sigma H \sigma^{-1}} &= \{\lambda \in K : \sigma h \sigma^{-1}(\lambda) = \lambda, \forall h \in H\} \\ &= \{\lambda \in K : h \sigma^{-1}(\lambda) = \sigma^{-1}(\lambda)\} \\ &= \{\lambda \in K : h \sigma^{-1} \in K^H\} = \sigma(K^H) \end{aligned}$$

此时考虑 $G \twoheadrightarrow \text{Gal}(K/E)$, $\sigma \mapsto \sigma|_E$, 核显然为 $\text{Gal}(K/E)$, 则有群同态基本定理得证. □

对于偏序集 (L, \leq) , 可以画出所谓的 Hesse 图来表示偏序关系.

Example 4.11 记 $L_{12} = \{d : d \mid 12\} = \{1, 2, 3, 4, 6, 12\}$, 则可画出 L_{12} 的 Hesse 图. 进而有 $C_{12} = \langle \sigma \mid \sigma^{12} = 1 \rangle$ 的 Hesse 图.



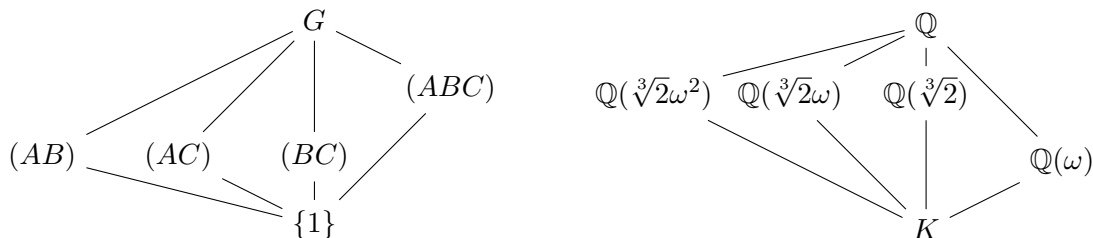
Example 4.12 令 $G = \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{1, \sigma, \dots, \sigma^{n-1}\}$, 其中 σ 为 Frobenius 自同构, 则有一一对应 $\text{Sub}(G) \leftrightarrow \text{Lat}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, $\langle \sigma^d \rangle \mapsto E_d = \{a \in \mathbb{F}_{p^n} : \sigma^d(a) = a\}$. 则借此可以画出 $\mathbb{F}_{p^{12}}$ 的 Hesse 图, 作为练习.

Example 4.13 考虑 $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. 则 $G = \text{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} S(A = \sqrt[3]{2}, B = \sqrt[3]{2}\omega, C = \sqrt[3]{2}\omega^2) = S_3$.

Galois 对应给出格同构 $\text{Sub}(G) \leftrightarrow \text{Lat}(K/\mathbb{Q})^{\text{op}}$, 则通过计算固定子域分别可以画出 $G = S_3$ 和 K 的 Hesse 图. 下面是一个计算固定子域的例子, 整体思路就是: 对于每个子群先找出在这个子群作用下的不变元, 再利用 $\dim_k K^H = [G : H]$ 得到 $\dim_k K^H$, 通过比较维数说明固定子域就是这些不变元生成的域.

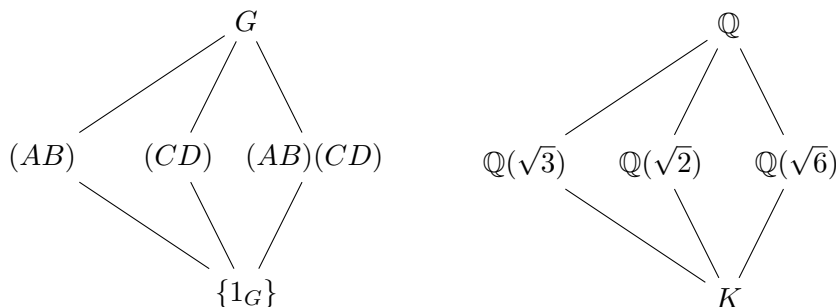
考虑 $H = \{\text{Id}, (ABC), (ACB)\}$, 则 $\dim_{\mathbb{Q}} K^H = [G : H] = 2$, 注意到 $\omega = \frac{B}{A} = \frac{C}{B} = \frac{A}{C}$ 在 (ABC) 和 (ACB) 下不变, 故 $\mathbb{Q}(\omega) \subseteq K^H$, 比较维数只能有 $K^H = \mathbb{Q}(\omega)$. 特别地, 由于 $(ABC) \triangleleft G$, 则 $\mathbb{Q}(\omega)/\mathbb{Q}$ 是 Galois 扩张, 这实际上也是显然的, 因为 $\mathbb{Q}(\omega) = (\mathbb{Q}, x^2 + x + 1)$.

