

第一章. 群论基础.

§1.1. 集合论回顾

$\subseteq, \subset, \emptyset, \neq, \cap, \cup, \sqcup$ (无交并)

U. 有限. $A_1, \dots, A_n \subseteq U$. 则 $|\bigcup_{i=1}^n A_i| = \sum_{r=1}^n (-1)^{r-1} \sum_{\{i_1, \dots, i_r\} \subseteq \{1, \dots, n\}} |A_{i_1} \cap \dots \cap A_{i_r}|$

笛卡尔积 $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

映射. $f: A \rightarrow B \quad a \mapsto f(a)$

$f^{-1}(b) = \{a \in A \mid f(a) = b\}$, $f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\}$.

单射. 满射. 双射.

映射的复合.

$$\text{map}(I, A) = \prod_{i \in I} A_i = A^I$$

$f: \underbrace{A \times A \times \dots \times A}_{n \text{ 个}} \rightarrow A$ 称为 A 上的一个 n 元运算.

若 $f(f(a, b), c) = f(a, f(b, c)) \quad \forall a, b, c$ 则称 f 满足结合律.

$$\begin{array}{ccc} A \times A \times A & \xrightarrow{\text{id} \times f} & A \times A \\ f \circ \text{id} \downarrow & & \downarrow f \\ A \times A & \xrightarrow{f} & A \end{array}$$

$$\Sigma(A) = \text{Map}(A, A), \quad A \xrightarrow{f} A \xrightarrow{g} A$$

$$\circ: \Sigma(A) \times \Sigma(A) \rightarrow \Sigma(A).$$

等价关系

定义 1.4. A 集合. A 上的关系 R 是指 $A \times A$ 的一个子集. $(a, b) \in R$ 则称 a 和 b 有关系 R . 也记作 aRb .

等价关系. 若

- (1) $(a, a) \in R$ (自反性).
- (2) $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$ (传递性).
- (3) $(a, b) \in R \Rightarrow (b, a) \in R$ (对称性).

用 $\sim$ 表示等价关系.

$$[a] \sim \quad [a] = \{b \mid b \sim a\}.$$

$$[a] \cap [b] = \begin{cases} \emptyset \\ [a] \end{cases} \quad A \text{ 可以拆分成一些子集 } [a] \text{ 的无交并}$$

在每个等价类中取出一个代表元. 形成的 A 的子集称为 A 在 $\sim$ 下的一个完全代表元系.

定理 1.5 集合 A 的拆分与 A 上的等价关系 $\sim$ 一一对应.

$A/\sim = \{[a], 1 a \in A\}$ 与任一完全代表元系 $\sim$ 一一对应.

§1.2. 群的基本概念与例子.

定义 2.1. $\phi \neq G$ 为非空集合, $\cdot$ 为 G 上的二元运算.

(1) 若 $\cdot$ 满足结合律, 称 G 是一个半群.

(2) 若存在 $e \in G$, 使得 $e \cdot a = a \cdot e = a \quad \forall a$, 则称 e 为半群 $(G, \cdot)$ 的单位元 (么元).

(3) $(G, \cdot)$ 为含么半群, $g \in G$, 若存在 $h \in G$ 使 $g \cdot h = h \cdot g = e$ 称 h 是 g 的一个逆元. 若 G 中任一元素都可逆, 则称 G 为一个群.

引理 2.2

(1) 半群 $(G, \cdot)$ 中的么元如果存在一定唯一.

(2) 含么半群中元素 g 的逆元如果存在, 一定唯一.

证. (1) 设 e, e' 两个么元

$$e \cdot e' = e = e'$$

$$(2) \quad gh = hg = e \quad hgh' = h = h'$$

$$gh' = h'g = e$$

G 么半群, $G^* = \{g \in G \mid g \text{ 可逆}\}$ G^* 是群.

例 $GL_n(\mathbb{C}) \quad S' = \{g \in G \mid |g| = 1\}$.

$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} \quad n \text{ 为素数} \quad \mathbb{Z}/n\mathbb{Z}^*$ 为群.

$S_n = \{1, 2, \dots, n\}$ 的置换的全体 $(\sigma: 1, \dots, n \rightarrow 1, \dots, n \text{ 双射})$

$An \leq S_n$ 偶置换 iR^2 上所有保持长度运动.

命题 2.2 设 M 为含么半群, 则 $M^* = \{a \in M \mid a \text{ 可逆}\}$ 在 M 乘法下构成群.
 例. $(M_n(\mathbb{C}), \cdot)$ 含么半群. $M_n(\mathbb{C})^* = GL_n(\mathbb{C})$ 一般线性群.

$\Sigma(X) = \text{Map}(X, X)$ $(\Sigma(X), \cdot)$ 么半群. $\Sigma(X)^*$ 群. X 的置换群.

定义 2.4. 元素个数有限的群称为有限群. 元素的个数称为群的阶.
 无限的称为无限群.

定义 2.5. 群 G 上的运算满足交换律. $gh = hg \quad \forall g, h \in G$ 则称 G 为交换群. (运算有时记为 $+$)

定义 2.6. 设 G 为群 $\phi \neq H \subseteq G$ 且 H 在 G 的乘法下形成群. 则称 H 为 G 的一个子群. 记作 $H \leq G$.

命题 2.3 $\phi \neq H \subseteq G$ 则下列命题等价

- (1) $H \leq G$
- (2) (a) $1_G \in H$ (b) $\forall h_1, h_2 \in H, h_1 h_2 \in H$ (c) $h^{-1} \in H, \forall h \in H$.
- (3) $h_1 h_2^{-1} \in H, \forall h_1, h_2 \in H$.

典型群:

$GL_n(\mathbb{C}) \quad \mathbb{R}, \mathbb{Q}$

(1) $SL_n(\mathbb{C}) = \{A \in GL_n(\mathbb{C}) \mid \det A = 1\}$ 特殊线

(2) 取 $X \in GL_n(\mathbb{F})$ 非称

$$G_X = \{A \in GL_n(\mathbb{F}) \mid A^T X A = X\} \leq GL_n(\mathbb{F})$$

注 $\mathbb{F} = \mathbb{R}, X = I_n, A^T A = I_n \Rightarrow O_n$

$$SO_n = O_n \cap SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$$

$X = \begin{pmatrix} & I_n \\ -I_n & \end{pmatrix} \quad \mathbb{F} = \mathbb{R}, G_X = Sp_n$ 辛群. symplectic.

$I_p, q \triangleq X = \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix} \quad G_X = O_{p,q}$ 伪正交群.

No.

Date. / /

$$F = \mathbb{C}, X = I_n, G_X = \{ A \in GL_n(\mathbb{C}) \mid \bar{A}^T X A = X \}$$

U_n 酉群, SU_n 特殊酉群.

$$\text{例 } SO_2 = \left\{ \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \right\} \quad O_2 = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix} \right\}$$

$$Sp_2 = SL_2(\mathbb{R}) \quad U(1) = S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \} \quad SU(1) = \{1\}$$

$$SU(2) = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid |\alpha|^2 + |\beta|^2 = 1 \right\} = S^3$$

$$\phi * A \subseteq G.$$

$$\text{令 } G_A \triangleq \{ g \in G \mid gA = A \}. \quad \exists 1_G.$$

$$\text{则 } G_A \leq G.$$

$$1_G \in G. \quad h_1, h_2 \in G_A \Rightarrow h_1 h_2 \in G_A \quad (h_1 h_2 A = h_1 (h_2 A) = h_1 A = A).$$

例 $\phi * A \subseteq G, |A| = n < \infty$, 则下列描述等价.

$$(i) \quad A \leq G$$

$$(ii) \quad G_A = A$$

$$(iii) \quad 1 \in A \quad \text{且 } |G_A| = n.$$

$$(iii) \Rightarrow (ii): \quad 1 \in A \Rightarrow gA = A \Rightarrow g \cdot 1 \in A \Rightarrow G_A \subseteq A$$

定义 2.8 群 G 到 H 的映射 $f: G \rightarrow H$ 称为一个群同态. 若 $f(g_1 g_2) = f(g_1) f(g_2)$
 $\forall g_1, g_2 \in G$. 单同态 满同态 同构

引理 2.9. $f: G \rightarrow H$ 为同态, 则

$$(1) \quad f(1_G) = 1_H$$

$$(2) \quad f(g^{-1}) = f(g)^{-1}$$

注. 半群不一定能把么元映到么元 $\mathbb{R} \rightarrow M_2(\mathbb{R}) \quad x \mapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$

M_1, M_2 为么半群 $f: M_1 \rightarrow M_2$ 为么半群同态. 若

$$(1) \quad f(ab) = f(a)f(b) \quad \forall a, b \quad (2) \quad f(1_{M_1}) = 1_{M_2}$$

例 11. $H \leq G$. 1. $H \hookrightarrow G$. 嵌入. 群的单同态.

(2) $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ $i \mapsto \bar{i}$ 满同态.

(3) $f: \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mu_n = \{ \zeta \in \mathbb{C} \mid \zeta^n = 1 \}$ $\bar{k} \mapsto e^{\frac{2\pi i k}{n}}$

(4) $\det: GL_n(F) \rightarrow F^*$

(5) $f: S_n \rightarrow GL_n(F)$ $\sigma: (\sigma(1) \dots \sigma(n)) \mapsto E_{\sigma(1),1} + \dots + E_{\sigma(n),n}$

(6) $S^1 = U(1) \xrightarrow{\sim} SO_2(\mathbb{R})$ $e^{i\theta} \mapsto \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$

(7) $\exp: \mathbb{R} \rightarrow S^1$ $\theta \mapsto e^{i\theta}$

(8) $\exp: \mathbb{R} \xrightarrow{\sim} \mathbb{R}^+$ $x \mapsto e^x$

(9) $f: \mathbb{R}^+ \times S^1 \xrightarrow{\sim} \mathbb{C}$ $(r, \theta) \mapsto re^{i\theta}$

定义 2.10. 群 G 到自身的同构称为 G 的一个自同构 (Automorphism)

命题 2.11. (1) G 的所有自同构在映射的复合下形成群. $\text{Aut}(G)$

(2) $\varphi: G \xrightarrow{\sim} H$. 则 G 到 H 的群同构的全体为 $\varphi \cdot \text{Aut}(G) = \{ \varphi \cdot f \mid f \in \text{Aut}(G) \}$

$= \text{Aut}(H) \cdot \varphi$.

proof (1). $|\text{Aut}(G)| = \text{Id}_G$.

$f \in \text{Aut}(G)$ 说明 $f^{-1}(g_1) f^{-1}(g_2) = f^{-1}(g_1 g_2)$

$\Leftrightarrow f(f^{-1}(g_1) f^{-1}(g_2)) = f(f^{-1}(g_1 g_2))$ 成立.

(2). $\varphi: G \xrightarrow{\sim} H \xrightarrow{\sim} G$

$\varphi_1 = (\varphi \circ \varphi^{-1}) \varphi_1 = \varphi(\varphi^{-1} \varphi_1)$ 自同构

例. $\text{Aut}(\mathbb{Z}, +) = \{ \pm 1 \} = \mathbb{Z}^*$

$\text{Aut}(\mathbb{Q}, +) = \mathbb{Q}^*$

$\text{Aut}(\mathbb{Z}/n\mathbb{Z}, +)$ $\varphi_n: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ $\bar{i} \mapsto \bar{a}$ φ_n 为同构 $\Leftrightarrow (a, n) = 1$
 $= (\mathbb{Z}/n\mathbb{Z})^*$

例 $f: G \rightarrow G$
 $a \mapsto a^2$ $\Rightarrow$ Abelian 群是同态

§ 13. 陪集分解

定义 3.1. $g \in G$. 若存在一个正整数 n 使 $g^n = 1$. 则称 g 为有限阶元. 满足上述性质的最小的正整数记为 g 的阶, 记为 $\text{ord}(g)$

G 中有唯一的 1 阶元 1_G

命题 3.2 设 $g, h \in G$ $\text{ord}(g) = m$ $\text{ord}(h) = n$.

$$(1) \text{ord}(g^k) = \frac{m}{(m, k)}$$

$$(2) \text{若 } gh = hg \text{ } (m, n) = 1, \text{ 则 } \text{ord}(gh) = m \cdot n$$

proof. (1) 令 $r = \text{ord}(g^k)$

$$(g^k)^{\frac{m}{(k, m)}} = (g^m)^{\frac{k}{(k, m)}} = 1_G \Rightarrow r \mid \frac{m}{(k, m)}$$

$$g^{kr} = (g^k)^r = 1_G \Rightarrow m \mid kr \Rightarrow \frac{m}{(k, m)} \mid \frac{k}{(k, m)} \cdot r$$

$$\text{又 } (\frac{m}{(k, m)}, \frac{k}{(k, m)}) = 1 \Rightarrow \frac{m}{(k, m)} \mid r$$

$$\Rightarrow r = \frac{m}{(m, k)}$$

$$(2) \text{ 令 } \text{ord}(gh) = S$$

$$(gh)^{m \cdot n} = g^{mn} h^{mn} = 1_G \Rightarrow S \mid m \cdot n$$

$$(gh)^S = 1_G \Rightarrow (gh)^{S \cdot n} = 1_G \Rightarrow g^{S \cdot n} = 1_G \Rightarrow m \mid S \cdot n$$

$$\text{又 } (m, n) = 1 \Rightarrow m \mid S \quad \text{同理 } n \mid S$$

$$\text{由 } (m, n) = 1 \Rightarrow mn \mid S$$

$$\Rightarrow mn = S$$

注. $gh = hg$

$\Rightarrow \text{ord}(gh) \mid [\text{ord}(g), \text{ord}(h)]$ 一般来说不等

定义 3.3. $S \subseteq G$. G 中包含 S 的最小的一个子群称为 S 的生成子群. 记作 $\langle S \rangle$. 若 $G = \langle S \rangle$ 则称 S 为 G 的一组生成元.

可以由 1 个元素生成的群称为循环群.

$$\text{注 } \langle S \rangle = \bigcap_{S \subseteq H \leq G} H = \{ g_1^{n_1} g_2^{n_2} \dots g_s^{n_s} \mid g_i \in S \quad S = \pm 1 \}$$

$$\text{例 } G = SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{matrix} ad-bc=1 \\ a, b, c, d \in \mathbb{Z} \end{matrix} \right\} = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \rangle$$

$$G = (\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$$

$$\langle m, n \rangle = \langle (m, n) \rangle \quad m, n \in \mathbb{Z}$$

$$G = GL_n(\mathbb{F}) \quad \mathbb{F} \text{ 域}$$

$$= \langle T_{ij}(a), P_{ij}, D_i(\lambda) \mid \lambda \neq 0 \rangle$$

$$= \langle T_{12}(a), P_{ij}, D_i(\lambda) \mid \lambda \neq 0 \rangle$$

$$G = SL_2(\mathbb{Z}/n\mathbb{Z}) = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \rangle$$

引理 3.4. 设 g 有限阶元 则 $\text{ord}(g) = |\langle g \rangle|$

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

定理 3.5. 设 $G = \langle g \rangle$ 为循环群,

$$\text{则 (1) } |G| = \infty \Rightarrow G \cong \mathbb{Z}$$

$$(2) |G| = n \Rightarrow G \cong \mathbb{Z}/n\mathbb{Z}$$

$$\text{proof. (1) } |G| = \infty \quad |G| = \{g^i \mid i \in \mathbb{Z}\}$$

$$\Rightarrow g^i \neq g^j \quad \forall i \neq j$$

$$f: \mathbb{Z} \rightarrow G \quad i \mapsto g^i \quad \text{则 } f \text{ 为同构}$$

$$(2) |G| = n.$$

$$f: \mathbb{Z}/n\mathbb{Z} \rightarrow G \quad \bar{i} \mapsto g^i$$

命题 3.6. $G = \langle g \rangle$ 循环群

则 (1) $G \cong \mathbb{Z}$ 则 G 的生成元为 g 或 g^{-1}

(2) $G \cong \mathbb{Z}/n\mathbb{Z}$ 则 G 的生成元为 g^d ($d, n = 1$)

定义 3.7. $a \in G, H \leq G$

$aH = \{ ah \mid h \in H \}$ 称为群 G 对于子群 H 的一个左陪集

$Ha \dots$ 右陪集

No.

Date. / /

引理 3.8 (1). $\forall a, b \in G$. $aH = bH$ 或 $aH \cap bH = \emptyset$. 且 $aH = bH \Leftrightarrow b^{-1}a \in H$ ($a^{-1}b \in H$)

(2). $\forall a, b \in G$. $Ha = Hb$ 或 $Ha \cap Hb = \emptyset$. 且 $Ha = Hb \Leftrightarrow ba^{-1} \in H$

证明 (1) 假设 $aH \cap bH \neq \emptyset$. 要证 $aH = bH$.

此时 $\exists x \in aH$. $x \in bH$. $x = ah_1$ $x = bh_2$ $h_1 \in H$. $h_2 \in H$.

$$\Rightarrow b^{-1}a = h_2h_1^{-1} \in H.$$

$ah = b(b^{-1}ah) \in bH$ 即 $aH \subseteq bH$. 同理 $bH \subseteq aH \Rightarrow bH = aH$.

注 G 可写为若干个左(右)陪集的不交并

$$G = \bigcup_{a \in S} aH \quad S \text{ 为左陪集的一个完全代表元系,}$$

$a \sim b \Leftrightarrow aH = bH$. 为等价关系, 等价类即为左陪集

定义 3.9. 称 $S \subseteq G$. 为 G 对于子群 H 的一个左陪集完全代表元系. 若 $G = \bigcup_{a \in S} aH$

引理 3.10 S 为 G 对于子群 H 的一个左陪集完全代表元系, 则 $S^{-1} = \{s^{-1} \mid s \in S\}$ 为...右...

$$\text{证 } s_1, s_2 \in S. \quad Hs_1^{-1} \cap Hs_2^{-1} \neq \emptyset \Leftrightarrow S_1^{-1} = S_2^{-1} \Leftrightarrow S_1 = S_2$$

$$Hs_1^{-1} \cap Hs_2^{-1} \neq \emptyset \Leftrightarrow (Hs_1^{-1})^{-1} \cap (Hs_2^{-1})^{-1} \neq \emptyset \Leftrightarrow s_1H \cap s_2H \neq \emptyset \Leftrightarrow S_1 = S_2$$

$$\forall g \in G. \Rightarrow \exists! s \in S \text{ 使 } g^{-1} \in sH$$

$$\Rightarrow g \in Hs^{-1}$$

定义 3.10. G 对于子群 H 的左(右)陪集的个数称作 G 对于子群 H 的指数 (index) 记作 $[G:H]$

定理 3.12 $1 \leq |G| < \infty$ $H \leq G$. 则 $|G| = |H| \cdot [G:H]$ (Lagrange

推论 3.13. $|G| < \infty$. $\forall g \in G$ $\text{ord}(g) \mid |G|$ $g^{|G|} = 1_G$

推论 3.14. 素数阶群必为循环群.

