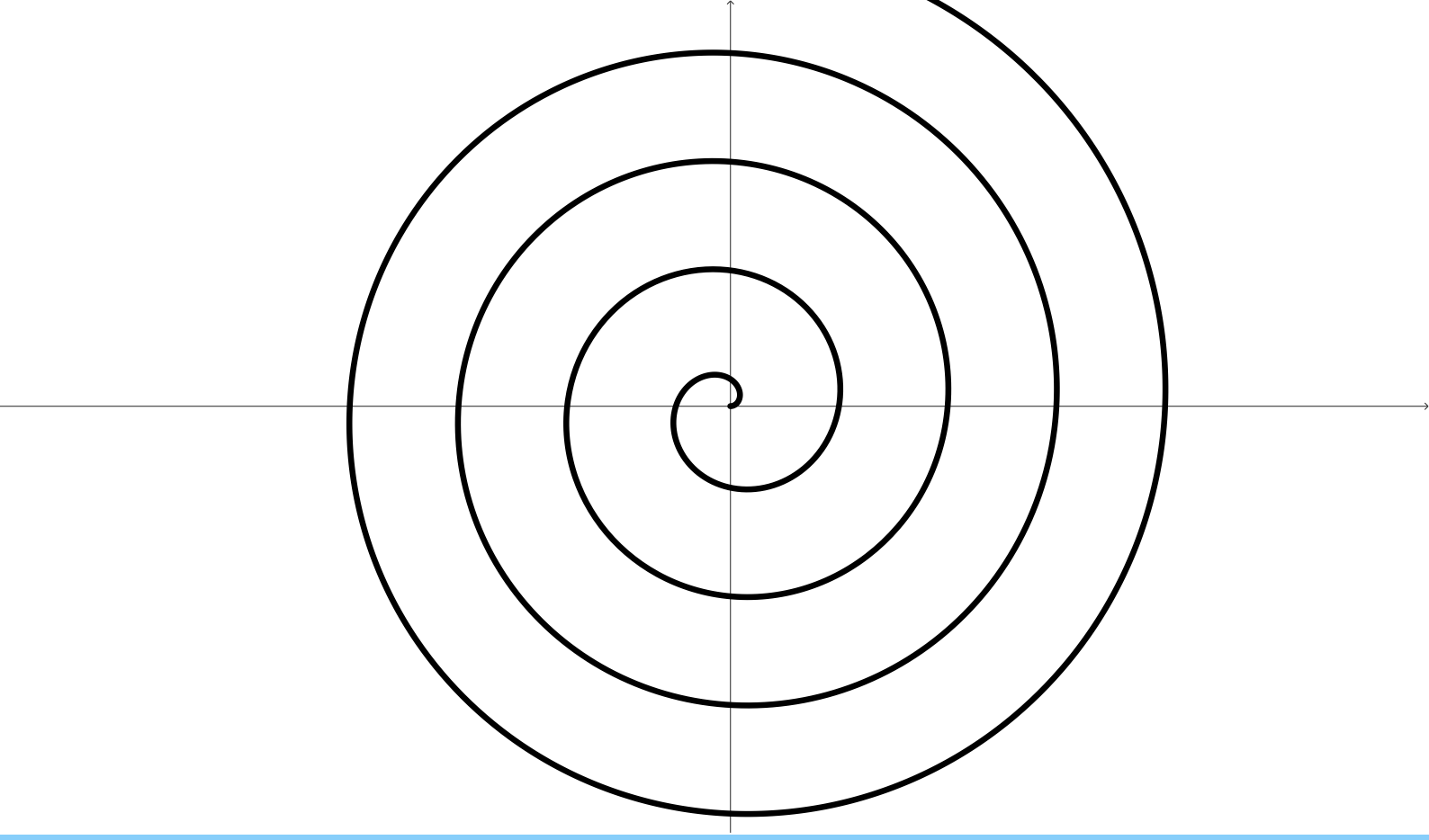

抽象代数基础 - 丘维声 - 笔记

作者：若水
邮箱：ethanmxzhou@163.com
主页：helloethanzhou.github.io
时间：July 18, 2024

目录

第一章 群

1.1 群的定义

定义 1.1.1 (群)

称 $(G,*)$ 为群，如果二元运算 $*:G\times G\to G$ 满足如下运算法则。

1. 单位元：存在 $e\in G$，使得对于任意 $a\in G$，成立 $ea=ae=a$。
2. 逆元：对于任意 $a\in G$，存在 $b\in G$，使得成立 $ab=ba=e$。
3. 结合律：$(ab)c=a(bc)$

定义 1.1.2 (Abel 群)

称满足交换律 $ab=ba$ 的群为 Abel 群。

定义 1.1.3 (群的阶)

群的阶 $|G|$ 表示 G 中元素的个数。

命题 1.1.1 (群的性质)

1. 单位元存在且存在唯一。
2. 逆元存在且存在唯一。
3. 不同元素的逆元不同。
4. 左右消去律成立。

1.2 群的例子

定义 1.2.1 (数域群)

$$(\mathbb{Z},+),\quad (\mathbb{Z}\setminus\{0\},\times),\quad (\mathbb{R},+),\quad (\mathbb{R}\setminus\{0\},\times),\quad (\mathbb{R}^+,\times)$$

定义 1.2.2 (n 次单位根乘法群)

$$U_n=\{\omega:\omega^n=1\}=\{\omega^k:0\le k<n,k\in\mathbb{N}\}=\langle\omega\rangle$$

定义 1.2.3 (模 p 剩余类加法群)

$$\mathbb{Z}_p=\{\overline{n}:0\le n<p,n\in\mathbb{N}\}=\langle\overline{1}\rangle$$

定义 1.2.4 ($\mathbb{Z}_p$ 的单位乘法群)

$$\mathbb{Z}_p^*=\{\overline{n}:\exists m,\overline{mn}=\overline{1}\}=\{\overline{n}:(n,p)=1\}$$

定义 1.2.5 (二面体群)

对于正 n 边形，令 σ 表示绕中心旋转 $\frac{2\pi}{n}$，τ 表示关于某条对称轴的反射，那么正 n 边形的对称群为

$$D_n = \langle \sigma, \tau : \sigma^n = \tau^2 = \sigma\tau\sigma\tau = \mathbb{1} \rangle = \{\sigma^i\tau^j : \sigma^n = \tau^2 = \sigma\tau\sigma\tau = \mathbb{1}, 0 \le i < n, j \in \{0,1\}\}$$

♣

定义 1.2.6 (矩阵群)

$$\begin{aligned}
&\mathrm{GL}_n(\mathbb{R}) = \{\text{可逆} n \text{ 阶实矩阵}\} \\
&\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : \det(M) = 1\} \\
&\mathrm{O}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : MM^t = M^tM = I_n\} \\
&\mathrm{SO}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : \det(M) = 1, MM^t = M^tM = I_n\}
\end{aligned}$$

$$\begin{aligned}
&\mathrm{GL}_n(\mathbb{C}) = \{\text{可逆} n \text{ 阶复矩阵}\} \\
&\mathrm{SL}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : \det(M) = 1\} \\
&\mathrm{U}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : MM^\dagger = M^\dagger M = I_n\} \\
&\mathrm{SU}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : \det(M) = 1, MM^\dagger = M^\dagger M = I_n\}
\end{aligned}$$

♣

1.3 对称群

定义 1.3.1 (全变换群)

对于非空集合 Ω，定义 Ω 的全变换群为

$$S_\Omega = (\mathscr{F}, \circ), \qquad \mathscr{F} = \{\sigma : \Omega \to \Omega \text{为双射}\}$$

♣

定义 1.3.2 (对称群)

对于 n 个元素的集合 Ω，定义 Ω 的 n 元对称群为

$$S_n = (\mathscr{F}, \circ), \qquad \mathscr{F} = \{\sigma : \Omega \to \Omega \text{为双射}\}$$

♣

定义 1.3.3 (置换群)

称 n 元对称群 S_n 的子群为 n 元置换群。

♣

定义 1.3.4 (变换群)

称全变换群 S_Ω 的子群为变换群。

♣

定义 1.3.5 (置换)

对于 n 个元素的集合 Ω，称 Ω 的一个置换为双射 $f : \Omega \to \Omega$。

♣

定义 1.3.6 (r-轮换)

定义 n 元置换 σ 关于元素 $i_1, \cdots, i_r$ 的 r-轮换为

$$(i_1 \cdots i_r) = i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_r \mapsto i_1$$

♣

定义 1.3.7 (对换)

定义 2-轮换为对换。

定理 1.3.1 (轮换的逆)

$$(i_1 \cdots i_r)^{-1} = (i_1 i_r i_{r-1} \cdots i_2)$$

定理 1.3.2 (轮换的分解)

任意一个非单位元的置换都存在且存在唯一的两两不相交的轮换积，其中唯一性是建立在轮换次序意义上。

$$(i_1 \cdots i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_2)$$

定义 1.3.8 (不交轮换)

称轮换 $(i_1 \cdots i_r)$ 和 $(j_1 \cdots j_s)$ 是不相交的，如果对于任意 k 和 l，成立 $i_k \neq j_l$。

定义 1.3.9 (奇置换)

如果置换可表示为奇数个对换的乘积，那么称该置换为奇置换。

定义 1.3.10 (偶置换)

如果置换可表示为偶数个对换的乘积，那么称该置换为偶置换。

命题 1.3.1 (置换的奇偶性的性质)

1. 置换具有且仅具有一种奇偶性。
2. 奇奇得偶，偶偶得偶，奇偶得奇。
3. 置换与其逆置换具有相同奇偶性。
4. 奇偶置换数相同。
5. r-轮换的奇偶性与 r 的奇偶性相反。

定义 1.3.11 (交错群)

$$A_n = \{\sigma \in S_n \text{ 为偶置换}\}$$

1.4 子群

定义 1.4.1 (子群)

称非空集合 $(H, *)$ 为群 $(G, *)$ 的子群，记作 $H < G$，如果满足如下其中一个命题。

1. $H \subset G$，且 $(H, *)$ 构成群。
2. $H \subset G$，且对于任意 $a, b \in H$，成立 $ab \in H$ 且 $b^{-1} \in H$。
3. $H \subset G$，且对于任意 $a, b \in H$，成立 $ab^{-1} \in H$。

定义 1.4.2 (生成群)

对于群 $(G,*)$ 的非空子集 $S\subset G$，定义由 S 生成的生成群为

$$\langle S\rangle=\bigcap_{S\subset H<G}H=\{a_1^{m_1}*\cdots*a_n^{m_n}:a_k\in S,m_k\in\mathbb{Z}\}$$

定义 1.4.3 (生成元集)

称 $S\subset G$ 为群 G 的生成元集，如果 $\langle S\rangle=G$。

定义 1.4.4 (有限生成群)

称 G 为有限生成群，如果存在有限集 $S\subset G$，使得成立如果 $\langle S\rangle=G$。

定义 1.4.5 (循环群)

称群 $(G,*)$ 为循环群，如果存在 $a\in G$，使得成立 $G=\langle a\rangle$。

定义 1.4.6 (群元素的阶)

对于群 $(G,*)$，定义元素 $a\in G$ 的阶为

$$|a|=\begin{cases}\min\{n\in\mathbb{N}^*:a^n=e\}, & \exists n\in\mathbb{N}^*,a^n=e\\ \infty, & \forall n\in\mathbb{N}^*,a^n\neq e\end{cases}$$

命题 1.4.1 (群元素阶的性质)

1. 如果 $|a|=n$，那么
$$\langle a^p\rangle<\langle a\rangle\iff p\mid n$$
2. 如果 $|a|=n$，那么
$$a^m=e\iff n\mid m$$
3. 如果 $|a|=n$，那么对于任意 $m\in\mathbb{N}^*$，成立 $|a^m|=\dfrac{n}{(m,n)}$。
4. 如果 $|a|=m,|b|=n$，且 $ab=ba$，同时 $(m,n)=1$，那么 $|ab|=mn$。

1.5 陪集

定义 1.5.1 (左陪集)

对于群 $(G,*)$，定义子群 $H\subset G$ 关于元素 $a\in G$ 的左陪集为

$$aH=\{a*h:h\in H\}$$

定理 1.5.1 (左陪集的等价关系)

对于群 $(G,*)$ 的子群 $H\subset G$，定义等价关系

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

那么

$$aH=\overline{a}$$

定义 1.5.2 (左商集)

定义群 G 关于子群 $H \subset G$ 的左商集为

$$(G/H)_l = \{aH : a \in G\}$$

♣

定义 1.5.3 (右陪集)

对于群 $(G, *)$，定义子群 $H \subset G$ 关于元素 $a \in G$ 的右陪集为

$$Ha = \{h * a : h \in H\}$$

♣

定理 1.5.2 (右陪集的等价关系)

对于群 $(G, *)$ 的子群 $H \subset G$，定义等价关系

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

那么

$$Ha = \overline{a}$$

♡

定义 1.5.4 (右商集)

定义群 G 关于子群 $H \subset G$ 的右商集为

$$(G/H)_r = \{Ha : a \in G\}$$

♣

定理 1.5.3 (左右商集的同构)

对于群 G 以及其子群 $H \subset G$，存在群同构映射

$$f : (G/H)_l \longrightarrow (G/H)_r$$
$$aH \longmapsto Ha^{-1}$$

♡

定义 1.5.5 (子群的指数)

群 G 关于其子群 $H \subset G$ 的左/右商集的基数称为 H 在 G 中的指数，记作 $[G : H]$。

♣

定义 1.5.6 (左陪集分解式)

