①

例42 设 $G_3 = \{e, a, b\}$ 是群
$(G_3 *, e)$ 是群

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

群乘法表的构造

设 $G_n = \{g_1, g_2, \cdots g_n\}$. $(G_n, *, g_1)$ 是群

	$g_1 \cdots\cdots$	$g_j \cdots\cdots$	g_n
g_1	$g_1^2 \cdots\cdots$	$g_1 g_j \cdots\cdots$	$g_1 g_n$
$\vdots$		$\cdots$	
g_i	$g_i g_1 \cdots\cdots$	$g_i g_j \cdots\cdots$	$g_i g_n$
$\vdots$		$\cdots$	
g_n	$g_n g_1 \cdots\cdots$	$g_n g_j \cdots\cdots$	g_n^2

$$\underbrace{g_i g_1 \cdots g_i g_j \cdots g_i g_n}_{第i行} 是 \underbrace{L_{g_j}(g_1), \cdots, L_{g_j}(g_n)}_{两两不同}$$

$$第j列 \quad \begin{matrix} g_1 g_j \\ \vdots \\ g_n g_j \end{matrix} \quad 是 \quad \left.\begin{matrix} R_{g_j}(g_1) \\ \vdots \\ R_{g_j}(g_n) \end{matrix}\right\} 两两不同$$

G_3 的实例

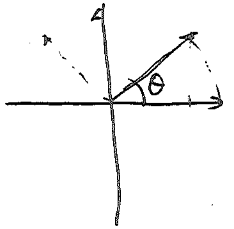
$(\mathbb{Z}_3, +, 0)$ $\quad e = \bar{0}, \quad a = \bar{1}, \quad b = \bar{2}$

$$G = \left\{ \underset{E}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}, \underset{A}{\begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}}, \underset{B}{\begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}} \right\}$$

$$A^2 = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = B$$

$$AB = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

同样 $BA = E$, $B^2 = A$



$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \theta = 120^\circ$$

$\mathrm{card}(G)=4$ 实例

$\mathbb{Z}_4=\{\overset{e}{\bar{0}},\overset{a}{\bar{1}},\overset{b}{\bar{2}},\overset{c}{\bar{3}}\}$ $(\mathbb{Z}_4,+,\bar{0})$ 是群

(with $\bar{0}=e$, $\bar{1}=a$, $\bar{2}=b$, $\bar{3}=c$)

+	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\mathbb{Z}_2\times\mathbb{Z}_2=\{(\bar{0},\bar{0}),(\bar{1},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{1})\}$

$(\bar{0},\bar{0})=e$, $(\bar{1},\bar{0})=a$, $(\bar{0},\bar{1})=b$, $(\bar{1},\bar{1})=c$

$\forall (x_1,x_2),\ (y_1,y_2)\in\mathbb{Z}_2\times\mathbb{Z}_2,$

$(x_1,x_2)+(y_1+y_2):=(x_1+x_2,\ y_1+y_2)$

则 $(\mathbb{Z}_2\times\mathbb{Z}_2,+\ (\bar{0},\bar{0}))$ 是群

+	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

§2.2 群同态

定义：设 $(G,*,e)$，$(H,\star,\varepsilon)$ 是两个群

$\varphi: G\to H$ 称为从 G 到 H 的同态

如果 $\forall g_1,g_2\in G$

$$\varphi(g_1*g_2)=\varphi(g_1)\star\varphi(g_2)$$

特别地 群同态

$\varphi\begin{cases}\text{单射}\\\text{满射}\\\text{双射}\end{cases}$ 则称 φ 是群 $\begin{cases}\text{单同态}\\\text{满同态}\\\text{同构}\end{cases}$

同态：homomorphism. 同构. isomorphism

引理2.1 设 φ 是~~群~~从群 $(G,*,e)$ 到 $(H,\star,\varepsilon)$ 的同态

则 (i) $\varphi(e)=\varepsilon$

(ii) $\varphi(g^{-1})=\varphi(g)^{-1}$

(iii) φ 是同构，则 φ^{-1} 也是同构

证: (i) $\varphi(e) = \varphi(e*e) = \varphi(e)☆\varphi(e)$
$\hookrightarrow$ φ是同态

$\varphi(e)☆\varphi(e)^{-1} = (\varphi(e)☆\varphi(e))☆\varphi(e)^{-1}$

$\|$ 　　　　$\|$ ← 结合律

ε 　　　　$\varphi(e)☆[(\varphi(e))☆\varphi(e^{-1})]$

$\|$

$\varphi(e)☆\varepsilon = \varphi(e)$

于是 $\varphi(e) = \varepsilon$.