推论 3.15 (Fermat's 定理). 设 p 为素数 $a \in \mathbb{Z}$ ($a, p = 1$).

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

proof $(\mathbb{Z}/p\mathbb{Z})^\times$ 为 $p-1$ 阶群 $\therefore$

注 $(\mathbb{Z}/n\mathbb{Z})^\times$ n 正整数

($a, n = 1$) $\Leftrightarrow a$ 在 $\mathbb{Z}/n\mathbb{Z}$ 中可逆

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n) \rightarrow \text{欧拉函数}$$

命题 3.16. 有限非阿贝尔群阶最小为 6

$|G| = 2, 3, 5$ 循环群 $\Rightarrow$ 交换

$|G| = 4$. G 含有 4 阶元 $\Rightarrow$ 循环群.

G 中元素阶为 2

$$(ab)^2 = 1$$

"

$$abab = aabb \Rightarrow ab = ba$$

命题 3.17. 设 $G = \langle g \rangle$, $|G| = n$. 则 G 的任一子群都是循环群. 且对 $\forall d | n$
 $d \geq 1$, $\exists$ 唯一 d 阶子群. $G_d = \{1, g^{\frac{n}{d}}, g^{\frac{2n}{d}}, \dots, g^{\frac{(d-1)n}{d}}\} = \{x \in G \mid x^d = 1\}$

推论 3.18. 对 $\forall n \in \mathbb{Z}_+$, $n = \sum_{d|n} \varphi(d)$

proof. $\mathbb{Z}/n\mathbb{Z}$ 中的 d 阶元个数恰好为 $\varphi(d)$ 个.

恰为 $\mathbb{Z}/n\mathbb{Z}$ 中的唯一 d 阶子群的所有生成元

$$G = \bigcup_{d|n} \{g \in G \mid g \text{ 的阶为 } d\}$$

定理 3.19. $A \leq B \leq G$, $[G:A] < \infty \Leftrightarrow [G:B] < \infty$ 且 $[B:A] < \infty$.

$$\text{此时 } [G:A] = [G:B][B:A],$$

$$\text{proof } G = \bigcup_{s \in S} sB \quad B = \bigcup_{t \in T} tA$$

$$\Rightarrow G = \bigcup_{\substack{s \in S \\ t \in T}} s \cdot tA \quad s \cdot tA = s' \cdot t'A \Leftrightarrow S = S' \quad T = T'$$

$N \triangleleft G$. 正规

$$N \leq G. \quad \forall g \in G, \quad g^{-1}Ng \subseteq N$$

$$\Leftrightarrow g^{-1}Ng = N$$

$$\Leftrightarrow gN = Ng$$

G/N 陪集集合

上可定义乘法 $aN \cdot bN \triangleq abN$

$(G/N, \cdot)$ 形成群. 商群.

$\varphi: G \rightarrow H$. 群同态

$$\text{Im } \varphi \triangleq \{\varphi(g) \mid g \in G\} \quad \ker \varphi \triangleq \varphi^{-1}(1_H) = \{g \in G \mid \varphi(g) = 1_H\}$$

$$\text{Im } \varphi \leq H. \quad \ker \varphi \leq G. \quad (\ker \varphi \triangleleft G)$$

$$\varphi \text{ 满} \Leftrightarrow \text{Im } \varphi = H$$

$$\varphi \text{ 单} \Leftrightarrow \ker \varphi = \{1\}$$

$$\bar{\varphi}: G/\ker \varphi \xrightarrow{\sim} \text{Im } \varphi.$$

$$g \ker \varphi \mapsto \varphi(g)$$

$$\begin{aligned} \bar{\varphi} \text{ 定义合理} \quad \bar{\varphi}(g_1 \ker \varphi \cdot g_2 \ker \varphi) &= \bar{\varphi}(g_1 g_2 \ker \varphi) \\ &\stackrel{\vee}{=} \bar{\varphi}(g_1 \ker \varphi) \cdot \bar{\varphi}(g_2 \ker \varphi) \stackrel{\vee}{=} \varphi(g_1) \varphi(g_2) \\ &\stackrel{\vee}{=} \varphi(g_1 g_2) \end{aligned}$$

$\bar{\varphi}$ 群同态. $\bar{\varphi}$ 满

$$\bar{\varphi}(g \ker \varphi) = 1_H \Rightarrow \varphi(g) = 1_H \Rightarrow g \in \ker \varphi \Rightarrow g \ker \varphi = \ker \varphi$$

定理 4.3. 群同态基本定理

$\varphi: G \rightarrow H$ 群同态, 则

$$(1) \quad \ker \varphi \triangleleft G$$

$$(2) \quad \text{Im } \varphi \leq H.$$

$$(3) \quad \varphi \text{ 诱导群同构} \quad \bar{\varphi}: G/\ker \varphi \xrightarrow{\sim} \text{Im } \varphi. \quad \bar{\varphi}(g \ker \varphi) = \varphi(g)$$

No.

Date.

$$\text{Ex 11. } S' \xrightarrow{\sim} \mathbb{R}/\mathbb{Z}$$

$$\text{Exp: } \mathbb{R} \rightarrow S' \quad a \mapsto e^{i2\pi a}$$

$$\ker(\text{Exp}) = \mathbb{Z}$$

$$\text{Ex 1. } \det: \text{GL}_n(\mathbb{F}) \rightarrow \mathbb{F}^*$$

$$\ker \det = \text{SL}_n(\mathbb{F})$$

$$\text{GL}_n(\mathbb{F}) / \text{SL}_n(\mathbb{F}) \cong \mathbb{F}^*$$

$$\text{Ex 1. } \varphi: \text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/n\mathbb{Z}) \quad (\text{满})$$

$$\ker \varphi = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \equiv 1 \pmod{n}, b, c \equiv 0 \pmod{n} \right\} = \Gamma(n)$$

主同余子群

$$\text{Ex 1. } \Gamma(n) \rightarrow \text{SL}_2(\mathbb{Z}) \rightarrow \text{PSL}_2(\mathbb{Z}) = \text{SL}_2(\mathbb{Z}) / \{\pm I_2\}$$

设 λ

$$G \xrightarrow{f} H \xrightarrow{g} K$$

$$\ker g = \{1_H\} \Rightarrow \ker(g \circ f) = \ker g$$

$$G \xrightarrow{f} H \Rightarrow \ker(g \circ f) = G \cap \ker g$$

$$N \triangleleft G. \Rightarrow \forall m. N \leq m \leq G \Rightarrow N \triangleleft m \quad m/N \leq G/N$$

$$\bar{m} \leq G/N$$

$$\bigcup_{aN \in \bar{m}} aN \leq G.$$

命题 4.4. $N \triangleleft G$. 则

$$\text{双射 } \{m \mid N \triangleleft m \leq G\} \xrightarrow{H} \{\bar{m} \mid \bar{m} \leq G/N\}$$

$$m \mapsto m/N$$

$$\bigcup_{aN \in \bar{m}} aN \leftarrow \bar{m}$$

命题 45. 1) $N \trianglelefteq G$. $H \leq G$.

则 $N \cap H \trianglelefteq H$. $N \trianglelefteq HN$

$$\text{且 } \frac{HN}{N} \cong \frac{H}{H \cap N}$$

(2) $N \trianglelefteq G$. $M \trianglelefteq G$. $N \leq M$

$$\text{则 } \frac{G}{M} \cong \frac{G/N}{M/N}$$

proof. 1)
$$\begin{array}{ccc} N \cap H & \leq & H \\ \downarrow & & \downarrow \\ \pi & & h \end{array}$$

$$h^{-1}xh \in N. \quad h^{-1}xh \in H \Rightarrow N \cap H \trianglelefteq H.$$

$$HN \leq G.$$

$$h_1 n_1 \cdot h_2 n_2 = h_1 h_2 n'_1 n_2 \in HN$$

$$(h n)^{-1} = n^{-1} h^{-1} = h^{-1} n^{-1}$$

$$\varphi: H \rightarrow HN \rightarrow \frac{HN}{N} \quad \varphi(h) = hN$$

$$\varphi \text{ 满射 } \ker \varphi = H \cap N$$

$$\Rightarrow \frac{H}{H \cap N} \cong \frac{HN}{N}$$

$$(2) \quad \psi: \frac{G}{N} \rightarrow \frac{G}{M}$$

$$gN \rightarrow gM$$

$$\psi \text{ 定义合理 } (g_1 N = g_2 N \Rightarrow g_1 M = g_2 M)$$

ψ 群同态

$$gN \in \ker \psi \Rightarrow gM = M \Rightarrow g \in M$$

$$\Rightarrow \ker \psi = \frac{M}{N}$$

$$\Rightarrow \frac{G}{M} = \frac{G/N}{M/N}$$

例 $n|m$. m, n 正整数

$$m\mathbb{Z} \leq n\mathbb{Z} \leq \mathbb{Z}$$

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}/m\mathbb{Z}}{n\mathbb{Z}/m\mathbb{Z}}$$

第二章 群在集合上的作用

2.1. 对称群.

 S_n $\{1, \dots, n\}$ 上置换的全体定义 4.1. $1 \leq k \leq n$. $\{a_1, \dots, a_k\} \subseteq \{1, 2, \dots, n\}$ $a_i \neq a_j$ $i \neq j$ 置换 $\sigma: (a_1 \dots a_k)$ 定义为 $\sigma(a_1) = a_2$ $\sigma(a_2) = a_3 \dots \sigma(a_k) = \sigma(a_1)$ 其余不变例 $n=4$. $(3, (1, 2)) : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ 形如 $(a_1 \dots a_k)$ 的置换称为 k -轮换. 2-轮换称为对换

注. 1 轮换为恒同

$$(a_1 \dots a_k)^{-1} = (a_k a_{k-1} \dots a_1)$$

$$(a_1 a_2 \dots a_k) = (a_2 a_3 \dots a_k a_1)$$

定义 1.2. $\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_l\} = \emptyset$ 则称轮换 $(a_1 \dots a_k)$ 与 $(b_1 \dots b_l)$ 不相交 disjoint

$$\text{此时 } (a_1 \dots a_k) (b_1 \dots b_l) = (b_1 \dots b_l) (a_1 \dots a_k)$$

定理 1.3. (1) 不相交的轮换是可交换的

(2) 任一 $\sigma \in S_n$ 可写成两两不交的轮换的乘积, 且不计次序下唯一

$$\text{例. } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 4 & 1 & 2 & 5 \end{pmatrix} = (1, 3, 7, 5) (2, 6)$$

$$(1, 3, 5) (5, 6) (4, 6, 7) = (1, 3, 5, 6, 7, 4)$$

$$(1, 3, 5) (5, 7, 4, 2) (5, 3, 1) = (1, 7, 4, 2)$$

$$\sigma(a_1 \dots a_k) \sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k))$$

$$\text{例. } S_2: 1, (1, 2)$$

$$S_3: 1, (1, 2), (1, 3), (2, 3), (1, 2, 3), (3, 2, 1), (3, 1, 2)$$

$$S_4: 1, (1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)$$

$$(2, 3, 4), (2, 4, 3), (1, 3, 4), (1, 4, 3), (1, 2, 4), (1, 4, 2), (1, 2, 3), (1, 3, 2)$$

(1234), (1243), (1342), (1324), (1423), (1432)

定义 $\sigma \in S_n$ 设 σ 可以写成 互不相交轮换乘积. 其中 k -轮换的个数为 λ_k . 则称 σ 的型为 $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$

注. 1. σ 固定点的个数为 λ_1

$$2. n = n\lambda_n + (n-1)\lambda_{n-1} + 2\lambda_2 + \lambda_1$$

$$S_5: 5^1, 4^1, 3^1, 2^1 3^1, 2^2, 2^1, 1^5$$

$$24 \quad 30 \quad 20 \quad 20 \quad 15 \quad 10 \quad 1$$

命题 25 $\sigma, \sigma' \in S_n$

σ, σ' 同型 $\Leftrightarrow \sigma$ 与 σ' 共轭

proof $\Leftarrow \checkmark$ $\sigma = (a_1 \dots a_k) (b_1 \dots b_l) \dots$

$$\tau \sigma \tau^{-1} = (\tau(a_1) \dots \tau(a_k)) (\tau(b_1) \dots \tau(b_l)) \dots$$

$$\Rightarrow \sigma = (a_1 \dots a_k) (b_1 \dots b_l) \dots$$

$$\sigma' = (a'_1 \dots a'_k) (b'_1 \dots b'_l) \dots$$

构造 $\tau: a \rightarrow a'$

$$\tau \sigma \tau^{-1} = \sigma'$$

命题 26. (1) k -轮换可写成 $(k-1)$ 个对换的乘积.

(2) S_n 可由 $(12), (13), \dots, (1n)$ 生成

$$(1) \dots (a_1 \dots a_k) = (a_1 a_2) (a_2 a_3) \dots (a_k a_{k-1})$$

$$= (a_1 a_k) (a_1 a_{k-1}) \dots (a_1 a_2)$$

$$(2) (i, j) = (1 i) (1 j) (1 i)$$

定理 27 存在唯一的群同态 $\epsilon: S_n \rightarrow \{\pm 1\}$. 使得对 $\forall$ 对换 σ : 均有 $\epsilon(\sigma) = -1$

证明. 引理 逆序数

$$\# \{ (i, j) \mid 1 \leq i < j \leq n, \pi(i) > \pi(j) \}$$

No.

Date. / /

断言: $(i,j)\sigma$ 或 $\sigma(i,j)$ 改变逆序数奇偶性

$$\epsilon(\sigma) = \begin{cases} 1 \\ -1 \end{cases}$$

注 $\ker(\epsilon) = \{ \text{偶置换} \} \triangleq A_n$

$$|A_n| = \frac{1}{2} n! \quad \text{交错群}$$

引理 1.8. A_n 可由三轮换生成

proof. $(ij)(rs) = \begin{cases} (ij) & \{i,j\} = \{r,s\} \\ (ijrs) & \{i,j\} \cap \{r,s\} = \emptyset \\ (ijr) & \{i,j\} \cap \{r,s\} = \{r\} \\ (ijs) & \{i,j\} \cap \{r,s\} = \{s\} \end{cases}$

S_n 生成元

$$(12), (13), \dots, (1n)$$

$$(12), (23), \dots, (n-1, n)$$

$$(12), (12 \dots n)$$

定义 1.9. 称不含非平凡正规子群的群为单群.

例. $\mathbb{Z}/n\mathbb{Z}$ 正整数 n 阶循环群为单群 $\Leftrightarrow n$ 为素数

G 为 Abel 群且为单群 $\Leftrightarrow G \cong \mathbb{Z}/p\mathbb{Z}$ p 素 $\Leftrightarrow |G| = p$ p 素

定理 1.10. A_n ($n \geq 5$) 为单群.

注 $n=4$ A_4 不为单群.

S_4 :

$$1 \quad \text{偶}$$

$$2^1 \quad (12), (13), (14), (23), (24), (34) \quad \text{奇}$$

$$3^1 \quad (123), (132), (124), (142), (134), (143), (234), (243) \quad \text{偶}$$

$$2^2 \quad (12)(34), (14)(23), (13)(24) \quad \text{偶}$$

$$4^1 \quad (1234), (1243), (1324), (1342), (1423), (1432) \quad \text{奇}$$

$$\{1, (12)(34), (14)(23), (13)(24)\} \text{ 是 } A_4 \text{ 子群, } \triangle A_4$$

注 $|G| < 60 \Rightarrow G$ 不是单群 (后面证)

proof. $N \triangleleft A_n$

N 含有某个 3 轮换 则 N 含有所有 3 轮换 $\rightarrow$ 一定有一个偶

$$(\text{取 } (a b) \cap \{i, j, k\} = \emptyset \quad (a b) \sigma (i, j, k) (a b) \sigma^{-1} = \sigma (i, j, k) \sigma^{-1} = (i', j', k'))$$

下证 N 包含某个 3 轮换 取 $1 \neq \sigma \in N$

$$(1) \sigma \text{ 恰好变动两个元素} \Rightarrow \sigma = (ij) \notin A_n$$

$$(2) \sigma \text{ 变动三个元素} \Rightarrow \sigma = (ijk) \in A_n \Rightarrow N \text{ 含所有三轮换} \Rightarrow N = A_n$$

$$(3) \sigma \text{ 变动四个元素} \quad \sigma = (ij)(kl) \text{ 或 } (ij k l) \notin A_n$$

$$\exists m \neq ijkl.$$

$$(ij)(lm) = (klm)(ij)(kl)(klm)^{-1} \in N$$

$$\Rightarrow (ij)(kl)(ij)(lm) = (klm) \in N$$

(4) σ 至少变动 5 个元素,

$$\sigma = (a_1 a_2 a_3 a_4 a_5 \dots)$$

$$\sigma_1 = (a_1 a_3 a_4 a_2 a_5 \dots) = (a_2 a_3 a_4) \sigma (a_1 a_2 a_4)^{-1}$$

$$\sigma_1 \sigma^{-1} = (a_2 a_3 a_4) \in N. \quad \checkmark$$

$$\sigma = (a_1 a_2 a_3 a_4) (\dots)$$

$$\sigma_1 = (a_1 a_3 a_4 a_2) (\dots) \in N$$

$$\sigma_1 \sigma^{-1} = (a_1 a_2 a_3) \in N$$

其余情况同理.

§2.2. 群在集合上的作用.