对于群 G 以及其子群 $H \subset G$，如果 $[G : H] = r$，那么存在左陪集代表系 $\{a_1, \cdots, a_r\}$，使得成立群 G 关于子群 H 的左陪集分解式

$$G = \bigsqcup_{k=1}^{r} a_k H$$

♣

定理 1.5.4 (Lagrange 定理)

对于有限群群 G 以及其子群 $H \subset G$，成立

$$|G| = |H|[G : H]$$

♡

推论 1.5.1

对于有限群 G，以及任意 $a \in G$，成立 $|a| \mid |G|$。

♡

推论 1.5.2

素数阶群为循环群，且任意非单位元元素为其生成元。

定理 1.5.5 (Fermat 小定理)

对于素数 p，如果 $p \nmid a$，那么

$$a^{p-1} \equiv 1 \mod p$$

命题 1.5.1 (循环群的生成元结构)

对于 n 阶循环群 $\langle a \rangle$，成立

$$\langle a^p \rangle = \langle a \rangle \iff (p, n) = 1$$

命题 1.5.2 (循环群的子群结构)

1. 循环群的子群为循环群。
2. $\mathbb{Z}$ 的子群为 $\mathbb{Z}_n$，其中 $n \in \mathbb{N}^*$。
3. $$\mathbb{Z}_p < \mathbb{Z}_n \iff p \mid n$$
4. 如果 $p \mid n$，那么 $$|\mathbb{Z}_p| = \frac{n}{p}$$

引理 1.5.1

对于有限阶 Abel 群 G，存在 $g \in G$，使得对于任意 $a \in G$，成立 $|a| \mid |g|$。

定理 1.5.6 (有限 Abel 群为循环群的充要条件)

对于有限阶 Abel 群 G，G 为循环群，当且仅当对于任意 $n \in \mathbb{N}^*$，方程 $x^n = e$ 在 G 中的解的个数不多于 n。

定理 1.5.7 (Wilson 定理)

对于素数 p，成立

$$(p-1)! \equiv -1 \mod p$$

1.6 群的同构

定义 1.6.1 (同构映射)

对于群 $(G, *)$ 和 $(H, *)$，称映射 $\sigma : G \to H$ 为同构映射，如果 σ 为双射，且对于任意 $a, b \in G$，成立 $\sigma(ab) = \sigma(a)\sigma(b)$。

命题 1.6.1 (群同构映射的性质)

1. $\sigma(e_G) = e_H$
2. $\sigma(a^{-1}) = \sigma(a)^{-1}$
3. $|\sigma(a)| = |a|$

4. 如果 $K < G$，那么 $\sigma(K) < H$。

定义 1.6.2 (同构)

称群 $(G,*)$ 和 $(H,*)$ 是同构的，且记为 $G \cong H$，如果存在同构映射 $\sigma : G \to H$。

命题 1.6.2 (群同构的性质)

1. $|G| = |H|$
2. 如果 G 为循环群，那么 H 为循环群。
3. 如果 G 为交换群，那么 H 为交换群。

定理 1.6.1 (循环群的结构)

无限循环群与 $\mathbb{Z}$ 同构，n 阶循环群与 $\mathbb{Z}_n$ 同构。

1.7 群的直积

定义 1.7.1 (Klein 群)

$\mathbb{Z}_2 \times \mathbb{Z}_2$，4 阶非循环 Abel 群。

定义 1.7.2 (直积)

对于群 $(G,*)$ 和 $(H,*)$，定义其直积为

$$G \times H = \{(a,b) : a \in G, b \in H\}, \qquad (a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2)$$

命题 1.7.1 (群直积的性质)

1. 如果 $|G| = \infty$ 或 $H = \infty$，那么 $|G \times H| = \infty$。
2. 如果 $|G| < \infty$ 且 $|H| < \infty$，那么 $|G \times H| = |G||H|$。
3. 如果 G 和 H 为 Abel 群，那么 $G \times H$ 为 Abel 群。
4. $G \times H \cong H \times G$，其同构映射为 $(a,b) \mapsto (b,a)$。
5. $G \times \{e_H\} < G \times H$，且 $G \cong G \times \{e_H\}$，其同构映射为 $a \mapsto (a, e_H)$。
6. $\{e_G\} \times H < G \times H$，且 $H \cong \{e_G\} \times H$，其同构映射为 $b \mapsto (e_H, b)$。

定理 1.7.1 (循环群的直积)

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff (m,n) = 1$$

定义 1.7.3 (内直积)

对于群 $(G,*)$，称 G 为子群 $H, K < G$ 的内直积，且记作 $G = H \times K$，如果 $G \cong H \times K$，其同构映射为 $h * k \mapsto (h,k)$。

定理 1.7.2 (内直积定理)

对于群 $(G,*)$，以及子群 $H, K < G$，如果 $G = HK$，且 $H \cap K = \{e\}$，同时对于任意 $a \in H, b \in K$，成立 $a * b = b * a$，那么 $G \cong H \times K$。

1.8 群同态

定义 1.8.1 (同态映射)

对于群 $(G,*)$ 和 $(H,*)$，称映射 $\sigma: G \to H$ 为群同态映射，如果对于任意 $a,b \in G$，成立 $\sigma(ab) = \sigma(a)\sigma(b)$。♣

定义 1.8.2 (自同态映射)

群 G 的自同态映射为同态映射 $\sigma: G \to G$。群 G 的自同态映射构成群 $\mathrm{Aut}(G)$。♣

定义 1.8.3 (内自同态映射)

群 $(G,*)$ 的内自同态映射为自同态映射 $\gamma_a(x) = a * x * a^{-1}$。群 G 的内自同态映射构成群 $\mathrm{Inn}(G)$。♣

1.9 正规子群

定义 1.9.1 (正规子群)

称群 $(G,*)$ 的子群 $(N,*)$ 为正规子群，并记做 $N \triangleleft G$，如果满足如下命题之一。

1. 对于任意 $g \in G$，以及 $n \in N$，成立 $g * n * g^{-1} \in N$。
2. 对于任意 $g \in G$，成立 $g * N = N * g$。
3. 对于任意 $g \in G$，成立 $g * N \subset N * g$。
4. 对于任意 $g \in G$，成立 $N * g \subset g * N$。
5. 对于任意 $g \in G$，成立 $g * N * g^{-1} = N$。
6. 对于任意 $g \in G$，成立 $g * N * g^{-1} \subset N$。
7. 对于任意 $g \in G$，成立 $N \subset g * N * g^{-1}$。

♣

命题 1.9.1 (正规子群的性质)

1. 对于群同态映射 $\sigma: G \to H$，成立 $\mathrm{Ker}\,\sigma \triangleleft G$。
2. Abel 群的子群为正规子群。
3. 对于群 G 的子群 N，如果 $[G:N] = 2$，那么 $N \triangleleft G$。

♠

1.10 商群

定义 1.10.1 (商群)

定义群 $(G,*)$ 关于正规子群 $(N,*)$ 的商群为 $G/N = \{a * N : a \in G\}$。♣

定理 1.10.1 (群同构定理)

对于群同态映射 $\sigma: G \to H$，成立

$$G/\mathrm{Ker}\,\sigma \cong \mathrm{Im}\,\sigma$$

♡

定理 1.10.2 (第一同构定理)

$$H < G,\quad N \triangleleft G \implies HN < G,\quad (H \cap N) \triangleleft H,\quad \frac{H}{H \cap N} \cong \frac{HN}{N}$$

♡

定理 1.10.3 (第二同构定理)

$$N \subset H, \quad N, H \triangleleft G \implies \frac{H}{N} \triangleleft \frac{G}{N}, \quad \frac{G/N}{H/N} \cong \frac{G}{H}$$

♡

1.11 单群与换位子群

定义 1.11.1 (单群)

称仅存在平凡正规子群的群为单群。

♣

命题 1.11.1

Abel 群 G 为单群 $\iff$ G 为素数阶群。

♠

定义 1.11.2 (换位子群/导群)

对于群 $(G,*)$，定义其换位子群为

$$[G,G] = \langle g * h * g^{-1} * h^{-1} : g, h \in G \rangle$$

♣

命题 1.11.2 (换位子群的性质)

1. 群 G 为 Abel 群 $\iff$ $[G,G] = \{e\}$
2. 对于群 G，成立 $[G,G] \triangleleft G$，且 $G/[G,G]$ 为 Abel 群。
3. 对于群同态映射 $\varphi : G \to H$，成立

$$\operatorname{im}\varphi \text{ 为 Abel 群} \iff [G,G] \subset \ker\varphi$$

4. 如果 N 为群 G 的正规子群，那么

$$\frac{G}{N} \text{ 为 Abel 群} \iff [G,G] \subset N$$

♠

定义 1.11.3 (导群列)

对于群 $(G,*)$，定义 $G^{(1)} = [G,G]$，$G^{(n+1)} = [G^{(n)}, G^{(n)}]$，可得递减正规子群列 $\cdots \triangleleft G^{(2)} \triangleleft G^{(1)} \triangleleft G$。

♣

定义 1.11.4 (可解群)

称群 $(G,*)$ 为可解群，如果存在 $n \in \mathbb{N}^*$，使得成立 $G^{(n)} = \{e\}$。

♣

命题 1.11.3

非 Able 群可解群不为单群。

♠

1.12 群作用

定义 1.12.1 (作用)

称集合函数 $\circ : G \times \Omega \to \Omega$ 为群 $(G, *)$ 关于集合 Ω 的作用，如果成立

$$e \circ x = x, \qquad (a * b) \circ x = a \circ (b \circ x)$$

♣

定理 1.12.1 (作用的本质)

1. 如果 $\circ : G \times \Omega \to \Omega$ 为群 $(G, *)$ 关于集合 Ω 的作用，那么可定义群同态映射 $\Psi : G \to S_\Omega, \quad a \mapsto \psi_a$，其中集合函数 $\psi_a : \Omega \to \Omega, \quad x \mapsto a \circ x$。
2. 如果 $\Psi : G \to S_\Omega, \quad a \mapsto \psi_a$ 为群同态映射，那么可定义群 $(G, *)$ 关于集合 Ω 的作用 $\circ : G \times \Omega \to \Omega, \quad (a, x) \mapsto \psi_a(x)$。

♡

定义 1.12.2 (作用的核)

定义群 $(G, *)$ 关于集合 Ω 的作用 $\circ : G \times \Omega \to \Omega$ 的核 $\ker \circ$ 为群同态映射 $\Psi : G \to S_\Omega, \quad a \mapsto \psi_a$ 的核 $\ker \Psi$，其中集合函数 $\psi_a : \Omega \to \Omega, \quad x \mapsto a \circ x$。事实上

$$\ker \circ = \ker \Psi = \{a \in G : \psi_a = \mathbb{1}_\Omega\} = \{a \in G : a \circ x = x, \forall x \in \Omega\}$$

♣

定义 1.12.3 (忠实的)

称群 $(G, *)$ 关于集合 Ω 的作用 $\circ : G \times \Omega \to \Omega$ 为忠诚的/有效的，如果满足如下性质之一。

1. $\circ$ 是单的。
2. 作用 $\circ : G \times \Omega \to \Omega$ 对应的群同态映射 $\Psi : G \to S_\Omega, \quad a \mapsto \psi_a$ 为单态射，其中集合函数 $\psi_a : \Omega \to \Omega, \quad x \mapsto a \circ x$。
3. $\ker \circ = \ker \Psi = \{e\}$
4. $\{a \in G : a \circ x = x, \forall x \in \Omega\} = \{e\}$

♣

定义 1.12.4 (可传递的)

称群 $(G, *)$ 关于集合 Ω 的作用 $\circ : G \times \Omega \to \Omega$ 为可传递的，如果对于任意 $x, y \in \Omega$，存在 $a \in G$，使得成立 $y = a \circ x$。

♣

定义 1.12.5 ((关于群的) 左作用)

群 $(G, *)$ 关于集合 G 的忠实的左作用为 $(a, x) \mapsto a * x$。

♣

定义 1.12.6 ((关于群的) 右作用)

群 $(G, *)$ 关于集合 G 的忠实的右作用为 $(a, x) \mapsto x * a$。

♣

定义 1.12.7 ((关于左商集的) 左作用)

群 $(G, *)$ 关于左商集 $(G/H)_l$ 的左作用为 $(a, x * H) \mapsto (a * x) * H$。

♣

定义 1.12.8 ((关于右商集的) 右作用)

群 $(G, *)$ 关于右商集 $(G/H)_r$ 的右作用为 $(a, H * x) \mapsto H * (x * a)$。

♣

定义 1.12.9 (共轭作用)

群 $(G,*)$ 关于集合 G 的共轭作用为 $(a,x)\mapsto a*x*a^{-1}$。

定理 1.12.2 (共轭作用的本质)

群 $(G,*)$ 关于集合 G 的共轭作用为 $(a,x)\mapsto a*x*a^{-1}$ 对应的群同态映射为 $\Gamma:G\to S_\Omega,\quad a\mapsto\gamma_a$，其中群自同构态射 $\gamma_a:G\to G,\quad x\mapsto a*x*a^{-1}$ 为群内自同构态射。

定理 1.12.3 (Cayley 定理)

群同构于对称群的子群。

证明 给定群 $(G,*)$，可诱导忠实作用，即群同态映射 $\Psi:G\to S_\Omega,\quad a\mapsto\psi_a$，其中集合函数 $\psi_a:\Omega\to\Omega,\quad x\mapsto a\circ x$。由于 Ψ 为单态射，那么 $G\cong\operatorname{im}\Psi<S_G$。

