解和子群

2022年11月30日 6:56

回忆：设 $(G,*,e)$ 和 $(H,\star,\varepsilon)$

是群，$\varphi: G\to H$ 是同态

$\Leftarrow$ [同态保持单位元]

(i) $\varphi(e)=\varepsilon$

$\Leftarrow$ [同态保逆元]

$\forall x\in G \quad \varphi(x^{-1})=\varphi(x)^{-1}$

(ii) 如果 φ 是同构，则 φ^{-1} 也是

(iii) 再设 $(M,\diamond,\varepsilon)$ 是群，$\psi: H\to M$ 是同态，则 $\psi\circ\varphi$ 也是同态。

当 ψ,φ 是同构时，$\psi\circ\varphi$ 也是

证：(ii) $\varphi^{-1}: H\to G$

设 $u,v\in H$，$\because \varphi$ 是双射

$\therefore \exists x,y\in G.\ \varphi(x)=u,\ \varphi(y)=v$

$\because \varphi$ 是同态 $\because \varphi(x*y)=\varphi(x)\star\varphi(y)$

$=u\star v$

$\because \varphi$ 是双射 $\therefore \varphi^{-1}(u\star v)=x*y$

$=\varphi^{-1}(u)*\varphi^{-1}(v)$

于是 φ^{-1} 是同态

(iii)

$G\xrightarrow{\varphi}H$

设 $x,y\in G$

$\psi\circ\varphi(x*y)$

$\psi\circ\varphi$ → M 上 $\sim$

$= \psi(\varphi(x * y))$

$= \psi(\varphi(x) \star \varphi(y))$

$= \psi(\varphi(x)) \diamond \psi(\varphi(y))$

$= \psi\circ\varphi(x) \diamond \psi\circ\varphi(y)$

$\Rightarrow \psi\circ\varphi$ 是同态 □

$x * y = xy$

$\varphi(x) * \varphi(y) = \varphi(x)\varphi(y)$

注：$\sim$ 是由群构成集合上的等价关系

且同映射是同构

自反 (i)

对称 (ii)

传递 (iii) ✓

群论的基本问题

设 G 是一类群，"$\sim$" 是 G 上等价关系。问：$G/\sim$ 是什么样？

把每个同构类，找一个典型代表元

G 是有限阿贝尔群的集合

例：证明 $(\mathbb{Z}_4, +, \bar{0})$ 和 $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0}))$ 是不同构的。

证：假设 $\varphi: \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ 是同构。只有

$$\varphi(\bar{0}) = (\bar{0}, \bar{0})$$

$$\varphi(\bar{1}) = \begin{cases} (\bar{1}, \bar{0}) \\ (\bar{0}, \bar{1}) \\ (\bar{1}, \bar{1}) \end{cases}$$

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

$\varphi(\bar{2}) = (\bar{0}, \bar{0})$

$\because \varphi$ 是单射 $\therefore \bar{2} = \bar{0}$ ⇒⇐

同理 $\varphi(\bar{1}) \neq (\bar{0}, \bar{1})$ $\varphi(\bar{1}) \neq (\bar{1}, \bar{1})$

故 φ 不可能是同构 图

1阶群
2阶
3阶
4阶 } 在同构的意义下只有一个

有两个

习题1 证明：S_3 和 $(\mathbb{Z}_6, +, \bar{0})$

例：设 S_3 和 $(\mathbb{Z}_6, +, \bar{0})$ 是不同构的

证：假设 $\varphi: \mathbb{Z}_6 \longrightarrow S_3$ 是同构。则 $\exists$ $a, b \in \mathbb{Z}_6$ 使得

$\varphi(a) = (12)$, $\varphi(b) = (23)$

$\varphi(a+b) = \varphi(a)\varphi(b) = (12)(23)$

$\varphi(b+a) = \varphi(b)\varphi(a) = (23)(12)$

但 $(12)(23) \neq (23)(12)$. $\rightarrow\leftarrow$

§2.4 子群 subgroup

定义：设 $(G, \cdot, e)$ 是群 $H \subset G$. 如果 $(H, \cdot, e)$ 也是群，则称 H 是 G 子群.

