

§1.5 正规子群, 单群与可解群

定义: G 的子群 H 称为正规子群如果 $gHg^{-1} = H$ 对 $\forall g \in G$.

问题: 给定 G , 如何构造 G 的正规子群?

方法1 同态核

$\ker(\phi)$

设 $\phi: G \rightarrow G'$ 为群同态, 则 $\ker(\phi) = \{g \in G \mid \phi(g) = e'\}$ 为 G 的正规子群.

方法2 群的中心

$Z(G)$

$$Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$$

群的全体自同构群记为 $\text{Aut}(G)$, 下面来定义 $\text{Aut}(G)$ 的一个子群.

$\forall g \in G$, 新映射 $\phi_g: G \rightarrow G$ 满足 $\phi_g(h) = ghg^{-1}$

可以验证 ϕ_g 为 G 到 G 的同构且 $\phi_{g_1} \circ \phi_{g_2} = \phi_{g_1 g_2}$. ϕ_g 称为由 g

导出的共轭变换. 全体共轭变换构成 $\text{Aut}(G)$ 的子群, 记为 $\text{In}(G)$

称为 G 的内自同构群. 考虑映射 $\phi: G \rightarrow \text{In}(G)$ 满足 $\phi(g) = \phi_g$

显然 ϕ 为满同态. 且 $\ker(\phi) = Z(G)$. 所以 $G/Z(G) \cong \text{In}(G)$

由此可知 $Z(G) \trianglelefteq G$. 进一步, 我们欲证明: $\text{In}(G) \trianglelefteq \text{Aut}(G)$

事实上, $\forall \phi_g \in \text{In}(G), \sigma \in \text{Aut}(G)$, 对 $\forall x \in G$, 则有

$$\begin{aligned} \sigma \phi_g \sigma^{-1}(x) &= \sigma \phi_g(\sigma^{-1}(x)) = \sigma(g \sigma^{-1}(x) g^{-1}) = \sigma(g) x \sigma(g)^{-1} \\ &= \phi_{\sigma(g)}(x) \end{aligned}$$

即有 $\sigma \phi_g \sigma^{-1} = \phi_{\sigma(g)} \in \text{In}(G)$

方法3 换位子群

G''

$\forall a, b \in G, ab = ba x \Rightarrow x = a^{-1}b^{-1}ab \triangleq [a, b]$ 称为 a, b 的换位子

注：两个换位子相乘不一定是换位子

定义：由 G 的所有换位子 生成的群 称为 G 的换位子群，记为 $G^{(1)}$

注：换位子群中元素，不一定是换位子!!!

定理： $G^{(1)}$ 为 G 的正规子群。

证明：只需验证对 $G^{(1)}$ 的生成元即换位子都在共轭变换下仍然为换位子

$$\forall g \in G \quad \phi([a, b]) = g a^{-1} b^{-1} a b g^{-1} = [\phi_g(a), \phi_g(b)] \in G^{(1)}$$

定义：如果 G 没有非平凡的正规子群，则称 G 为单群

如果存在正整数 k 使得 $G^{(k)} = (G^{(k-1)})^{(1)} = \{e\}$

则称 G 为可解群，即有

$$G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots \supseteq \{e\} \quad (\text{正规子群列})$$

例子

1) 交换群为可解群

2) S_n 可解 $\Leftrightarrow n \leq 4$

证明 对 $n \leq 4$ ，直接计算可得 (i) S_1, S_2 为交换群

(ii) $G = S_3$, $G^{(1)} = \{e, (1, 2, 3), (1, 3, 2)\} = A_3$, $G^{(2)} = \{e\}$

(iii) $G = S_4$, $G^{(1)} = A_4$, $G^{(2)} = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$, $G^{(3)} = \{e\}$.

(iv) 对 $n \geq 5$, $S_n^{(1)} \subseteq A_n \trianglelefteq S_n$ 且 $S_n^{(1)} \neq \{e\}$.

由于 $S_n^{(1)}$ 为 S_n 的正规子群且 A_n 为单群，则 $S_n^{(1)} = A_n$

A_n 为非交换群，则 $A_n^{(1)} = A_n$.