定义 1.12.10 (群的中心)

定义群 $(G,*)$ 的中心为 $\mathrm{Z}(G)=\{x\in G:a*x=x*a,\forall a\in G\}$。

命题 1.12.1

群的中心为正规子群

证明 $\mathrm{Z}(G)$ 为群 $(G,*)$ 关于集合 G 的共轭作用 $(a,x)\mapsto a*x*a^{-1}$ 的核。亦为群同态映射 $\Gamma:G\to S_\Omega,\quad a\mapsto\gamma_a$ 的核，其中群内自同构态射 $\gamma_a:G\to G,\quad x\mapsto a*x*a^{-1}$。因此 $\operatorname{Ker}\Gamma=\mathrm{Z}(G)\triangleleft G$。

1.13 轨道与稳定子

定义 1.13.1 (轨道)

对于群 $(G,*)$ 关于集合 Ω 的作用 $\circ:G\times\Omega\to\Omega$，定义 $x\in\Omega$ 的轨道为

$$\mathrm{Orb}_G(x)=\{a\circ x:a\in G\}$$

命题 1.13.1 (轨道的等价关系)

1. 对于任意 $x,y\in\Omega$，或 $\mathrm{Orb}_G(x)=\mathrm{Orb}_G(y)$，或 $\mathrm{Orb}_G(x)\cap\mathrm{Orb}_G(y)=\varnothing$。
2. 可传递作业的轨道存在且存在唯一。

定义 1.13.2 (稳定子)

对于群 $(G,*)$ 关于集合 Ω 的作用 $\circ:G\times\Omega\to\Omega$，定义 $x\in\Omega$ 的稳定子为

$$\mathrm{Stab}_G(x)=\{a\in G:a\circ x=x\}$$

定义 1.13.3 (不动点集)

定义群 $(G,*)$ 关于集合 Ω 的作用 $\circ:G\times\Omega\to\Omega$ 的不动点集为

$$\mathrm{F}(\Omega)=\{x\in\Omega:a\circ x=x,\forall a\in G\}$$

定义 1.13.4 (p-群)

对于素数 p，称群 G 为 p-群，如果存在 $n\in\mathbb{N}^*$，使得成立 $|G|=p^n$。

命题 1.13.2

如果 p-群在有限集合 Ω 上存在作用 $\circ : G \times \Omega \to \Omega$，那么 $|\mathrm{F}(\Omega)| \equiv |\Omega| \mod p$。

命题 1.13.3

p-群存在非平凡中心。

定义 1.13.5 (共轭类)

定义 $x \in G$ 关于群 $(G, *)$ 的共轭作用的轨道为 x 的共轭类，即

$$\mathrm{Orb}_G(x) = \{a * x * a^{-1} : a \in G\}$$

定义 1.13.6 (中心化子)

定义 $x \in G$ 关于群 $(G, *)$ 的共轭作用的稳定子为 x 的中心化子，即

$$\mathrm{Stab}_G(x) = \{a \in G : a * x = x * a\}$$

定理 1.13.1 (p^2 阶群的结构)

对于素数 p，p^2 阶群 G 成立或 $G \cong \mathbb{Z}_{p^2}$，或 $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$。

定理 1.13.2 (轨道-稳定子定理)

如果群 $(G, *)$ 在集合 Ω 上存在作用 $\circ : G \times \Omega \to \Omega$，那么对于任意 $x \in \Omega$，存在双射

$$\varphi : (G/\mathrm{Stab}_G(x))_l \longrightarrow \mathrm{Orb}_G(x)$$
$$g\mathrm{Stab}_G(x) \longmapsto g \circ x$$

特别的，如果 $|G| < \infty$，那么

$$|G| = |\mathrm{Stab}_G(x)||\mathrm{Orb}_G(x)|$$

1.14 Sylow 定理

引理 1.14.1

对于素数 p，如果 $(n, p) = 1$，那么对于任意 $0 \leq k \leq r$，成立

$$p^{r-k} \mid C_{np^r}^{p^k}, \qquad p^{r-k+1}\mathbb{N}ot \mid C_{np^r}^{p^k}$$

定义 1.14.1 (Sylow p-群)

对于素数 p，如果 $(n, p) = 1$，那么称 np^r 阶群的 p^r 阶子群为该群的 Sylow p-子群。

定理 1.14.1 (Sylow 第一定理存在性定理)

对于素数 p，如果 $(n, p) = 1$，那么对于任意 $0 \leq k \leq r$，np^r 阶群存在 p^k 阶子群。

定理 1.14.2 (Sylow 第二定理包含定理与共轭定理)

对于素数 p，如果 $(n, p) = 1$，那么对于任意 $0 \leq k \leq r$，np^r 阶群的任意 p^k 阶子群包含于某一 p^r 阶子群，且 p^r 阶子群共轭。

定理 1.14.3 (Sylow 第三定理计数定理)

对于素数 p，如果 $(n,p)=1$，那么 np^r 阶群的 p^r 阶子群数 m 成立 $m\equiv 1 \mod p$，且 $m\mid n$。

推论 1.14.1

1. 有限群的 Sylow p-子群为正规子群 $\iff$ 其存在且存在唯一 Sylow p-子群。
2. 如果 p 为 $|G|$ 的素因子，那么群 G 存在 p 阶元。
3. 如果素数 p,q 满足 $(p,q)=1$，那么如果 $(p^m-1)!<q^n$，那么 p^mq^n 阶群不为单群。

1.15 有限 Abel 群的结构

定义 1.15.1 (p-Abel 群的初等因子)

对于素数 p，称如下多重集合为 p^r 阶 Abel 群的初等因子。

$$\{p^{r_1},\cdots,p^{r_k}:r_1\le\cdots\le r_k,r_1+\cdots+r_k=r\}$$

定义 1.15.2 (Abel 群的初等因子)

对于互异素数 $p_1,\cdots,p_n$，称如下多重集合为 p^r 阶 Abel 群的初等因子。

$$\left\{p_i^{r_i^{(j)}}:1\le i\le n,1\le j\le k_i,r_i^{(1)}\le\cdots\le r_i^{(k_i)},r_i^{(1)}+\cdots+r_i^{(k_i)}=r_i\right\}$$

定理 1.15.1 (p-Abel 群的结构)

对于素数 p，p^r 阶 Abel 群的结构为 $\mathbb{Z}_{p^{r_1}}\times\cdots\times\mathbb{Z}_{p^{r_k}}$，其中 $r_1\le\cdots\le r_k$，且 $r_1+\cdots+r_k=r$。

定理 1.15.2 (Abel 群的结构)

对于互异素数 $p_1,\cdots,p_n$，$p_1^{r_1}\cdots p_n^{r_n}$ 阶 Abel 群的结构为 $\prod\limits_{i=1}^{n}\prod\limits_{j=1}^{k_i}\mathbb{Z}_{p_i^{r_i^{(j)}}}$，其中 $r_i^{(1)}\le\cdots\le r_i^{(k_i)}$，且 $r_i^{(1)}+\cdots+r_i^{(k_i)}=r_i$。

第二章 环

2.1 环的定义

定义 2.1.1 (环)

称 $(R,+,\cdot)$ 为群，如果加法运算 $+:R\times R\to R$ 和乘法运算 $\cdot:R\times R\to R$ 满足如下运算法则。

1. 加法单位元：存在 $0\in R$，使得对于任意 $a\in R$，成立 $0+a=a+0=a$。
2. 加法逆元：对于任意 $a\in R$，存在 $-a\in R$，使得成立 $a+(-a)=(-a)+a=0$。
3. 加法交换律：$a+b=b+a$
4. 加法结合律：$(a+b)+c=a+(b+c)$
5. 乘法结合律：$(ab)c=a(bc)$
6. 左分配律：$a(b+c)=ab+ac$
7. 右分配律：$(a+b)c=ac+bc$

♣

定义 2.1.2 (交换环)

称环 R 为交换环，如果

$$\forall a,b,\quad ab=ba$$

♣

定义 2.1.3 (幺环)

称环 R 为幺环，如果

$$\exists 1,\quad \forall a\in R,\quad 1a=a1=a$$

♣

2.2 可逆元与零因子

定义 2.2.1 (可逆元)

称 $a\in R$ 为幺环 R 的可逆元，如果

$$\exists a^{-1},\quad aa^{-1}=a^{-1}a=1$$

♣

定义 2.2.2 (左零因子)

称 $a\in R$ 为环 R 的左零因子，如果

$$\exists b\neq 0,\quad ab=0$$

♣

定义 2.2.3 (右零因子)

称 $a\in R$ 为环 R 的右零因子，如果

$$\exists b\neq 0,\quad ba=0$$

♣

定义 2.2.4 (零因子)

左零因子与右零因子统称为零因子；换言之，称 $a\in R$ 为环 R 的零因子，如果

$$\exists b\neq 0,\quad ab=0\text{ 或}ba=0$$

♣

定义 2.2.5 (非零因子)

称 $a \in R$ 为环 R 的非零因子，如果成立如下性质之一。

1.
$$\forall b, \quad b \neq 0 \implies ab \neq 0 \text{ 且 } ba \neq 0$$

2.
$$\forall b, \quad ab = 0 \text{ 或 } ba = 0 \implies b = 0$$

2.3 无零因子环、整环、除环与域

定义 2.3.1 (无零因子环)

称无非平凡零因子的环为无零因子环；换言之，称环 R 为无零因子环，如果

$$\forall a, b, \quad ab = 0 \implies a = 0 \text{ 或 } b = 0$$

定义 2.3.2 (整环)

称无零因子非零交换幺环为整环；换言之，称环 R 为整环，如果

$$\begin{aligned} &\forall a, b, && ab = ba \\ &\exists 1 \neq 0, \forall a \in R, && 1a = a1 = a \\ &\forall a, b, && ab = 0 \implies a = 0 \text{ 或 } b = 0 \end{aligned}$$

定义 2.3.3 (除环)

称非零元可逆的非零幺环为除环；换言之，称环 R 为除环，如果

$$\begin{aligned} &\exists 1 \neq 0, \forall a \in R, && 1a = a1 = a \\ &\forall a \neq 0, \exists a^{-1}, && aa^{-1} = a^{-1}a = 1 \end{aligned}$$

定义 2.3.4 (域)

交换除环称为域；换言之，称环 R 为域，如果

$$\begin{aligned} &\forall a, b, && ab = ba \\ &\exists 1 \neq 0, \forall a \in R, && 1a = a1 = a \\ &\forall a \neq 0, \exists a^{-1}, && aa^{-1} = a^{-1}a = 1 \end{aligned}$$

2.4 理想

定义 2.4.1 (子环)

称 $S \subset R$ 为环 R 的子环，如果 S 构成环。

定义 2.4.2 (理想)

称 $I \subset R$ 为环 R 的理想，如果

$$\forall a, b \in I \qquad a - b \in I$$
$$\forall a \in R, \qquad aI \subset I \text{ 且 } Ia \subset I$$

命题 2.4.1 (理想的性质)

1. $I \subset \mathbb{Z}$ 为 $\mathbb{Z}$ 的理想 $\iff$ 存在 $n \in \mathbb{N}^*$，使得成立 $I = n\mathbb{Z}$。
2. 对于任意 $f(x) \in R[x]$，$f(x)R[x]$ 为 $R[x]$ 的理想。
3. 对于幺环 R，以及 $a \in R$，aR 为 R 的理想。

定义 2.4.3 (理想的运算)

对于环 R 的理想 I, J，定义理想的加法和乘法

$$I + J = \{a + b : a \in I, b \in J\}$$
$$IJ = \{a_1 b_1 + \cdots + a_n b_n : a_k \in I, b_k \in J, n \in \mathbb{N}^*\}$$

命题 2.4.2 (理想运算的性质)

1. 如果 I, J 为环 R 的理想，那么 $IJ \subset I \cap J \subset I + J$ 为 R 的理想。
2. 如果如果 I, J, K 为环 R 的理想，那么成立如下性质。
   (a). 加法交换律：
   $$I + J = J + I$$
   (b). 加法结合律：
   $$(I + J) + K = I + (J + K)$$
   (c). 乘法结合律：
   $$(IJ)K = I(JK)$$
   (d). 左分配律：
   $$I(J + K) = IJ + IK$$
   (e). 右分配律：
   $$(I + J)K = IK + JK$$
3. 对于整数环 $\mathbb{Z}$，成立
   $$(m)(n) = (mn)$$
   $$(m) \cap (n) = ([m, n])$$
   $$(m) + (n) = ((m, n))$$

定义 2.4.4 (主理想)

对于环 R，定义由 $a \in R$ 生成的主理想为

$$(a) = \bigcap_{I \mathbb{N} ia} I$$

特别的，对于交换幺环 R，由 $a \in R$ 生成的主理想为 $(a) = aR$。

命题 2.4.3

1. 对于任意 $n \in \mathbb{Z}$，(n) 为 $\mathbb{Z}$ 的主理想。
2. 对于任意 $f(x) \in R[x]$，$(f(x))$ 为 $R[x]$ 的主理想。

♠

定义 2.4.5 (生成理想)

对于环 R，定义由子集 $S \subset R$ 生成的理想为

$$(S) = \bigcap_{I \supset S} I$$

特别的，对于交换幺环 R，由 $\{a_1, \cdots, a_n\}$ 生成的主理想为

$$(a_1, \cdots, a_n) = \{r_1 a_1 + \cdots + r_n a_n : r_k \in R\}$$

♣

定义 2.4.6 (互素)