再考虑 (AB) 不是 G 的自由子群, 则它对应的固定子域扩张 $\mathbb{Q}(\sqrt[3]{2}\omega^2)/\mathbb{Q}$ 不是 Galois 扩张.



Example 4.14 考虑 $K = (\mathbb{Q}, (x^2 - 2)(x^2 - 3)) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, 则 $\dim_{\mathbb{Q}} K = 4$, 且有 Galois 群的嵌入 $G = \text{Gal}(K/\mathbb{Q}) \hookrightarrow S(\sqrt{2} = A, -\sqrt{2} = B, \sqrt{3} = C, -\sqrt{3} = D) = S_4$, 由于为 Galois 扩张, 则 $|G| = \dim_k K = 4$, 进而 $G = K_4 = \{\text{Id}, (AB), (CD), (AB)(CD)\}$.

仍然可以通过找固定子域的方式画出 G 和 K 的 Hesse 图.



特别地 K 的非平凡子域只有 $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ 和 $\mathbb{Q}(\sqrt{6})$ 三个. 取 $u = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, 其中 a, b, c 至少有两个非 0, 则 u 不属于任意一个中间域, $K = \mathbb{Q}(u)$.

下面再看几个抽象的应用.

Theorem 4.5 (Steinitz)

设 K/k 为有限维扩张, 则 K/k 为单扩张 $\iff K/k$ 只有有限个中间域.



证明 \Rightarrow : 设 $K = k(\alpha)$, 则任取中间域 $k \subseteq E \subseteq K$, 设 α 在 E 上的最小多项式 $g(x) \in E[x] \subseteq K[x]$. 并取 α 在 k 上的最小多项式 $f(x) \in k[x]$, 有 $g(x) \mid f(x)$. 故 $g(x)$ 只有有限多个.

记 $g(x) = x^m + c_1x^{m-1} + \cdots + c_m, c_i \in E$, 则令 $B = k(c_1, \dots, c_m)$, 有 $g(x) \in B[x], B \subseteq E$. 此时有 $K = k(\alpha) = E(\alpha) = B(\alpha)$. 又由于 $[K : E] = m = [K : B]$, 则 $E = B$. 又 $g(x)$ 只有有限多个, 则对应的系数只有有限多种, 即 $E = B$ 只有有限多个.

\Leftarrow : 当 k 是有限域的时候有限维扩张 K/k 始终为单扩张, 则无需证明. 故设 k 是无限域. 设 $K = k(\alpha_1, \dots, \alpha_t)$, 则对 $\forall t \in k$, 有 $k \subseteq E_t = k(\alpha_1 + t\alpha_2) \subseteq k(\alpha_1, \alpha_2) \subseteq K$.

由于中间域只有有限个, 则存在 $t_1 \neq t_2 \in k$ 使得 $E_{t_1} = E_{t_2} = E$, 即 $\alpha_1 + t_1\alpha_2, \alpha_1 + t_2\alpha_2 \in D$, 进而 $\alpha_1, \alpha_2 \in E$. 故 $E = k(\alpha_1, \alpha_2) = k(\alpha_1 + t_1\alpha_2)$. 则用新的 E 代替 k , $K = E(\alpha_1 + t_1\alpha_2, \alpha_3, \dots, \alpha_t)$. 反复运用同样的论证可知 K/k 为单扩张. \square

Theorem 4.6 (Galois 本原元定理)

设 K/k 为有限维可分扩张, 则为单扩张. 这里可分扩张指任意 $\alpha \in K$, α 在 k 上的最小多项式可分.