3) Feit-Thompson 定理：奇数阶的有限群都是可解的！

注：群的可解性在伽罗瓦理论中扮演重要角色。因为给定多项式的根式可解性与其相对应伽罗瓦群的可解性是等价的。

西罗定理 (Sylow's Theorems)

Lagrange 定理表明, H 为 G 的子群且 G 为有限群, 则 $|H| \mid |G|$.
那么 $|G|$ 的任一因子是否有相应阶数的子群?

设 $|G| = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$, 其中 p_i 为素数

定义: 有限群 G 称为 p -群 如果 $|G| = p^k$ ($k \geq 1$)

$Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$ G 的中心

定理: p -群必有非平凡的中心.

西罗定理: 设 G 为有限群, $n = |G|$, p 为素数

1) 如果 $p^k \mid |G|$ ($k \geq 0$), 那么 G 中必有阶为 p^k 的子群

► 设 $|G| = p^l \cdot m$, $(p, m) = 1$, 则阶数为 p^l 的子群称为 G 的西罗 p -子群

2) 设 P 为 G 的一个西罗 p -子群. 则 G 的任意阶为 p^k 的子群 H 一定包含在一个与 P 共轭的西罗 p -子群中

3) 设 k 为 G 中全部西罗 p -子群的个数, 则 $k \equiv 1 \pmod{p}$.

推论

① 任意两个西罗 p -子群互相共轭 即 $P_1 = g P_2 g^{-1}$
for some $g \in G$

② G 中全部西罗 p -子群的个数 k 是 $|G|$ 的因子
若 $|G| = p^l \cdot m$, $(p, m) = 1$, 则 k 为 m 的因子

③ 设 H 为 G 的子群, $N(H) = \{g \in G \mid gHg^{-1} = H\}$ 称为 H 的正规化子. 则有 ~~$N(H) = H$~~ $H \trianglelefteq N(H)$.

若 P 为 G 的西罗 p -子群, 则 $N(N(P)) = N(P)$.

§1.6 环及其理想

定义: 设 $(R, +, \cdot)$ 为代数系统. 如果 R 满足如下条件:

- 1) $(R, +)$ 为阿贝尔群 (交换群)
- 2) 乘法结合律: $\forall a, b, c \in R, (ab)c = a(bc)$.
- 3) 分配律: $\forall a, b, c \in R$
$$a(b+c) = ab+ac$$
$$(b+c)a = ba+ca.$$

则称 $(R, +, \cdot)$ 为环 (ring). 设 S 为 R 的非空集. 如果 S 关于 R 中的两个运算也构成环, 则称 S 为 R 的子环 (subring)

例子 1) $(\mathbb{Z}, +, \cdot)$ 整数环

2) 设 K 为数域 (如 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$). 当数取自 K 的所有 $n \times n$ 矩阵关于矩阵加法与乘法构成环, 称为 K 上 $n \times n$ 矩阵环, 记为 $M_n(K)$.

3) 设 K 为数域, $K[x_1, \dots, x_n]$ 关于多项式的加法与乘法构成环.

如果 $(R, +, \cdot)$ 中关于乘法存在单位元, 则称 R 为含么环. 可以证明任意环 R 都可以嵌入到一个含么 $\bar{R}$ 中 (见 Jacobson Basic Algebra I, P40) 所以我们假设以后讨论的环都是含么环. 如果 $(R, +, \cdot)$ 关于乘法为交换的, 则称为交换环. 设 $a \in R, a \neq 0$, 如果存在 $b \in R, b \neq 0$ 使得 $ab=0$, 则称 a 为左零因子; 如果 $ba=0$, 则称 a 为右零因子. 含么交换环如果不存在零因子则称为整环

定义: 设 $(R, +, \cdot)$ 为环. 如果 $(R, \cdot)$ 构成阿贝尔群, 则称 R 为域 (field).

定理: 有限整环一定是域.