称幺环 R 的理想 I 与 J 互素，如果 $I + J = R$。

♣

命题 2.4.4

1. 对于幺环 R 的理想 I, J, K，如果 I 与 K 互素且 J 与 K 互素，那么 I 与 J 互素。
2. 对于交换幺环 R 的理想 I 与 J，如果 I 与 J 互素，那么 $IJ = I \cap J$。

♠

2.5 环的同态

定义 2.5.1 (环同态映射)

对于环 R 与 S，称 $\varphi : R \to S$ 为环同态映射，如果成立

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$
$$\varphi(1) = 1$$

♣

定义 2.5.2 (环同构映射)

对于环 R 与 S，称环同态映射 $\varphi : R \to S$ 为环同构映射，如果 φ 为双射。

♣

定义 2.5.3 (环同构)

称环 R 与 S 同构，并记为 $R \cong S$，如果存在环同构映射 $\varphi : R \to S$。

♣

定理 2.5.1 (核为理想)

环同态映射 $\varphi : R \to S$ 的核 $\operatorname{Ker} \varphi$ 为 R 的理想。

♡

定理 2.5.2 (理想为核)

理想 I 为环同态映射 $\varphi : R \to R/I$ 的核 $\operatorname{Ker} \varphi$。

♡

2.6 商环

定义 2.6.1 (商环)

定义环 R 关于理想 I 的商环为

$$R/I = \{r + I : r \in R\}$$
$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = (ab) + I$$

♣

定理 2.6.1 (群同构定理)

对于环同态映射 $\sigma : R \to S$，成立

$$R/\mathrm{Ker}\,\sigma \cong \mathrm{Im}\,\sigma$$

♡

定理 2.6.2 (第一同构定理)

对于环 R，S 为 R 的子环，I 为 R 的理想，那么 $S + I$ 为 R 的子环，$S \cap I$ 为 R 的理想，并且

$$\frac{S}{I \cap S} \cong \frac{S + I}{I}$$

♡

定理 2.6.3 (第二同构定理)

对于环 R，I, J 为 R 的理想，I 为 J 的子环，那么 J/I 为 R/I 的理想，并且

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

♡

2.7 环的直和

定义 2.7.1 (环的直和)

定义环 R 与 S 的直和为

$$R \oplus S = \{(r, s) : r \in R, s \in S\}$$
$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$$

♣

定义 2.7.2 (环直和的分解)

$$R' = \{(r, 0) : r \in R\}, \qquad S' = \{(0, s) : s \in S\}$$

♣

命题 2.7.1

1. R', S' 为 $R \oplus S$ 的理想。
2. $R' + S' = R \oplus S$
3. $R' \cap S' = (0, 0)$
4. $R' \cong R$

♠

定义 2.7.3 (内直和)

称环 R 为理想 I 与 J 的内直和，如果 $R \cong I \oplus J$，其环同构映射为 $i+j \mapsto (i,j)$。

♣

定理 2.7.1 (内直和定理)

对于环 R 为理想 I 与 J，如果 $R = I + J$，且 $I \cap J = \{0\}$，那么 $R \cong I \oplus J$。

♡

定理 2.7.2 (内直和同构定理)

对于非零幺环 R，如果理想 $\{I_k\}_{k=1}^n$ 两两互素，那么

$$R \Big/ \bigcap_{k=1}^{n} I_k \cong \bigoplus_{k=1}^{n} R/I_k$$

♡

定理 2.7.3 (中国剩余定理)

对于非零幺环 R,，如果理想 $\{I_k\}_{k=1}^n$ 两两互素，那么对于任意 $\{a_k\}_{k=1}^n \subset R$，同余方程组

$$\begin{cases} x \equiv a_1 \mod I_1 \\ \quad \vdots \\ x \equiv a_n \mod I_n \end{cases}$$

在 R 内存在解；且对于两个解 x 与 y，成立

$$x \equiv y \mod \bigcap_{k=1}^{n} I_k$$

♡

证明 由于理想 $\{I_k\}_{k=1}^n$ 两两互素，那么对于任意 $1 \leq k \leq n$，成立

$$I_k + I_1 \cdots I_{k-1} I_{k+1} \cdots I_n = R$$

从而存在 $b_k \in I_k$，$e_k \in I_1 \cdots I_{k-1} I_{k+1} \cdots I_n$，使得成立 $b_k + e_k = 1$，因此

$$e_k \equiv 1 \mod I_k$$

由于当 $i \neq j$ 时，成立

$$e_i \in I_1 \cdots I_{i-1} I_{i+1} \cdots I_n \subset \bigcap_{j \neq i} I_j \subset I_j$$

因此

$$e_i \equiv 0 \mod I_j, \qquad i \neq j$$

进而同余方程组

$$\begin{cases} x \equiv 0 \mod I_1 \\ \quad \vdots \\ x \equiv 0 \mod I_{k-1} \\ x \equiv 1 \mod I_k \\ x \equiv 0 \mod I_{k+1} \\ \quad \vdots \\ x \equiv 0 \mod I_n \end{cases}$$

在 R 内存在解 e_k。那么同余方程组在 R 内的解为

$$x=\sum_{k=1}^{n}a_ke_k$$

如果 x,y 满足同余方程组

$$\begin{cases}x\equiv a_1 \mod I_1\\ \vdots\\ x\equiv a_n \mod I_n\end{cases},\qquad \begin{cases}y\equiv a_1 \mod I_1\\ \vdots\\ y\equiv a_n \mod I_n\end{cases}$$

那么

$$\begin{cases}x\equiv y \mod I_1\\ \vdots\\ x\equiv y \mod I_n\end{cases}$$

因此对于任意 $1\leq k\leq n$，成立 $x-y\in I_k$，进而

$$x-y\in\bigcap_{k=1}^{n}I_k\iff x\equiv y \mod \bigcap_{k=1}^{n}I_k$$

命题 2.7.2

对于互异奇素数 p,q，求方程 $x^2=n^2$ 在 $\mathbb{Z}/pq\mathbb{Z}$ 中的解。

♠

证明 方程 $x^2=n^2$ 在 $\mathbb{Z}/pq\mathbb{Z}$ 中的解满足

$$\begin{cases}x\equiv n \mod p\\ x\equiv n \mod q\end{cases},\quad \begin{cases}x\equiv n \mod p\\ x\equiv -n \mod q\end{cases},\quad \begin{cases}x\equiv -n \mod p\\ x\equiv n \mod q\end{cases},\quad \begin{cases}x\equiv -n \mod p\\ x\equiv -n \mod q\end{cases}$$

由于 $(p,q)=1$，那么存在 a,b，使得成立 $ap+bq=1$。因此方程 $x^2=n^2$ 在 $\mathbb{Z}/pq\mathbb{Z}$ 中的解为

$$n,\qquad -n,\qquad n-2anp,\qquad 2anp-n$$

2.8 素理想与极大理想

定义 2.8.1 (素理想)

称非零交换幺环 R 的真理想 $P\subsetneq R$ 为素理想，如果对于任意 $r,s\in R$，成立 $rs\in P\implies r\in P$ 或 $s\in P$。

♣

命题 2.8.1 (素理想的性质)

1. P 为环 R 的素理想 $\iff$ R/P 为整环。
2. p 为素数 $\iff$ (p) 为 $\mathbb{Z}$ 的素理想。
3. 对于域 F，I 为 $F[x]$ 的理想 $\iff$ 存在 $f(x)\in F[x]$，使得成立 $I=(f(x))$。
4. 对于域 F，$p(x)\in F[x]$ 为不可约多项式 $\iff$ $(p(x))$ 为 $F[x]$ 的素理想。
5. (0) 为环 R 的素理想 $\iff$ R 为整环。

♠

定义 2.8.2 (谱)

称非零交换环 R 的素理想族为 R 的谱，记作 $\operatorname{Spec}R$。

♣

命题 2.8.2 (谱的性质)

1. Spec $\mathbb{Z} = \{(p) : p0\}$
2. 对于代数封闭域 F，Spec $F[x] = \{(0)\} \cup \{(x + a_0) : a_0 \in F\}$。

♠

定义 2.8.3 (代数封闭域)

称域 F 为代数封闭域，如果 $F[x]$ 中的一次多项式在 F 中存在根。

♣

定义 2.8.4 (极大理想)

称环 R 的真理想 $M \subsetneq R$ 为极大理想，如果成立

$$I \supset M \text{ 为} R \text{ 的理想} \implies I = M \text{ 或} I = R$$

♣

命题 2.8.3 (极大理想的性质)

1. 对于非零交换幺环 R，M 为 R 的极大理想 $\iff$ R/M 为域。
2. p 为素数 $\iff$ (p) 为 $\mathbb{Z}$ 的极大理想。
3. 对于域 F，$p(x) \in F[x]$ 为不可约多项式 $\iff$ $(p(x))$ 为 $F[x]$ 的极大理想。
4. (0) 为环 R 的极大理想 $\iff$ R 为域。
5. 非零幺环存在极大理想。

♠

2.9 有限域的构造

定理 2.9.1 (有限域的阶)

有限域的阶为素数幂。

♡

定理 2.9.2 (域扩张)

对于 p^r 阶域 F_p，如果 $f(x)$ 为 $F_p[x]$ 的 n 次不可约多项式，那么 $F_p[x]/(f(x))$ 为 p^{nr} 阶域，且对于任意 $F(x) \in F_p[x]/(f(x))$ 可唯一表示为

$$F(x) = \sum_{k=0}^{n-1} a_k x^k + (f(x)) = \sum_{k=0}^{n-1} (a_k + (f(x)))(x + (f(x)))^k, \qquad a_k \in F_p$$

♡

2.10 代数数域

定义 2.10.1 (扩环)

称非零交换幺环 R 为非零交换幺环 R_0 的扩环，如果存在单的环同态映射 $R_0 \to R$。

♣

定义 2.10.2 (生成子环)

对于非零交换幺环 R 的非零交换幺扩环 S，定义 R 关于 $x \in S$ 的生成子环为

$$R[x] = \bigcap_{K \supset R \cup \{x\} S} K = \left\{ \sum_{k=0}^{n} a_k x^k : a_k \in R, n \in \mathbb{N} \right\}$$

♣

定义 2.10.3 (代数数)

称 $x \in \mathbb{C}$ 为代数数，如果存在非零多项式 $f(x) \in \mathbb{Q}[x]$，使得成立 $f(z) = 0$；否则，称为超越数。 ♣

定义 2.10.4 (代数整数)

称 $x \in \mathbb{C}$ 为代数整数，如果存在首一多项式 $f(x) \in \mathbb{Z}[x]$，使得成立 $f(z) = 0$。 ♣

定义 2.10.5 (代数数域)

称 $\mathbb{Q}[z]$ 为代数数域，如果 z 为代数数。 ♣

定义 2.10.6 (本原 n 次单位根)

称 $x \in \mathbb{C}$ 为本原 n 次单位根，如果 $\langle x \rangle = \{z \in \mathbb{C} : z^n = 1\}$。 ♣

定义 2.10.7 (第 n 个分圆域)

称 $\mathbb{Q}[e^{i\frac{2\pi}{n}}]$ 为第 n 个分圆域。 ♣

2.11 Galois 环的构造

定义 2.11.1 (基本不可约多项式)

对于素数 p，称 $f(x) \in \mathbb{Z}_{p^r}[x]$ 为 $\mathbb{Z}_{p^r}[x]$ 的基本不可约多项式，如果 $f(x)$ 在 $\mathbb{Z}_p[x]$ 中不可约。 ♣

定义 2.11.2 (Galois 环)

对于素数 p，如果 $f(x) \in \mathbb{Z}_{p^r}[x]$ 为 $\mathbb{Z}_{p^r}[x]$ 的 n 次基本不可约多项式，那么商环 $\mathbb{Z}_{p^r}[z]/(f(x))$ 为 p^{nr} 阶环，称之为 Galois 环，记作 $\mathrm{GR}(p^r, n)$。 ♣

定理 2.11.1

对于 $f(x) = \sum_{k=0}^{n} a_n x^n \in \mathbb{Z}[x]$，其中 $a_n \neq 0$，如果 $f(x)$ 存在即约有理根 q/p，那么

$$q \mid a_0, \qquad p \mid a_n$$

特别的，如果首一多项式 $f(x) \in \mathbb{Z}[x]$ 存在有理根，那么其为 a_0 的因子。 ♡

定理 2.11.2 (Eisenstein 判别法)

对于 $f(x) = \sum_{k=0}^{n} a_n x^n \in \mathbb{Z}[x]$，其中 $a_n \neq 0$，如果存在素数 p，使得成立

$$p \nmid a_n, \qquad p^2 \nmid a_0, \qquad p \mid a_k, \quad 0 \leq k < n$$

那么 $f(x)$ 在 $\mathbb{Q}[x]$ 上不可约。 ♡

第三章 整环

3.1 整除

定义 3.1.1 (整除)

对于整环 R，称 $b \in R$ 整除 $a \in R$，并记做 $b \mid a$，如果存在 $c \in R$，使得成立 $a = bc$。

命题 3.1.1 (整除的性质)

1. 整除具有自身性和传递性。
2. $b \mid a \iff (a) \subset (b)$
3. e为单位 $\iff e \mid 1 \iff (e) = R \iff \forall a \in R, (a) \subset (e) \iff \forall a \in R, e \mid a$
4. $b \mid a_1, b \mid a_2 \implies \forall r_1, r_2 \in R, b \mid (r_1 a_1 + r_2 a_2)$
5. $\forall a \in R, a \mid 0$