(ii) 设 $g \in G$.

$\varphi(g*g^{-1}) = \varphi(g)☆\varphi(g^{-1})$
$\hookrightarrow$ φ是同态

$\|$

$\varphi(e)$

(i) $\rightarrow$ $\|$

ε

$\Rightarrow \varphi(g)☆\varphi(g^{-1}) = \varepsilon$

$\Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$ [命题2.1]

(iii) 设 $h_1, h_2 \in H$. $\exists!\ g_1, g_2 \in G$

使得 $\varphi(g_1) = h_1$, $\varphi(g_2) = h_2$

即 $h_1 = \varphi^{-1}(g_1)$, $h_2 = \varphi^{-1}(g_2)$

$\varphi(g_1 * g_2) = \varphi(g_1)☆\varphi(g_2) = h_1☆h_2$

$\varphi^{-1}(h_1☆h_2) = g_1 * g_2 = \varphi^{-1}(h_1)☆\varphi^{-1}(h_2)$

$\Rightarrow \varphi^{-1}$是同态 $\Rightarrow \varphi^{-1}$是同构的 □

例: $\pi_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$ 商映射
$a \mapsto \bar{a}$

是 $(\mathbb{Z}, +, 0)$ 到 $(\mathbb{Z}_n, +, \bar{0})$ 的同态

证: 设 $a, b \in \mathbb{Z}$

$\pi_n(a+b) =$ ~~π_n~~ $\overline{a+b}$ [商映射的定义]

$= \bar{a} + \bar{b}$ [$\mathbb{Z}_n$中加法的定义]

$= \pi_n(a) + \pi_n(b)$ [商映射的定义]

$\det: GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$

是 $GL_n(\mathbb{R})$ 到 $(\mathbb{R}^*, \cdot, 1)$ 的同态

证: $A, B \in GL_n(\mathbb{R})$. 则 ~~det~~(A), det(B)

推荃 $\det(AB) = \det(A)\det(B)$

[行列式乘积定理] !

例：<u>证明</u> $(\mathbb{Z}_2, +, \bar{0})$ 与 $(\{1,-1\}, \cdot, 1)$ 同构：

$$\varphi: \mathbb{Z}_2 \longrightarrow \{1,-1\}$$
$$\bar{0} \mapsto 1$$
$$\bar{1} \mapsto -1$$

φ是双射. $\varphi(\bar{0}+\bar{1}) = \varphi(\bar{1}) = -1$

$\varphi(\bar{0})\varphi(\bar{1}) = 1\cdot(-1) = -1$

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

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

$\varphi(\bar{1})\cdot\varphi(\bar{1}) = (-1)(-1) = 1$ $\Rightarrow \varphi(\bar{1}+\bar{1}) = \varphi(\bar{1})\cdot\varphi(\bar{1})$

类似可以验证 $\varphi(\bar{0}+\bar{0}) = \varphi(\bar{0})\varphi(\bar{0})$

于是 φ 是同构

自己证明：当 card(G)=3 时. 讲义中的两个实例同构.

例 证明 $(\mathbb{Z}_4, +, \bar{0})$ 与 $(\mathbb{Z}_2\times\mathbb{Z}_2, +, (\bar{0},\bar{0}))$ 不同构.

<u>证</u>: 假设

$\varphi: (\mathbb{Z}_4, +, \bar{0}) \longrightarrow (\mathbb{Z}_2\times\mathbb{Z}_2, +, (\bar{0},\bar{0}))$

是同构.

则 $\varphi(\bar{0}) = (\bar{0},\bar{0})$ [引理2.1]

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

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

φ 不是双射 →←

同理：当 $\varphi(\bar{1}) = (\bar{0},\bar{1})$, 或 $\varphi(\bar{1}) = (\bar{1},\bar{1})$ 时 都可以导致 $\varphi(\bar{2}) = (\bar{0},\bar{0})$ →←. 故

φ不是同构.