命题：设 G 是群，$H \subset G$ 非空

则 H 是 G 子群

$\Longleftrightarrow \forall h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$

证：$\Rightarrow$ ，$\because H$ 是群

$\therefore h_2 \in H \Rightarrow h_2^{-1} \in H$,

$\because h_1 \in H \therefore h_1 h_2^{-1} \in H$

$\Leftarrow$ 设 $h_1 \in H$ 则

$h_1 h_1^{-1} \in H \Rightarrow e \in H$

于是 H 中有单位元

$\because e \in H \therefore e \cdot h_1^{-1} \in H \Rightarrow h_1^{-1} \in H$

于是 H 中每个元素在 H 中有逆

结合律由 G 中运算的结合律

得出

设 $h_1, h_2 \in H \quad \because h_2 \in H \therefore h_2^{-1} \in H$

$\because h_2^{-1} \in H \therefore h_1 (h_2^{-1})^{-1} \in H$

$\because h_1 (h_2^{-1})^{-1} = h_1 h_2 \therefore h_1 h_2 \in H$ 证

例: 设 S 是所有偶数的集合

则 $(S, +, 0)$ 是 $(\mathbb{Z}, +, 0)$ 的子群

验证: 因为两个偶数之差也是偶数

例: 设 A_n 是 S_n 的置换的集合

则 $(A_n, \cdot, e)$ 是 S_n 的子群

验证: 设 $\sigma, \tau \in A_n$

验证：设 $\sigma, \tau \in A_n$

π_i 是对换

λ_j ···

则 $\sigma = \pi_1 \cdots \pi_{2k}$,

$\tau = \lambda_1 \cdots \lambda_{2l}$

$\sigma\tau^{-1} = (\pi_1 \cdots \pi_{2k})(\lambda_1 \cdots \lambda_{2l})^{-1}$

$= \pi_1 \cdots \pi_{2k} \lambda_{2l}^{-1} \cdots \lambda_1^{-1}$

$= \underbrace{\pi_1 \cdots \pi_{2k} \lambda_{2l} \cdots \lambda_1}_{2(k+l)} \in A_n$

因

例：设 $GL_n(\mathbb{Q}) = \{A \in GL_n(\mathbb{R}) \mid A$ 中元素都是有理数$\}$

验证 $GL_n(\mathbb{Q})$ 是 $GL_n(\mathbb{R})$ 的子群

$A, B \in GL_n(\mathbb{Q})$ 要证

$AB^{-1} \in GL_n(\mathbb{Q})$

$B^{-1} = \frac{1}{\det(B)} B^V$

∵ B 中的元素都是有理数

∴ $\det(B) \in \mathbb{Q}$, B^V 是 $\mathbb{Q}$ 上的行列

故 $B^{-1} \in GL_n(\mathbb{Q})$

$\Rightarrow AB^{-1} \in GL_n(\mathbb{Q})$

$\Rightarrow GL_n(\mathbb{Q})$ 是子群

$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$

$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A)=1\}$

证明 $SL_n(\mathbb{R})$ 是 $GL_n(\mathbb{R})$ 的子群

设 $A, B \in SL_n(\mathbb{R})$

$\begin{cases} \det(B)=1 \\ \det(B)\det(B^{-1}) = \det(BB^{-1}) = \det(E)=1 \\ \Rightarrow \det(B^{-1})=1 \end{cases}$

$\Rightarrow B^{-1} \in SL_n(\mathbb{R})$

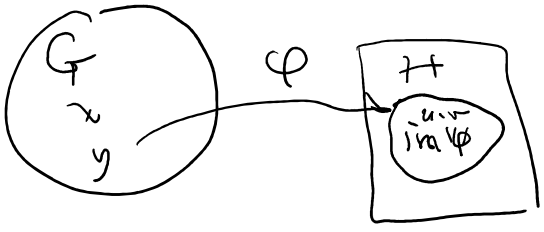
$\det(AB^{-1}) = \det(A)\det(B^{-1})$

$= 1$ ✓

命题：设 G, H 是群，$\varphi: G \to H$ 是同态，则 $\mathrm{im}(\varphi)$ 是 H 的子群

证：设 $u, v \in \mathrm{im}(\varphi)$ 则 $\exists x, y \in G$

$\varphi(x)=u, \quad \varphi(y)=v$



$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1})$

$= \varphi(x)\varphi(y)^{-1}$ [同态作用]