定义 3.1.2 (因子)

对于整环 R，称 $b \in R$ 为 $a \in R$ 的因子，如果 $b \mid a$。

定义 3.1.3 (倍元)

对于整环 R，称 $a \in R$ 为 $b \in R$ 的倍元，如果 $b \mid a$。

定义 3.1.4 (相伴)

对于整环 R，称 $a \in R$ 与 $b \in R$ 相伴，并记做 $a \sim b$，如果 $a \mid b$ 且 $b \mid a$。

命题 3.1.2 (相伴的性质)

1. 相伴为等价关系。
2. $a \sim b \iff (a) = (b) \iff$ 存在单位$e, a = be$
3. $a \sim b, c \sim d \implies ac \sim bd$

定义 3.1.5 (真因子)

对于整环 R，称 $b \in R$ 为 $a \in R$ 的真因子，如果 $b \mid a$，且 $a \nmid b$。

命题 3.1.3 (真因子的性质)

1. 真因子为因子，但不为相伴元。
2. 任意非零元为 0 的真因子。
3. 单位没有真因子。

定义 3.1.6 (平凡因子)

对于整环 R，称 $a \in R$ 的平凡因子为单位和相伴元。

命题 3.1.4 (平凡因子的性质)

1. 非平凡因子为真因子。
2. 单位没有非平凡因子。

定义 3.1.7 (不可约元)

对于整环 R，称非零非单位 $a \in R$ 为不可约元，如果 a 仅存在平凡因子。

命题 3.1.5 (不可约元的性质)

1. 不可约元的因子为单位或相伴元。
2. 不可约元的相伴元为不可约元。
3. 不可约元为非单位。

定义 3.1.8 (素元)

对于整环 R，称非零非单位 $a \in R$ 为素元，如果

$$p \mid ab \implies p \mid a \text{或} p \mid b$$

命题 3.1.6 (素元的性质)

1. 素元为不可约元。
2. a为素元 $\iff$ (a)为非零素理想

定义 3.1.9 (公因子)

对于整环 R，称 $c \in R$ 为 $a \in R$ 与 $b \in R$ 的公因子，如果 $c \mid a$ 且 $c \mid b$。

定义 3.1.10 (最大公因子)

对于整环 R，称 $a \in R$ 与 $b \in R$ 的公因子 $(a,b) \in R$ 为最大公因子，如果

$$\forall b, c \in R, \qquad c \mid a, c \mid b \implies c \mid (a,b)$$

命题 3.1.7 (最大公因子的性质)

1. 最大公因子不一定存在。
2. 最大公因子互为相伴元。
3. $(0,a) \sim a, (e,a) \sim a$，其中 e 为单位。

3.2 唯一因子分解整环

定义 3.2.1 (唯一因子分解整环/Gauss 整环/UFD)

称整环为唯一因子分解整环/Gauss 整环，如果其任意非零非单位的元素在相伴与置换顺序意义下存在且存在唯一有限不可约元分解。

定义 3.2.2 (最大公因子条件)

称整环 R 成立最大公因子条件，如果对于任意 $a,b \in R$，存在 a,b 的最大公因子 (a,b)。

定义 3.2.3 (素元性条件)

称整环 R 成立素元性条件，如果 R 的不可约元为素元。 ♣

定义 3.2.4 (因子链条件)

称整环 R 成立因子链条件，如果序列 $\{a_n\}$ 对于任意 n，a_{n+1} 为 a_n 的真因子，那么该序列为有限序列。 ♣

引理 3.2.1

如果整环 R 满足元素间最大公因子条件，那么对于任意 $a,b,c\in R$，成立 $(ab,ac)\sim a(b,c)$。 ♡

证明 果 $a=0$，那么 $(ab,ac)\sim a(b,c)\sim 0$。如果 $(b,c)=0$，那么 $b=c=0$，从而 $(ab,ac)\sim a(b,c)\sim 0$。下面不妨假设 $a\neq 0$ 且 $(b,c)\neq 0$，记 $d=(b,c)$ 且 $e=(ab,ac)$，那么

$$d\mid b,d\mid c\implies ad\mid ab,ad\mid ac\implies ad\mid (ab,ac)\iff ad\mid e\iff \exists u\in R,e=adu$$

注意到

$$e\mid ab\iff \exists v\in R,ab=ev\implies ab=aduv\iff b=duv$$
$$e\mid ac\iff \exists v'\in R,ac=ev'\implies ac=aduv'\iff c=duv'$$

那么

$$du\mid (b,c)\iff du\mid d\iff \exists u'\in R,d=duu'\iff uu'=1\iff u\text{为单位}\implies e=ad$$

定理 3.2.1 (最大公因子条件 $\implies$ 素元性条件)

如果整环成立元素间最大公因子条件，那么成立素元性条件。 ♡

证明 任取整环 R 的不可约元 a，以及 $b,c\in R$，成立 $a\mid bc$。由于 $(a,b)\mid a$，那么 $(a,b)\sim a$，或 (a,b) 为单位。如果 $(a,b)\sim a$，那么 $a\mid (a,b)$，进而 $a\mid b$；如果 (a,b) 为单位，那么由引理3.2.1

$$(a,b)\sim 1\implies c(a,b)\sim c\implies (ac,bc)\sim c$$

由于 $a\mid bc$ 且 $a\mid ac$，那么 $a\mid (ac,bc)$，因此 $a\mid c$。综上所述，a 为素元。

定理 3.2.2 (UFD $\implies$ 最大公因子条件)

如果整环为唯一因子分解整环，那么成立最大公因子条件。 ♡

证明 对于整环 R，任取 $a,b\in R$，如果 $a=0$，那么 $b=(0,b)$；如果 a 为单位，那么 $a=(a,b)$。下面假设 a,b 均为非零的非单位元。由于 R 为唯一因子分解整环，那么存在两两不相伴的不可约元 $\{p_k\}_{k=1}^n$ 与单位 u,v，使得成立

$$a=up_1^{\alpha_1}\cdots p_n^{\alpha_n},\qquad \alpha_k\geq 0$$
$$b=vp_1^{\beta_1}\cdots p_n^{\beta_n},\qquad \beta_k\geq 0$$

其中存在 k_a,k_b，使得成立 $\alpha_{k_a}>0$ 且 $\beta_{k_b}>0$。令

$$d=p_1^{\min\{\alpha_1,\beta_1\}}\cdots p_n^{\min\{\alpha_n,\beta_n\}}$$

那么 d 为 a,b 的公因子。如果 c 为 a,b 的公因子，那么存在单位 w，使得成立

$$c=wp_1^{\gamma_1}\cdots p_n^{\gamma_n},\qquad \gamma_k\leq \min\{\alpha_k,\beta_k\}$$

因此 $c\mid d$，进而 $d=(a,b)$。

定理 3.2.3 (UFD $\implies$ 因子链条件)

如果整环为唯一因子分解整环，那么成立因子链条件。 ♡

证明 对于整环 R，任取序列 $\{a_n\} \subset R$，满足对于任意 n，a_{n+1} 为 a_n 的真因子。如果 a_1 为单位，那么 a_1 没有真因子，因此该序列仅存在第一项。如果 $a_1 = 0$，那么 a_1 的真因子为非零元。因此不妨假设 a_1 非零且非单位。由于 R 为唯一因子分解整环，那么存在两两不相伴的不可约元 $\{p_k\}_{k=1}^n$ 与单位 u，使得成立

$$a_1 = up_1^{\alpha_1} \cdots p_n^{\alpha_n}, \qquad \alpha_k \geq 1$$

那么 a_1 的因子为

$$vp_1^{\beta_1} \cdots p_n^{\beta_n}, \qquad 0 \leq \beta_n \leq \alpha_n, v\text{为单位}$$

那么显然 a_1 的真因子有限。

定理 3.2.4 (素元性条件 + 因子链条件 $\Longrightarrow$ UFD)

如果整环成立素元性条件与因子链条件，那么为唯一因子分解整环。

证明 对于存在性，任取非零非单位的元素 $a \in R$，如果 a 不可约，那么命题得证！下面不妨假设 a 可约，由因子链条件，a 存在不可约真因子 p_1，于是 $a = p_1c_1$。如果 c_1 不可约，那么命题得证！如果 c_1 可约，容易知道 c_1 非零且非单位，那么由因子链条件，c_1 存在不可约真因子 p_2，于是 $c_1 = p_2c_2$。递归的，可得因子链 $\{p_k\}_{k=1}^n$，那么 $a = p_1 \cdots p_n$。

对于唯一性，如果非零非单位的元素 $a \in R$ 存在因子分解式

$$a = p_1 \cdots p_n, \qquad a = q_1 \cdots q_m$$

对 n 进行归纳。当 $n = 1$ 时，$a = p_1 = q_1 \cdots q_m$，如果 $m \geq 2$，那么

$$p_1 = q_1(q_2 \cdots q_m)$$

由于 p_1 不可约，那么 q_1 为 p_1 的平凡因子。由于 q_1 不为单位，因此 $q_1 \sim p_1$，于是 $q_1 = p_1u$，其中 u 为单位，从而

$$p_1 = p_1u(q_2 \cdots q_m) \implies 1 = u(q_2 \cdots q_m)$$

进而 q_2 为单位，矛盾！从而 $m = 1$，因此 $a = p_1 = q_1$。

如果 $n = k$ 时命题成立，那么当 $n = k+1$ 时，由于 p_1 不可约，那么 p_1 为素元。由于 $p_1 \mid q_1 \cdots q_m$ 可得不妨 $p_1 \mid q_1$。由于 q_1 不可约，那么 $p_1 \sim q_1$，于是 $p_1 = q_1v$，其中 v 为单位，进而

$$q_1vp_2 \cdots p_{k+1} = q_1 \cdots q_m \implies vp_2 \cdots p_{k+1} = q_2 \cdots q_m$$

由归纳假设 $m = k+1$，命题得证！

3.3 主理想整环

定义 3.3.1 (主理想整环/PID)

称整环为主理想整环，如果其理想为主理想。

引理 3.3.1

对于主理想整环 R，如果 p 不可约，那么 (p) 为极大理想。

证明 如果 p 不可约，那么 p 非零且非单位，因此 $(0) \subsetneq (p) \subsetneq R$。任取理想 $I \supset (p)$，由于 R 为主理想整环，那么存在 $a \in R$，使得成立 $I = (a) \supset (p)$，进而 $a \mid p$。由于 p 仅存在平凡因子，那么 $a \sim p$，或 a 为单位。如果 $a \sim p$，那么 $(a) = (p)$；如果 a 为单位，那么 $(a) = R$。综上，(p) 为极大理想。

定义 3.3.2 (PID $\Longrightarrow$ UFD)

主理想整环为唯一因子分解整环。

证明 对于主理想整环 R，由引理3.3.1，如果 p 为不可约元，那么 (p) 为非零极大理想，从而 (p) 为非零素理想，因此 p 为素元，进而 R 满足素元性条件。

任取 R 的序列 $\{a_n\}$，其中对于任意 n，a_{n+1} 为 a_n 的真因子，于是 $(a_n) \subsetneq (a_{n+1})$。令 $I = \bigcup_n (a_n)$，那么 I 为 R 的理想。由于 R 为主理想整环，那么存在 $d \in R$，使得成立 $I = (d)$。由于 $d \in \bigcup_n (a_n)$，那么存在 k，使得成立 $d \in (a_k)$，从而 $a_k \mid d$，于是 $(d) \subset (a_k)$。又由于 $(a_k) \subset (d)$，因此 $(a_k) = (d) = I$，进而序列 $\{a_n\}$ 仅存在 k 项，那么 R 满足因子链条件。

综上所述，R 为唯一因子分解整环。

3.4 Euclid 整环

定义 3.4.1 (Euclid 整环/ED)

称整环 R 为 Euclid 整环，如果存在映射 $\delta : R \setminus \{0\} \to \mathbb{N}$，使得对于任意 $a, b \in R$ 且 $b \neq 0$，存在 $h, r \in R$，使得成立

$$a = hb + r, \qquad r = 0 \text{或} r \neq 0, \delta(r) < \delta(b)$$

♣

定义 3.4.2 (ED $\Longrightarrow$ PID)

Euclid 整环为主理想整环。

♣

证明 对于 Euclid 整环 R，任取 R 的非零理想 I，取 $b \in I \setminus \{0\}$，使得对于任意 $x \in I \setminus \{0\}$，成立 $\delta(b) \leq \delta(x)$。显然 $(b) \subset I$。反之，任取 $a \in I$，由于 R 为 Euclid 整环，那么存在 $h, r \in R$，使得成立

$$a = hb + r, \qquad r = 0 \text{或} r \neq 0, \delta(r) < \delta(b)$$

如果 $r \neq 0$，那么显然矛盾！因此 $r = 0$，进而 $a = hb \in (b)$，于是 $I \subset (b)$。综上 $I = (b)$。

3.5 分式域

定义 3.5.1 (分式域)

称域 F 为整环 R 的分式域，如果存在单的环同态映射 $\varphi : R \to F$，使得成立

$$F = \{\varphi(a)\varphi(b)^{-1} : a, b \in R, b \neq 0\}$$

♣

定理 3.5.1 (分式域的存在性)