证明 设 $K = k(\alpha_1, \dots, \alpha_r)$, 其中 α_i 在 k 上的最小多项式为 $g_i[x] \in k[x]$. 令 $g(x) = g_1(x) \cdots g_r(x) \in k[x] \subseteq K[x]$ 可分, 则 $k \subseteq K \subseteq (K, g(x)) = (k, g(x)) = E$.

则 E/k 是 Galois 扩张且由 Galois 对应, 只有有限个中间域, 则由 Steinitz 定理, E/k 是单扩张, 则 K/k 是单的. \square

最后来证明知名的代数基本定理.

Theorem 4.7 (代数基本定理)

\mathbb{C} 是代数封闭的.

证明 (1) 若 $\mathbb{R} \subsetneq K$, 则取 $\alpha \in K$, 在 \mathbb{R} 上最小多项式 $f(x)$, 则由维数公式 $\deg f = \dim_{\mathbb{R}} \mathbb{R}(\alpha) \mid \dim_{\mathbb{R}} K$. 又熟知奇数次实多项式有实根, 只能 $\deg f$ 为偶数, 则 $\dim_{\mathbb{R}} K$ 为偶数.

(2) 若 $\mathbb{C} \subsetneq K$, 则 $\dim_{\mathbb{C}} K \neq 2$. 否则设 $K = \mathbb{C}(\alpha)$, 有 α 在 \mathbb{C} 上的最小多项式为 $x^2 + ax + b \in \mathbb{C}[x]$, 但不难验证这在 \mathbb{C} 上是可约的, 矛盾!

(3) 现在取 $h(x) \in \mathbb{C}[x]$ 不可约, 有 $\deg f(x) \geq 2$, 此时有 $\mathbb{R} \subseteq \mathbb{C} \subsetneq K = (\mathbb{C}, f(x)) = (\mathbb{R}, (x^2+1)f(x))$. 则 K/\mathbb{R} 为有限 Galois 扩张, 取 $G = \text{Gal}(K/\mathbb{R})$.

若 $|G| = 2^r m, 2 \nmid m$, 则取 Sylow 2-子群 P , 有 $[G : P]$ 为奇数, 进而 $\dim_{\mathbb{R}} K^P = [G : P]$ 为奇数, 由 (1) 只能 $m = 1$, 故 $|G| = 2^r, \dim_{\mathbb{C}} K = 2^{r-1}$.

再考虑 $G' = \text{Gal}(K/\mathbb{C}) \hookrightarrow G$, 有 $|G'| = 2^{r-1}$, 取 $H \leq G'$ 使得 $[G' : H] = 2$ (证明见后), 则有 $\dim_{\mathbb{C}} K^H = [G' : H] = 2$, 与 (2) 矛盾! \square

需要补充中间用到的一个引理.

Lemma 4.3

任意 p -群 U , 存在 $V \leq U$ 使得 $[V : U] = p$.

证明 设 $|G| = p^n$. 对 n 归纳, $n = 1$ 时显然, 若对 $1 \leq m < n$ 均成立, 则考虑 n 时的情形.

我们知道 $Z(G)$ 是非平凡的, 则 $|G/Z(G)| = p^m (0 \leq m < n)$. 若 $m < 0$, 则由归纳假设和商群的子群的对应存在 $G/Z(G)$ 的指数为 p 的子群 $N/Z(G)$, 故 N 为所求.

若 $m = 0$, 此时 $G = Z(G)$ 为 Abel 群, 故 $G = \mathbb{Z}_{p^{s_1}} \times \cdots \times \mathbb{Z}_{p^{s_t}}$, 其中 $s_i \geq 1$. 则取 $N = \mathbb{Z}_{p^{s_1-1}} \times \mathbb{Z}_{p^{s_2}} \times \cdots \times \mathbb{Z}_{p^{s_t}}$ 为所求. \square

4.4 Galois 大定理

Definition 4.3

域扩张 E/k 称为 *type- m 的根式扩张*, 若 $E = k(\alpha)$ 且 $\alpha^m = a \in k$.

若 $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$ 满足 E_i/E_{i-1} 均为根式扩张, 则称为根式扩张塔.