$= uv^{-1} \Rightarrow uv^{-1} \in \mathrm{im}(\varphi)$

由子群判别法可知，$\mathrm{im}(\varphi)$ 是子群

定理（Lagrange）设 G 是有限群

则

定理（Lagrange）：

H 是 G 的子群，则

$$\text{card}(H) \mid \text{card}(G)$$

证明：$\forall g \in G$，$L_g(H)$ 中含有 g（$g \cdot e = L_g(e) = g$）

于是

$$G = \bigcup_{g \in G} L_g(H)$$

$\because G$ 是有限群

于是 $\exists$ 最小正整数 k 和 $g_1, \dots g_k \in G$

使得 $G = L_{g_1}(H) \cup L_{g_2}(H) \cup \dots \cup L_{g_k}(H)$

断言：$\forall i, j \in \{1, 2 \dots k\}$

$$L_{g_i}(H) \cap L_{g_j}(H) = \Phi$$

断言的证明：假设

$$x \in L_{g_1}(H) \cap L_{g_2}(H)$$

则 $\exists h_1, h_2 \in H$

$$x = g_1 h_1, x = g_2 h_2$$

$$\Rightarrow g_1 h_1 = g_2 h_2$$

$$\dots g_1 h_1 h_1^{-1} = g_2 h_2 h_1^{-1}$$

$\Rightarrow g_1 h_1 h_1^{-1} = g_2 h_2 h_1^{-1}$

$\Rightarrow g_1 = g_2 h_2 h_1^{-1}$

$\Rightarrow g_1 \in Lg_2(H)$ $(\because h_2 h_1^{-1} \in H)$

$\forall h \in H$ $g_1 h = g_2 h_2 h_1^{-1} h$

$= g_2 (h_2 h_1^{-1} h)$

$\because h_2 h_1^{-1} h \in H \quad \therefore g_1 h \in Lg_2(H)$

$\Rightarrow Lg_1(H) \subset Lg_2(H)$

于是 $G = Lg_1(H) \cup Lg_2(H) \cup \cdots \cup Lg_k(H)$

$= Lg_2(H) \cup \cdots \cup Lg_k(H)$

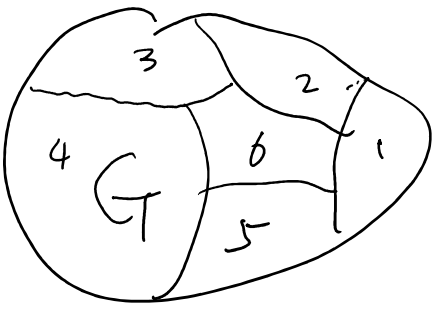
与 k 的极小性矛盾

于是断言对之

$G = Lg_1(H) \cup Lg_2(H) \cup \cdots \cup Lg_k(H)$

且 $Lg_1(H), Lg_2(H), \cdots Lg_k(H)$

两两互不相交



$\text{card}(G)$

$= \text{card}(Lg_1(H))$

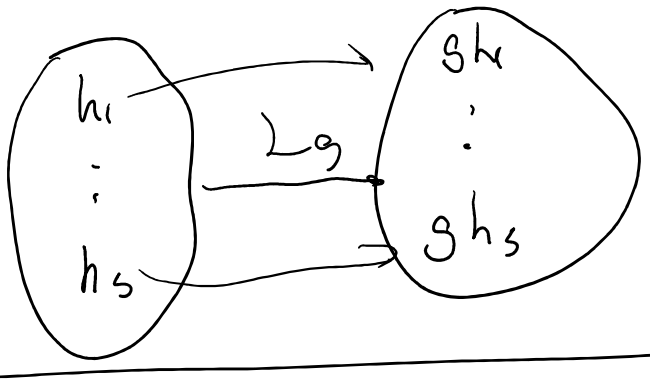
$+ \text{card}(Lg_2(H)) + \cdots$

$+ \text{card}(Lg_k(H))$

$\cdots$ 由加合

$+\operatorname{card}(L_{g_2}(H))$

$\because L_g$ 是等价. $\therefore L_{g_2}(H)$ 与 H 中的会元素个数相同



设 $s=\operatorname{card}(H)$

$\operatorname{card}(G)=sk$

$\Rightarrow s \mid \operatorname{card}(G)$ 且

上述讨论的这种 k 称为 H 在 G 中的指标. 记为 $[G:H]$

于是 Lagrange 定理可简述为

$$\operatorname{card}(G)=[G:H]\operatorname{card}(H)$$

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

例 计算 $[S_n:A_n]$ $n>1$

解: 设 σ 是 S_n 奇置换.