<u>引理2.2</u> 设 $(G, *, e)$, $(H, \star, \varepsilon)$
$(K, \diamond, \lambda)$ 是三个群

$\varphi: G \rightarrow H$, $\psi: H \rightarrow K$

是同态. 则 $\psi\circ\varphi: G \rightarrow K$

也是同态

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[dr, "\psi\circ\varphi"'] & H \arrow[d, "\psi"] \\ & K \end{tikzcd}$$

证：设 $g_1, g_2 \in G$

$$\begin{aligned} \psi\circ\varphi(g_1 * g_2) &= \psi(\varphi(g_1) \star \varphi(g_2)) \\ &= \psi(\varphi(g_1)) \diamond \psi(\varphi(g_2)) \\ &= \psi\circ\varphi(g_1) \diamond \psi\circ\varphi(g_2) \end{aligned}$$ ▨

定义：设 G, H 是两个群，~~如果存在~~ 群同构 $\varphi: G\to H$，则称 G 和 H 是同构的，记为 $G\simeq H$

命题2.3 "$\simeq$" 是等价关系

证：自反性. 设 G 是群 G $id_G: G\to G$ 是同构 $\Rightarrow G\simeq G$

对称性. 设群 G 和 H 同构

则 $\exists\ \varphi: G\to H$ 是同构

由引理2.2(iii)，$\varphi^{-1}: H\to G$ 也是同构. 从而 $H\simeq G$.

传递性 设 G, H, K 是群

$G\simeq H$, $H\simeq K$

则 $\exists\ \varphi: G\to H$, $\psi: H\to K$ 都是同构. 则 $\psi\circ\varphi$ 是 $\underbrace{\text{双射}}_{\text{第一章推论3.3 (讲义1-3, P4)}}$ 和 $\underbrace{\text{同态}}_{\text{引理2.3}}$

$\Rightarrow \psi\circ\varphi$ 是双射 $\Rightarrow \psi\circ\varphi$ 是同构

▨

$\Rightarrow G\simeq K$.

群论基本问题：给定一类群，求这类群在 "$\simeq$" 下的等价类，并对每个等价类找出一个代表元

例 一阶群，一个等价类 代表元 $(\{0\}, +, 0)$

二阶群：一个等价类，代表元 $(\mathbb{Z}_2, +, \bar{0})$

三阶群 . . . . 代表元 $(\mathbb{Z}_3, +, \bar{0})$

四阶群 两个等价类，代表元

$(\mathbb{Z}_2\times\mathbb{Z}_2, +, \{\bar{0}, \bar{0}\})$, $(\mathbb{Z}_4, +, \bar{0})$

五阶群 一个等价类 代表元 $(\mathbb{Z}_5, +, \bar{0})$

六阶群. 有点复杂

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

$\underset{a}{\underset{\shortparallel}{(12)}}, \underset{b}{\underset{\shortparallel}{(13)}} \in S_3$

$ab = (12)(13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\quad ab \neq ba$

$ba = (13)(12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

假设 $\varphi: \mathbb{Z}_6 \longrightarrow S_3$ 是同构

$\varphi(x) = a,\quad \varphi(y) = b$

$$\varphi(x+y) = \varphi(x)\varphi(y) = ab$$
$$\shortparallel \qquad\qquad\qquad \Rightarrow ab = ba \to\!\leftarrow$$
$$\varphi(y+x) = \varphi(y)\varphi(x) = ba$$

注: 交换群和非交换群不同构.

但它们之间可能同态. $\underset{\triangle}{\underline{\text{det}}}$.

§2.3 子群 (subgroups)

定义: 设 $(G, *, e)$ 是群. $H \subset G$

如果 $(H, *, e)$ 也是群. 则称 H 是 G

的子群.

注 群 G 有两个平凡子群. G 和 $\{e\}$

引理2.4 设 $(G, \cdot, e)$ 是群. H 是 G 的非空子集

$\Leftrightarrow \forall h_1, h_2 \in H.\quad h_1 h_2^{-1} \in H$

证: $\Leftarrow$ ∵ H 是群.

∴ $h_1, h_2^{-1} \in H \Rightarrow h_1 \cdot h_2^{-1} \in H$

"$\Rightarrow$" 设 $h \in H$. 则 $h h^{-1} \in H \Rightarrow e \in H$

由此 $e h^{-1} \in H$. $h^{-1} \in H$.