整环存在分式域。

♡

证明 对于整环 R，记

$$T = \{(a, b) : a, b \in R, b \neq 0\}$$

定义 T 上的等价关系

$$(a, b) \sim (c, d) \iff ad = bc$$

记

$$[(a, b)]_\sim = \frac{a}{b}$$

在商集 $F = T/\sim$ 中定义

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

容易知道该运算的定义良好性，且满足交换律、结合律、分配律，同时 $0/1$ 为加法单位元，$1/1$ 为乘法单位元，$(-a)/b$ 为 a/b 的加法逆元，b/a 为 a/b 的乘法逆元，于是 F 构成域，且

$$\begin{aligned}\varphi : R &\longrightarrow F\\ a &\longmapsto \frac{a}{1}\end{aligned}$$

为单的环同态映射，进而域 F 为整环 R 的分式域。

定理 3.5.2 (分式域的唯一性)

整环的分式域至多同构。

♡

证明 如果整环 R 存在分式域 F 与 G，那么存在单的环同态映射 $\varphi : R \to F$ 与 $\psi : R \to \psi$，定义

$$\begin{aligned}\pi : \quad F &\longrightarrow G\\ \varphi(a)\varphi(b)^{-1} &\longmapsto \psi(a)\psi(b)^{-1}\end{aligned}$$

由于

$$\begin{aligned}&\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}\\ \Longleftrightarrow\ &\varphi(a)\varphi(d) = \varphi(b)\varphi(c)\\ \Longleftrightarrow\ &\varphi(ab) = \varphi(bc)\\ \Longleftrightarrow\ &ab = bc\\ \Longleftrightarrow\ &\psi(ab) = \psi(bc)\\ \Longleftrightarrow\ &\psi(a)\psi(d) = \psi(b)\psi(c)\\ \Longleftrightarrow\ &\psi(a)\psi(b)^{-1} = \psi(c)\psi(d)^{-1}\end{aligned}$$

因此 π 为定义良好的单射。π 是满射是显然的。由于

$$\begin{aligned}\pi(\varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1}) =& \pi(\varphi(a)\varphi(d)\varphi(b)^{-1}\varphi(d)^{-1} + \varphi(b)\varphi(c)\varphi(b)^{-1}\varphi(d)^{-1})\\ =& \pi(\varphi(ad+bc)(\varphi(bd))^{-1})\\ =& \psi(ad+bc)(\psi(bd))^{-1}\\ =& \psi(a)\psi(d)\psi(b)^{-1}\psi(d)^{-1} + \psi(b)\psi(c)\psi(b)^{-1}\psi(d)^{-1}\\ =& \psi(a)\psi(b)^{-1} + \psi(c)\psi(d)^{-1}\\ \pi(\varphi(a)\varphi(b)^{-1}\varphi(c)\varphi(d)^{-1}) =& \pi(\varphi(ac)(\varphi(bd))^{-1})\\ =& \psi(ac)(\psi(bd))^{-1}\\ =& \psi(a)\psi(b)^{-1}\psi(c)\psi(d)^{-1}\end{aligned}$$

因此 π 为环同构映射，进而 $F \cong G$。

定理 3.5.3 (分式域的极小性)

整环 R 的分式域为包含 R 的最小域。

♡

定理 3.5.4

$$\text{整环同构} \Longrightarrow \text{分式域同构}$$

♡

第四章 域

4.1 域扩张

定义 4.1.1 (子域)
对于域 K, F，称 F 为 K 的子域，如果存在单的环同态映射 $\varphi : F \to K$。 ♣

定义 4.1.2 (扩域)
对于域 K, F，称 K 为 F 的扩域或域扩张，并记做 K/F，如果存在单的环同态映射 $\varphi : F \to K$。 ♣

定义 4.1.3 (域扩张)
对于域 K, F，称 K/F 为域扩张，如果存在单的环同态映射 $\varphi : F \to K$。 ♣

4.2 域的特征

定义 4.2.1 (中间域)
称域 L 为域扩张 K/F 的中间域，如果 $F \subset L \subset K$。特别的，称域 L 为域扩张 K/F 的真中间域，如果 $F \subsetneq L \subsetneq K$。 ♣

定义 4.2.2 (素域)
称域 F 为素域，如果 F 存在且仅存在平凡子域。 ♣

例题 4.1

1. $\mathbb{Q}$ 为素域。
2. 如果 p 为素数，那么 $\mathbb{Z}_p$ 为素域。

定义 4.2.3 (域的特征)
定义域 F 的特征为单位元 1 在加法群 $(F, +)$ 阶，并记作 $\operatorname{char} F$；特别的，如果单位元 1 在加法群 $(F, +)$ 阶为 ∞，那么 $\operatorname{char} F = 0$。 ♣

定义 4.2.4 (域的特征为 0 或素数)
域的特征为 0 或素数。 ♣

定理 4.2.1 (域特征的本质)
记域 F 的特征为 p，如果 $p = 0$，那么 F 存在同构于 $\mathbb{Q}$ 的子域；如果 p 为素数，那么 F 存在同构域 $\mathbb{Z}_p$ 的子域。 ♡

证明 考虑环同态映射

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow F \\ n &\longmapsto n1 \end{aligned}$$

由域特征的定义，$\ker\varphi = p\mathbb{Z}$。由环同构定理，$\mathbb{Z}/p\mathbb{Z} \cong \operatorname{im}\varphi$。如果 $p=0$，那么 F 存在同构于 $\mathbb{Z}$ 的子环，因此存在同构于 $\mathbb{Q}$ 的子域；如果 p 为素数，那么 F 存在同构域 $\mathbb{Z}_p$ 的子域。

推论 4.2.1

域存在且仅存在唯一素域。

♡

命题 4.2.1

域 F 的非零元在群 $(F,+)$ 中阶相同。

♠

证明 对于域 F，任取 $a,b \in F\setminus\{0\}$。如果 a 在群 $(F,+)$ 中为有限阶 n，且 b 在群 $(F,+)$ 中的阶为 ∞，那么 $na=0$，且对于任意 $m\in\mathbb{N}^*$，成立 $mb\neq 0$，因此

$$(nr)s=0 \iff r(ns)=0 \iff ns=0$$

矛盾！因此 F 中非零元在群 $(F,+)$ 中的阶均为无限阶或均为有限阶。

如果 a,b 在群 $(F,+)$ 中均为有限阶，那么记 a,b 在群 $(F,+)$ 的阶为 m,n，那么

$$ma=0 \implies (ma)b=0 \iff a(mb)=0 \iff mb=0 \implies n\mid m$$

同理可得，$m\mid n$，因此 $m=n$。

综上所述，无零因子环的非零元在加法群中的阶相同。

4.3 单扩张

定义 4.3.1 (生成子域)

对于域扩张 K/F，定义域 F 关于子集 $S\subset K$ 的生成子域为

$$F(S)=\bigcap_{\text{域}L\supset F\cup S} L$$

♣

引理 4.3.1

$$F(\alpha,\beta)=F(\alpha)(\beta)$$

♡

定义 4.3.2 (代数元)

对于域扩张 K/F，称 $\alpha\in K$ 为 F 的代数元，如果存在非零多项式 $f(x)\in F[x]$，使得成立 $f(\alpha)=0$。

♣

定义 4.3.3 (超越元)

对于域扩张 K/F，称 $\alpha\in K$ 为 F 的超越元，如果对于任意非零多项式 $f(x)\in F[x]$，成立 $f(\alpha)\neq 0$。

♣

定义 4.3.4 (极小多项式)

对于域扩张 K/F，称 F 的代数元 $\alpha\in K$ 在 F 上的极小多项式为 $p(x)$，如果 $p(x)\in F[x]$ 为以 α 为根的 $F[x]$ 的不可约首一多项式。

♣

定理 4.3.1

代数元的极小多项式存在且存在唯一。

♡

定义 4.3.5 (单扩张)

称域扩张 K/F 为单扩张，如果存在 $\alpha \in K$，使得成立 $K = F(\alpha)$。

定义 4.3.6 (单代数扩张)

称域扩张 K/F 为单代数扩张，如果存在 F 的代数元 $\alpha \in K$，使得成立 $K = F(\alpha)$。

定义 4.3.7 (单超越扩张)

称域扩张 K/F 为单超越扩张，如果存在 F 的超越元 $\alpha \in K$，使得成立 $K = F(\alpha)$。

定理 4.3.2 (单代数扩张的结构)

对于域扩张 K/F，如果 $\alpha \in K$ 为 F 的代数元，那么

$$F[x]/(p(x)) \cong F(\alpha)$$

其中 $p(x) \in F[x]$ 为 α 在 $F[x]$ 上的极小多项式。如果令 $n = \deg p(x)$，那么

$$F(\alpha) = \left\{ \sum_{k=0}^{n-1} a_k \alpha^k : a_k \in F \right\}$$

且 $F(\alpha)$ 中元素的多项式表示唯一。

证明 构造满的环同态映射

$$\begin{aligned} \varphi : F[x] &\longrightarrow F[\alpha] \\ f(x) &\longmapsto f(\alpha) \end{aligned}$$

那么

$$\ker \varphi = \{ f(x) \in F[x] : f(\alpha) = 0 \}$$

而 $F[x]$ 为域，进而为主理想整环，那么

$$\ker \varphi = (p(x))$$

其中 $p(x) \in F[x]$ 为 α 在 F 上的极小多项式，从而由环同构第一定理

$$F[x]/\ker \varphi_z \cong \operatorname{im} \varphi_z \iff F[x]/(p(x)) \cong F[\alpha]$$

由于 $p(x)$ 为 $F[x]$ 的不可约多项式，那么 $(p(x))$ 为 $F[x]$ 的极大理想，进而 $F[\alpha]$ 为域。而容易知道 $F(\alpha) \supset F[\alpha]$，因此 $F(\alpha) = F[\alpha]$，进而

$$F[x]/(p(x)) \cong F(\alpha)$$

定理 4.3.3 (单超越扩张的结构)

对于域扩张 K/F，如果 $\alpha \in K$ 为 F 的超越元，那么

$$F[x]\text{的分式域} \cong F(\alpha)$$

证明 构造满的环同态映射

$$\begin{aligned} \varphi : F[x] &\longrightarrow F[\alpha] \\ f(x) &\longmapsto f(\alpha) \end{aligned}$$

由于 α 为 F 的超越元，那么

$$\ker \varphi = \{ f(x) \in F[x] : f(\alpha) = 0 \} = (0)$$

由环同构第一定理

$$F[x]/\ker\varphi_z \cong \operatorname{im}\varphi_z \iff F[x] \cong F[\alpha]$$

而容易知道 $F(\alpha) \supset F[\alpha]$，因此 $F(\alpha)$ 为包含 $F[\alpha]$ 的最小域。由定理3.5.3，$F(\alpha)$ 为 $F[\alpha]$ 的分式域。由定理3.5.4

$$F[x]\text{的分式域} \cong F(\alpha)$$

推论 4.3.1 (有限域的扩张)

对于 p 阶域 F，如果 n 次多项式 $p(x)$ 为 $F(x)$ 上的不可约多项式，那么域 $F[x]/(p(x))$ 的阶为 p^n。♡

4.4 有限扩张与代数扩张

定义 4.4.1 (域扩张的向量空间性)

对于域扩张 K/F，可将 K 看作域 F 上的向量空间，其加法运算为 $+ : K \times K \to K$，数乘运算为 $\cdot : F \times K \to K$。♣

定义 4.4.2 (域扩张的次数)

定义域扩张 K/F 的次数为域 F 上的向量空间 K 的维数，并记作 $[K : F]$。♣

定理 4.4.1

对于有限域的域扩张 K/F，成立

$$[K : F] = \frac{\ln|K|}{\ln|F|}$$

♡

定义 4.4.3 (域扩张的基)

定义域扩张 K/F 的次数为域 F 上的向量空间 K 的基。♣

定义 4.4.4 (有限扩张)

称域扩张 K/F 为有限扩张，如果域 F 上的向量空间 K 为有限维向量空间。♣

定义 4.4.5 (代数扩张)

称域扩张 K/F 为代数扩张，如果对于任意 $\alpha \in K$，α 为域 F 上的代数元。♣

定理 4.4.2 (有限扩张 $\Longrightarrow$ 代数扩张)

有限扩张为代数扩张。♡

证明 对于有限扩张 K/F，记 $[K : F] = n$。任取 $\alpha \in K$，那么 $\{\alpha^k\}_{k=0}^n$ 在 F 上线性相关，因此存在不全为 0 的元素 $\{a_k\}_{k=0}^n \subset F$，使得成立

$$a_0 + a_1\alpha + \cdots a_n\alpha^n = 0$$

令

$$f(x) = a_0 + a_1\alpha + \cdots a_n\alpha^n \in F[x]$$

那么 $f(\alpha) = 0$ 且 $f(x) \neq 0$，因此 α 为 F 上的代数元。由 α 的任意性，域扩张 K/F 为代数扩张。

定理 4.4.3 (单代数扩张的基)

对于域扩张 K/F，如果 $\alpha \in K$ 为 F 上的代数元，且 α 在 $F[x]$ 上的极小多项式的次数为 n，那么

$$[F(\alpha):F]=n$$

且 $\{\alpha^k\}_{k=0}^{n-1}$ 为 $F(\alpha)/F$ 的基。

♡

证明 如果 $\{\alpha^k\}_{k=0}^{n-1}$ 在 F 上线性相关，那么存在不全为 0 的元素 $\{a_k\}_{k=0}^{n-1}\subset F$，使得成立

$$a_0+a_1\alpha+\cdots a_{n-1}\alpha^{n-1}=0$$

令

$$f(x)=a_0+a_1\alpha+\cdots a_{n-1}\alpha^{n-1}\in F[x]$$

那么 $f(\alpha)=0$ 且 $f(x)\neq 0$，这与 α 在 $F[x]$ 上的极小多项式的次数为 n 矛盾！进而 $\{\alpha^k\}_{k=0}^{n-1}$ 在 F 上线性无关。由定理4.3.2，$F(\alpha)=\text{span}\,\{\alpha^k\}_{k=0}^{n-1}$，因此 $[F(\alpha):F]=n$，且 $\{\alpha^k\}_{k=0}^{n-1}$ 为 $F(\alpha)/F$ 的基。