定义. 映射 $\phi: R_1 \rightarrow R_2$ 为 环同态, 如果 $\forall a, b \in R_1$

$$\phi(a+b) = \phi(a) + \phi(b)$$

$$\phi(ab) = \phi(a)\phi(b)$$

则称 $\ker(\phi) = \{a \in R_1 \mid \phi(a) = 0\}$ 为 ϕ 的核 (kernel)

$\text{Im}(\phi) = \{\phi(a) \mid a \in R_1\}$ 为 ϕ 的象 (Image)

若 ϕ 为双射, 则称 ϕ 为 环同构.

环同态基本定理: 设 $\phi: R_1 \rightarrow R_2$ 为 满同态, 则有

$$R_1 / \ker(\phi) \cong R_2$$

定义. 设 R 为环, I 为 R 中的一个加法子群. 如果又有

- 1) $\forall r \in R, a \in I$ 都有 $ra \in I$, 则称 I 为 R 的左理想 (left ideal)
- 2) $\forall r \in R, a \in I$ 都有 $ar \in I$, 则称 I 为 R 的右理想 (right ideal)

若 I 既为左理想又为右理想, 则称 I 为 R 的理想, 记为 $I \trianglelefteq R$.

性质. 设 $\{I_\lambda\}_{\lambda \in \Lambda}$ 为 R 的一族 (左, 右) 理想, 则 $\bigcap_{\lambda \in \Lambda} I_\lambda$ 也为 R 的 (左, 右) 理想.

定义. 设 S 为 R 的非空子集. 包含 S 的所有理想的交称为由 S 生成的理想, 记为 $\langle S \rangle$. 事实上, 我们有

$$\langle S \rangle = \left\{ \sum_{\text{有限和}} m_i s_i + \sum_{\text{有限和}} r_j s_j + \sum_{\text{有限和}} s_k t_k + \sum_{\text{有限和}} p_l s_l r_l \mid \begin{array}{l} m_i \in \mathbb{Z}, r_j, t_k, p_l, r_l \in R \\ s_i, s_j, s_k, s_l \in S \end{array} \right\}$$

设 I 为 R 的理想且 $I = \langle a \rangle$ for some $a \in R$, 则称 I 为主理想 (Principal ideal)

(注) 环的理想与群的同态核有相似之处

$H \trianglelefteq G \Rightarrow G/H$ 为群 (商群) $\phi: G_1 \rightarrow G_2$ 同态 $\Rightarrow \ker(\phi) \trianglelefteq G_1$

$I \trianglelefteq R \Rightarrow R/I$ 为环 (商环) $\phi: R_1 \rightarrow R_2$ 同态 $\Rightarrow \ker(\phi) \trianglelefteq R_1$

例2

1) $R = (\mathbb{Z}, +, \cdot)$ 为整环

所有偶数全体构成 R 的一个理想且为主理想 $\langle 2 \rangle$.

$$\mathbb{Z}/\langle 2 \rangle = \{\bar{0}, \bar{1}\}$$

性质: $\mathbb{Z}$ 的任何理想皆为主理想.

证明: 设 $I \subseteq \mathbb{Z}$. 若 $I = \{0\}$, 则 $I = \langle 0 \rangle$. 否则设 m 为 I 中

绝对值最小的正数. 下证 $I = \langle m \rangle$. $m \in I \Rightarrow \langle m \rangle \subseteq I$.

对 $\forall a \in I$, $a = qm + r$, 其中 $q, r \in \mathbb{Z}$. 则 $r = a - qm \in I$

如果 $r \neq 0$, 则与 m 的选取矛盾. 所以 $r = 0$, 即有 $a = qm \in \langle m \rangle$

所以 $I \subseteq \langle m \rangle$, 则 $I = \langle m \rangle$. 图

2) $(\mathbb{R}[x], +, \cdot)$ 中所有常数项为 0 的多项式全体构成 $\mathbb{R}[x]$ 的一个理想且为主理想 $\langle x \rangle$. 类似于 $\mathbb{Z}$, 可以证明 $\mathbb{R}[x]$ 中任意理想为主理想. 且 $\mathbb{R}[x]$ 为整环.