Example 4.15 若 E/k 为 type- m 的根式扩张, 且 k 包含 m 次本原单位根 ω , 则若 $E = k(\alpha), \alpha^m = a \in k$, 有 $x^m - a = (x - \alpha)(x - \omega\alpha) \cdots (x - \omega^{n-1}\alpha)$, 则 $E = (k, x^m - a)$, 为有限 Galois 扩张, 进而有嵌入 $\text{Gal}(E/k) \hookrightarrow (\mathbb{Z}_m, +), \sigma \mapsto \bar{i}$, 其中 $\sigma(\alpha) = \omega^i \alpha$, 则 $\text{Gal}(E/k)$ 是 Abel 群.

Example 4.16 仍然设 E/k 为 type- m 的根式扩张且设 E/k 是 Galois 扩张, 若 $\text{char } k = 0$, 则考虑 $E' = (E, x^m - 1)$ 和 $k' = (k, x^m - 1) = k(\omega)$, 由上面的例子有 Abel 群嵌入 $\text{Gal}(E'/k') \hookrightarrow (\mathbb{Z}_m, +)$, 且有另一组 Abel 群的嵌入 $\text{Gal}(k'/k) \hookrightarrow (\mathbb{Z}_m, +)$. 则考虑

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Gal}(E'/k') & \xrightarrow{\sigma} & \text{Gal}(E'/k) & \longrightarrow & \text{Gal}(k'/k) \longrightarrow 0 \\ & & & & \downarrow & & \\ & & & & \text{Gal}(E/k) & & \end{array}$$

Definition 4.4

$f(x) \in k[x]$ 称为 **根式可解**, 若存在根式扩张塔 $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$, 使得 $f(x)$ 在 E_n 中分裂.



Example 4.17 设 $f(x) = x^2 + bx + c \in \mathbb{C}[x]$, 则 $k = \mathbb{Q}(b, c) \subseteq \mathbb{C}$, $E = (k, f(x)) = k(r_1, r_2)$, 则有根式扩张塔 $k = E_0 \subseteq E = k(r_1, r_2) \subseteq E_1 = k(\alpha)$. 其中 r_1, r_2 为 $f(x)$ 的两个根, α 满足 $\alpha^2 = b^2 - 4c$.

此外我们有如下定义

Definition 4.5

(1) $f(x) \in k[x]$ 的 Galois 群为 $\text{Gal}_k(f) = \text{Gal}((k, f(x))/k)$.

(2) 有限群 G 称为 **可解群**, 若存在子群链 $G = G_0 \supseteq G_1 \cdots G_n = \{1\}$, 满足 $G_{i+1} \triangleleft G_i$ 且 G_i/G_{i+1} 为 Abel 群, 每个相邻子群的商也称为 **因子**.



Example 4.18 若有正合列 $0 \rightarrow G_1 \rightarrow G \rightarrow G/G_1 \rightarrow 0$ 且 $G_1, G/G_1$ 为 Abel 群, 则 G 可解. 特别地, S_3 可解: $0 \rightarrow A_3 \hookrightarrow S_3 \rightarrow C_2 \rightarrow 0$.

Example 4.19 若有 $0 \rightarrow G_2 \rightarrow G_1 \rightarrow G_1/G_2 \rightarrow 0$ 且 $G_1, G_1/G_2$ 为 Abel 群, 则 G_1 可解, 此时若还有 $0 \rightarrow G_1 \rightarrow G \rightarrow G/G_1 \rightarrow 0$ 且 G/G_1 为 Abel 群, 则 G 可解.

Example 4.20 Abel 群显然可解.

Example 4.21 p -群可解: $0 \rightarrow Z(G) \rightarrow G \rightarrow G/Z(G) \rightarrow 0$.

Example 4.22 (1) G 可解, 则 $H \leq G$ 也可解

(2) $N \triangleleft G$, 则 G 可解 $\iff N$ 和 G/N 都可解.

Example 4.23 $S_n (n \geq 5)$ 不可解, 进而 $A_5 \triangleleft S_5$ 不可解.

则可以讨论 Galois 大定理:

Theorem 4.8 (Galois 大定理)

$\text{char} k = 0, f(x) \in k[x]$, 则 $f(x)$ 根式可解 $\iff \text{Gal}_k(f)$ 可解.