定义 2.1. 群 G 在集合 X 上的一个左作用是给一个映射 $\varphi: G \times X \rightarrow X$

满足

$$(g \cdot x) \rightarrow \varphi(g, x) \quad g \cdot x$$

$$(1) \varphi(1_G, x) = x \quad 1_G \cdot x = x \quad \forall x \in X$$

$$(2) \varphi(g_2, \varphi(g_1, x)) = \varphi(g_2 g_1, x) \quad g_2(g_1 \cdot x) = (g_2 g_1) \cdot x$$

由 G 中元素

$$\begin{array}{ccc} G \times G \times X & \xrightarrow{m \circ Id_X} & G \times X \\ Id_G \times \varphi \downarrow & \hookrightarrow & \downarrow \varphi \\ G \times X & \xrightarrow{\quad} & X \end{array}$$

注类似地可定义右作用. $X \times G \rightarrow X$

$$\varphi: G \times X \rightarrow X$$

$$p_{(g)} = \varphi(g, \cdot) : X \rightarrow X \quad p_{(g)}^{-1} = p_{(g^{-1})}$$

$$p: G \rightarrow \text{Map}(X, X) \quad (\text{其实是 } S(X))$$

$$p(1_G) = \text{Id}_X$$

$$p(g_1 g_2) = p(g_1) p(g_2)$$

反之, 设有群同态 $p: G \rightarrow S(X)$

可定义 G 在 X 上的作用. $G \times X \rightarrow X$

$$(g, x) \mapsto (p(g))(x)$$

注. $G \curvearrowright X$. 若进一步, X 为线性空间, 且 $g \cdot \cdot : X \rightarrow X$ 为线性映射

对 $\forall g \in G$, 则称 G 线性作用在 X 上或 X 为 G 的线性表示.

$$\Leftrightarrow p: G \rightarrow GL_n(\mathbb{F})$$

$G \curvearrowright X$, 可在 X 上定义关系 $\sim: x \sim y \Leftrightarrow y = g \cdot x$.

则 $\sim$ 为等价关系.

定义 2.2. $G \curvearrowright X$ 对 $\forall x \in X$ $O_x = G \cdot x \triangleq \{g \cdot x \mid g \in G\}$ 称 x 在 G 作用下的轨道. 若 $X = O_x$, $x \in X$, 则称 G 在 X 上的作用可迁 (传递).

$G_x = \{g \in G \mid g \cdot x = x\} \leq G$ 称为 x 的稳定子群.

$\bigcap_{x \in X} G_x$ 称为群作用的核 ($= \ker p$ $p: G \rightarrow S(X)$)

$$1. S(X) \curvearrowright G \times X \leftarrow \text{Id} \quad S(x_1) \rightarrow S(x_2) \quad f \cdot x = f(x)$$

$$S_n \curvearrowright G \{1, \dots, n\}$$

$$GL_n(\mathbb{F}) \curvearrowright \mathbb{F}^n \text{ 左乘}$$



中国科学技术大学

University of Science and Technology of China

地址: 中国 安徽 合肥市金寨路96号 邮编: 230026
电话: 0551-63602184 传真: 0551-63631760 Http://www.ustc.edu.cn

1503 12 P₁ 24 P₁ 48 P₁ 120 P₁
12 P₂ 24 P₂ 48 P₂ 120 P₂
12 P₃ 24 P₃ 48 P₃ 120 P₃
12 P₄ 24 P₄ 48 P₄ 120 P₄

例. G 左乘作用在 G 上 $\varphi: G \times G \rightarrow G$
 $(g, x) \rightarrow g \cdot x$

$$\rho: G \rightarrow S(G)$$

$$g \mapsto \rho_g$$

$$f_g: G \rightarrow G$$

$x \mapsto g \cdot x$
是群同态, 但是双射

例. G 左乘作用在 G 上 $\varphi: G \times G \rightarrow G$
 $(g, x) \rightarrow g \cdot x$

$$G \text{ 作用在 } \{1, 2, \dots, 8\} \text{ 可逆}$$

$$8 = [G: G_1] \quad |G_1| = 3$$



Δ 的旋转

命题 2.5. $GGX \quad x \in X, \quad x' = a \cdot x \quad a \in G$

$$M = \{g \in G \mid g \cdot x = x'\} = a G_x$$

$$(2) \quad G \cdot x' = a G_x a^{-1}$$

$$g x' = x'$$

$$\Rightarrow g(a x) = (a x)$$

$$\Rightarrow a^{-1} g a \in G_x$$

$$\Rightarrow g \in a G_x a^{-1}$$

例. $H = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$

$$G = SL_2(\mathbb{R}) \quad G \curvearrowright H$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

验证: 上述映射给出群作用

作用可逆

$$G_i = SO_2 = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \quad 0 \leq \theta < 2\pi$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = i \quad ad-bc=1 \Rightarrow c=-b \quad a=d$$

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} z = z+n \quad n \in \mathbb{R}$$

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} z = a^2 z \quad a > 0$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} z = -\frac{1}{z} \quad \text{反演}$$

Inwasawa 分解.

$$SL_2(\mathbb{R}) = ANK$$

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \quad \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad SO_2$$

$$(NA)g \in K \Rightarrow g \in ANK$$

$$\text{轨道 } G \cdot x = \{g \cdot x \mid g \in G\}$$

命题 2.3 $GGX \quad x \in X$

$$\text{则有双射 } G/G_x \xrightarrow{\sim} G \cdot x$$

$$g \cdot G_x \mapsto g \cdot x$$

推论 2.4. X 有限集 G 有限群

$$(1) \quad |G \cdot x| = [G: G_x] \quad \text{轨道长度}$$

$$(2) \quad |X| = \sum_{x \in X} |G \cdot x| = \sum_{x \in X} [G: G_x]$$

1 为 x 在 G 作用下轨道的完全代表元系.

例. D_6 作用在 $\{1, 2, 3, 4, 5, 6\}$

$$|D_6| = 12 \quad 16 \text{ 个排列 } 6 \text{ 个旋转}$$

$$G = [D_6: G_x] = \frac{12}{2}$$

命题 2.6 (Cayley) 每个有限群可实化为排列群的子群.

$$G \subseteq G \text{ 左乘 } g \mapsto \rho_g \quad (G \rightarrow S(G))$$

命题 2.7. $4n+2$ 阶群有指数为 2 的正规子群, 从而非单群.

proof. G 中含 2 阶元

$$G = \bigcup_{x \in G} \{x, x^{-1}\} \quad \text{由 1 只含一个}$$

$$3 \times 1 \text{ 使 } |x, x^{-1}| = 1 \quad x = 1$$

$$\rho: G \subseteq S(G)$$

$$g \mapsto (a, g a^{-1}) (a, g a^{-1}) \dots$$

$2n+1$ 个排列

是奇置换

$$G \cong \operatorname{Im} \rho \leq S(G)$$

$\operatorname{Im} \rho$ 包含一个奇置换

$$|\operatorname{Im} \rho: \operatorname{Im} \rho \cap A_n| = 2$$

$$(H, K \leq G)$$

$$[G: K] \geq [H: H \cap K]$$

共轭作用

$\rho: G \times G \rightarrow G$
 $(g, x) \mapsto gxg^{-1}$

$\varphi \hookrightarrow \rho: G \rightarrow S(G)$

$\hookrightarrow \rho: G \rightarrow \text{Aut}(G)$

$(\rho(g))_{(xy)} = (\rho(g))_{(x)} \cdot (\rho(g))_{(y)}$

$\text{Imp} \leq \text{Aut}(G) \quad \text{Imp} = \text{Inn}G$

$\rho(g): x \mapsto gxg^{-1}$

称为内自同构. (inner automorphism)

且 $\text{Inn}G \triangleleft \text{Aut}(G)$

$\text{Aut}(G)/\text{Inn}(G) \cong \text{Out}(G)$

外自同构.

$x \in G, Z_G(x) = \{g \in G \mid gxg^{-1} = x\}$

称为 x 中心化子.

$C_x \triangleq \{gxg^{-1} \mid g \in G\}$ (轨道)

称为 x 所在的共轭类.

$T \subseteq G, Z_G(T) = \{g \in G \mid gt = tg, \forall t \in T\}$

$= \bigcap_{t \in T} Z_G(t)$

$Z(G) = \{g \in G \mid gx = xg, \forall x \in G\}$

群的中心

命题 26 设 $|G| < \infty$

(i) $|G| = |Z(G)| \cdot |C_x|$

(ii) $|G| = \sum_{x \in I} |C_x|$

$= |Z(G)| + \sum_{x \in I} |C_x|$

$|C_x| \geq 2$

I 为共轭类完全代表元系.

命题 27. G 为 p 群 (p 素, $|G| = p^n, n \geq 1$)

X 集合, $|X| = n, (p, n) = 1$, 则 G 作用在 X 上一定有不固定点.

特别地, G 有非平凡中心

($X = G \setminus \{1\}$, 有不固定点)

proof. $|X| = \sum_{i=1}^m |G \cdot x_i| = \sum_{i=1}^m [G : G_{x_i}]$

$p \nmid$ 素数, $p \nmid$ 幂.

右边的幂必有 1.

即: $[G : G_{x_i}] = 1 \Rightarrow x_i$ 为 G 作用下不动点.

$H \leq G$.

证 $X_H = \{gHg^{-1} \mid g \in G\}$ 与 H 共轭的子群集合

$G \setminus X_H, g \circ K = gKg^{-1}$

定义 2.10. H 在 G 共轭作用下的稳定

子群称为 H 在 G 中的正规化子. 记为

$N_G(H) \triangleq \{g \in G \mid gHg^{-1} = H\}$.

$H \triangleleft N_G(H) \leq G$.

注. $H \leq K \leq G$, 使得 $H \triangleleft K$, 则 $K \leq N_G(H)$

$H \triangleleft G \subseteq N_G(H) = G$.

$|G| = |N_G(H)| \cdot |X_H|$

$G \curvearrowright X_H, \rho: G \rightarrow S(X_H)$

$\ker \rho = \bigcap_{g \in G} N_G(gHg^{-1})$

$= \bigcap_{g \in G} g N_G(H) g^{-1}$

例. $N \leq G, [G : N] = p, p$ 为 $|G|$

的最小素因子. 则 $N \triangleleft G$.

proof. $G \curvearrowright G/N \xrightarrow{\rho} \rho: G \rightarrow S_p$

诱导群同态 $\rho: G \rightarrow S_p$

$\Rightarrow |p| \mid p!$

$|p| \mid |G| \Rightarrow |p| = p$.

$\Rightarrow \ker \rho = \bigcap_{g \in G} g N g^{-1} \leq N$

$\text{Imp} \subseteq G/\ker \rho$

$\Rightarrow \ker \rho = N, \Rightarrow N \triangleleft G$.

例. $H \leq G, [G : H] < \infty$.

$\Rightarrow \exists N \triangleleft G, \text{ s.t. } [G : N] < \infty$.

proof $G \curvearrowright G/H \hookrightarrow \rho: G \rightarrow S_n$

$\ker \rho$ 即为所求.

(易知 $\ker \rho \neq G$)

注. $G \curvearrowright X, G \curvearrowright Y$.

$\rightarrow G \curvearrowright X \times Y, G \curvearrowright X \cup Y$

$G \curvearrowright \mathcal{P}(X)$

X 的指数集 $= \{S \mid S \subseteq X\}$

$S \cdot S = \{g \cdot S \mid g \in G\}$

2.3. Sylow 定理及其应用

问 $d \mid |G|$ 是否存在 $H \leq G, |H| = d$.

定理 3.1 (Cauchy). $p \mid |G|$ 则

则 G 中含有 p 阶元.

$S = \{x_1 \dots x_p \in G \mid x_1 \dots x_p = 1\}$

$\subseteq G \times G \dots G$

$|S| = n^{p-1}, p \nmid n \Rightarrow p \mid |S|$

若 $(x_1 \dots x_p)$ 中 $\exists i \neq j, x_i \neq x_j$

则 $(x_1 \dots x_p), (x_2 \dots x_p, x_1), \dots, (x_p, x_1, \dots, x_{p-1})$

一定两两不同 (p 阶元在这里)

考虑 $\mathbb{Z}/p\mathbb{Z}$ 在 S 上作用.

$\sigma: (x_1 \dots x_p) \mapsto (x_2 \dots x_p, x_1)$

轨道长度要么是 p , 要么是 1

而有 $1(1 \dots 1)$ 轨道长度 1

$\Rightarrow \exists$ 长度为 1 的轨道 $(x_1 \dots x_p)$

$\Rightarrow x_1 = x_2 = \dots = x_p \Rightarrow x_1^p = 1 \in \text{PTN}$.

定义 3.2. $|G|$ 为素数 p 的幂, G 为 p 群

$H \leq G$, H 为 p 群. 称 H 为 G 的一个 p -子群.

$H \leq G, |H| = p^r, p^r \parallel |G|$

则称 H 为 G 的 Sylow p -子群

$$|G| = p^r \cdot m, (p, m) = 1, |P| = p^r, P \leq G \Rightarrow \text{Sylow-}p \text{子群}$$

$$Q \leq G, P\text{-子群}$$

$$P \cap Q = ? \quad N_G(P) \cap Q = H$$

$$\text{必须 } H \leq P$$

$$\text{由 } H, P \leq N_G(P) \quad P \triangleleft N_G(P) \Rightarrow PH \leq N_G(P)$$

$$|PH| = |P| \cdot \frac{|H|}{|H \cap P|} \Rightarrow PH \text{ 为 } P\text{-子群} \Rightarrow PH = P$$

$$\Rightarrow \frac{|H|}{|H \cap P|} = 1 \Rightarrow H \leq P \checkmark$$

定理 3.3. $|G| = p^r \cdot m = n$, (p, m) 互素. 记 $N(p)$ 为 G 的 Sylow- p 子群的个数.

(1) G 存在 Sylow- p 子群.

(2) 对 $\forall$ Sylow- p 子群 P 以及任 p -子群 Q 均存在 $g \in G$ 使 $Q \leq gPg^{-1}$

$$(3) N(p) \equiv 1 \pmod{p} \quad N(p) \mid |G|$$

$$\text{如 } 24 \text{ 阶群, } N(2) = 1 \text{ 或 } 2 \quad N(2) \mid 3 \Rightarrow N(2) = 1 \text{ 或 } 3$$

循环 S_4

proof (1). 对 $|G|$ 的阶归纳. 设该结论对阶 $< |G|$ 都成立

设 $g_1 \dots g_\alpha$ 为 G 的共轭类完全代表元系.

$$p^r m = |G| = |Z(G)| + \sum_{i=1}^{\alpha} [G : C_G(g_i)] \quad \text{稳定子群 (正规化子) 的阶数}$$

$$(1) p \mid |Z(G)|$$

则 $\exists p$ 阶子群 $N \leq Z(G)$ 则 $N \triangleleft G$

$$\{N \leq M \leq G\} \xrightarrow{1:1} \{G/N \text{ 子群}\}$$

$$\pi: G \rightarrow G/N$$

$$\pi^{-1}(P) = P$$

$\downarrow$
Sylow

G 中包含 N 的 Sylow p -子群 $\rightarrow G/N$ Sylow p -子群

$$(2) p \nmid |Z(G)|$$

$$\text{此时 } \exists i \text{ 使 } p \nmid [G : C_G(g_i)] \Rightarrow p^r \mid |C_G(g_i)| \Rightarrow C_G(g_i) \text{ 的 Sylow } p\text{-子群} \\ C_G(g_i) \neq G \text{ (阶小)} \Rightarrow \text{是 } G \text{ 的 Sylow } p\text{-子群}$$

$$(2). S = \{P \text{ 的所有共轭子群} \} = \{gPg^{-1} \mid g \in G\} = \{P_1 \dots P_k\}$$

Q 共轭作用在 S 上 轨道为 $O_1 \dots O_s \quad S = O_1 \cup \dots \cup O_s$

设 $P_1 \dots P_s$ 为轨道完全代表元系. P_i 稳定子群. $N_G(P_i) \cap Q = P_i \cap Q$

$$|O_i| = [Q : P_i \cap Q]$$

$$10:1=1 \Leftrightarrow Q \leq P_i \quad \text{否则} \quad P_i \nmid |Q|$$

特别地若 \$P\$ 在 \$S\$ 上共轭作用 \$\Rightarrow |S|=1 \pmod{p}\$

回到一般的 \$Q\$ 至少有一个轨道长度为 1

$$\Rightarrow \exists P_i \quad Q \leq P_i$$

特别地若 \$Q\$ 是 Sylow-\$p\$ 子群 \$\quad Q \leq gPg^{-1} \Rightarrow Q = gPg^{-1}\$

即 \$G\$ 的所有 Sylow-\$p\$ 子群相互共轭

$$\text{故 } \text{Sylow}_p(G) = S \quad |N_{P_i}| = |S| = 1 \pmod{p}$$

另一方面 \$G\$ 在 \$S\$ 上的共轭作用可迁 \$\Rightarrow |S| \mid |G|\$ (轨道长度整除)

定理 3.4. \$|G| = p^r m \quad (p, m) = 1, \quad 1 \leq k \leq r\$. 设 \$N\$ 为 \$G\$ 的 \$p^k\$ 阶子群, 个数 \$N \equiv 1 \pmod{p}\$

特别地, \$p^k\$ 阶子群存在.

proof. 记 \$S = \{x \in G \mid |x| = p^k\}\$ (子集)

$$G \times S \rightarrow S$$

$$(g, s) \mapsto gs$$

对 \$\forall x \in S\$: \$O_x\$ 中出现一个 \$(p^k\$ 阶) 子群 \$\Leftrightarrow |G_x| = p^k\$

此时 \$O_x\$ 中恰有一个群.

证 "\$\Rightarrow\$": \$O_x\$ 中有子群 \$H\$. 此时 \$G_H = H\$.

$$\Rightarrow |G_H| = p^k.$$

$$"$\Leftarrow$": $|G_x| = p^k$$$

$$\left. \begin{array}{l} \exists g \in S \text{ 使 } 1 \in gX \\ |G_{gX}| = p^k \end{array} \right\} \Rightarrow gX \text{ 是群} \quad \left(\begin{array}{l} G_{gX} = \{g' \in G \mid g' \cdot gX = gX\} \\ 1 \in gX \Rightarrow \forall g' \in G_{gX} \quad g' \in gX \\ \Rightarrow gX = G_{gX} \end{array} \right)$$

$$\text{此时 } |O_x| = p^{r-k} \cdot m$$

$$\text{而 } |G_x| = p^i \quad i=0, \dots, k$$

$$X = G_x \cdot x_1 \cup G_x \cdot x_2 \cup \dots \cup G_x \cdot x_d$$

$$x \in X \Rightarrow G_x \cdot x \subseteq X$$

对轨道进行分类

$$\Rightarrow t_0 \frac{n}{p^0} + t_1 \frac{n}{p^1} + \dots + t_k \frac{n}{p^k} = \frac{n!}{p^k! (n-p^k)!}$$

$$\Rightarrow t_0 p^k + t_1 p^{k-1} + \dots + t_{k-1} p + t_k = \frac{(n-1)!}{(p^{k-1})! (n-p^k)!} \equiv 1 \pmod{p}$$

推论 3.5 $P \in \text{Syl}_p(G)$. $N_G(P) \leq A \leq G \Rightarrow N_G(A) = A$

proof. $g \in N_G(A)$.

$$g N_G(A) g^{-1} = N_G(A) \supseteq N_G(P) \ni P$$

$$\Rightarrow g P g^{-1} \in \text{Syl}_p(A)$$

$$\Rightarrow g P g^{-1} = a P a^{-1} \quad \exists a \in A$$

推论 3.6 (Fratini) $M \trianglelefteq G$. $P \in \text{Syl}_p(M) \Rightarrow M \cdot N_G(P) = G$.