封闭性: 设 $h_1. h_2 \in H$

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

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

但 $h_2 h_2^{-1} = e \quad (h_2^{-1})^{-1} h_2^{-1} = e$

由命题2.1. $h_2 = (h_2^{-1})^{-1}$.

$\Rightarrow h_1 h_2 \in H$. ▨

注 设 G 是群. $(g^{-1})^{-1} = g$.

例: 设 $H \subset \mathbb{Z}$ 是所有偶数的集合

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

且 $H \simeq \mathbb{Z}$.

证: 设 $a, b \in H$ $a-b \in H \Rightarrow H$ 是子群

$$\varphi: \mathbb{Z} \to H$$
$$n \mapsto 2n$$

$\varphi(a+b) = 2(a+b) = 2a+2b = \varphi(a)+\varphi(b)$

φ 是双射. $\Rightarrow$ φ 是同构

例: 设 $GL_n(\mathbb{Q})$ 是元素为有理数的n阶方阵. $SL_n(\mathbb{R})$ 是 $GL_n(\mathbb{R})$ 中行列式为1的方阵的集合.

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

证: 设 $A, B \in GL_n(\mathbb{Q})$

则 $B^{-1} \in GL_n(\mathbb{Q})$ [第二章定理3.1]

于是 $AB^{-1} \in GL_n(\mathbb{Q})$. 节

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

设 $A, B \in SL_n(\mathbb{R})$

$|AB^{-1}| = |A||B^{-1}| = |B^{-1}|$

$BB^{-1} = E$ $|B| \cdot |B^{-1}| = 1 \Rightarrow |B^{-1}| = 1$

$\Rightarrow |AB^{-1}| = 1 \Rightarrow AB^{-1} \in SL_n(\mathbb{R})$

于是 ~~GL~~ $SL_n(\mathbb{R})$ 是 $GL_n(\mathbb{R})$ 子群

例: $A_n = \{\sigma \in S_n \mid \sigma$ 是偶~~奇~~置换$\}$

证明: A_n 是 S_n 的子群

设: ~~A_n~~, $\sigma, \tau \in A_n$

$\sigma = (i_1, j_1) \cdots (i_{2p}, j_{2p})$

$\tau = (k_1, l_1) \cdots (k_{2q}, l_{2q})$

$\tau^{-1} = (k_{2q}, l_{2q}) \cdots (k_1, l_1)$

$\sigma\tau^{-1} = (i_1, j_1) \cdots (i_{2p}, j_{2p})(k_{2q}, l_{2q}) \cdots (k_1, l_1) \in A_n$

补充内容: Lagrange 定理 (化简版)

设 G 是有限群. H 是 G 的子群.

则 $\mathrm{card}(H) \mid \mathrm{card}(G)$

证: 设 $g \in G$. $gH := \{gh \mid h \in H\}$

ad-hoc) 称为 H 的一个左倍集 (coset).

由引理2.2. $\mathrm{card}(gH) = \mathrm{card}(H)$.

($\because$ $gH = L_g(H)$ 而 L_g 是双射)

$\because$ $\mathrm{card}(G) < \infty$ ~~G是[illegible]~~ 且 $g \in gH$.

$\therefore$ G 是有限个 H 的左倍集的并

令 $G = g_1H \cup g_2H \cup \cdots \cup g_kH$

其中 $g_1, \dots g_k \in G$ 且 k 极小

断言: $g_1H, g_2H, \cdots g_kH$ 两两互不相交

断言的证明: 假设 $g_1H \cap g_2H \neq \emptyset$

则 $\exists\, a \in g_1H \cap g_2H$. 即 $\exists\, h_1 \in H, h_2 \in H$

使得 $a = g_1h_1 = g_2h_2$

于是 $g_2 = g_1(h_1h_2^{-1})$ ~~$\Rightarrow g_2 \in g_1H$~~

$\forall\, h \in H$ $g_2h = g_1(h_1h_2^{-1})h = g_1(h_1h_2^{-1}h) \in g_1H$

即 $g_2H \subset g_1H$

$\Rightarrow$ $G = g_1H \cup g_3H \cup \cdots \cup g_kH$. $\rightarrow\leftarrow$

断言成立.