3) $(M_n(\mathbb{R}), +, \cdot)$ 中设有非平凡(双边)理想 (设有非平凡理想的环称为单环) 该结论可参见其证明 Serge Lang, Algebra, P654.

环的直和: 设 $R_1, \dots, R_n$ 为环, $(R_1 \times \dots \times R_n)$ 上定义运算:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

$$(a_1, \dots, a_n)(b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$$

则 $R_1 \times \dots \times R_n$ 关于上述运算构成环, 称为 $R_1, \dots, R_n$ 的直和, 记为

$$R_1 \oplus R_2 \oplus \dots \oplus R_n. \quad \text{定义 } \tilde{R}_i = \{(0, \dots, 0, \underset{\substack{\uparrow \\ i\text{位置}}}{a_i}, 0, \dots, 0) \mid a_i \in R_i\} \quad i=1, 2, \dots, n$$

则有: 1) $\tilde{R}_i \subseteq R$ 且 $\tilde{R}_i \cong R_i$

$$2) R = \tilde{R}_1 + \dots + \tilde{R}_n$$

$$3) \tilde{R}_i \cap (\tilde{R}_1 + \dots + \tilde{R}_{i-1} + \tilde{R}_{i+1} + \dots + \tilde{R}_n) = (0) \quad i=1, \dots, n$$

反之满足以上条件的 R 的子环 $R_1, \dots, R_n$, 则有 $R \cong R_1 \oplus \dots \oplus R_n$.

定义. 设 I, J 为 R 的理想. 如果 $I+J=R$, 则称 I, J 互素

对 $a, b \in R$, 如果 $a-b \in I$, 则称 a, b 关于 I 同余, 记为 $a \equiv b \pmod{I}$.

中国剩余定理的理想版

设 R 为含么环, $I_1, \dots, I_n$ 为 R 中两两互素的理想, 则

$$R / I_1 \cap \dots \cap I_n \cong R / I_1 \oplus \dots \oplus R / I_n$$

而且令 $\sigma_i: R \rightarrow R / I_i$ 则有

$$\begin{aligned} \sigma: R &\longrightarrow R / I_1 \oplus \dots \oplus R / I_n \\ r &\longmapsto (\sigma_1(r), \dots, \sigma_n(r)) \end{aligned}$$

是满同态且 $\ker(\sigma) = I_1 \cap \dots \cap I_n$.

推论 (中国剩余定理) 设 $p_1, \dots, p_n$ 为互不相同的素数, 则

下方程在 $\mathbb{Z}$ 中恒有解:

$$\begin{cases} x \equiv b_1 \pmod{p_1} \\ \vdots \\ x \equiv b_n \pmod{p_n} \end{cases} \quad \text{其中 } b_i \in \mathbb{Z}.$$

定义. 设 I 为 R 的理想, 如果 $\forall a, b \in R, ab \in I \Rightarrow a \in I$ 或 $b \in I$ 则称 I 为 素理想, 如果 $I \neq R$ 且不存在 R 中理想 J 使得 $I \subsetneq J$, 则称 I 为 R 的 极大理想.

定理: 设 R 为交换么环, 则有

I 为 R 的素理想 $\Leftrightarrow R/I$ 为整环

I 为 R 的极大理想 $\Leftrightarrow R/I$ 为域.

所以在交换么环中, 极大理想均为素理想.

整环: $ED \Rightarrow PID \Rightarrow UFD$

定义. 设 R 为整环. $p \in R$ 称为 R 中的素元 如果 $\forall a, b \in R, p|ab \Rightarrow p|a$ 或 $p|b$.
 R 中元素 a, b 称为相伴的 如果存在 R 中元素 u 使得 $a = ub$, 记为 $a \sim b$.
 $p \in R$ 称为 R 中不可约元, 如果 $p = p_1 \cdot p_2 \Rightarrow p_1 \sim p$ 或 $p_2 \sim p$.

性质 在整环中, 素元 $\neq 0$ 为不可约元.