证. $\forall g \in G$. $g P g^{-1} \leq g M g^{-1} = M$. $\Rightarrow g P g^{-1} \in \text{Syl}_p(M)$

$\Rightarrow \exists m \in M$. $g P g^{-1} = m P m^{-1}$ (Sylow P 子群都是共轭)

$$\Rightarrow (m^{-1}g)P(m^{-1}g)^{-1} = P \Rightarrow m^{-1}g \in N_G(P)$$

$$\Rightarrow g \in m \cdot N_G(P) \Rightarrow M N_G(P) = G.$$

例. 150 阶群不是单群

proof $150 = 2 \times 3 \times 5^2$

$$N(5) \equiv 1 \pmod{5} \mid \Rightarrow N(5) = 1 \text{ 或 } 6$$

$$N(5) \mid 6$$

$N(5) = 1 \Rightarrow$ 150 阶 Sylow 5 子群一定为正规子群.

$\text{Syl}_5(G) = \{P_1, \dots, P_6\}$. G 在 $\text{Syl}_5(G)$ 上的共轭作用

诱导群同态 $\rho: G \rightarrow S_6$ 作用可迁

$$\Rightarrow \ker \rho \neq G. \quad \text{由 } 150 \nmid 720 \Rightarrow \ker \rho \neq \{1\}$$

$\Rightarrow \ker \rho$ 是非平凡的正规子群.

命题 3.8. p, q 素数. 则 pq . p^2q 阶群非单.

proof. 由 3.7. 不妨设 $p < q$.

$$|G| = pq \quad N(q) = 1 \quad \checkmark$$

$$\neq |G| = p^2q$$

$$N(q) \equiv 1 \pmod{q}, \quad N(q) \mid p^2$$

$$\text{① } N(q) = 1 \quad \checkmark$$

④ $N(g) = p^2$.

每一个 Sylow p -子群含有 $p-1$ 个互不相同的 p 阶元

任两个 Sylow p -子群的交只有 $\{1\}$

$\Rightarrow G$ 中共有 $p(p-1)$ 个 p 阶元. 剩下 p^2 个元素组成 G 的 Sylow p -子群

它是正规子群

($p > 3$ 时证明类似)

定理 3.9. G 为有限单群. 则 $|G| \geq 60$

注 $|A_5| = 60$. A_5 为单群.

除去 p 除. $p \nmid |G|$. $p \nmid p^2$. $4n+2$

还剩 24 36 40 48 56

$48 = 2^4 \cdot 3$

$N(2) = 1 \quad \checkmark$

$N(2) = 3$. $p: G \rightarrow S_3$ 取 $\ker p$

$56 = 2^3 \cdot 7$

$N(2) = 1$ 或 7

~~7阶元~~ $N(7) = 8$ 时 7阶元 $8 \times 6 = 48$

$N(7) = 1$ 或 8

$56 - 48 = 8 \rightarrow$ 唯一 Sylow 2-子群

§2.4. 自由群与群的表现

$\phi \in S$ 集合 (字母的集合) $x \in S$ 称为字母

$x_1 \dots x_n$ 文字. 1. 空文字. $w(S)$ S 上文字的所有集合

命题 4.1 $w(S)$ 在字符串连接运算下形成一个自由半群. 其中 ϵ 元为空文字. 称为 S 生成的自由半群.

定义 4.2. $w \in w(S \cup S^{-1})$ 称为一个既约文字. 若 w 中不含形如 aa^{-1} 或 $a^{-1}a$ 的子文字. 若 w' 可以通过对 w 进行若干次约化得到. 则称 w' 为 w 的一个既约形式.

引理 4.3. 任一 $w \in W(SUS^{-1})$ 具有唯一的既约形式

proof. 可对 $|w|$ (文字的长度) 归纳

$$\begin{array}{ccc} \bar{x} a a^{-1} \bar{y} & & \bar{x} a a^{-1} \bar{y} b b^{-1} \bar{z} \\ \swarrow \quad \searrow & & \swarrow \quad \searrow \\ \bar{x} a \bar{y} & \bar{x} a \bar{y} & \bar{x} \bar{y} b b^{-1} \bar{z} \quad \bar{x} a a^{-1} \bar{y} \bar{z} \\ & & \swarrow \quad \searrow \\ & & \bar{x} \bar{y} \bar{z} \end{array}$$

注. 在 $W(SUS^{-1})$ 上定义等价关系

$w_1 \sim w_2 \iff w_1, w_2$ 具有相同的既约形式

$$F(S) = W(SUS^{-1}) / \sim$$

有完全代表元系, $\{ \text{既约文字} \} R(S)$.

引理 4.4. $w_1, w_2, w_3, w_4 \in W(SUS^{-1})$

$$w_1 \sim w_1' \quad w_2 \sim w_2'$$

$$\Rightarrow w_1 w_2 \sim w_1' w_2'$$

定理 4.5. $F(S)$ 在字符串连接意义下形成群 称为 S 生成的自由群

定理 4.6 G 为群. $\varphi \neq \emptyset$ 集合. $f: \varphi \rightarrow G$ 集合的映射. 则 $\exists$ 唯一群同态

$$\tilde{f}: F(S) \rightarrow G \quad \tilde{f}|_S = f.$$

推论 4.7 任一群为自由群的商群 任一有限生成群为有限生成自由群的商群

proof

$$\begin{array}{ccc} S \subseteq G & & \pi([a_1^{\pm} \dots a_n^{\pm}]) = a_1^{\pm} \dots a_n^{\pm} \\ \downarrow \quad \nearrow \pi & & \\ F(S) & & \end{array}$$

G 由形如 $a_1^{\pm} \dots a_n^{\pm}$ 的元素组成. 故 π 为满射

$$\Rightarrow G \cong F(S) / \ker \pi$$

$$SL_2(\mathbb{Z}) / \langle \pm I \rangle$$

$$\text{例 } PSL_2(\mathbb{Z}) = \langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mid S^2 = 1 \quad (ST)^3 = 1 \rangle$$

定义 4.8. $G = F(S)/N$ 可以记作 $G = \langle S \mid r=1, r \in N \rangle$

若 $R \subseteq N$ 在 $F(S)$ 中生成的正规子群为 N . 称

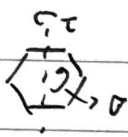
$G = \langle S \mid r_1=1 \dots r_n=1 \quad r_i \in R \rangle$ 为 G 的一个表现.

$G = F(S)/\langle R \rangle$ $\langle R \rangle$ 为 $F(S)$ 中包含子集 R 的最小正规子群

($\bigcup_{g \in G} g R g^{-1}$ 生成的子群)

例 1. $\mathbb{Z} = \langle a \rangle \quad \mathbb{Z}/n\mathbb{Z} = \langle a \mid a^n = 1 \rangle$

2. $G = \langle x_1 \dots x_n \mid x_i x_j x_i^{-1} x_j^{-1} = 1 \quad \forall i, j \rangle$

3.  $D_n = \langle \tau, \sigma \mid \sigma^n = 1, \tau^2 = 1, (\tau\sigma)^2 = 1 \rangle$
即 $D_n \cong F(T, \bar{Z}) / \langle \bar{Z}^n, T^2, (T\bar{Z})^2 \rangle$

$\pi: F(T, \bar{Z}) \rightarrow D_n \quad \tau \mapsto \tau, \bar{Z} \mapsto \sigma$

$\ker \pi \cong \langle \bar{Z}^n, \sigma^n, (T\sigma)^2 \rangle$

$\tilde{\pi}: \tilde{G} = \frac{F(T, \bar{Z})}{\langle \bar{Z}^n, T^2, (T\bar{Z})^2 \rangle} \rightarrow D_n = \frac{F(T, \bar{Z})}{\ker \pi}$

要证 $\tilde{\pi}$ 为单射. 只要证明 $|\tilde{G}| = 2n$

因为 $\tilde{G}$ 中元素具有形式 $T^i \bar{Z}^j$

(4) $Q_8 = \langle a, b \mid a^4 = 1, a^2 = b^2, ba = a^3b \rangle \quad a^i b^j \quad i=0,1,2,3 \quad j=0,1$

$|Q_8| \leq 8$

$G = \left\{ \begin{array}{l} (1, 1) \quad (1, -1) \quad (-1, -1) \quad (-1, 1) \\ (i, i) \quad (-i, -i) \quad (-i, i) \quad (i, -i) \end{array} \right\}$

(5) $S_n = \langle x_1, \dots, x_{n-1} \mid x_i^2 = \dots = x_{n-1}^2 = 1, x_i = x_j, i=j+1, 2 \dots (x_i x_{i+1})^3 = 1 \rangle$
(12) (23) ... (n-1 n) 即 $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$ 换位关系.

对 n 进行归纳 $G_n = G_{n-1} \cup x_{n-1} G_{n-1} \cup x_{n-2} x_{n-1} G_{n-1} \cup \dots \cup x_1 \dots x_{n-1} G_{n-1}$

25. 有限生成的 Abel 群

定义 5.1 G -群, $a, b \in G$, $aba^{-1}b^{-1}$ 称为 a 与 b 的换位子 记作 $[a, b]$. G 中所有换位子生成子群 称为换位子群 (或导子群).

命题 1.2. (1) $G' \triangleleft G$. 且 G/G' 为 Abel 群.

(2). $\forall \varphi: G \rightarrow A$ 其中 A 为 Abel 群 φ 为群同态. 则 $\ker \varphi \supseteq G'$

proof. (1) 记 S 为换位子的全体.

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$$

$$g(aba^{-1}b^{-1})g^{-1} = gag^{-1}gbg^{-1}gb^{-1}g^{-1}gb^{-1}g^{-1}$$

即 S 在共轭下封闭. 故 S 生成的子群在共轭下封闭.

$$G/N \text{ 为 Abel 群} \Leftrightarrow \bar{a}\bar{b} = \bar{b}\bar{a} \quad \forall a, b \Leftrightarrow \overline{aba^{-1}b^{-1}} = \bar{1} \Rightarrow aba^{-1}b^{-1} \in N \quad \forall a, b.$$

(2) $\varphi: G \rightarrow A$.

$$\varphi([a, b]) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} = 1_A.$$

$$\Rightarrow \ker \varphi \supseteq G'$$

例. $G = F(S)$. $G' = \langle xyx^{-1}y^{-1}, x, y \in S \rangle_N$. 生成的正规子群.

$$S_n' = A_n$$

$$i([12], [13]) = (123) \text{ 包含所有三轮换正规子群} \Rightarrow A_n$$

$$A_3' = \{1\} \quad A_4' = K_4 = \{1, (12)(34), (13)(24), (14)(23)\}$$

$$A_5' = A_5 \dots \quad A_n' = A_n \quad (A_n \text{ 单}).$$

注 G' 为使得 G/N 为 Abel 群 的最小正规子群.

定义 5.3 $\mathbb{Z}(S) = \langle S \mid xyx^{-1}y^{-1}, x, y \in S \rangle$ 称为由 S 生成的自由阿贝尔群
 S 称为 $\mathbb{Z}(S)$ 的一组基. 若 $|S| < \infty$, 称 $\mathbb{Z}(S)$ 有限生成

例 $\mathbb{Z}$ 为自由 Abel 群

$\mathbb{Z}/n\mathbb{Z}$ 不为自由 Abel 群.

定义 5.4. 设 I 为指标集, X_i 为阿贝尔群, $X_i \cong \mathbb{Z}$, $\forall i \in I$. $\bigoplus X_i = \{(x_i)_{i \in I} \mid x_i \in X_i \text{ 及有限个 } x_i \neq 0\}$ 为 Abelian 群. 记作 $\mathbb{Z}^{\oplus I}$

引理 5.5. $G_1 \times \dots \times G_n \trianglelefteq G$, $n \geq 2$. TFAE

(1) $0 \cong G_1 \times \dots \times G_n$ (φ 同构)

$$g_1 g_2 \dots g_n \mapsto (g_1, \dots, g_n)$$

(2) $\forall g \in G$, $\exists ! (g_1, \dots, g_n) \in G_1 \times \dots \times G_n$ $g_1 \dots g_n = g$. (φ 双射)

(3) $G = G_1 \dots G_n$, 且 $G_1 \dots G_{i-1} \cap G_i = \{1\}$.

proof. (1) $\Rightarrow$ (2). $\checkmark$

(2) $\Rightarrow$ (3). φ 为满射 $\Rightarrow G = G_1 \times \dots \times G_n$.

若 $\exists g_i \in G_1 G_2 \dots G_{i-1} \cap G_i$

$$\Rightarrow g_i = g_1 g_2 \dots g_{i-1} \quad \exists g_1 \in G_1 \dots g_{i-1} \in G_{i-1}$$

$$= \varphi(g_1, \dots, g_{i-1}, 1, \dots, 1) = \varphi(1, \dots, 1, g_i, 1, \dots, 1)$$

$$\Rightarrow g_1 = \dots = g_i = 1$$

(3) $\Rightarrow$ (1).

$$n=2. \quad G = G_1 G_2 \quad G_1 \cap G_2 = \{1\}$$

$$\forall g \in G. \exists ! g_1 \in G_1, g_2 \in G_2. \text{ 使 } g = g_1 g_2$$

$$\varphi: G \rightarrow G_1 \times G_2$$

$$g \mapsto (g_1, g_2)$$

$$g = g_1 g_2 \quad g' = g'_1 g'_2 \Leftrightarrow g g' = (g_1 g'_1) (g_2 g'_2)$$

$$\Leftrightarrow g_1 g_2 g'_1 g'_2 = g_1 g'_1 g_2 g'_2$$

$$\Leftrightarrow g_2 g'_1 = g'_1 g_2$$

$$(n_1 \trianglelefteq G, n_2 \trianglelefteq G, n_1 n_2 = n_1 n_2 n_1^{-1} n_1 = n_1' (n_1 n_2 n_1^{-1}))$$

$$\Rightarrow n_1 = n_1' \quad n_2 = n_1 n_2 n_1^{-1}$$

然! 归纳即得.

定理 5.6. (1) $\mathbb{Z}(1) \cong \mathbb{Z}^{\oplus 1}$

$$(2) \quad m \neq n \Rightarrow \mathbb{Z}^m \not\cong \mathbb{Z}^n$$

$$\frac{F(x)}{(xyx^{-1}y^{-1}, x \in I)} \rightarrow \mathbb{Z} \quad \text{①.} \quad \forall x \in I \quad x \mapsto e_x = (1 \dots 1 \overset{x}{1} \dots 1)$$

$$x^{n_x} y^{n_y} \dots \rightarrow n_x e_x + n_y e_y + \dots$$

$$\prod_{x \in I} x^{n_x} \leftarrow \sum_{x \in I} n_x e_x$$

proof. p. 3. A Abelian 群 $p_A = \{p \cdot a \mid a \in A\}$

$$f: A \hookrightarrow B. \Rightarrow p_A \stackrel{\sim}{=} p_B \Rightarrow \frac{A}{p_A} \hookrightarrow \frac{B}{p_B}$$

$$\frac{\mathbb{Z}^m}{p\mathbb{Z}^m} = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^m \quad \left|\frac{\mathbb{Z}^m}{p\mathbb{Z}^m}\right| = p^m \quad m \neq n \text{ 时个数不一样.}$$

定义 5.7. 设 $\{x_i \mid i \in I\}$ 为自由阿贝尔群 F 的子集. 满足 $F = \bigoplus_{i \in I} \mathbb{Z} x_i$.
 则称 $\{x_i \mid i \in I\}$ 为 F 的一组基. $|I|$ 称为 F 的秩.

例. $\mathbb{Q}$ 不是自由群.

因为 $\mathbb{Q}$ 中任一两个元素是 $\mathbb{Z}$ -线性相关的 ($p\frac{q}{p} = p'\frac{q'}{p'}$)

且 $\mathbb{Q} \neq \mathbb{Z}$

(因为 $\mathbb{Z}$ 可以由 1 生成但 $\mathbb{Q}$ 不是有限生成的)

$\Rightarrow \mathbb{Q}$ 没有一组基 I , 使 G 中元素唯一写成 I 中元素的 $\mathbb{Z}$ -线性组合

定理 5.8. G 有限生成自由 Abelian 群 ^{非平凡} $H \leq G$, 则 H 也是自由生成 Abelian 群.
具体地, 存在 G 的一组基 $(x_1, \dots, x_n)$ 以及 $m_1 | m_2 | m_3 \dots | m_r$.

使得 $m_1 x_1, m_2 x_2, \dots, m_r x_r$ 为 H 的一组基.

例 $G = \mathbb{Z}^2 = \{(a, b) \mid a, b \in \mathbb{Z}\}$ $((1, 0), (0, 1))$

$H = \{(2m, 4n) \mid m, n \in \mathbb{Z}\}$ $H \leq G$. $((2, 0), (0, 4))$

证明 $I = \{d \in \mathbb{Z} \mid \exists H \text{ 中的元素 } x, \text{ 以及 } G \text{ 的一组基 } (x_1, \dots, x_n) \\ x = d x_1 + d_2 x_2 + \dots + d_n x_n \quad \exists d_2, \dots, d_n\}$

取 I 中的最小正整数 m_1

$\exists x \in H$ G 中基元 $y_1, \dots, y_n$ $x = m_1 y_1 + d_2 y_2 + \dots + d_n y_n$

Claim $m_1 | d_i \quad i \geq 2$. 否则取余数可以取到更小的

即 $x = m_1 (y_1 + f_2 y_2 + \dots + f_n y_n) = m_1 x_1$

$x_1 = y_1 + f_2 y_2 + \dots + f_n y_n$

$\tilde{G} = \mathbb{Z} y_2 + \dots + \mathbb{Z} y_n$ 为秩为 $n-1$ 的自由 Abelian 群

Claim $H = \mathbb{Z} (m_1 x_1) \oplus (H \cap \tilde{G})$

显然 $\forall y \in H \quad y = f_1 x_1 + f_2 y_2 + \dots + f_n y_n$

f_1 一定是 m_1 的倍数. 否则用 $m_1 x_1$ 一直减能找到更小的

记 $\tilde{H} = H \cap \tilde{G} \leq \tilde{G}$ $\tilde{G}$ 是秩为 $n-1$ 的自由 Abelian 群

非秩归纳假设 $\exists$ 一组基 $x_2, \dots, x_r$ 以及 $m_2 | m_3 | \dots | m_r$

使 $m_2 x_2, m_3 x_3, \dots, m_r x_r$ 是 $\tilde{H}$ 的一组基

故 $x_1, \dots, x_n$ 为 G 的基 $m_1 x_1, \dots, m_r x_r$ 为 H 的基.