于是 $\mathrm{card}(G) = \mathrm{card}(g_1H) + \cdots + \mathrm{card}(g_kH)$

$= k\,\mathrm{card}(H)$ ▨

例: 设 $\mathrm{card}(G)$ 是素数. 则 G 没有非平凡子群

证: 设 H 是 G 的子群. 由 Lagrange 定理

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

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

$\Rightarrow$ $H = \langle e \rangle$ 或 $H = G$ ▨

§2.4 群的生成元

记号: 设 ~~G是群~~. $(G, \cdot, e)$ 是群

$m \in \mathbb{Z}$. $g \in G$

$$g^m = \begin{cases} \underbrace{g \cdots g}_{m} & m > 0 \\ e & m = 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{-m} & m < 0 \end{cases}$$

自己验证: $\forall m, n \in \mathbb{Z}$

$$g^{m+n} = g^m g^n \qquad g^{mn} = (g^m)^n = (g^n)^m$$

当群 G 是 $(G, +, 0)$ 时

$$mg := \begin{cases} \underbrace{g+\cdots+g}_{m} & m>0 \\ 0 & m=0 \\ \underbrace{(-g)+\cdots+(-g)}_{-m} & m<0 \end{cases}$$

自己验证 $\forall m+n \in \mathbb{Z}$

$$(m+n)g = mg + ng. \qquad (mn)g = m(ng) = n(mg)$$

定义: 设 $(G, \cdot, e)$ 是群. $S \subset G$
非空

$$\langle S \rangle := \{ x_1^{i_1} \cdots x_n^{i_n} \mid \text{其中 } n \geq 1, x_1 \cdots x_n \in S, i_1 \cdots i_n \in \mathbb{Z} \}$$

称 $\langle S \rangle$ 为由 S 生成的子群.

验证 ~~G~~ $\langle S \rangle$ 是 G 的子群.

设 $a = x_1^{i_1} \cdots x_m^{i_m}$. $b = y_1^{j_1} \cdots y_n^{j_n}$.
其中 $x_1, \cdots x_m, y_1, \cdots y_n \in S$. $i_1, \cdots i_m, j_1, \cdots j_n \in \mathbb{Z}$

$$ab^{-1} = (x_1^{i_1} \cdots x_m^{i_m})(y_1^{j_1} \cdots y_n^{j_n})^{-1}$$
$$= (x_1^{i_1} \cdots x_m^{i_m})(y_n^{-j_n} \cdots y_1^{-j_1})$$
$$= x_1^{i_1} \cdots x_m^{i_n} y_n^{-j_n} \cdots y_1^{-j_1} \in \langle S \rangle$$

由引理2.4. $\langle S \rangle$ 是 G 的子群

例: $(\mathbb{Z}, +, 0)$. $\mathbb{Z} = \langle \{1\} \rangle = \langle 1 \rangle$

$(\mathbb{Z}_n, +, \overline{0})$ $\mathbb{Z}_n = \langle \overline{1} \rangle$

$GL_n(\mathbb{R})$ 由 $\mathbb{R}$ 上所有 n 阶初等矩阵
生成 [见讲义2-5 p16 例]

S_n 由所有循环生成 [第一章定理5.1]
也可由所有对换生成 [讲义1-4 p11 注]

$S_n = \langle (12), (12 \cdots n) \rangle$ [书上 p128.10]

§2.5 群中元素的阶.

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 记为 $\mathrm{ord}(g)=\infty$.

设 g 是有限阶, 则存在最小正整数 k 使得 $g^k=0$. 称 k 为 g 的阶. 记为 $\mathrm{ord}(g)=k$.

例: 在 S_n 中 $\sigma\in S_n$ 的阶与第一章的阶一致

例: 在 $(\mathbb{Z},+,0)$ 中 任何非零元都是无穷阶的

例: 在 $(\mathbb{Z}_{10},+,0)$ 中求 $\bar{2}$ 和 $\bar{7}$ 的阶

$\underbrace{\bar{2}+\cdots+\bar{2}}_{5}=\bar{0} \Rightarrow \mathrm{ord}(\bar{2})=5$

$k\cdot\bar{7}=\bar{0} \Rightarrow \overline{7k}=\bar{0}$

$\Rightarrow 10\mid 7k$

$\Rightarrow k=10 \Rightarrow \mathrm{ord}(\bar{7})=10$.