证明 \Rightarrow : 若 $f(x) \in k[x]$ 根式可解, 则存在 $k \subseteq K = (k, f(x)) \subseteq E$ 使得 E/k 为根式扩张塔, 且 E/k 为有限 Galois 扩张. 又由于 K 为可分多项式 $f(x)$ 分裂域有 K/k 为有限 Galois 扩张. 则有

$$\text{Gal}(E/K) \xrightarrow{\triangleleft} \text{Gal}(E/k) \twoheadrightarrow \text{Gal}_k(f)$$

则只需证 $\text{Gal}(E/k)$ 可解.

考虑根式扩张塔 $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E$, 其中 E_i/E_{i-1} 为 $\text{type-}m_i$ 的根式扩张.

(i) 若 k 有充分多的单位根, 由上面的例 4.15, 不断使用 Galois 对应, 有 $\forall i, E_i/E_{i-1}$ 是 Galois 扩张, 且 $\text{Gal}(E_i/E_{i-1})$ 是 Abel 群: 考虑正规子群链 $\text{Gal}(E_m/E_0) \supseteq \text{Gal}(E_m/E_1) \supseteq \cdots$ 即可. 此时 $\text{Gal}(E_n/k)$ 可解.

(ii) 对一般的特征 0 的 k , 设 $E = k(\alpha_1, \cdots, \alpha_r)$, 取 α_i 的最小多项式 $f_i(x) \in k[x]$, 故 $g(x) = f_1(x) \cdots f_r(x)$ 可分, 定义 $K = (E, g(x)) = (k, g(x))$, 则 K/k 为 Galois 扩张, 设 $\text{Gal}(K/k) = \{1 = \sigma_0, \sigma_1, \cdots, \sigma_p\}$.

考虑 $k \cdots \subseteq E \subseteq E \vee \sigma_1(E) \subseteq E \vee \sigma_1(E) \vee \sigma_2(E) \cdots \subseteq E \vee \sigma_1(E) \cdots \vee \sigma_p(E) = E_m$. 这仍然是一个根式扩张塔, 并且 $\forall 1 \leq i \leq p$, 有 $\sigma_i(E_m) = E_m$ (自行验证!). 故 E_m/k 为 Galois 扩张.

现在转化为考察根式扩张塔 $k = E_0 \subseteq E_1 \cdots \subseteq E_m$ 使得 E_m/k 为 Galois 扩张, 取 M 为每一步根式扩张的 type 的最小公倍数, 令 $E'_m = (E_m, x^M - 1)$ 和 $k' = (k, x^M - 1)$, 则由 (i) 可知 $\text{Gal}(E'_m/k')$ 是可解群, 且也有 $\text{Gal}(k'/k)$ 是 Abel 群, 则可以考虑

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Gal}(E'_m/k') & \hookrightarrow & \text{Gal}(E'_m/k) & \longrightarrow & \text{Gal}(k'/k) \longrightarrow 0 \\ & & & & \downarrow & & \\ & & & & \text{Gal}(E_m/k) & & \\ & & & & \downarrow & & \\ & & & & \text{Gal}((k, f(x))/k) = \text{Gal}_k(f) & & \end{array}$$

则 $\text{Gal}(E'_m/k)$ 是可解群, 故 $\text{Gal}(E_m/k)$ 作为其商群为可解群, 进而 $\text{Gal}_k(f)$ 作为 $\text{Gal}(E_m/k)$ 的商群也可解.

\Leftarrow : 设 $K = (k, f(x))$ 且 $\text{Gal}(K/k) = G$ 可解.

(i) 若 k 中有 $|G|$ 次本原单位根. 首先由于 G 可解, 有正规子群链 $G \supseteq G_1 \cdots$, 则 $Z = G/G_1$ 是

Abel 群. 可以找到 (自行验证!) Z 的子群 Z' 使得指数 $[Z : Z'] = p$ 为素数. 则由商群的子群对应, 存在 $H \triangleleft G$ 使得 $G/H \simeq Z/Z' \simeq C_p$ 为阶 p 的循环群.