易验证 $m_1 | m_2$

No.

Date. / /

定理 5.9. A 有限生成 Abel 群 则 $\exists r \in \mathbb{N}$ 以及 $m_1, m_2, \dots, m_s \in \mathbb{Z}^+$

$$\text{使 } A \cong \mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/m_s\mathbb{Z}$$

proof $A \cong G/H$. G 自由 Abel $H \leq G$.

$\Rightarrow \exists G$ 的一组基 $x_1, \dots, x_n$ $m_1, m_2, \dots, m_s$ $m_1 x_1, \dots, m_s x_s$ 为 H 的基

$$\frac{\mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \dots \oplus \mathbb{Z}x_s \oplus \dots \oplus \mathbb{Z}x_n}{\mathbb{Z}m_1x_1 \oplus \mathbb{Z}m_2x_2 \oplus \dots \oplus \mathbb{Z}m_sx_s \oplus \dots \oplus \mathbb{Z}x_n} = \frac{\mathbb{Z}x_1}{\mathbb{Z}m_1x_1} \oplus \dots \oplus \frac{\mathbb{Z}x_s}{\mathbb{Z}m_sx_s} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$$

(注. $G = G_1 \times G_2$ $H_1 \leq G_1$ $H_2 \leq G_2$

$$\Rightarrow H_1 \times H_2 \leq G_1 \times G_2$$

$$\text{且 } \frac{G_1 \times G_2}{H_1 \times H_2} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2}$$

定义 5.10. A Abel 群 $A_t = \{a \in A \mid \text{ord}(a) < \infty\} \leq A$.

称为 A 的扭子群 (torsion)

注 Abel 群是必要的如 $\text{PSL}(\mathbb{Z}_2)$ $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 是 3 阶元

命题 5.11.

(1). $A = A_t \oplus A_f$. 其中 A_f 为自由 Abel 群.

(2). $A \cong B \Leftrightarrow A_t \cong B_t$. $A_f \cong B_f$.

注 A_f 选取不唯一. 同构意义下唯一

proof (1) 5.9

$$(2). \quad f: A \xrightarrow{\sim} B \\ \begin{matrix} \uparrow & \uparrow f^{-1} \\ A_t & \xrightarrow{f} B_t \\ \downarrow & \downarrow f^{-1} \end{matrix} \Rightarrow f|_{A_t}: A_t \xrightarrow{\sim} B_t$$

$$\begin{array}{ccc} A_t & & B_t \\ \downarrow & & \downarrow \\ A & \xrightarrow{f} & B \\ \downarrow & \searrow & \downarrow \\ A_f & \xrightarrow{f} & B_f \end{array}$$

定理 5.12 A 为有限阿贝尔群

$$(1) A \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z} \quad m_1 | \cdots | m_s \quad \text{不变因子}$$

$$(2) A \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{r_k}\mathbb{Z} \quad (\mathbb{Z}/m_n\mathbb{Z} = \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \quad (m, n)=1)$$

p_i 素数 $r_i \geq 1$ p_i 可能相等 $p_i^{r_i}$ 初等因子.

定理 5.13 (有限生成 Abel 群结构定理).

(1) A 有限生成 Abel 群, 则

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z} \quad m_1 | \cdots | m_s$$

$$\cong \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{r_k}\mathbb{Z}$$

r 秩 不变因子, 初等因子, 由 A 唯一确定

$$(2) A \cong B \text{ 同构} \Leftrightarrow \text{rank } A = \text{rank } B \quad \text{不变因子相同}$$

证明 " $\Rightarrow$ " A 的不变因子组唯一确定

$$A_{p_i} = \{x \in A \mid \text{ord}(x) = p_i^{r_i}\} \quad \text{为 } p \text{ 群}$$

是 A 的唯一一个 Sylow- p 子群.

$$A = A_{p_1} \oplus A_{p_2} \oplus \cdots \oplus A_{p_k} \quad p_i \neq p_j \quad \forall i \neq j$$

$$\text{只须证 } \mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{r_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{r_k}\mathbb{Z} \quad r_1, r_2, \dots, r_k$$

$$\cong \mathbb{Z}/p_1^{r'_1}\mathbb{Z} \oplus \mathbb{Z}/p_1^{r'_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_1^{r'_s}\mathbb{Z} \quad r'_1 \geq r'_2 \geq \cdots \geq r'_s$$

$$\Rightarrow s=t \quad \text{且} \quad r_1=r'_1, r_2=r'_2, \dots, r_k=r'_k$$

$$A_{p_i} \cong \underbrace{\mathbb{Z}/p^{d_\alpha}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{d_\alpha}\mathbb{Z}}_{d_\alpha} \oplus \underbrace{\mathbb{Z}/p^{d_{\alpha-1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{d_{\alpha-1}}\mathbb{Z}}_{d_{\alpha-1}} \cdots \oplus \underbrace{\mathbb{Z}/p^{d_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{d_1}\mathbb{Z}}_{d_1}$$

只须证明 $d_\alpha, d_{\alpha-1}, \dots, d_1$ 由 A 唯一确定 (p^α 为 A_{p_i} 元素最大阶)

$$|p^{\alpha-1} A_{p_i}| = p^{d_\alpha} \quad d_\alpha \text{ 由 } A \text{ 唯一确定}$$

$$|p^{\alpha-2} A_{p_i}| = p^{2d_\alpha + d_{\alpha-1}} \Rightarrow d_{\alpha-1} \text{ 由 } A \text{ 唯一确定} \cdots \text{以此类推}$$

例 1) 1500 阶 Abel 群

$$2^3 \times 3 \times 5^3$$

$$\{2^3\} \quad \{3\} \quad \{5^3\}$$

$$\{2, 2^2\} \quad \{5, 5^2\}$$

$$\{5, 5, 5\}$$

例 8 阶群.

Abel. $\mathbb{Z}/8\mathbb{Z} \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

非 Abel. $D_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = (\sigma\tau)^2 = 1 \rangle$

$Q_8 = \langle \sigma, \tau \mid \sigma^4 = 1, \sigma^2 = \tau^2, \sigma\tau = \tau\sigma^{-1} \rangle$

$\exists$ 四阶元 $\sigma, \sigma^4 = 1$ 取 $\tau \notin \{1, \sigma, \sigma^2, \sigma^3\}$

$\tau^2 = 1$ 或 $\tau^4 = 1$

由 τ, τ^2 不在同一个陪集 $\Rightarrow \tau^2 \in \langle \sigma \rangle$

$\tau\sigma\tau^{-1} = \sigma^i \Rightarrow \tau^2\sigma\tau^{-2} = \sigma^{i^2}, \sigma = \sigma^{i^2} \Rightarrow i^2 = 1$ 或 3

又 $i \neq 1 \Rightarrow \tau\sigma\tau^{-1} = \sigma^3$

例 $|GL_3(\mathbb{F}_2)| = ?$

$(8-1) \cdot (8-2) \cdot (8-4) = 168$

$\alpha_1 = 0 \quad \alpha_2 \notin \mathbb{F}_2(\alpha_1) \quad \alpha_3 \notin \mathbb{F}_2(\alpha_1, \alpha_2)$

找一个 G 的 Sylow-2 子群, 8 阶 $\left\{ \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} \right\}$

$|GL_n(\mathbb{F}_p)| = ?$ Sylow- p 子群?

第三章. 环和域

§ 3.1 定义与例子

定义 1.1. 一个环指三元组 $(R, +, \cdot)$

其中 R 为非空集合 (i) $(R, +)$ 形成加法群 (Abel)

(2) $(R, \cdot)$ 为一个乘法半群.

(3) 满足分配律 $a(b_1 + b_2) = ab_1 + ab_2$

$(b_1 + b_2) \cdot a = b_1 a + b_2 a$

若进一步.

(4) $(R, \cdot)$ 为含么半群. 则 R 称为含么环. 乘法元记作 1_R

(5) $ab = ba, \forall a, b$. 则 R 为交换环

(6) 若 $R \setminus \{0\}$ 为阿贝尔群. 则称 R 为域

域 $\subseteq$ 含幺交换环 $\subseteq$ 交换环 $\subseteq$ 环
 $\subseteq$ 含幺环

例. 1. $R = \{x\}$ 为独点环. 称 R 为零环

2. $\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z}$ 3. $M_n(R)$. R 为环. 全矩阵环

4. $H = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$

四元数 (Hamilton) $i^2 = j^2 = k^2 = ijk = -1$.

$$ij = k = -ji$$

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k)$$

$$= aa' - bb' - cc' - dd' + (ab' + ba' + cd' - c'd) i$$

$$+ (ac' + ca' + db' - d'b) j + (ad' + da' + bc' - b'c) k$$

$$(a + bi + cj + dk)^{-1} = (a - bi - cj - dk), \quad x^{-1} = \frac{\bar{x}}{|x|^2}$$

但 H 不交换. 是体 (除环) (skew-field, division ring)

思考. $\mathbb{R}$ 上所有有限维可除代数只有 $\mathbb{R}$. $\mathbb{C}$. H .

5. $H' = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$

H' 为 $M_2(\mathbb{C})$ 的子环

$$H \supset H'$$

A. 阿贝尔群.

$\text{End}_{\mathbb{Z}}(A) = \{f: A \rightarrow A \mid f \text{ 为群同态}\}$

$$(f+g)(a) \triangleq f(a) + g(a) \quad f \cdot g$$

构成含幺环

若 R 为环

$$L: R \rightarrow \text{End}_{\mathbb{Z}}(R)$$

$$a \mapsto L_a: x \mapsto ax$$

$$L_a \circ L_b = L_{ab} \quad R \text{ 含幺. 则 } L \text{ 为单射}$$

$$\text{例6. } R[x] = \{ a_0 + a_1x + \dots + a_nx^n \mid a_i \in R, n \geq 0 \}$$

7. R 环. G 群

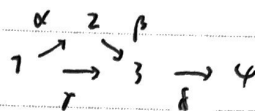
$$R[G] = \bigoplus_{g \in G} Rg = \{ \sum_{g \in G} a_g g \mid a_g \in R, g \in G \text{ 有限多个系数非零} \}$$

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

$$\sum_{g \in G} a_g g \cdot \sum_{g \in G} b_g g = \sum_{g, h \in G} a_g b_h (gh) = \sum_{k \in G} \left(\sum_{\substack{g, h \in G \\ gh=k}} (a_g b_h) \right) \cdot k$$

8. $\mathbb{F}$ 域 Q 有向图 (quiver)

$\mathbb{F}Q$ 基为所有道路



平凡道路 e_1, e_2, e_3, e_4

加法自伴

长度 1 $\alpha, \beta, \gamma, \delta$

$$\text{乘法 } p \cdot q = \begin{cases} pq & p \text{ 的终点} = q \text{ 的起点} \\ 0 & \text{否则} \end{cases}$$

2 $\alpha\beta, \beta\delta, \gamma\delta$

3. $\alpha\beta\gamma$

$(\mathbb{F}Q, \cdot)$ 形成一个环. $\mathbb{F}$ -代数

$\mathbb{F}$ -代数 $(A, +, \cdot)$

$(A, +, \cdot)$ 为环. $(A, +, \cdot)$ $\mathbb{F}$ 向量空间

且乘法 $\cdot: A \times A \rightarrow A$ 为双线性映射

(其实是 $(\lambda a) \cdot b = a \cdot (\lambda b) = \lambda(a \cdot b) \quad \forall \lambda \in \mathbb{F}, a, b \in A$)

命题. $A/\mathbb{F}$ (是 $\mathbb{F}$ 上线性空间) $\cdot$ 为 A 上的双线性二元运算

结论 $\cdot$ 满足结合律 (即 $(A, +, \cdot)$ 形成环)

$\Rightarrow$ 对 A 的任一组基 $e_i: i \in I, (e_i \cdot e_j) \cdot e_k = e_i \cdot (e_j \cdot e_k) \quad \forall i, j, k \in I$

$\Rightarrow \exists A$ 的 i -组基 $\dots$

$R \rightarrow$ 含幺环 $\tilde{R} = R \oplus \mathbb{Z}$

$$(a, n) \cdot (b, m) = (ab + nb + ma, mn) \quad \text{幺元为 } (0, 1)$$

命题 设 R 为环, 则

$$(1) \quad 0 \cdot a = a \cdot 0 = 0 \quad \forall a \in R$$

$$(2) \quad (na) \cdot b = n(a \cdot b) \quad \forall n \in \mathbb{Z}, a, b \in R$$

$$(3) \quad \sum_{i=1}^m a_i \cdot \sum_{j=1}^n b_j = \sum_{i,j} a_i b_j$$

$$\text{例 } x, y \in R \quad xy = yx$$

$$\Rightarrow (x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

$$xy = qyx \quad q \neq 0 \quad \text{非单位根}$$

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} q^k y^k x^{n-k}$$

$$[n]_q! = \frac{1-q^n}{1-q} [n]_q! = [n]_q [n-1]_q! \cdots [1]_q!$$

$$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q! [n-k]_q!}$$

定义 1.3. $0 \neq a, b \in R$. 若 $a \cdot b = 0$ 则称 a 为 R 的一个左零因子, b 为右零因子. 左 + 右零因子

定义 1.4. R 含 1_R 则称 b 左可逆, a 为 b 的一个左逆, a 为右可逆, a 为右逆, 左可逆 + 右可逆

注. 左(右)逆可能有无限多个

$$V = \mathbb{F}(e_1, e_2, e_3, \dots)$$

$$\text{End}(V): f: e_1 \rightarrow e_2 \rightarrow e_3 \cdots \quad f \circ g = \text{id}_V$$

$$g: e_1 \rightarrow e_1 \quad e_2 \rightarrow e_1, e_3 \rightarrow e_2 \cdots$$

$$|R| < \infty$$

左可逆 $\Leftrightarrow$ 非左零因子 $\Leftrightarrow$ 右可逆 $\Leftrightarrow$ 非右零因子

$$\exists a \quad ab=1$$

$$\exists x \quad bx=0$$

$$\ker(l_b) = \{0\}$$

$$l_b \text{ "单射"} \Rightarrow \text{同构} \Rightarrow 1 \in \text{Im}(l_b)$$

R 中的乘法可逆元称为 R 中的单位 (unit)

$$R^* = U(R) = \{R \text{ 中乘法可逆元全体}\}$$

No.

Date. / /

定义 1.5. 无零因子的交换环称为整环 ($\mathbb{Z}$, $\mathbb{F}[x]$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$)

非零元均可逆的环称为体 (skew field / division ring)

交换环称为域

子环

定义 1.6. $\emptyset \neq S \subseteq R$. R 环若 S 在 R 的加法乘法运算下形成一个环, 则称 S 为 R 的子环

注. 1. S 为 R 子环.

$\Leftrightarrow S$ 为 R 的加法子群, 乘法子半群.

$\Leftrightarrow \forall a, b \in S, a-b \in S, ab \in S$

2. 若 R 为含么环, 一般要求 $1_R \in S$

(不能只要求 S 为含么子环, 么元可能不一样)

例 $R = \{ \begin{pmatrix} a & b \end{pmatrix} \mid a, b \in \mathbb{R} \}$

U
 $S = \{ \begin{pmatrix} a & 0 \end{pmatrix} \mid a \in \mathbb{R} \}$

S 含么但 $1_R \notin S$

命题 1.7. 子环的交为子环

§ 3.2 环同态

定义 2.1 设 R_1, R_2 为环, 称 $f: R_1 \rightarrow R_2$ 为环同态, 若

(1) $f(a+b) = f(a) + f(b)$

(2) $f(ab) = f(a)f(b)$

若进一步, R_1, R_2 均为含么环, 称 f 为含么环同态, 若

(3) $f(1_{R_1}) = 1_{R_2}$

(如上例中 $S \hookrightarrow R$ 不是含么环同态)

单满同构

例 1. $\mathbb{H} \hookrightarrow \mathbb{H}'$

$$\left\{ \begin{array}{l} a+bi+cj+dk \\ a, b, c, d \in \mathbb{R} \end{array} \right\} \xrightarrow{\quad} \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \alpha \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$$

$$a+bi+cj+dk \rightarrow \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

2. $M_n(\mathbb{R}) \rightarrow M_{n+r}(\mathbb{R})$

$$A_{n \times n} \rightarrow \begin{pmatrix} A_{n \times n} & 0 \\ 0 & 0 \end{pmatrix}_{(n+r) \times (n+r)} \quad \text{不能保持元}$$

3. $M_m(\mathbb{R}) \times M_n(\mathbb{R}) \rightarrow M_{m+n}(\mathbb{R})$

$$(A, B) \rightarrow \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

4. $S \subseteq R$ 子环

$\text{inc}: S \hookrightarrow R$ 为环同态

5. $1_R \in R$ (含幺)

$$\Rightarrow \exists ! \varphi_R: \mathbb{Z} \rightarrow R \\ 1 \mapsto 1_R$$

6. $\text{Aut}(\mathbb{R})$ $\mathbb{R}$ 的自同构

$$\text{Aut}(\mathbb{Q}) \quad f: \mathbb{Q} \rightarrow \mathbb{Q} \quad (\text{因为 } f(1) = f(1^2) = f(1)^2 \\ = \{id\} \quad 1 \mapsto 1)$$

$$\Rightarrow q \mapsto q, \quad \frac{1}{p} \mapsto \frac{1}{p} \quad \Rightarrow \frac{q}{p} \mapsto \frac{q}{p}$$

同理 $\text{Aut}(\mathbb{C}) = \{id\}$

$$\text{Aut}(\mathbb{R}) \quad f|_{\mathbb{Q}} \xrightarrow{id} \mathbb{Q} \\ \uparrow \quad \uparrow \\ f: \mathbb{R} \xrightarrow{id} \mathbb{R}$$

$$r > 0 \Rightarrow f(r) > 0 \quad (\text{有平方根}) \Rightarrow f \uparrow$$

$$\text{而 } f|_{\mathbb{Q}} = id \Rightarrow f = id$$

No.