引理2.5 设 G 是群, $g\in G$, $\mathrm{ord}(g)=k<\infty$

[illegible] $g^n=e$ $\Longleftrightarrow$ $k\mid n$.

证: "$\Rightarrow$" $n=qk+r$, 其中 $q\in\mathbb{Z}$ $r\in\{0,1,..k-1\}$

$e=g^n=g^{qk}\cdot g^r=(g^k)^q\cdot g^r=e^q\cdot g^r$

$\Rightarrow e=g^r \Rightarrow r=0$

"$\Leftarrow$" 设 $n=qk$, $q\in\mathbb{Z}$

$g^n=g^{qk}=(g^k)^q=e$. □

引理2.6 设 $g\in G$. (G 是群)

(i) 如果 $\mathrm{ord}(g)=\infty$, 则 $\forall i,j\in\mathbb{Z}, i\neq j$, $g^i\neq g^j$

(ii) 设 如果 $\mathrm{ord}(g)=k<\infty$, 则

$\{g^n \mid n\in\mathbb{Z}\}$ $\langle g\rangle=\{e,g,..g^{k-1}\}$

证: (i) 若 $g^i=g^j$ (设 $i>j$), 则

$g^{i-j}=e \Rightarrow g$ 阶有限 $\rightarrow\leftarrow$

(ii) 设 $n\in\mathbb{Z}$ 则 $n=qk+r$, $r\in\{0,1,..k-1\}$

$g^n=g^{qk}\cdot g^r=g^r\in\{e,g,..g^{k-1}\}$

设 ∃ $i,j \in \{0,1,\dots k-1\}$. 满足 $g^i = g^j$

则 不妨设 $j \geq i$. 则

$$g^{j-i} = e$$

由 $k > j-i \geq 0$ 可知 $j=i$. ▨

推论)(Lagrange)

~~Cauchy 定理~~: 设 G 是有限群

则 $\forall g \in G$. $\mathrm{ord}(g) < \infty$ 且 $\mathrm{ord}(g) \mid \mathrm{card}(G)$

证: 因为 $\langle g \rangle \subset G$. 所以 $\mathrm{card}(\langle g \rangle)$ 有限

$\Rightarrow$ $\mathrm{ord}(g)$ 有限. [引理2.6 (i)]

设 $\mathrm{ord}(g) = k < \infty$

则 $\langle g \rangle = \{e, g, \dots g^{k-1}\}$ [引理2.6(iii)]

于是 $\mathrm{card}\langle g \rangle = k$. $\Rightarrow$ $k \mid \mathrm{card}(G)$

[Lagrange 定理] ▨

~~例: 证明, 设 G 是含有4个元素的群. 证明 G 共有同构~~

§2.5 ~~群循群~~ 循环群

定义: 设 $(G, \cdot, e)$ 是群 如果

存在 $g \in G$ 使得 $G = \langle g \rangle$,

则称 G 是循环群.

定理2.1 设 G 是循环群. $\mathrm{card}(G) > 1$

(i) 如果 $\mathrm{card}(G) = \infty$. 则 $G \cong (\mathbb{Z}, +, 0)$

(ii) 如果 $\mathrm{card}(G) = n < \infty$. 则 $G \cong (\mathbb{Z}_n, +, \bar{0})$

证: (i) 设 $G = \langle g \rangle$. 因为 G 是无限群

所以 $\mathrm{ord}(g) = \infty$ [引理2.6]

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

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

$$\varphi: G \longrightarrow \mathbb{Z}$$

$$g^n \longmapsto n.$$

是良定义的双射

$\varphi(g^n \cdot g^m) = \varphi(g^{m+n}) = m+n$

$= \varphi(g^m) + \varphi(g^n)$.

φ 是同构.

(ii). 设 $G = \langle g \rangle$. 因为 G 有限

g 是有限阶的. [引理2.6]

设 $n = \mathrm{ord}(g)$ 则

$G = \{g^0, g^1, \cdots g^{n-1}\}$

$$\begin{aligned} \varphi:\ G &\longrightarrow \mathbb{Z}_n \\ g^k &\longmapsto \overline{k}, \quad k = 0, 1, \cdots n-1 \end{aligned}$$

则 φ 是良定义的双射.