(注) 在整环中, 不可约元不一定是素元. 例如, $R = \mathbb{Z}[\sqrt{-5}]$, $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$.
元素 2 为 $\mathbb{Z}[\sqrt{-5}]$ 中不可约元, 但不是素元.

三类重要的整环: 设 R 为整环.

① 如果存在函数 $d: R \setminus \{0\} \rightarrow \mathbb{N}$ 满足: $\forall a, b \in R, b \neq 0$, 存在 $q, r \in R$ 使得 $a = q \cdot b + r$, 其中 $r = 0$ 或 $r \neq 0$ 满足 $d(r) < d(b)$.
则称 R 为欧几里得整环 ($ED = \text{Euclidean Domain}$)

② 如果 R 中任何理想皆为主理想, 则称 R 为主理想整环 ($PID = \text{Principal Ideal Domain}$)

③ 如果对 $\forall a \in R$, 皆可写成有限个不可约元的乘积, $a = p_1 p_2 \cdots p_r$
并且该分解在相伴与对调因子的意义下是唯一的. 即如

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

则有 $r=s$ 且 $p_i \sim q_{\sigma(i)}$, σ 为 $1, 2, \dots, r$ 的置换.

则称 R 为唯一分解整环 或 高斯整环 ($UFD = \text{Unique Factorization Domain}$)

定理: $ED \Rightarrow PID \Rightarrow UFD$.

例:

- 1) $K[x_1, \dots, x_n]$ 是 UFD 但不是 PID ($n \geq 2$)
- 2) $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ 是 PID 但不是 ED .
- 3) $\mathbb{Z}[\sqrt{-5}]$ 不是 UFD , $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

定义. 设 R 为含幺交换环. 如果 R 的理想 I , 都存在有限个 R 中之素 $a_1, \dots, a_n \in R$ 使得 $I = \langle a_1, \dots, a_n \rangle$, 则称 R 为诺特环.

定理: R 为诺特环 $\Leftrightarrow R$ 中的每个理想升链 $I_1 \subset I_2 \subset \dots$ 都稳定, 即 $\exists m$ s.t. $I_m = I_{m+1} = \dots$

定理: 设 R 为含幺交换环.

1) 若 R 为诺特环, 则 $R[x]$ 仍为诺特环. (希尔伯特基定理)

2) 若 R 为 UFD, 则 $R[x]$ 仍为 UFD

推论: 设 K 为域, 则 $K[x_1, \dots, x_n]$ 为 UFD 且为诺特环.

整环的特征

设 R 为整环. 定义映射: $\phi: \mathbb{Z} \rightarrow R$, 其中 e 为 R 的乘法单位元

$$n \mapsto n \cdot e$$

则有 $(n+m) \cdot e = ne + me$ 即 $\phi(n+m) = \phi(n) + \phi(m)$

$(n \cdot m) \cdot e = (nm)e^2 = (ne)(me)$ 即 $\phi(nm) = \phi(n)\phi(m)$

$1 \cdot e = e$ 即 $\phi(1) = e$

由此 ϕ 为环 $\mathbb{Z}$ 到 R 的同态. 则 $\ker(\phi) = (k)$ for some $k \in \mathbb{Z}$.

因为 $\mathbb{Z}$ 为主理想整环. 如果 $k=0$, 则称 R 为 特征为 0 的整环

如果 $k > 0$, 下面证明 k 为素数. 如果 $k = p_1 p_2$ $\frac{p_1 < k, p_2 < k}{\text{且 } p_1, p_2 \in \mathbb{Z}}$, 则 $k \in \ker(\phi)$

$\Rightarrow (p_1 p_2)(e) = (p_1 e)(p_2 e) = 0$, 由于 R 为整环 (无零因子), 有 $p_1 e = 0$ 或 $p_2 e = 0$

$\Rightarrow p_1 \in \ker(\phi)$ 或 $p_2 \in \ker(\phi) \Rightarrow k \nmid p_1$ 或 $k \nmid p_2$. 矛盾.

称 k 为 R 的特征, 若 $k > 0$ 时. R 称为 特征为正的整环