Date. / /

$$\ker f = f^{-1}(0)$$

$$\operatorname{Im} f = \{f(r) \mid r \in R\}$$

$$\varphi_R: \mathbb{Z} \rightarrow R \quad m \mapsto m \cdot 1_R$$

$$\ker \varphi_R \leq \mathbb{Z} \Rightarrow \ker \varphi_R = \begin{cases} 0 & n=0 \\ n\mathbb{Z} & n>0 \end{cases}$$

定义 2.2. R 为含幺环. 设 $\ker \varphi_R = n\mathbb{Z}$. $n \geq 0$. 则称 n 为 R 的特征 $n = \operatorname{char}(R)$

例. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. $\operatorname{char} = 0$

$$R = \mathbb{Z}/n\mathbb{Z} \quad \operatorname{char} R = n$$

命题 2.3. R, R' 交换环 $\varphi: R \rightarrow R'$ 环同态.

(1) $\forall \alpha' \in R'$. $\exists$ 唯一 $\tilde{\varphi}: R[x] \rightarrow R'$ 使得

$$\tilde{\varphi}(r) = \varphi(r) \quad \tilde{\varphi}(x) = \alpha'$$

(2) $\forall \alpha'_1 \dots \alpha'_n \in R'$. $\exists!$ $\tilde{\varphi}: R[x_1 \dots x_n] \rightarrow R'$

$$\tilde{\varphi}|_R = \varphi, \quad \tilde{\varphi}(x_i) = \alpha'_i$$

注. 1. $\varphi: R \rightarrow R'$

$$\mapsto \tilde{\varphi}: R[x] \rightarrow R'[x]$$

2. $a \in R$.

$\operatorname{ev}_a: R[x] \rightarrow R$ 赋值映射 非交换环不一定是同态
 $f(x) \mapsto f(a)$

例. $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ 满射

{

$$\mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x]$$

$$\alpha \in \mathbb{C} \quad \mathbb{Z} \hookrightarrow \mathbb{C}$$

$$\varphi_\alpha: \mathbb{Z}[\alpha] \rightarrow \mathbb{C}$$

$$f(x) \mapsto f(\alpha)$$

$\ker \varphi_\alpha \neq 0$. 则称 α 为代数数. $\ker \varphi_\alpha = 0$ 超越数

证明 加法群 $A \sim \rightarrow$ 正规子群
 $I \subseteq R$ $(R/I, +, \cdot)$

定义 $\bar{a} \cdot \bar{b} = \overline{ab}$

$$(a+i_1)(b+i_2) - ab = a i_2 + i_1 b + i_1 i_2$$

需要 $\forall i_1 \in I, i_2 \in I, i_1 b \in I, a i_2 \in I$

定义 2.4. R 为环. $I \neq R \subseteq R$.

满足 (i) I 为加法子群.

$$(ii) \forall a \in I \quad aR \subseteq I, Ra \subseteq I$$

称 I 是 R 的一个理想

平凡理想 $\{0\} \subseteq R$ 真理想 (proper) $I \neq R$

例 $\mathbb{Z}$. $\{n\mathbb{Z} \mid n \in \mathbb{Z}\}$ 是理想

$\mathbb{R}$ 理想平凡

$\varphi: R \rightarrow S$. 环同态 $\varphi \neq 0$

$\ker \varphi \neq R$ $\ker \varphi$ 为理想

I_1, I_2 理想. $I_1 + I_2, I_1 \cap I_2$ 都是理想

$\sum_{\alpha \in A} I_\alpha, \bigcap_{\alpha \in A} I_\alpha$ 都是理想

定义 2.5 $S \subseteq R$. $\exists \mathbb{Z} \langle S \rangle$ 包含 S 的 R 的最小理想. 称为 S 生成的理想

$$\langle S \rangle = \bigcap_{\substack{I \subseteq R \\ S \subseteq I}} I. \quad S = \{x\}. \quad \langle x \rangle \text{ 称为主理想.}$$

定义 2.6. 整环 (交换无 0 因子) R 的理想均为主理想. 则称 R 为主理想整环

PID. Principal Ideal Domain.

例. $\mathbb{Z}$. PID. $\mathbb{Q}[x]$. PID. $\mathbb{C}$ PID

$\mathbb{F}[x]$. $\mathbb{F}$ 是域 PID

No.

Date. / /

命题. 定义 2.7. $I \triangleleft R$. 则

(1) $\bar{R} = R/I$. 上唯一地诱导出一个环的结构使得 $\pi: R \rightarrow \bar{R}$ 为环同态
 $r \mapsto \bar{r}$

(2) $\ker \pi = I$.

此时, R/I 称为 R 对于理想 I 的商环

定理 2.8. $f: R \rightarrow R'$ 为环同态 (加法群同态 + 乘法半群同态)

(1) $\ker f \triangleleft R$. $\text{Im } f \leq R' \rightarrow$ 子环

(2) f 诱导环同构

$$\tilde{f}: R/\ker f \xrightarrow{\sim} \text{Im } f, \quad \bar{r} \mapsto f(r)$$

证. 由群同态基本定理, $\tilde{f}: R/\ker f \xrightarrow{\sim} \text{Im } f$ 是 Abel 群同构
而 $\tilde{f}$ 显然保持乘法

定理 2.9. $J \triangleleft R$. $\bar{R} = R/J$ $\pi: R \rightarrow \bar{R}, r \mapsto \bar{r}$. 则

$$(1) \{ I \triangleleft R \mid J \subseteq I \} \xrightarrow{1:1} \{ \bar{I} \triangleleft \bar{R} \}$$

$$(2) J \leq I \triangleleft R \Rightarrow R/I \cong \frac{R/J}{I/J}$$

例 $\mathbb{Z}[i]/(1+3i) \rightarrow$ 模 10 的复数主理想

$$\cong \mathbb{Z}/10\mathbb{Z}$$

$$f: \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}[i]/(1+3i) \quad \text{要说明 } \text{Im } f = \mathbb{Z}[i]/(1+3i)$$

$$\ker f = (10)$$

$$\overline{1+3i} = 0 \Rightarrow \overline{i-3} = 0 \Rightarrow \bar{i} = \bar{3} \Rightarrow \bar{i} \in \text{Im } f \Rightarrow \text{Im } f = \mathbb{Z}[i]/(1+3i)$$

$$\bar{10} = \overline{(1-3i)(1+3i)} = \bar{0}$$

$$\forall n. \quad n = (1+3i)(a+bi) \Rightarrow n^2 = 10(a^2+b^2) \Rightarrow 10 \mid n^2 \Rightarrow 10 \mid n$$

$$\Rightarrow \ker f = (10)$$

$$\Rightarrow \mathbb{Z}[i]/(1+3i) \cong \mathbb{Z}/10\mathbb{Z}$$

R 整环. (交换, 含幺, 无零因子)

$$\varphi_R: \mathbb{Z} \rightarrow R, \quad n \mapsto n \cdot 1_R$$

$$\text{char } R = \begin{cases} 0 & \mathbb{Z} \subset R \\ m & m \text{ 素}, \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subseteq R \end{cases}$$

(否则 $m = a \cdot b$ $a \cdot 1_R \neq 0$ $b \cdot 1_R \neq 0$ $a \cdot b \cdot 1_R = 0$ 矛盾)

命题 2.9 R 交换, $\text{char } R = p$, p 素, 则 $(x+y)^p = x^p + y^p$.

$$(x+y)^p = x^p + \dots + \binom{p}{i} x^i y^{p-i} \dots + y^p = x^p + y^p$$

推论 R 整, $\text{char } R = p$ 素数, 则 $\sigma: R \rightarrow R$ $\sigma(r) = r^p$ 为环的单同态

例 $\mathbb{C}[x, y]/(xy) \cong I$. 其中 $I = \{(p(x), q(y)) \mid p(0) = q(0)\} \subseteq \mathbb{C}[x] \times \mathbb{C}[y]$

$$f: \mathbb{C}[x, y] \rightarrow \mathbb{C}[x] \times \mathbb{C}[y]$$

$$h(x, y) \mapsto (h(x, 0), h(0, y)) \quad x\tilde{p}(x) + y\tilde{q}(y) + c$$

$$I \cap f = I \quad (I \cap f \subseteq I) \quad f^{-1}(p(x), q(y)) = x\tilde{p}(x) + y\tilde{q}(y) + c$$

$$h(x, y) \in \ker f \quad h(0, y) = 0 \quad h(x, 0) = 0$$

$$\Rightarrow h(x, y) = xy \tilde{h}(x, y) \quad \checkmark$$

定理 2.12 R 含幺环 $1, \dots, 1_n \in R$. 两两互素: $1_i + 1_j = R \quad \forall i \neq j$. 则有环同构

$$R/1_n \cdot 1_n \xrightarrow{\sim} R/1_1 \times \dots \times R/1_n$$

proof. $f: R \rightarrow R/1_1 \times \dots \times R/1_n$

$$r \mapsto (r+1_1, \dots, r+1_n)$$

$$\ker f = 1_1 \cap \dots \cap 1_n$$

要证满射, 只要证 $(\bar{0} \dots \bar{1} \dots \bar{0}) \in \text{Im } f$.

不妨取 $(\bar{1}, \bar{0} \dots \bar{0})$

$$n=2 \text{ 时 } 1_1 + 1_2 = R$$

No.

Date. / /

$$\Rightarrow r_1 + r_2 = 1 \quad \Rightarrow \begin{cases} r_2 \equiv 0 \pmod{I_2} \\ r_2 \equiv 1 \pmod{I_1} \end{cases}$$

$$\begin{aligned} I_1 + I_2 &= R \\ I_1 + I_3 &= R \end{aligned} \quad \Rightarrow \quad I_1 + I_2 \cap I_3 = R$$

因为 $1 = i_1 + i_2 = i_1' + i_3 \Rightarrow 1 = \underbrace{i_1 i_1'}_{I_1} + \underbrace{i_1 i_3 + i_1 i_2' + i_2 i_3}_{I_2 \cap I_3}$

由归纳 $I_1 + I_2 \cap I_3 \cap \dots \cap I_n = R$

$$\Rightarrow r_1 + r_0 = 1$$

$$\Rightarrow \begin{cases} r_0 \equiv 0 \pmod{I_j} & j=2, 3, \dots, n \\ r_0 \equiv 1 \pmod{I_1} \end{cases}$$

例. $m_1, m_2, \dots, m_n$ 互素

$$\frac{\mathbb{Z}}{m_1 m_2 \dots m_n \mathbb{Z}} \cong \frac{\mathbb{Z}}{m_1 \mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{m_n \mathbb{Z}}$$

§3.3. 整环与域

以下假设 R 含么. 交换

定义 3.1 $I \triangleleft R$ 称为素理想. 若 $\forall a, b \in R, ab \in I \Rightarrow a \in I$ or $b \in I$.

m 为极大理想 若 $m \neq R$ 且 $\forall I \triangleleft R$

$$m \subseteq I \Rightarrow I = m \text{ 或 } I = R$$

$$\Leftrightarrow R/m \text{ 无非平凡理想,}$$

命题 3.2 $P \triangleleft R$, 则下述等价

(1) P 素

$$(2) S_1, S_2 \subseteq P \Rightarrow S_1 \subseteq P \text{ 或 } S_2 \subseteq P$$

(3) R/P 为整环

proof (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1)

$$(1) \Rightarrow (2) \quad \bar{a} \cdot \bar{b} = 0 \Rightarrow ab \in P \Rightarrow a \in P \vee b \in P \Rightarrow a=0 \vee b=0 \quad \checkmark$$

$$(2) \Rightarrow (1) \quad \text{推逆否} \quad S_1 \not\subseteq P \quad S_2 \not\subseteq P \Rightarrow S_1 S_2 \not\subseteq P$$

$$\text{即} \quad \exists s_1 \in S_1 \quad s_2 \in S_2 \quad s_1 \notin P \quad s_2 \notin P$$

$$\Rightarrow \bar{s}_1 \neq 0 \quad \bar{s}_2 \neq 0 \Rightarrow \bar{s}_1 \bar{s}_2 \neq 0$$

$$\Rightarrow S_1 S_2 \not\subseteq P \Rightarrow S_1 S_2 \not\subseteq P$$

$$(2) \Rightarrow (1) \quad \text{取} \quad S_1 = \{0\} \quad S_2 = \{1\} \quad \text{即} \quad \checkmark$$

$$\text{例1.} \quad I \subset R \quad I \subset P_1 \cup \dots \cup P_n \quad P_i \text{ 素}$$

$$\Rightarrow \exists i \text{ 使 } I \subseteq P_i$$

$$\text{proof. 设 } I \cap P_i \not\subseteq \bigcup_{j \neq i} P_j \quad \forall i$$

(否则可以去掉 P_i)

$$\text{取 } a_1 \in (I \cap P_1) \setminus (P_2 \cup \dots \cup P_n)$$

$$\vdots$$

$$a_i \in (I \cap P_i) \setminus P_j$$

$$\text{取 } a_1 + a_2 + \dots + a_n \in I \quad \text{矛盾}$$

$$\begin{array}{c} \subset \\ P_i \end{array} \quad \begin{array}{c} \subset \\ P_i \end{array} \quad \not\subseteq P_1 \cup \dots \cup P_n$$

$$\subset P_i \quad \subset P_i \quad \forall i$$

命题 3.3. $m \not\subseteq R$. 则下述等价

(1). m 极大理想

(2). R/m 为域

推论 3.4. 极大理想为素理想

proof. (1) $\Rightarrow$ (2)

任取 $a \in m$. $a \in R$.

$$m \subset Ra + m \Rightarrow Ra + m = R$$

$$\Rightarrow \exists b \in R \quad m \subset m \quad ba + m = R$$

$$\Rightarrow \bar{b} \cdot \bar{a} = \bar{1}$$

(默认 R 是交换环)

No.

Date. / /

非交换就没有这么好的性质了。

如 $I \trianglelefteq M_n(\mathbb{R}) \Rightarrow I = \{0\}$ 或 $M_n(\mathbb{R})$

$$M_n(\mathbb{R}) / \{0\} = M_n(\mathbb{R})$$

$\text{Spec } R$. R 的素谱. 即所有素理想的集合.

$\text{Max } R$. R 的极大谱. 可如上定义 Zariski 拓扑.

例. (1) $R = \mathbb{Z}$ $\text{Spec } R$: $n\mathbb{Z}$. $n=0$ $n>0$ 素.

$\text{Max } R$. $n\mathbb{Z}$. $n>0$ 素.

$$\text{Spec } R = \text{Max } R \cup \{0\}.$$

(2) F -域 $R = F[x]$. $\rightarrow$ 主理想. $I = (f(x))$

$$\text{Max } R = \{(f(x)) \mid f(x) \text{ 不可约}\}.$$

$$\text{Spec } R = \text{Max } R \cup \{0\}.$$

(3). $R = \mathbb{Z}[x]$. (p) 素. (x) 素.

$$\mathbb{Z}[x]/(p) \cong \mathbb{Z}/p\mathbb{Z}[x].$$

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

$$(0) \subseteq \overset{(p)}{(x)} \subseteq (p, x)$$

$$\mathbb{Z}[x]/(p, x) \cong \mathbb{Z}/p\mathbb{Z}.$$

命题 3.5. $I \trianglelefteq R$. 理想. 则存在 R 的极大理想 m . 使得 $I \subseteq m$.

证. 令 $S = \{J \trianglelefteq R \mid I \subseteq J\}$.

则 S 满足 Zorn 引理的条件

$\Rightarrow S$ 中有极大元.

Zorn 引理. $(S, \supseteq)$ 为偏序集 $x \subseteq S$. 满足 x 中的任一链. (含序子集) 在 x 中有上界. 则 x 必有极大元.

$\forall \{J_\alpha\}$. 含序子集. 取 $\bigcup J_\alpha$. 即上界. 且不为 R . (因为不能有 1)

推论 3.6. R 含么交换 $\Rightarrow R$ 存在极大理想 $\Rightarrow R$ 存在素理想

局部化与商域

定义 3.7. R 含么交换环, $S \subseteq R$ 称为 R 的一个乘法子集, 若

$$(1) 1 \in S, 0 \notin S$$

$$(2) s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$$

注. $1 \in R$ 真理想

I 为素理想 $\Leftrightarrow R/I$ 为乘法子集

$$\text{对 } R \times S, \quad \frac{r_1}{s_1} \sim \frac{r_2}{s_2} \Leftrightarrow \exists s \in S, s r_1 s_2 = s r_2 s_1$$

引理 3.8. $\sim$ 为 $R \times S$ 上一个等价关系, 记 $S^{-1}R = \frac{R \times S}{\sim}$

定理 3.9. $(S^{-1}R, +, \cdot)$ 形成一个含么交换环, 其中 $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + s_1 r_2}{s_1 s_2}$

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

且 (1) $f: R \rightarrow S^{-1}R, r \mapsto \frac{r}{1}$ 为环同态, $f(s) \in (S^{-1}R)^\times$

(2) $\varphi: R \rightarrow T$ 为含么环同态, 且 $\varphi(s) \in T^\times$, 则 $\exists! \tilde{\varphi}: S^{-1}R \rightarrow T$ 使 $\varphi = \tilde{\varphi} \circ f$

证. 等价关系: $\frac{r}{s} \sim \frac{r'}{s'} \Leftrightarrow rs' = r's$

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \quad \frac{r_2}{s_2} \sim \frac{r_3}{s_3} \quad s r_1 s_2 = s r_2 s_1 \quad s' r_2 s_3 = s' r_3 s_2$$

$$\Rightarrow (s s' s_2 r_2) r_1 s_3 = (s s' r_2 s_2) r_3 s_1 \Rightarrow \frac{r_1}{s_1} \sim \frac{r_3}{s_3}$$

$$\text{加法定义合理} \quad \frac{r_1}{s_1} \sim \frac{r'_1}{s'_1} \Leftrightarrow s r_1 s'_1 = s r'_1 s_1$$

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} \sim \frac{r'_1}{s'_1} + \frac{r_2}{s_2} \Leftrightarrow s(s'_1 s_2 r_1 s_2 + s'_1 s_2 s_1 r_2) = s(s'_1 s_2 r'_1 s_2 + s'_1 s_2 s_1 r_2)$$

$$(2) \tilde{\varphi}(\frac{r}{s}) \stackrel{\circ}{=} \varphi(r) \varphi(s)^{-1}$$

$$\text{注 (1) } \ker \tilde{\varphi} = \{ r \in R \mid \frac{r}{1} \sim 0 \} = \{ r \in R \mid \exists s \in S, \text{ 使 } rs = 0 \}$$

$$= \{ s \text{ 所有的零化子} \}$$

若 R 为整环, 则 f 单.