定理 4.4.4 (望远镜定理)

对于域 $F\subset L\subset K$，成立

$$[K:F]<\infty \iff [K:L]<\infty 且 [L:F]<\infty$$

此时成立

$$[K:F]=[K:L][L:F]$$

♡

证明 对于必要性，如果 $[K:F]=n$，那么由于 L 为 K 的子空间，因此 $[L:F]\leq n$。设 $\{\alpha_k\}_{k=1}^{n}$ 为向量空间 K/F 的基，那么对于任意 $\beta\in K$，存在且存在唯一 $\{b_k\}_{k=1}^{n}\subset F$，使得成立

$$\beta=b_1\alpha_1+\cdots+b_n\alpha_n$$

由于 $F\subset L$，那么 $\{b_k\}_{k=1}^{n}\subset L$，从而 $\{\alpha_k\}_{k=1}^{n}$ 为向量空间 K/L 的生成元，因此 $[K:L]\leq n$。

对于充分性，如果 $[K:L]=m$，$[L:F]=n$，且 $\{\beta_k\}_{k=1}^{m}$ 为向量空间 K/L 的基，$\{\gamma_k\}_{k=1}^{n}$ 为向量空间 L/F 的基。对于任意 $\alpha\in K$，存在且存在唯一 $\{a_k\}_{k=1}^{m}\subset L$，且存在且存在唯一 $\{b_{ij}\}_{m\times n}\subset F$，使得成立

$$\alpha=a_1\beta_1+\cdots+a_m\beta_m,\qquad a_i=b_{i1}\gamma_1+\cdots+b_{in}\gamma_n$$

从而

$$\alpha=\sum_{i,j}b_{ij}(\gamma_j\beta_i)$$

由于

$$\{\gamma_j\beta_i:1\leq i\leq m,1\leq j\leq n\}\subset K$$

在 F 上线性无关，那么其为 K/F 的基，因此

$$[K:F]=mn=[K:L][L:F]$$

4.5 分裂域

定义 4.5.1 (分裂域)

对于域扩张 K/F，称域 K 为多项式 $f(x)\in F[x]$ 在 F 上的分裂域，如果 $f(x)$ 在 $K[x]$ 可完全分解为

$$f(x)=a(x-\alpha_1)\cdots(x-\alpha_n),\qquad \alpha_k\in K$$

且

$$K=F(\alpha_1,\cdots,\alpha_n)$$

♣

例题 4.2

- $x^2-1\in\mathbb{R}[x]$ 在 $\mathbb{R}$ 上的分裂域为 $\mathbb{R}$。
- $x^2+1\in\mathbb{R}[x]$ 在 $\mathbb{R}$ 上的分裂域为 $\mathbb{C}$。
- $x^p-1\in\mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上的分裂域为 $\mathbb{Q}(\omega)$，其中 p 为素数，且 $\omega=\mathrm{e}^{i\frac{2\pi}{p}}$。$\omega$ 的极小多项式为

  $$x^{p-1}+\cdots+x+1$$

  因此域扩张 $\mathbb{Q}(\omega)/\mathbb{Q}$ 的扩张次数为 $p-1$。
- $x^3-2\in\mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上的分裂域为 $\mathbb{Q}(\sqrt[3]{2},\omega)$，其中 $\omega=\mathrm{e}^{i\frac{2\pi}{3}}$，域扩张 $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ 的扩张次数为

  $$[\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=2\times3=6$$

定理 4.5.1 (分裂域的存在性)

域 F 的 $n\geq1$ 次多项式 $f(x)\in F[x]$ 在 F 上存在分裂域 K，且

$$[K:F]\leq n!$$

♡

证明 对于多项式 $f(x)\in F[x]$ 的次数 n 作数学归纳。当 $n=1$ 时，$f(x)=a(x-\alpha_1)$，那么 $\alpha_1\in F$，因此 F 为多项式 $f(x)$ 在 F 上存在分裂域，且 $[F:F]=1\leq1!$。

如果当 $n\leq N$ 时，命题得证，那么当 $n=N+1$ 时，任取 $f(x)$ 的不可约因式 $p(x)$，由于 $F[x]/(p(x))$ 为域，那么由定理4.3.2，令 $\alpha_1=x+(p(x))$，可得 $F[x]/(p(x))=F(\alpha_1)$，且 $p(\alpha_1)=0$，从而 $f(\alpha_1)=0$。记 $L=F(\alpha_1)$，那么

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_m)g(x),\qquad \alpha_k\in L$$

其中 $g(x)\in L[x]$。

如果 $\deg g(x)=0$，那么 L 为多项式 $f(x)$ 在 F 上的分裂域，且由定理4.4.3

$$[L:F]=[F(\alpha_1):F]\leq\deg p(x)\leq\deg f(x)=N+1\leq(N+1)!$$

如果 $\deg g(x)\geq1$，那么由于 $\deg g(x)=N+1-m\leq N$，结合归纳假设，$g(x)$ 在 L 上存在分裂域 K，且

$$[K:L]\leq(N+1-m)!\leq N!$$

于是

$$g(x)=c(x-\beta_1)\cdots(x-\beta_{N+1-m})$$

且

$$K=L(\beta_1,\cdots,\beta_{N+1-m})$$

从而

$$f(x)=c(x-\alpha_1)\cdots(x-\alpha_m)(x-\beta_1)\cdots(x-\beta_{N+1-m})$$

且由定理4.3.1

$$K=F(\alpha_1)(\beta_1,\cdots,\beta_{N+1-m})=(\alpha_1,\beta_1,\cdots,\beta_{N+1-m})$$

于是 K 为 $f(x)$ 在 F 上的分裂域，且由望远镜定理4.4.4

$$[K:F]=[K:L][L:F]\leq N!(N+1)=(N+1)!$$

由数学归纳原理，原命题得证！

引理 4.5.1

如果 $\varphi: F \to F'$ 为域同构映射，且 $n \geq 1$ 次多项式

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$$

在 F 上的分裂域为 K，多项式

$$f_\varphi(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n \in F'[x]$$

在 F' 上的分裂域为 K'，那么 φ 可扩张为域同构映射 $K \to K'$。 ♡

证明 对于 $[K:F]$ 作数学归纳法，当 $[K:F]=1$ 时，$K=F$，从而

$$f(x) = a_n(x-\alpha_1)\cdots(x-\alpha_n), \qquad \alpha_k \in F$$

于是

$$f_\varphi(x) = \varphi(a_n)(x-\varphi(\alpha_1))\cdots(x-\varphi(\alpha_n)), \qquad \varphi(\alpha_k) \in F'$$

于是 F' 为 $f_\varphi(x)$ 在 F' 上的分裂域，因此 $K'=F'$，于是 φ 为域同构映射 $F \to F'$。

假设当 $[K:F] < m$ 时，命题成立，其中 $m \geq 2$，那么当 $[K:F]=m$ 时，由 $m \geq 2$ 可知 $f(x)$ 存在 $r \geq 2$ 次不可约因式 $p(x)$。记 α_1 为 $p(x)$ 在 K 上的根，那么由定理4.4.3，$[F(\alpha_1):F] = r > 1$。由于 K 为 $f(x)$ 在 F 上的分裂域，那么

$$f(x) = c(x-\alpha_1)\cdots(x-\alpha_l)(x-\beta_1)\cdots(x-\beta_{n-l}), \qquad \alpha_k \in F(\alpha_1), \beta_k \in K \setminus F(\alpha_1)$$

由定理4.3.1

$$K = F(\alpha_1,\cdots,\alpha_l,\beta_1,\cdots,\beta_{n-l}) = F(\alpha_1,\cdots,\alpha_l)(\beta_1,\cdots,\beta_{n-l}) = F(\alpha_1)(\beta_1,\cdots,\beta_{n-l})$$

因此 K 为 $f(x)$ 在 $F(\alpha_1)$ 上的分裂域。

由于 $p(x)$ 在 $F[x]$ 中不可约，那么 $p_\varphi(x)$ 在 $F'[x]$ 中不可约，且 $\deg p_\varphi(x) = \deg p(x) = r$。记 γ_1 为 $p_\varphi(x)$ 在 K' 中的根，那么同理可知 K' 为 $f_\varphi(x)$ 在 $F'(\gamma_1)$ 上的分裂域。构造映射

$$\begin{aligned} \psi: \quad F(\alpha_1) &\longrightarrow F'(\gamma_1) \\ \sum_{k=0}^{r-1} a_k \alpha_1^k &\longmapsto \sum_{k=0}^{r-1} \varphi(a_k)\gamma_1^k \end{aligned}$$

由定理4.3.1，$\{\alpha_1^k\}_{k=0}^{r-1}$ 为域扩张 $F(\alpha_1)/F$ 的基，且 $\{\gamma_1^k\}_{k=0}^{r-1}$ 为域扩张 $F'(\gamma_1)/F'$ 的基，那么该映射定义良好，且为双射，同时容易知道 ψ 为域同构。由望远镜定理4.4.4

$$m > [K:F] = [K:F(\alpha_1)][F(\alpha_1):F] = r[K:F(\alpha_1)] > [K:F(\alpha_1)]$$

由归纳假设，域同构 $\psi: F(\alpha_1) \to F'(\gamma_1)$，可扩张为域同构 $K \to K'$。由归纳假设原理，命题得证！

定理 4.5.2 (分裂域的唯一性)

如果 K 与 L 均为域 F 的 $n \geq 1$ 次多项式 $f(x) \in F[x]$ 在 F 上的分裂域，那么 $K \cong L$，且存在域同构映射 $\varphi: K \to L$，使得成立 $\varphi|_F = \mathbb{1}$。 ♡

证明 由引理4.5.1，取 $F'=F$，且 $\varphi = \mathbb{1}$，那么 φ 可扩张为域同构映射 $K \to L$，因此 $K \cong L$。

4.6 Galois 域

定义 4.6.1 (Galois 域)

对于素数 p，定义 p^n 阶域为 Galois 域，记作 $\mathrm{GF}(p^n)$。

定理 4.6.1 (有限域为 Galois 域)

对于有限域 F，其素域为 P，令 $\mathrm{char}\, F = p$，且 $[F:P] = n$，那么 $|F| = p^n$。

证明 将 F 看作 P 上的向量空间，由于 $[F:P] = n$，那么 $\{\alpha_k\}_{k=1}^n \subset F$ 为 P 上的向量空间 F 的基，那么

$$F = \{a_1\alpha_1 + \cdots + a_n\alpha_n : a_k \in P\}$$

因此 $|F| = p^n$。

定理 4.6.2 (Galois 域的存在性)

对于素数 p，存在 Galois 域 $\mathrm{GF}(p^n)$。

证明 由定理4.5.1，多项式 $x^{p^n} - x \in \mathbb{Z}_p[x]$ 在 $\mathbb{Z}_p$ 上存在分裂域 K，那么 $x^{p^n} - x$ 在 K 上存在且仅存在 p^n 个互异根 $A = \{\alpha_k\}_{k=1}^{p^n}$，因此 $K = \mathbb{Z}_p(A)$。由于在 $\mathbb{Z}_p[x]$ 中，成立

$$(\alpha_i - \alpha_j)^{p^n} = \alpha_i^{p^n} - \alpha_j^{p^n} = \alpha_i - \alpha_j \implies \alpha_i - \alpha_j \in A$$
$$(\alpha_i\alpha_j^{-1})^{p^n} = \alpha_i^{p^n}(\alpha_j^{p^n})^{-1} = \alpha_i\alpha_j^{-1}\alpha_i\alpha_j^{-1} \in A$$

因此 A 为域。容易知道 $\overline{1} \in A$，那么 $\mathbb{Z}_p \subset A$，因此 $K = A$，进而存在 Galois 域 $\mathrm{GF}(p^n)$ 为多项式 $x^{p^n} - x \in \mathbb{Z}_p[x]$ 在 $\mathbb{Z}_p$ 上的分裂域 K，亦为多项式 $x^{p^n} - x$ 在 K 上的 p^n 个互异根 $A = \{\alpha_k\}_{k=1}^{p^n}$。

定理 4.6.3 (Galois 域的唯一性)

对于素数 p，Galois 域 $\mathrm{GF}(p^n)$ 同构于多项式 $x^{p^n} - x \in \mathbb{Z}_p[x]$ 在 $\mathbb{Z}_p$ 上的分裂域。

证明 对于 p^n 阶域 F，其素域为

$$P = \{k1 : 0 \le k < p\} \cong \mathbb{Z}_p$$

由于 $F \setminus \{0\} \cong \mathbb{Z}_{p^n-1}$，那么对于任意 $\alpha \in F \setminus \{0\}$，成立 $\alpha^{p^n-1} = 1$，从而 $\alpha^{p^n} - \alpha = 0$，因此 F 中的元素均为多项式 $x^{p^n} - x \in P[x]$ 在 F 中的根，进而 F 同构于多项式 $x^{p^n} - x \in \mathbb{Z}_p[x]$ 在 $\mathbb{Z}_p$ 上的分裂域。