则 $L_\sigma(A_n)$ 奇置换

$\forall S_n$ 中的奇置换 τ $\Rightarrow \tau \in L_\sigma(A_n)$

$\sigma(\sigma^{-1}\tau)$

↳ 偶置换

$\therefore A_n$ 的每个奇置换的集合

$L_\sigma(A_n)$ 是所有奇置换的集合

$S_n = A_n \cup L_\sigma(A_n)$

$\Rightarrow [S_n : A_n] = 2.$

(已证 $\mathrm{card}(A_n) = \frac{n!}{2}$ 一致).

注 设 G 是群. G 平凡子群是指 $\{e\}$ 和 G 称为 G 的平凡子群.

例 设 p 是素数. G 是含有 p 个元素的群. 证明 G 不含非平凡子群

证: 设 H 是 G 的子群. 由 Lagrange 定理 $\mathrm{card}(H) \mid \mathrm{card}(G) = p$ ↪ 素数

$\mathrm{card}(H) = 1$ 或 $\mathrm{card}(H) = p$

$\Downarrow$ $\Downarrow$

$H = \{e\}$ $H = G$

且

---

§2.5 生成元和群中元素的阶

定义: 设 G 是群. S 是 G 中非空集

合. 在 G 中生成的子群是指

证：
由 S 在 G 中生成的子群是
$$\langle S\rangle := \{x_1^{e_1}\cdots x_m^{e_m} \mid m\in\mathbb{Z}^+, x_1,\cdots x_m\in S, e_1,\cdots e_m\in\mathbb{Z}\}$$
如果 $G=\langle S\rangle$，则称 S 是 G 的一组生成元

验证 $\langle S\rangle$ 是子群

设 $a,b\in\langle S\rangle$

则 $\exists x_1,\cdots x_m, y_1,\cdots y_n\in S$
$k_1,\cdots k_m, l_1,\cdots l_n\in\mathbb{Z}$

使得
$$a=x_1^{k_1}\cdots x_m^{k_m},\quad b=y_1^{l_1}\cdots y_n^{l_n}$$
注意到 $b^{-1}=y_n^{-l_n}\cdots y_1^{-l_1}$ [幸福投资]
$$ab^{-1}=x_1^{k_1}\cdots x_m^{k_m}y_n^{-l_n}\cdots y_1^{-l_1}\in\langle S\rangle$$
故 $\langle S\rangle$ 是子群

注 $\langle S\rangle$ 是 G 中包含 S 的“最小”子群

验证：设 $S\subset H$ 且 H 是子群
则 $\forall x_1,\cdots x_n\in S,\ e_1,\cdots e_n\in\mathbb{Z}$
$x_1^{e_1}\cdots x_n^{e_n}\in H \Rightarrow \langle S\rangle\subset H$.

$x_1, \cdots, x_n$

注 如果 $(G, +, 0)$ 是群. 则

$$\langle S \rangle = \left\{ e_1 x_1 + \cdots + e_m x_m \;\middle|\; \begin{array}{l} m \in \mathbb{Z}^+ \\ x_1, \cdots x_m \in S, \\ e_1, \cdots e_n \in \mathbb{Z} \end{array} \right\}$$

定义: 设 $(G, \cdot, e)$ 是群. $g \in G$

如果不存在 $n \in \mathbb{Z}^+$ 使得

$$g^n = e$$

则称 g 是无穷阶的

如果存在正整数 $n \in \mathbb{Z}^+$ 使得

$$g^n = e \quad (*)$$

则满足 $(*)$ 的最小正整数称为 g 的阶

g 的阶记为 $ord(g)$

注 $(S_n, \circ, e)$ 是阶为第一章中置换的阶一致

设 $G = (\mathbb{Z}, +, 0)$

$ord(1) = \infty$ $\quad \forall x \in \mathbb{Z} \setminus \{0\}$

$ord(x) = \infty$

命题: 设 G 是群, $g \in G$

则

命题：设 G 是 [illegible]

(i) 如果 $\mathrm{ord}(g)=\infty$，则

$\forall i,j\in\mathbb{Z}$，$g^i=g^j\Leftrightarrow i=j$

(ii) 设 $k=\mathrm{ord}(g)<\infty$，则

$\forall i,j\in\mathbb{Z}$，$g^i=g^j\Leftrightarrow k\mid(i-j)$

特别地，如果 $g^m=e$，则 $k\mid m$

证：(i) "$\Leftarrow$" ✓

"$\Rightarrow$" 设 $g^i=g^j$，则

$g^{i-j}=e$ ∵ $\mathrm{ord}(g)=\infty$

$\Rightarrow i=j$. ✓

(ii) 设 $g^i=g^j$，($i\neq j$)