(2) 若 R 不交换, 如何局部化

(ore 条件)

定义 3.10. $S^{-1}R$ 称为 R 对于乘法子集 S 的局部化

特别地 $S = R \setminus P$, P 素理想, $S^{-1}R$ 称为 R 在 P 处的局部化, localization
记作 R_P . 此时 R_P 具有唯一极大理想 $P R_P = \{ \frac{p}{s} \mid p \in P, s \notin P \}$
(因为不可逆元生成的主理想是真理想, 一定落在某个极大理想内)

例 (1) $R = \mathbb{Z}$, P 素, $S = \{1, p, p^2, \dots\}$

$$S^{-1}R = \{ \frac{n}{p^i} \mid i \geq 0, n \in \mathbb{Z} \}$$

(2) $\mathbb{Z}$, P 素, $P = p\mathbb{Z}$

$$\mathbb{Z}_P = \{ \frac{n}{p^i} \mid (p, n) = 1, n \in \mathbb{Z} \}$$

(3) $R = \mathbb{F}[x]$, $S = \{1, x, x^2, \dots\}$

$$\begin{aligned} S^{-1}R &= \{ \frac{f(x)}{x^i} \mid i \geq 0, f(x) \in \mathbb{F}[x] \} \\ &= \mathbb{F}[x, x^{-1}] = \mathbb{F}(x) / (x \neq 0) \end{aligned}$$

第四章 环的因子分解

不加说明, 以下假定 R 为整环

§4.1. 唯一因子分解整环

定义 1.1. R 整, $a, b \in R$, $b = a \cdot x$, $a \neq 0$, 则称 a 为 b 的因子, b 为 a 的陪元
记作 $a \mid b$ 称 a 与 b 相伴若 $a \mid b, b \mid a$. 此时记作 $a \sim b$

进一步, 若 $x \in R^*$, 则称 a 为 b 的真因子.

命题 1.2. $a, b \in R \setminus \{0\}$, $u \in R^*$

$$(1) a \mid b \Leftrightarrow (a) \supseteq (b)$$

$$(2) u \sim 1 \text{ 且 } \forall 0 \neq r \in R^* \text{ } u \text{ 为 } r \text{ 的真因子 } (r = u \cdot u^{-1}r)$$

$$(3) a = bu \Leftrightarrow a \mid b \text{ (需要整环)}$$

$$(4) a \text{ 为 } b \text{ 真因子} \Leftrightarrow (a) \subsetneq (b)$$

$$\text{proof } (1) a \mid b \Rightarrow b = ax \Rightarrow b \in (a) \Rightarrow (b) \subseteq (a)$$

$$(b) \subseteq (a) \Rightarrow b \in (a) \Rightarrow \exists x \quad b = ax$$

$$(3) \Rightarrow a = bu \Rightarrow b = au^{-1} \Rightarrow a \sim b$$

$$\Leftarrow b = ax \quad a = by \Rightarrow a = a(xy) \Rightarrow xy = 1 \Rightarrow x \in R^*$$

(4) $\Rightarrow$ 由 (3) 易知.

定义 1.3. (1) $p \neq 0, p \in R^*, p|ab \Rightarrow p|a$ 或 $p|b, \forall a, b \in R. \triangleq p$ 素元

(2) $a \in R^*, a \neq 0$. 若 $a = bc \Rightarrow b \in R^*$ 或 $c \in R^*. \triangleq a$ 不可约元

例. $R = \mathbb{Z}, \neq \{x\}$. 素元 = 不可约元

命题 1.4. $p, a \in R \setminus \{0\}$.

(1) p 素元 $\Leftrightarrow (p)$ 为主理想.

(2) a 不可约 $\Leftrightarrow (a)$ 为主理想中极大元

(3) 素元 $\Rightarrow$ 不可约元

(4) 若 R 为 PID (主理想整环) 则不可约 $\Rightarrow$ 素.

proof (1) p 素 $\Leftrightarrow \forall a, b, p|ab \Rightarrow p|a$ 或 $p|b$

即 $\forall a, b, ab \in (p) \Rightarrow a \in (p)$ 或 $b \in (p)$

$\Leftrightarrow (p)$ 是素理想.

$$(2) \quad a = bc \Rightarrow b \in R^* \text{ 或 } c \in R^*$$

$$\begin{array}{ccc} \Downarrow & \Downarrow & \Downarrow \\ (a) \subseteq (b) & (a) = (c) & (a) = (b) \end{array}$$

$$(a) \subseteq (c) \quad (a) \subseteq (b) \Rightarrow a = b \cdot c \Rightarrow (b) = R \text{ 或 } (a) = (b)$$

$$(3) \quad p \text{ 素} \quad p = ab$$

$$\Rightarrow \begin{array}{l} p|a \Rightarrow a = px \Rightarrow p = px \cdot b \Rightarrow xb = 1 \\ p|b \Rightarrow \dots \end{array}$$

(4). R 为 PID. $\Rightarrow R$ 中所有理想都是主理想

a 不可约 $\Rightarrow (a)$ 极大理想 $\Rightarrow (a)$ 素 $\Rightarrow a$ 素.

No.

Date. / /

定义 1.5. 设整环 R 满足

$$(UF1) \quad \forall 0 \neq a \in R \quad a \in R^\times \quad a = c_1 \cdots c_n \quad c_i \text{ 不可约}$$

$$(UF2) \quad a = c_1 \cdots c_n = d_1 \cdots d_m \quad c_i, d_j \text{ 不可约} \quad \text{则 } n=m$$

$$\text{且 } \exists \sigma \in S_n \text{ 使得 } c_i \sim d_{\sigma(i)} \quad \forall i$$

则称 R 为唯一分解整环 (Uniquely Factorized Domain UFD)

$$\text{例 (1) } \mathbb{F}[x_1, x_2, \dots] \quad x_2^2 = x_1 \quad x_3^2 = x_2$$

不能分解. 因为 $x_1 = x_2^2 = x_3^4 = \dots$ UFD 不成立

$$(2) \quad R = \mathbb{Z}[\sqrt{-5}]$$

$$6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3 \quad (\text{利用模长整除关系证明})$$

定义 1.6. R 整. $a, b \in R, (a, b) \neq (0, 0)$

若 $\exists d$ 满足

$$(1) \quad d|a, \quad d|b$$

$$(2) \quad \forall d'|a, d'|b \Rightarrow d'|d$$

则称 d 为 a, b 的最大公因子. $\gcd(a, b) = (a, b)$

→ 不一定存在

同理, 可定义最小公倍数 $\text{lcm}(a, b) = [a, b]$

引理 1.7. 设 R 中最大公因子存在 $a, b, c \in R \setminus \{0\}$

$$(1) \quad (u, 0) \sim 1 \quad \forall u \in R^\times$$

$$(2) \quad (ca, b), c) \sim (a, (b, c))$$

$$(3) \quad d(a, b) \sim (da, db)$$

$$(4) \quad (a, b) \sim 1 \quad (a, c) \sim 1 \Rightarrow (a, bc) \sim 1$$

$$\text{proof (2) } \left. \begin{array}{l} (a, (b, c)) \mid (a, b) \\ (a, (b, c)) \mid c \end{array} \right\} \Rightarrow (a, (b, c)) \mid ((a, b), c) \stackrel{(1)}{\sim} 1 \Leftarrow$$

$$(5) \quad d(a, b) \mid da$$

$$\Rightarrow d(a, b) \mid (da, db)$$

$$d(a, b) \mid db$$

$$d \mid (da, db) \Rightarrow (da, db) = d \cdot c$$

$$dc \mid da \Rightarrow c \mid a \quad \text{同 } c \mid b \Rightarrow c \mid (a, b)$$

$$\Rightarrow (da, db) \sim (da, b)$$

$$\text{REMEMBER: } (a, b) \sim ((a, ac), bc) \sim (a, (ac, bc)) \sim (a, c(a, b)) \sim (ac) \sim 1$$

定理 1.8. $R: UFD$, 则

(1). (诺特性). 主理想升链稳定

$$\forall (a_1) \subseteq (a_2) \subseteq \dots \quad \exists N \quad (a_N) = (a_{N+1}) = \dots$$

(2) R 上不可约元为素元

(3) 最大公因子存在 $\forall a, b \neq 0 \quad (a, b) \exists$.

proof. (1) 反之设 $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$ 存在

$$a_1 = a_2 x_1 \quad x_1 \text{ 均不为单位.}$$

$$a_2 = a_3 x_2 \quad \Rightarrow \quad a_1 = a_n x_{n-1} x_{n-2} \dots x_1$$

$$\vdots \quad R: UFD \quad \Rightarrow \quad a_1 = c_1 c_2 \dots c_m \quad c_i \text{ 不可约}$$

写成不可约因子乘积最多 m 个. 取 $n > m+1$ 矛盾

故这样严格递增的主理想升链不存在.

(2) 设 a 不可约 $a|bc$ 即 $bc = a \cdot x$

$$b_1 \dots b_t c_1 \dots c_u \sim a \cdot x_1 \dots x_s$$

$$\Rightarrow \exists j \quad a \sim b_j \text{ 或 } a \sim c_j \quad \Rightarrow a|b \text{ 或 } a|c$$

$$(3) \quad a \sim p_1^{u_1} \dots p_s^{u_s} \quad p_i \neq p_j \quad \forall i \neq j$$

$$b \sim p_1^{v_1} \dots p_s^{v_s} \quad u_i, v_i \text{ 可为 } 0$$

$$(a, b) \sim p_1^{\min(u_1, v_1)} \dots p_s^{\min(u_s, v_s)}$$

定理 1.9.

$$UFD \Leftrightarrow (1) + (3)$$

$$\Rightarrow (1) + (2)$$

$$\text{证. } (1) + (3) \Rightarrow (2)$$

设 a 不可约. $a|bc$.

$$\text{若 } a \nmid b \quad a \nmid c \Rightarrow (a, b) \sim 1 \quad (a, c) \sim 1$$

$$\Rightarrow (a, bc) \sim 1 \quad \text{矛盾}$$

即 $a|b$ 或 $a|c$ a 为素元

$$(1) + (2) \Rightarrow UFD$$

存在性由 (1) 给出

断言 $0 \neq a \in R$, $a \in R^*$ a 存在不可约因子

反设, $\exists 0 \neq a \in R^*$ a 不含不可约因子

则 $a = a_1 b_1$, $a_1, b_1 \in R^*$

$\Rightarrow a_1, b_1$ 都不含不可约因子 故可一直分解

$b_1 = a_2 b_2$ $b_2 = a_3 b_3$ $\dots$ $b_i, a_i \in R^*$

$(a) \subsetneq (b_1) \subsetneq (b_2) \subsetneq (b_3) \dots$ 与 (1) 矛盾

故 a 有不可约因子

下设 $0 \neq a \in R^*$. 由断言 $\exists a$ 不可约 $a = a_1 b_1$

若 $b_1 \in R^*$ 结束.

若 $b_1 \notin R^*$. $\exists a_2$ 不可约 $b_1 = a_2 b_2$

断言. 有限步后 b_i 是单位. 否则与 (1) 矛盾

$a = a_1 \dots a_n b_n$ a_i 不可约. $b_n \in R^*$ 分解的存在性.

唯一性由 (2) 给出

$b_1 \dots b_n \sim c_1 \dots c_n$ b_i, c_j 不可约

$b_1 \mid c_1 \dots c_n$ b_1 素 $\Rightarrow b_1 \mid c_i \exists i$

$\Rightarrow b_2 \dots b_n \sim c_1 \dots c_{i-1} c_{i+1} \dots c_n$ $\begin{pmatrix} ax \sim by \\ \Leftrightarrow x \sim y \end{pmatrix}$

重复上述构造

定义 1.10. R 整. 若存在 $\varphi: R \setminus \{0\} \rightarrow \mathbb{Z}_+$ 且 $\forall a, b \in R$. $a \neq 0$ $\exists q, r$ 使 $b = qa + r$ 且 $r = 0$ 或 $\varphi(r) < \varphi(a)$ 则称 R 为欧氏整环 (E.D)

例 $\mathbb{Z}$. $\varphi(n) = |n|$

$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ $\varphi(x) = |x|^2$

$K[X]$. K 域 φ 多项式次数

命题 1.11. $ED \Rightarrow PID \Rightarrow UFD$.

$ED \Rightarrow PID$ 取 $a \in I$ 设 $\varphi(a)$ 最小.

$PID \Rightarrow UFD$

要证 1.8. (1) (2) (满足?)

若 R PID , $(a) + (b) = (a, b)$

$$(a) \cap (b) = ([a, b])$$

$$(a_1) \subseteq (a_2) \subseteq \dots$$

$$\bigcup_{i=1}^{\infty} (a_i) = (a) \Rightarrow \exists n. a \in (a_n) \Rightarrow (a) \subseteq (a_n) \Rightarrow (a_n) = \bigcup_{i=1}^{\infty} (a_i)$$

$$\begin{array}{l} \text{例 } \mathbb{Z}[\sqrt{-1}] \\ \mathbb{Z}[\sqrt{-2}] \end{array} \quad \begin{array}{l} \supset \\ \supset \end{array} ED$$

$$\varphi(x+y\sqrt{-1}) = x^2+y^2$$

$$\varphi(x+y\sqrt{-2}) = x^2+2y^2$$

$$D: UFD \Rightarrow D[x] \text{ UFD}$$

§4.2 多项式环

R 含幺环, $R[x]$

引理 2.1.

$$(1) \deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$$

$$(2) \deg(f(x) \cdot g(x)) \leq \deg f(x) + \deg g(x)$$

引理 2.2. D 环

$$D[x] \text{ 整环} \Leftrightarrow D \text{ 为整环}$$

$$\left(\begin{array}{l} D[x] \text{ 含幺} \Leftrightarrow D \text{ 含幺} \\ D[x] \text{ 交换} \Leftrightarrow D \text{ 交换} \end{array} \right)$$

R 整

(R 不整不行 如 $\exists \varepsilon \in R, \varepsilon^2=0$)

$$f(x) \in R[x]^* \Leftrightarrow f(x) \in R^*$$

$$(1+\varepsilon x)(1-\varepsilon x) = 1$$

No.

Date.

引理 2.3 R 为 $f(x), g(x) \in R[x]$. 且 $g(x)$ 首项 $\in R^*$

则 $\exists$ 唯一 $q(x) \in R[x], r(x) \in R[x]$. 使得 $f(x) = g(x)q(x) + r(x)$

$$\deg r(x) < \deg g(x).$$

注其实对一般的含 x 环都成立

proof. 对 $\deg f(x)$ 归纳即可

$$f(x) = a_n x^n + \dots + a_0 \quad g(x) = b_m x^m + \dots + b_0 \quad b_m \in R^*$$

$$n < m \quad \text{取 } g(x) = 0 \quad r(x) = f(x)$$

唯一性

$$n \geq m \quad f(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

$$(\tilde{f}(x) - q(x))g(x) = r(x) - \tilde{r}(x)$$

只能左右为 0

推论 2.4. (余数定理).

$$f(x) \in R[x], c \in R. \exists \text{ 唯一 } g(x) \in R[x], f(x) = g(x)(x-c) + f(c)$$

特别地 R 含 x 交换. 则 c 为 $f(x)$ 的根 $\Leftrightarrow (x-c) \mid f(x)$

$$\text{注 } R \text{ 非交换 } (fg)(c) \neq f(c)g(c)$$

推论 2.5. $D \subseteq E$. 为整环

$f(x) \in D[x]$ 在 E 中最多有 $\deg f$ 个根.

proof. 对 $f(x)$ 的次数进行归纳

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

$$f\left(\frac{p}{q}\right) = 0 \quad p, q \in \mathbb{Z}, p, q \neq 0, (p, q) = 1$$

$$\Rightarrow p \mid a_n \quad q \mid a_0$$

命题 2.6. 设 D 为 UFD. F 为 D 的分式

$$f(x) = a_n x^n + \dots + a_0 \text{ 为 } D[x] \text{ 的 } n \text{ 次多项式}$$

$$\text{若 } u = \frac{c}{d} \quad (c, d \in D, (c, d) = 1, d \neq 0)$$

$$\text{为 } f(x) \text{ 的根} \quad \text{则} \quad d \mid a_n \quad c \mid a_0$$

定义 2.7 R 整环.

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x], \text{ 的次数 } \geq 1$$

$$f'(x) = n a_n x^{n-1} + \dots + a_1$$

$$f(x) = (x-c)^n g(x), \quad g(c) \neq 0$$

称 c 为 $f(x)$ 的 n 重根.