$\varphi(g^k g^l) = \varphi(g^{k+l})$

设 $k+l = qn + r$

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

$\varphi(g^{k+l}) = \varphi(g^r) = \overline{r}$

$\varphi(g^k) + \varphi(g^l) = \overline{k} + \overline{l} = \overline{k+l} = \overline{r}$

于是 φ 是同构 ▨

例: 设 G 是含有 4 个元素的群

则 $G \simeq (\mathbb{Z}_4, +, \overline{0})$ 或 $G \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\overline{0}, \overline{0}))$

证: 由 ~~Cauchy~~ Lagrange 定理的推论. G 中元素的阶

是 1, 2 或 4.

如果 G 中有一个元素阶是 4, 则

$G = \langle g \rangle \simeq (\mathbb{Z}_4, +, \overline{0})$ [定理2.1]

否则. $G = \{e, a, b, c\}$. a, b, c 的阶都是 2

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & \mathbb{Z}_2 \times \mathbb{Z}_2 \\ & e & \longmapsto & (\overline{0}, \overline{0}) \\ & a & \longmapsto & (\overline{1}, \overline{0}) \\ & b & \longmapsto & (0, \overline{1}) \\ & c & \longmapsto & (\overline{1}, \overline{1}) \end{array}$$

验证: $\varphi(ex) = \varphi(e) + \varphi(x) \quad (\forall x \in \{a, b, c\}$

注意到
~~$\varphi(ab)=$~~

$ab\neq a$, $ab\neq b$. $ab\neq e$
$(b\neq e)$ $(a\neq e)$ $(\because a^2=e)$

$\Rightarrow$ $ab=c$ $\varphi(ab)=\varphi(c)=(\bar{1},\bar{1})$

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

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

类似可以验证: $\varphi(ac)=\varphi(a)+\varphi(c)$
$\varphi(bc)=\varphi(b)+\varphi(c)$.

于是 φ 是同构 ▨

§2.6. ~~自~~ Cayley定理和自同构

引理2.7. 设 $\varphi: G\longrightarrow H$ 是群同态

则 $\mathrm{im}(\varphi)$ 是 H 的子群.

证: 设 $h_1, h_2\in \mathrm{im}(\varphi)$.

则 $\exists\, g_1, g_2\in G$. 使得 $h_1=\varphi(g_1)$
$h_2=\varphi(g_2)$

由引理2.2 $\varphi(g_2^{-1})=h_2^{-1}$

$\varphi(g_1g_2^{-1})=\varphi(g_1)\varphi(g_2^{-1})=h_1h_2^{-1}\in \mathrm{im}(\varphi)$

由引理2.4 ~~$\varphi=$~~ $\mathrm{im}(\varphi)$是子群 ▨

定义: 设 X 是非空集. $T_X=\{f: X\to X \mid f双射$

则 $(T_X, \circ, \mathrm{id}_X)$ 称为 X 上变换群

Cayley定理: 设 G 是群, 则 G 同构于 T_G 的一个子群.

证: $\varphi:$ $G\longrightarrow T_G$
$g\longmapsto L_g$ (左平移)

由引理2.1 $L_g\in T_G$

设 $g_1, g_2\in G$

$\varphi(g_1g_2)=L_{g_1g_2}$

$\forall\, x\in G$ $L_{g_1g_2}(x)=(g_1g_2)x=g_1(g_2x)=g_1L_{g_2}(x)$
$=L_{g_1}(L_{g_2}(x))=L_{g_1}g_2(x)$

$\varphi(g_1g_2)=L_{g_1}L_{g_2}=L_{g_1}\circ L_{g_2}=\varphi(g_1)\circ\ \varphi(g_2)$

§3 环 (ring)

§3.1 环的定义

定义：设 $(R, +, 0)$ 是交换群

$(R, \cdot, 1)$ 是含幺半群.

如果 $\forall x, y, z \in R$

$$x(y+z) = xy + xz$$

$$(x+y)z = xz + yz$$

则称 $(R, +, 0, \cdot, 1)$ 是环. 当 $(R, \cdot, 1)$ 是交换含幺半群时, R 称为交换环.