则 $g^{i-j}=e$

由带余除法 $i-j=qk+r$

其中 $q\in\mathbb{Z}$，$r\in\{0,1,\cdots k-1\}$

$e=g^{i-j}=g^{qk+r}=(g^k)^q g^r$

$=e^q g^r=e\,g^r=g^r$

由所证之 $r=0\Rightarrow k\mid(i-j)$

$g^m=e=g^0\Rightarrow k\mid(m-0)$

$\rightarrow k\mid m$ 证

$g=e=y$ 二下

$\Rightarrow k \mid m$ 证

推论 设 G 是群，$g \in G$，$m=\operatorname{ord}(g)<\infty$

设 $k \in \mathbb{Z}^+$

则 $\operatorname{ord}(g^k)=\dfrac{m}{\gcd(m,k)}=\dfrac{\operatorname{lcm}(m,k)}{k}$

[$mk=\gcd(m,k)\operatorname{lcm}(m,k)$]

证：设 $s=\dfrac{\operatorname{lcm}(m,k)}{k}$

则 $\operatorname{lcm}(m,k)=sk=nm$ [$n \in \mathbb{Z}^+$]

$(g^k)^s=g^{ks}=g^{nm}=(g^m)^n=e^n=e$

设 $\operatorname{ord}(g^k)=l$

$g^{kl}=e$

$m \mid kl \Rightarrow kl$ 既是 k 的倍式又是 m 的倍式，

$\Rightarrow kl$ 是 k 与 m 公倍式

$\Rightarrow sk \mid kl \Rightarrow s \mid l \Rightarrow s \le l$

$\Rightarrow s=l$ 证

例：在 $(\mathbb{Z}_{10},+,\bar{0})$ 中求

$\operatorname{ord}(\bar{2})$，$\operatorname{ord}(\bar{4})$，$\operatorname{ord}(\bar{5})$

$\bar{3}=3\bar{1}$ 而 $\operatorname{ord}(\underset{g}{\bar{1}})=10$

g^3

$$ord(\bar{3}) = \frac{lcm(10,3)}{3} = 10$$

$$ord(\bar{4}) = \frac{lcm(10,4)}{4} = \frac{20}{4} = 5$$

$$ord(\bar{5}) = \frac{lcm(10,5)}{5} = \frac{10}{5} = 2$$

引理 设 G 是群，且 $g \in G$.

设 $ord(g) < \infty$.

则 $card(\langle g \rangle) = ord(g)$

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

证：设 $k = ord(g)$ 我们事实上

$\langle g \rangle = \{ e, g, \cdots g^{k-1} \}$

显然 $\{ e, g, \cdots g^{k-1} \} \subset \langle g \rangle$

设 $m \in \mathbb{Z}$ 带余除法

$m = qk + r$, $q \in \mathbb{Z}$, $r \in \{0, 1, \cdots k-1\}$

$g^m = g^{qk+r} = (g^k)^q g^r = g^r \in \{e, g, \cdots g^{k-1}\}$

$\Rightarrow \langle g \rangle \subset \{ e, g, \cdots g^{k-1} \}$

$\langle g \rangle = \{ e, g, \cdots g^{k-1} \}$

再证：$e, g, \cdots g^{k-1}$ 两两不同

$\cdots \; a^{i-j} = e$

再证: $e, g, \cdots g^{k-1}$ 两两不等

设 $k-1 \geq i \geq j \geq 0$ $g^i = g^j \Rightarrow g^{i-j} = e$

$\Rightarrow k \mid (i-j)$ $\because 0 \leq i-j < k$

$\therefore i-j=0 \Rightarrow i=j$

于是 $\text{card}\langle g \rangle = k$ 证

定理 设 G 是有限群, $g \in G$

则 $\text{ord}(g) \mid \text{card}(G)$

即 $g^{\text{card}(G)} = e$.

证: $\because \langle g \rangle$ 是 G 的子群

$\therefore \text{card}(\langle g \rangle) \mid \text{card}(G)$

由上述命题

$\text{ord}(\langle g \rangle) \mid \text{card}(G)$. 证

---

§2-6. 置换群的生成元

$S_n = \langle (12), (23) \cdots (n-1, n) \rangle$

$= \langle (12), (12\cdots n) \rangle$

$A_n = \langle (123), (124) \cdots (12n) \rangle$