定理 2.8. D 整环. $0 \in D$. $f(x) \in D[x]$. $c \in D$

$$(1) \quad c \text{ 为 } f(x) \text{ 的 } n \text{ 重根} \iff f(c) = f'(c) = \dots = f^{(n-1)}(c) = 0, \quad f^{(n)}(c) \neq 0$$

$$(2) \quad \text{若 } \text{char } D = 0 \text{ 或 } \text{char } D > \deg f(x) \implies c \text{ 为 } n \text{ 重根} \iff f(c) = f'(c) = \dots = f^{(n-1)}(c) = 0, \quad f^{(n)}(c) \neq 0$$

$$(3) \quad D \text{ 为域 } (f, f') = 1 \implies f(x) \text{ 无重根.}$$

证 (1) $m=1$. $f(c) = 0, \quad f'(c) \neq 0$

$$\implies f(x) = (x-c)g(x), \quad g(c) \neq 0$$

$$\text{设 } f(x) = (x-c)^r g(x)$$

$$f'(x) = (x-c)^{r-1} (r g(x) + (x-c) g'(x))$$

$$f'(c) \neq 0 \implies r=1, \quad g(c) \neq 0 \quad \text{故 } c \text{ 的重数为 } 1$$

$m > 1$ 归纳法

$$\text{若 } m=2 \quad f(c) = f'(c) = 0, \quad f''(c) \neq 0$$

$$f(x) = (x-c)^r g(x), \quad f'(x) = (x-c)^{r-1} (r g(x) + (x-c) g'(x)) = (x-c)^r h(x)$$

$$| \quad r \geq 2 \implies r=2 \text{ 且 } r g(c) \neq 0 \implies r=2, \quad g(c) \neq 0$$

$$| \quad r g(c) = 0 \implies r=0 \text{ in } D \implies f(x) = (x-c)^r g(x) \implies f'(x) = (x-c)^r g'(x), \quad \text{若}$$

D 是 UFD $\implies D[x]$ 是 UFD

定义 2.9. D 是 UFD. $0 \neq f(x) = a_n x^n + \dots + a_0 \in D[x]$. $f(x)$ 的容积分 (content) 为 $\gcd(a_n, \dots, a_0)$

记作 $c(f)$. 若 $c(f) \sim 1$ 则称 f 为本原多项式

引理 2.10. (Gauss 引理) D 是 UFD. $f(x), g(x) \in D[x]$

$$\text{则 } c(fg) = c(f) c(g)$$

$\implies$ 两个本原多项式的乘积为本原多项式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$$

$$\text{v.p.f. } (fg) = \sum_k \left(\sum_{r+s=k} a_r b_s \right) x^k$$

$$\text{要 } \exists k. \quad p \nmid c_k$$

$$\begin{array}{l} p \mid a_0 \dots a_{i-1} \quad p \nmid a_i \\ p \mid b_0 \dots b_{j-1} \quad p \nmid b_j \end{array} \quad C_{i+j} = \underbrace{a_i \dots a_i}_{b_j \dots b_j} \underbrace{a_{i-1} \dots a_0}_{b_{j+1} \dots b_{i+j}} \quad p \nmid C_{i+j}$$

引理 2.11. $D: UFD$. $K = \mathbb{Q}(D)$ 商域. $f, g \in D[x]$ 为本原多项式

$$f \sim^{D[x]} g \Leftrightarrow f \sim^{K[x]} g$$

proof. $\Rightarrow$ 显然

$$\Leftarrow f \sim^{K[x]} g \quad \text{即 } \exists u = \frac{d}{c} \in K^+ \quad f = \frac{d}{c} g(x), \quad c, d \in D$$

$$\Rightarrow \text{在 } D[x] \text{ 中有 } c f(x) = d g(x) \quad \text{两边取容和}$$

$$c \sim d \text{ in } D \quad \frac{d}{c} \in D^*$$

引理 2.12. $f(x) \in D[x]$.

$f(x)$ 不可约 $\Leftrightarrow f$ 满足下述之一

(1) $f(x) = p$. p 为 D 中不可约元

(2) $f(x)$ 本原, 且 $f(x)$ 在 $K[x]$ 中不可约

proof $\Leftarrow f(x) \in D[x]$. 若满足 (1), (2). 则 $f(x)$ 在 $D[x]$ 中不可约

$$\text{若 } f(x) = f_1(x) f_2(x) \quad \text{d.g. } f_1, f_2 \neq 1 \in K[x]$$

$$= \frac{c}{d} \tilde{f}_1(x) \tilde{f}_2(x) \quad \tilde{f}_1, \tilde{f}_2 \in D[x] \text{ 本原.}$$

$$\Rightarrow d f(x) = c \tilde{f}_1(x) \tilde{f}_2(x)$$

$$\Rightarrow d \sim c \quad \Rightarrow \text{与 } f(x) \text{ 不可约矛盾}$$

定理 2.13. (Gauss 定理) D 为 UFD $\Rightarrow D[x]$ 为 UFD

proof 分解存在性.

$$\begin{aligned} f(x) &= f_1(x) f_2(x) \cdots f_n(x) \quad f_i(x) \in K[x] \xrightarrow{\text{UFD}} \text{不可约} \\ &= \frac{c}{d} \tilde{f}_1(x) \tilde{f}_2(x) \cdots \tilde{f}_n(x) \quad \tilde{f}_i \in D[x] \text{ 本原} \quad \tilde{f}_i \xrightarrow{K[x]} f_i(x) \quad \tilde{f}_i \text{ 不可约} \\ &\Rightarrow d \mid c f_1 \sim c \quad \Rightarrow \frac{c}{d} \in D \rightarrow \text{UFD} \\ &\Rightarrow \frac{c}{d} = a_1 \cdots a_s \xrightarrow{\text{不可约}} f(x) = a_1 \cdots a_s \tilde{f}_1(x) \cdots \tilde{f}_n(x) \end{aligned}$$

$$a_1 \cdots a_s f_1 \cdots f_r = b_1 \cdots b_u g_1 \cdots g_v$$

取范数 $a_1 \cdots a_s \stackrel{D}{\sim} b_1 \cdots b_u$ 由 D UFD

$$f_1 \cdots f_r \stackrel{K[x]}{\sim} g_1 \cdots g_v$$

定理 (Eisenstein) $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. 若存在 p 素, 使 $p \mid a_0, \dots, a_{n-1}$, $p^2 \nmid a_0$. 则 $f(x)$ 为不可约多项式

proof 反设 $f(x) = f_1(x) f_2(x)$ f_i 首一.

$$f_1 = x^r + b_{r-1}x^{r-1} + \cdots + b_0 \quad f_2 = x^s + c_{s-1}x^{s-1} + \cdots + c_1x + c_0$$

不妨设 $p \mid b_0, p \mid c_0$

$$\text{设 } \exists i: p \mid b_0, b_1, \dots, b_i \quad p \nmid b_{i+1} \quad 0 \leq i \leq r-1$$

$$a_i = \underbrace{b_0 c_i + b_1 c_{i-1} + \cdots + b_{i-1} c_1}_{\sim} + b_i c_0 \quad \times$$

$$(1) \quad \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

$$\rightarrow \pi: \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$$

$$f(x) \mapsto \bar{f}(x) = x^n = \bar{f}_1(x) \bar{f}_2(x)$$

$$\Rightarrow \bar{f}_1(x) = x^r, \quad \bar{f}_2(x) = x^s$$

$$\Rightarrow p \mid b_0 \cdots b_{r-1} \quad p \mid c_0 \cdots c_{s-1} \Rightarrow p^2 \mid a_0 \text{ 矛盾}$$

第五章. 有限域

§5.1 域扩张

$$\mathbb{Z} \hookrightarrow \mathbb{F}$$

$$\cap \mathbb{Q} \hookrightarrow$$

$$\text{char } \mathbb{F} = 0$$

$$\mathbb{Z} \hookrightarrow \mathbb{F}$$

$$\mathbb{F}_p \hookrightarrow$$

$$\text{char } \mathbb{F} = p$$

$\mathbb{Q}, \mathbb{F}_p$ 素域

任一域包含 $\mathbb{Q}$ 或 $\mathbb{F}_p$ 作为子域

$$F \subseteq K, \quad \varphi: F[x] \rightarrow K$$

$$\ker \varphi = 0 \quad \text{或} \quad \ker \varphi = (f(x)) \quad f \text{ 首一}$$

$$\ker \varphi = 0 \quad F[x] \hookrightarrow K \quad \text{单射}$$

$$\begin{matrix} F[x] \\ \downarrow \cap \\ F[x] \end{matrix} \quad \nearrow$$

$$\ker \varphi = (f(x)) \quad F[x]/(f(x)) \hookrightarrow K$$

定义 1.1. $F \subseteq K$ 子域, 则称 K 为 F 的一个域扩张, 记作 K/F

$\alpha \in K \quad F(\alpha) \quad K$ 中包含 α, F 的最小子域

$F[\alpha], K$ 中包含 α, F 的最小环

例 $\mathbb{C}/\mathbb{Q}$

$$\sqrt{-1}: \quad \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$$

$$\pi: \quad \mathbb{Q}(\pi) = \{a_0 + a_1\pi + \dots + a_n\pi^n \mid a_i \in \mathbb{Q}\}$$

$$\mathbb{Q}(\pi) = \left\{ \frac{g(\pi)}{f(\pi)} \mid f(x), g(x) \in \mathbb{Q}[x], f(x) \neq 0 \right\}$$

$K = F(\alpha) \quad \text{单扩张}$

$K = F(S) \quad |S| < \infty \quad \text{有限生成扩张}$

定义 1.2. $K/F, \quad \alpha \in K$

$$\varphi_\alpha: F[x] \rightarrow K$$

$$f(x) \mapsto f(\alpha)$$

$\ker \varphi_\alpha = 0$ 称 α 为 F 上的超越元

$\ker \varphi_\alpha \neq 0 \quad \dots \quad \text{代数元}$

$\ker \varphi_\alpha = (f(x)) \quad \exists! f(x) \text{ 首一} \quad \alpha \text{ 的极小多项式}$

注. $0 \neq \ker \varphi_\alpha$ 中元素 $g(x)$ 称为 α 的一个零化多项式

命题 1.3. (i) α 超越 $\Rightarrow F(\alpha) \cong F[x]$

(ii) α 代数 $\Rightarrow F(\alpha) \cong F[x]/(f(x))$

$f(x)$ 为 α 的极小多项式

定义 1.4. K/F . K 为 F -向量空间

$\dim_F K$ 称为扩张次数, 记作 $[K:F]$

有限扩张 $[K:F] < \infty \Rightarrow$ 有限生成

无限扩张

命题 1.5. $K = F(\alpha)$, $f(x)$ 为 α 的极小多项式, 则 $[K:F] = \deg f = n$

此时 $1, \alpha, \dots, \alpha^{n-1}$ 为 K 的一组基. 反之, 若 $[F(\alpha):F] < \infty$ 则 α 有 F 上代数
proof. $\because f(\alpha) = 0$.

$1, \alpha, \dots, \alpha^{n-1}$ 线性无关

若 $\exists b_0, \dots, b_{n-1}$ $b_0 + b_1 \alpha + \dots + b_{n-1} \alpha^{n-1} = 0 = g(\alpha)$

$g(x)$ 是零化多项式 $\deg g < \deg f$ 与 f 极小矛盾

$$\alpha^n = -a_{n-1} \alpha^{n-1} - a_{n-2} \alpha^{n-2} \dots - a_0$$

归纳知 $1, \alpha, \dots, \alpha^{n-1}$ 生成 $F(\alpha)$

(2) $1, \alpha, \dots, \alpha^{n-1}, \dots$ 线性相关

$\Rightarrow \alpha$ 代数

定理 1.6 $K/M/F$. $[K:F] = [K:M] \cdot [M:F]$

推论 1.7 K/F .

$$[K:F] = n, \Rightarrow \forall \alpha \in K \quad [F(\alpha):F] \mid n$$

推论 1.8. 若 $[K:F] = p$, 则 $\forall \alpha \in K \mid F$

α 在 F 上极小多项式次数为 p . $F(\alpha) = K$.

命题 1.9. 有限扩张 = 有限生成代数扩张.

命题 1.10. $K/M/F$

K/F 代数 $\Leftrightarrow K/M, M/F$ 代数

prop. " $\Leftarrow$ " $\alpha \in K$.

α 在 F 上代数 $\Leftrightarrow [F(\alpha):F] < \infty$.

K/M 代数

$$\Rightarrow \alpha^n + a_{n-1}\alpha^{n-1} + \dots + \alpha_1\alpha + a_0 = 0$$

$$[F(\alpha, a_0, a_1, \dots, a_{n-1}) : F(a_0, a_1, \dots, a_{n-1})] < \infty$$

$$[F(a_0, \dots, a_{n-1}) : F] < \infty$$

$$\Rightarrow [F(\alpha, a_0, \dots, a_{n-1}) : F] < \infty$$

$$\Rightarrow [F(\alpha) : F] < \infty.$$

定理 1.11 K/F . 则 K 中所有在 F 上代数的元素, 构成 K 的子域

称为 F 在 K 中的代数闭包

证明 α, β 在 F 上代数 $\Rightarrow \alpha \pm \beta, \alpha \cdot \beta \in F(\alpha, \beta)$

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)] \cdot [F(\alpha) : F]$$

$$\leq [F(\beta) : F] \cdot [F(\alpha) : F] < \infty$$

定义 1.12. 称 F 为代数闭域. 若 F 不存在非平凡有限扩张.

注 F 代数闭 $\Leftrightarrow F[x]$ 中不可约元均为 1 次

$$\Leftrightarrow \forall f(x) \in F[x] \text{ 首一}, f(x) = (x-x_1) \cdots (x-x_n) \quad \exists x_i \in F$$

$\Leftrightarrow F$ 上任一非常值多项式有根

$$\text{因为 } [F(x)/_{f(x)} : F] = \deg f$$

K/F . 代数扩张. K 代数闭. 称 K 为 F 的代数闭包 $K = \bar{F}$

定理 1.13. 代数闭包存在唯一

定理 1.14. (代数基本定理) $\mathbb{C} = \bar{\mathbb{C}}$

注 K/F . $K = \bar{K} \Rightarrow F$ 在 K 中的代数闭包即为 F 的代数闭包

例 $\mathbb{Q}$ 代数数 $= \{\alpha \in \mathbb{C} \mid f(\alpha) = 0, \exists f(x) \in \mathbb{Q}[x]\}$

5.2. 有限域

$|F| = q$. 称 F 为有限域 $\mathbb{F}_q$

引理 2.1. F 为有限域 则 q 为 p^r p 为素.

$$\text{char } F = p. \quad \mathbb{F}_p \subset F$$

设 $[F: \mathbb{F}_p] = r$ 有限生成 $\Rightarrow |F| = p^r$

例 $\mathbb{F}_4 = \{1, \alpha, (1+\alpha), 0\}$

$$\alpha(1+\alpha) = 1 = (1+\alpha)\alpha$$

$$\alpha \cdot \alpha = 1 + \alpha$$

$$(1+\alpha)(1+\alpha) = \alpha$$

$$\alpha^2 + \alpha + 1 = 0$$

定理 2.2. 设 p 素, $r \geq 1$, $q = p^r$

(i) $\mathbb{F}_q$ 存在

(ii) $\overline{\mathbb{F}_p}$ 中存在唯一的一个 q 元子域 $\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^q - \alpha = 0\}$ 且所有 q 元域均同构

(iii) $|K| = q \Rightarrow K^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$

(iv) $|K| = q \quad \alpha^q - \alpha = 0 \quad \forall \alpha \in K \quad x^q - x = \prod_{\alpha \in K} (x - \alpha)$

(v) $\mathbb{F}_p$ 上所有 r 次不可约多项式均为 $x^q - x$ 因子. 且 $x^q - x = \prod_{d|r} \prod_{f \in \mathcal{P}_d} f(x)$
 不可约

(vi) $K, K' \subseteq \overline{\mathbb{F}_p} \quad |K| = p^r, |K'| = p^{r'} \quad K \supseteq K' \Leftrightarrow r' | r.$

(vii) $\sigma: \mathbb{F}_q \rightarrow \mathbb{F}_q \quad x \mapsto x^p$ 则 $\text{Aut}(\mathbb{F}_q) = \langle \sigma \rangle$ 为 r 阶循环群

证明 (iii) + (vi).

$\therefore$ 要 $\mathbb{F}_q \triangleq \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^q = \alpha\}$ 为子域 (对加乘逆封闭)

说明 $x^q - x$ 无重根

求导为 $-1 \quad \checkmark$

设 $F' \subseteq \overline{\mathbb{F}_p}$ 为另一个 q 元子域 $\forall 0 \neq \alpha' \in F' \quad \alpha'^{q-1} = 1$ 即 $F' \subseteq F$

设 F'_i 为另一个 q 元域

$$\mathbb{F}_p \subseteq F'_i \subseteq \overline{\mathbb{F}_p}$$

(3) 3/理 K 为 $\mathbb{C}$ -域 $G \leq K^*$ $|G| = n < \infty$

$\Rightarrow G$ 为循环群

$$G \subseteq \{a \in K \mid a^n = 1\}$$

$$G \cong \frac{\mathbb{Z}}{n_1} \mathbb{Z} \oplus \cdots \oplus \frac{\mathbb{Z}}{n_s} \mathbb{Z} \quad n_1 \mid n_2 \mid \cdots \mid n_s$$

$$n_1 \cdots n_s = n$$

$\forall g \in G$, $\text{ord}(g) \mid n_s$. 则 G 中元素为 $x^{n_s} - 1 = 0$ 的根

至多 n_s 个互异 $\Rightarrow |G| \leq n_s$ 而 $|G| = n \Rightarrow n_s = n$

$$\Rightarrow G \cong \frac{\mathbb{Z}}{n} \mathbb{Z}$$

(4) $\forall \alpha \in K$, $\alpha^q = \alpha$.

即 $x - \alpha$ 为 $x^q - x$ 的因子. $\Rightarrow \prod_{\alpha \in K} (x - \alpha) \mid x^q - x$

$$\Rightarrow \prod_{\alpha \in K} (x - \alpha) = x^q - x$$

(5) $f(x)$ 为 $\mathbb{F}_p$ 上的 r 次首一不可约多项式. 任取 $f(x)$ 在 $\overline{\mathbb{F}_p}$ 中的一个根 α .

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = r$$

$$\Rightarrow |\mathbb{F}_p(\alpha)| = p^r = q \Rightarrow \mathbb{F}_p(\alpha) = \mathbb{F}_q$$

故 $f(x)$ 的所有根均包含于 $\mathbb{F}_q$

$$(6) \Rightarrow K' \subseteq K \Rightarrow |K| = |K'|^{[K:K']}$$

$$\in r' \mid r \quad K' = \{x^{r'} - x \text{ 的根} \mid \in K = \{x^r - x \text{ 的根} \}$$

(7) $\sigma \in \text{Aut}(\mathbb{F}_q) \cup$

$\mathbb{F}_q^* = \langle \alpha \rangle$ 为 $q-1$ 阶循环

$$\mathbb{F}_p(\alpha) = \mathbb{F}_q$$

$$\sigma^r(\alpha) = \alpha^{p^r} = \alpha \quad \sigma^r = \text{id}$$

$$\sigma^{r'}(\alpha) = \alpha \Rightarrow r \mid r' \Rightarrow \text{ord}(\sigma) = r.$$

而 α 在 $\mathbb{F}_p$ 上的极小多项式是 r 次的 $f_\alpha(x)$.

在 $\overline{\mathbb{F}_p}$ 中最多 r 个根 $\alpha_1 = \alpha \cdots \alpha_r$

$$\tau \in \text{Aut}(\mathbb{F}_q)$$

$$\mathbb{F}_q = \mathbb{F}_p(\alpha) \quad \tau \text{ 由 } \tau(\alpha) \text{ 来生成}$$

而 $\tau(\alpha)$ 也满足 $f_\alpha(x)$

注. 1. $f(x)$ 为 $\mathbb{F}_p$ 上 r 次首-不可约. α 为 $f(x)$ 的一个根. 则

$$f(x) = (x - \alpha)(x - \alpha^p) \cdots (x - \alpha^{p^{r-1}})$$

2. $\overline{\mathbb{F}_p} = \bigcup_{r \geq 1} \mathbb{F}_{p^r}$