则此时 K^H/k 为有限 Galois 扩张, 且 $\text{Gal}(K^H/k) \simeq G/H \simeq C_p$. 由条件 k 中包含 p 次单位根 ω . 取 $c \in K^H - k$ 使得 $K^H = k(c)$, 并记 $c_i = \sigma^{i-1}(c) (1 \leq i \leq p)$.

定义 $d_i = c_1 + c_2\omega^i + c_3\omega^{2i} + \cdots + c_p\omega^{(p-1)i} \in K^H$, 则

$$\sigma(d_i) = c_2 + c_3\omega^i + \cdots + c_1\omega^{(p-1)i} = \omega^{-i}d_i$$

进而 $\sigma(d_i^p) = d_i^p, d_i^p \in k$. 同时 d_1, \dots, d_p 由 c_1, \dots, c_p 乘上由 $1, \omega, \dots, \omega^{p-1}$ 组成的 Vandermonde 矩阵得到, 该行列式非零, 故 c_1, \dots, c_p 也是 d_1, \dots, d_p 的 k -线性组合, 由 $c \notin k$ 可知必然存在 $d_i \notin k$. 则 $K^H = k(d_i)$ 且 $d_i^p \in k$, 故 K^H/k 为 type p -的根式扩张.

记 $K^H = k_1$, 则有 $k \subseteq k_1 \subseteq K$, 其中 k_1/k 根式扩张, 且由于 $\text{Gal}(K/k_1)$ 为 $\text{Gal}(K/k)$ 的子群故也可解, 则通过和上面一样的论证存在 $k_1 \subseteq k_2 \subseteq K$, 且 k_2/k_1 为根式扩张.

反复进行同样的论证, 则有根式扩张塔 $k = k_0 \subseteq k_1 \subseteq k_2 \cdots \subseteq k_m = K$, 有 $f(x)$ 根式可解.

(ii) 一般情况下, 考虑 $k \subseteq K \subseteq K' = K(\omega), k' = k(\omega)$, 其中 ω 为 $|G|$ 次本原单位根. 则 $k \subseteq k'$ 为根式扩张, 由于 $K \subseteq K'$, 故 $f(x)$ 在 K' 中分裂, 故只需证 $k' \subseteq K'$ 存在根式扩张塔. 由 (i) 只需证明 $\text{Gal}(K'/k')$ 也可解. 事实上有如下的

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Gal}(K'/K) & \hookrightarrow & \text{Gal}(K'/k) & \twoheadrightarrow & \text{Gal}(K/k) = G \longrightarrow 0 \\ & & & & \uparrow & \nearrow & \\ & & & & \text{Gal}(K'/k') & & \end{array}$$

其中利用 Galois 对应, 有 $\text{Gal}(K'/K) \cap \text{Gal}(K'/k') = \text{Gal}(K'/K \vee k') = \text{Gal}(K'/K') = \text{Id}_{K'}$, 故确实有嵌入 $\text{Gal}(K'/k') \hookrightarrow G$, 由 G 可解有 $\text{Gal}(K'/k') \hookrightarrow G$ 可解, 则得证. \square

最后来给出应用 Galois 大定理的例子, 其中包含了著名的高次 (≥ 5 次) 一般方程根式不可解.

Example 4.24 对 $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ 不可约, 不难验证 $\text{Root}_{\mathbb{C}}(f) = \{\alpha_1, \dots, \alpha_5\}$, 其中 α_1, α_2 为共轭复根, $\alpha_3, \alpha_4, \alpha_5$ 为实根.

考虑分裂域 $K = \mathbb{Q}(\alpha_1, \dots, \alpha_5) \subseteq \mathbb{C}$, 则有 $G = \text{Gal}_{\mathbb{Q}}(f) \hookrightarrow S_5 = S(\alpha_1, \dots, \alpha_5)$.

首先有 $\dim_{\mathbb{Q}} \mathbb{Q}(r_1) = 5$, 则 $5 \mid \dim_{\mathbb{Q}} E = |\text{Gal}_{\mathbb{Q}}(f)|$, 进而 G 中有五阶元, 即存在某个 5-轮换 σ .

其次 $\sigma : K \rightarrow K, z \mapsto \bar{z} \in G$, 且对应 $(12) \in S_5$, 故 $(12) \in G$.