定义 4.6.2 (正规扩张)

称代数扩张 K/F 为正规扩张，如果 $F[x]$ 的在 K 中存在根的不可约多项式在 $K[x]$ 中完全分解为一次因式的积。

定理 4.6.4

对于有限扩张 K/F，成立

$$K/F\text{为正规扩张} \iff \text{存在}f(x) \in F[x], \text{使得}K\text{为}f(x)\text{在}F\text{上的分裂域}$$

4.7 Galois 群

定义 4.7.1 (F-同态映射)

对于域扩张 K/F 与 L/F，称域同态映射 $\varphi: K \to L$ 为 F-同态映射，如果 $\varphi|_F = \mathbb{1}$。

定义 4.7.2 (F-同构映射)

对于域扩张 K/F 与 L/F，称域同构映射 $\varphi: K \to L$ 为 F-同构映射，如果 $\varphi|_F = \mathbb{1}$。

定义 4.7.3 (F-自同构映射)

对于域扩张 K/F，称域同构映射 $\varphi: K \to K$ 为 F-自同构映射，如果 $\varphi|_F = \mathbb{1}$。

定义 4.7.4 (Galois 群)

对于域扩张 K/F，称域 K 的 F-自同构映射全体对于映射复合运算构成的群为域 K 在域 F 上的 Galois 群，记作 $\mathrm{Gal}(K/F)$。

引理 4.7.1

对于域扩张 K/F 与 K'/F'，$\varphi: F \to F'$ 为域同构映射，$\alpha \in K$ 为 F 上的代数元，其在 F 上的极小多项式为

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in F[x]$$

令

$$f_\varphi(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_{n-1})x^{n-1} + x^n \in F'[x]$$

成立

$$\varphi\text{可扩张为单的域同态映射}F(\alpha) \to K' \iff f_\varphi(x)\text{在}K'\text{存在根}$$

此时 φ 的扩张数目为 $f_\varphi(x)$ 在 K' 中的不同根的数目。

定理 4.7.1

如果 $\varphi: F \to F'$ 为域同构映射，且 $n \geq 1$ 次多项式

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$$

在 F 上的分裂域为 K，多项式

$$f_\varphi(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n \in F'[x]$$

在 F' 上的分裂域为 K'，那么 φ 可扩张为域同构映射 $K \to K'$，且 φ 的扩张数目 $\leq [K:F]$，同时当 $f_\varphi(x)$ 在 K' 中的存在且仅存在单根时等号成立。

定义 4.7.5 (可分不可约多项式)

对于域 F，称 F 上的不可约多项式 $p(x) \in F[x]$ 为可分的，如果 $p(x)$ 在其分裂域中存在且仅存在单根。

定义 4.7.6 (可分多项式)

对于域 F，称 F 上的非常数项多项式 $f(x) \in F[x]$ 为可分的，如果其不可约因式为可分的。

定义 4.7.7 (可分代数元)

对于域扩张 K/F，称 F 上的代数元 $\alpha \in K$ 为可分的，如果 α 在 F 上的极小多项式为可分的。 ♣

定义 4.7.8 (可分扩张)

称域扩张 K/F 为可分扩张，如果对于任意 $\alpha \in K$，α 为可分的。 ♣

定理 4.7.2

如果域 K 为可分多项式 $f(x) \in F[x]$ 在域 F 上的分裂域，那么

$$|\mathrm{Gal}(K/F)| = [K : F]$$

♡

证明 设 $f(x)$ 在 $F[x]$ 中的标准分解式为

$$f(x) = a p_1^{r_1}(x) \cdots p_n^{r_n}(x)$$

其中 $p_1(x), \cdots, p_n(x) \in F[x]$ 为 F 上的互异首一不可约多项式。令

$$f_0(x) = a p_1(x) \cdots p_n(x)$$

那么 K 为 $f_0(x) \in F[x]$ 在 F 上的分裂域。由于 $f(x)$ 在 F 上可分，那么每一个 $p_k(x)$ 在 F 上可分，因此 $f_0(x)$ 在 K 中的根均互异。由定理4.7.1，域同构映射 $\mathbb{1} : F \to F$ 的扩张为域同构映射 $\varphi : K \to K$ 的数目为 $[K : F]$，即 K 的 F-自同构映射数目为 $[K : F]$，进而 K 的每一个的 F-自同构映射均由域同构映射 $\mathbb{1} : F \to F$ 扩张而成，从而

$$|\mathrm{Gal}(K/F)| = [K : F]$$

定理 4.7.3 (有限域的 Galois 群)

对于素数 p，成立

$$\mathrm{Gal}(\mathrm{GF}(p^n)/\mathrm{GF}(p)) \cong \mathbb{Z}_n$$

♡

证明 由定理4.6.2与4.6.3，Galois 域 $\mathrm{GF}(p^n)$ 同构于多项式 $x^{p^n} - x \in \mathbb{Z}_p[x]$ 在 $\mathbb{Z}_p$ 上的分裂域，且 $x^{p^n} - x$ 在 $\mathrm{GF}(p^n)$ 上存在且仅存在 p^n 个互异根。由定理4.8.2，$\mathrm{GF}(p^n)/\mathrm{GF}(p)$ 为 Galois 扩张。由推论4.8.1与定理4.4.1

$$|\mathrm{GF}(p^n)/\mathrm{GF}(p)| = [\mathrm{GF}(p^n) : \mathrm{GF}(p)] = n$$

定义映射

$$\begin{aligned} \varphi_p : \mathrm{GF}(p^n) &\longrightarrow \mathrm{GF}(p^n) \\ \alpha &\longmapsto \alpha^n \end{aligned}$$

由于

$$\varphi_p(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \varphi_p(\alpha) + \varphi_p(\beta)$$

$$\varphi_p(\alpha\beta) = (\alpha\beta)^p = \alpha^p \beta^p = \varphi_p(\alpha)\varphi_p(\beta)$$

那么 φ_p 为域自同态映射。由于 $\ker \varphi_p$ 为域 $\mathrm{GF}(p^n)$ 的理想，而域为主理想整环，因此 $\ker \varphi_p = (0)$，因此 φ_p 为单射。而域 $\mathrm{GF}(p^n)$ 为有限域，因此 φ_p 为满射，进而 φ_p 为域自同构映射。由于对于任意 $\alpha \in \mathrm{GF}(p)$，成立

$$\varphi_p(\alpha) = \alpha^p = \alpha$$

因此 $\varphi_p|_{\mathrm{GF}(p)} = \mathbb{1}$，进而 φ_p 为 $\mathrm{GF}(p)$-自同构映射，从而 $\varphi_p \in \mathrm{GF}(p^n)/\mathrm{GF}(p)$。容易知道 φ_p 的阶为 n，那么

$$\mathrm{Gal}(\mathrm{GF}(p^n)/\mathrm{GF}(p)) = \langle \varphi_p \rangle \cong \mathbb{Z}_n$$

110

4.8 Galois 扩张

定义 4.8.1 (G-不动域)

定义域 F 关于自同构映射群 G 的 G-不动域为

$$\mathrm{Inv}_F(G)=\{\alpha\in F:\varphi(\alpha)=\alpha,\forall\varphi\in G\}$$

♣

定理 4.8.1 (Artin 引理)

对于域 F 的有限自同构映射群 G，成立

$$[F:\mathrm{Inv}_F(G)]\leq|G|$$

♡

定义 4.8.2 (Galois 扩张)

称域扩张 K/F 为 Galois 扩张，如果 $\mathrm{Inv}_K(\mathrm{Gal}(K/F))=F$。

♣

定理 4.8.2

对于域扩张 K/F，如下命题等价。

1. K/F 为有限可分正规扩张。
2. K 为可分多项式 $f(x)\in F[x]$ 在 F 上的分裂域。
3. K/F 为有限 Galois 扩张。

♡

推论 4.8.1

如果域扩张 K/F 为有限 Galois 扩张，那么

$$|\mathrm{Gal}(K/F)|=[K:F]$$

♡

证明 由定理4.8.2与4.7.2，命题得证！

推论 4.8.2

如果域扩张 K/F 为有限 Galois 扩张，那么对于任意 $\alpha\in K$，α 在 F 上的极小多项式 $p(x)\in F[x]$ 为可分的，且 $p(x)$ 在 K 中的全部根为

$$A=\{\varphi(\alpha):\varphi\in\mathrm{Gal}(K/F)\}$$

进而由于 $F(A)$ 为 $p(x)$ 在 F 上的分裂域，于是 $F(A)/F$ 为有限 Galois 扩张，且存在 $G<S_A$，使得成立 $\mathrm{Gal}(F(A)/F)\cong G$。

♡

证明 由定理4.8.2，对于任意 $\alpha\in K$，α 在 F 上的极小多项式 $p(x)\in F[x]$ 为可分的，且 $p(x)$ 在 K 中的全部根为

$$A=\{\varphi(\alpha):\varphi\in\mathrm{Gal}(K/F)\}$$

同理，对于域扩张 $F(A)/F$，可知对于任意 $\varphi\in\mathrm{Gal}(F(A)/F)$，成立 $\varphi(A)=A$，因此 φ 诱导置换

$$\begin{aligned}\pi_\varphi:A&\longrightarrow A\\ \alpha&\longmapsto\varphi(\alpha)\end{aligned}$$

令

$$\begin{aligned}\Psi:\mathrm{Gal}(F(A)/F)&\longrightarrow S_A\\ \varphi&\longmapsto\pi_\varphi\end{aligned}$$

由于

$$\pi_{\varphi\psi}(\alpha)=(\varphi\psi)(\alpha)=\varphi(\psi(\alpha))=\varphi(\pi_\psi(\alpha))=\pi_\varphi(\pi_\psi(\alpha))=(\pi_\varphi\pi_\psi)(\alpha),\qquad\forall\alpha\in A$$

因此 $\Psi(\varphi\psi)=\Psi(\varphi)\Psi(\psi)$，于是 Ψ 为群同态映射。容易知道 Ψ 为单的，那么由群同构定理

$$\mathrm{Gal}(F(A)/F)\cong \mathrm{im}\ \Psi$$

命题 4.8.1

如果域 F 存在有限自同构群 G，那么 $F/\mathrm{Inv}_F(G)$ 为有限 Galois 扩张，且 $\mathrm{Gal}(F/\mathrm{Inv}_F(G))=G$。

命题 4.8.2

对于域 $F\subset L\subset K$，如果 K/F 为有限 Galois 扩张，那么 K/L 为有限 Galois 扩张，且

$$\mathrm{Gal}(K/L)<\mathrm{Gal}(K/F),\qquad \mathrm{Inv}_K(\mathrm{Gal}(K/L))=L$$

4.9 Galois 基本定理

定理 4.9.1 (Galois 基本定理)

对于有限 Galois 扩张 K/F，成立如下命题

1. 存在双射

$$\begin{aligned}\varphi:\{\text{域}L:K\subset L\subset F\}&\longrightarrow\{\text{群}G:G\subset\mathrm{Gal}(K/F)\}\\ L&\longmapsto\mathrm{Gal}(K/L)\end{aligned}$$

其逆映射为

$$\begin{aligned}\varphi^{-1}:\{\text{群}G:G\subset\mathrm{Gal}(K/F)\}&\longrightarrow\{\text{域}L:K\subset L\subset F\}\\ G&\longmapsto\mathrm{Inv}_K(G)\end{aligned}$$

2. $$\mathrm{Inv}_K(\mathrm{Gal}(K/L))=L,\qquad \mathrm{Gal}(K/\mathrm{Inv}_K(G))=G$$

3. $$E\subset F\iff \mathrm{Gal}(K/E)\supset\mathrm{Gal}(K/F)$$

4. $$|\mathrm{Gal}(K/\mathrm{Inv}_K(G))|=[K:\mathrm{Inv}_K(G)],\qquad [\mathrm{Gal}(K/F):G]=[\mathrm{Inv}_K(G):F]$$

5. $$\varphi^{-1}(G)=L\implies \varphi^{-1}(\sigma G\sigma^{-1})=\sigma(L),\forall\sigma\in G$$

6. $$G\lhd\mathrm{Gal}(K/F)\iff \mathrm{Inv}_K(G)\text{为}F\text{上的正规扩张}$$

此时

$$\mathrm{Gal}(\mathrm{Inv}_K(G)/F)\cong\mathrm{Gal}(K/F)/G$$

定理 4.9.2

对于域 F 上的 n 次多项式

$$f(x)=x^n-a_1x^{n-1}+a_2x^{n-2}-\cdots+(-1)^na_n\in F(a_1,\cdots,a_n)[x]$$

如果 $f(x)$ 在 $F(a_1,\cdots,a_n)$ 上的分裂域为 K，那么 $f(x)$ 在 K 中存在且仅存在 n 个互异根，且

$$\mathrm{Gal}(K/F(a_1,\cdots,a_n))\cong S_n$$

定理 4.9.3 (方程根式可解的判别准则)

对于无限域 F 上的多项式 $f(x) \in F[x]$，成立

$$\text{方程} f(x) = 0 \text{根式可解} \iff f(x) \text{的分裂域的 Galois 群可解}$$

♡

定理 4.9.4 (Abel-Ruffini 定理)

对于无限域 F 上的 n 次方程

$$x^n - a_1 x^{n-1} + a_2 x^{n-2} - \cdots + (-1)^n a_n = 0$$

当且仅当 $n \geq 5$ 时不为根式可解。

♡