事实上, 任意一个 5-轮换 σ 和 (12) 能生成 S_5 (自行验证!), 则只能 $G \simeq S_5$, 不可解! 进而 $f(x)$ 不根式可解, $\mathbb{Q} \subseteq K$ 不能嵌入到根式扩张塔中.

Example 4.25 考虑 n 元有理函数域 $F = k(t_1, t_2, \dots, t_n)$, 其一般方程为 $f(x) = x^n - t_1x^{n-1} + t_2x^{n-2} +$

$\cdots + (-1)^n t_n \in F[x]$, 则引入 n 个变元 y_1, \cdots, y_n , 并记 p_1, \cdots, p_n 为 y_1, \cdots, y_n 为对应的对称多项式, 则考虑环同态: $\sigma : k[t_1, \cdots, t_n] \rightarrow k[p_1, \cdots, p_n], t_i \mapsto p_i$, 它显然是一个满同态.

设 $f(x)$ 在 F 上的分裂域为 $E = F(x_1, \cdots, x_n)$, 则考虑环同态 $\tau : k[y_1, \cdots, y_n] \rightarrow k[x_1, \cdots, x_n], y_i \mapsto x_i$. 此时有 $\tau(\sigma(t_i)) = \tau(\sum y_{j_1} \cdots y_{j_i}) = \sum x_{j_1} \cdots x_{j_i} = t_i$, 即 $\tau\sigma = 1$, 进而 σ 也是单同态, 则为环同构.

进而可以扩张成商域的同构, 仍然记为 $\sigma : F = k(t_1, \cdots, t_n) \xrightarrow{\sim} k(p_1, \cdots, p_n)$. 设 $\sigma(f(x)) = g(x)$, 则 $k(y_1, \cdots, y_n)$ 为 $g(x)$ 在 $k(p_1, \cdots, p_n)$ 上的分裂域, $k(x_1, \cdots, x_n)$ 为 F 上的分裂域, 进而有分裂域同构 $\sigma : k(x_1, \cdots, x_n) \rightarrow k(y_1, \cdots, y_n)$, 且 $\sigma(F) = k(p_1, \cdots, p_n)$.

有 Galois 群同构 $\text{Gal}_F(f) = \text{Gal}(k(x_1, \cdots, x_n)/k(t_1, \cdots, t_n)) \simeq \text{Gal}(k(y_1, \cdots, y_n)/k(p_1, \cdots, p_n)) \simeq S_n$.

于是若 $\text{char } k = 0$ 且 $n \geq 5$ 时, 一般方程 $f(x) = 0$ 根式不可解.

附录 A 2024 春近世代数 (H) 期末

由本人考后回忆, 可能与原题有小偏差.

一、设 E/\mathbb{Q} 为 $x^4 - 18 \in \mathbb{Q}[x]$ 的分裂域.

- (1) 计算 $\dim_{\mathbb{Q}} E$.
- (2) 判断 $x^4 - 18$ 在 $\mathbb{Q}(i)[x]$ 上是否可约.
- (3) 计算 $\dim_{\mathbb{Q}}(E \cap \mathbb{Q}(\sqrt{2} + \sqrt{3}))$.
- (4) 写出 $\text{Gal}(E/\mathbb{Q})$ 在 $S(\text{Root}(x^4 - 18))$ 中的像.
- (5) 写出 E 的所有子域.

二、令 $L_n = \mathbb{C}(x^n + x^{-n})$.

- (1) 计算 $\dim_{L_n} \mathbb{C}(x)$.
- (2) 判断: 是否有 $L_n \subseteq L_m \iff m|n$?
- (3) 写出 $\mathbb{C}(x)/L_4$ 的所有中间域.

三、设 G 为有限群, $H \leq G$ 为真子群, 则 $G \neq \cup_{g \in G} Hg^{-1}$, 并在 G 是无穷群时给出反例.

四、对秩为 2 的有限生成 Abel 群 A 以及满同态 $\theta: A \twoheadrightarrow \mathbb{Z} \oplus \mathbb{Z}$, 证明 $\ker(\theta) = t(A)$. 这里 $t(A)$ 指 A 的扭子群.