例：$(\mathbb{Z}, +, 0, \cdot, 1)$ 是交换环

$(\mathbb{Z}_n, +, \overline{0}, \cdot, \overline{1})$ 是交换环

$(M_n(\mathbb{R}), +, O_{n\times n}, \cdot, E_n)$ 是非交换环

例：证明

① $\forall r \in R$, $0 \cdot r = r \cdot 0 = 0$

② $\forall r \in R$ $r + (-1)r = r + r(-1) = 0$

③ $(-1)(-1) = 1$

证：① $0 + 0 = 0$

$$(0+0)r = 0r \underset{\text{分配}}{\Longrightarrow} 0 \cdot r + 0 \cdot r = 0 \cdot r$$

$$\Rightarrow 0 \cdot r = 0$$

② $1 + (-1) = 0 \Rightarrow (1 + (-1))r = 0 \cdot r$

$$\Rightarrow 1 \cdot r + (-1)r = 0 \Longrightarrow r + (-1)r = 0$$

③ $(-1)(-1) = -(-1) = 1$

定理 3.1 (广义分配律)

设 R 是环, $a_1, \dots a_m, b_1, \dots b_n \in R$

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right)$$

$$= \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j = \sum_{j=1}^{n} \sum_{i=1}^{m} a_i b_j$$

φ 是同态

设 $\varphi(g_1)=\varphi(g_2)$，则 $L_{g_1}=L_{g_2}$

设 e 是 G 中单位元

$L_{g_1}(e)=L_{g_2}(e) \Rightarrow g_1e=g_2e \Rightarrow g_1=g_2$

$\Rightarrow \varphi$ 是单射

于是 φ 是从 G 到 $\mathrm{im}(\varphi)$ 的同构 ☒

推论2.1 设 G 是含有 n 个元素的有限群

则 $G \simeq S_n$ 中的某个子群.

定义：设 G 是群

$\varphi: G \longrightarrow G$ 是同构

则称 φ 是 G 上的自同构.

例：设 $g\in G$ $\quad \varphi_g: G \longrightarrow G$, $x \longmapsto g^{-1}xg$

$\varphi_g(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg$

$= \varphi_g(x)\varphi_g(y) \Rightarrow \varphi_g$ 是同态.

$\varphi_g(x)=\varphi_g(y) \Rightarrow g^{-1}xg = g^{-1}yg$

$\Rightarrow g^{-1}x = g^{-1}y$

$\Rightarrow x=y$. $\quad \varphi$ 单

$\forall z\in G$

$gzg^{-1}\in G \Rightarrow \varphi_g(gzg^{-1}) = g^{-1}(gzg^{-1})g = z$

所以，φ_g 是同构

命题2.4 设 $\mathrm{Aut}(G)$ 是群 G 上所有自同构构成的集合

则 $(\mathrm{Aut}(G), \circ, \mathrm{id}_G)$ 是 S_G 的子群

证：设 $\varphi, \psi \in \mathrm{Aut}(G)$

$\varphi\circ\psi^{-1} \in \mathrm{Aut}(G)$

(引理 2.2, 2.3) ☒

证: 先证: $\forall b \in R$

$$(a_1+\cdots+a_m)\, b = a_1 b + \cdots + a_m b \quad (*)$$

$m=1$. 显然

设 $m-1$ 时 $(*)$ 成立.

$$(a_1+\cdots+a_{m-1}+a_m)\, b = [\underbrace{(a_1+\cdots+a_{m-1}) + a_m}_{\text{广义结合}}]\, b$$

$$= \underbrace{(a_1+\cdots+a_{m-1})b + a_m b}_{\text{分配}}$$

$$= a_1 b + \cdots + a_{m-1} b + a_m b \quad \text{(归纳假设)}$$

于是 $(*)$ 成立.

对 n 归纳 $n=1$ 即 $(*)$ ✓

设 $n-1$ 时 定理成立.

$$(a_1+\cdots+a_m)(b_1+\cdots+b_{n-1}+b_n)$$

$$= (a_1+\cdots+a_m)(b_1+\cdots+b_{n-1}) + (a_1+\cdots+a_m)\, b_n$$

$$= \sum_{i=1}^{m}\sum_{j=1}^{n-1} a_i b_j + \sum_{i=1}^{m} a_i b_n$$

$$= \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j.$$

另一形式的证明类似 □

推论3.1 设 $a, b \in R$, $m, n \in \mathbb{Z}$

则 $(ma)(nb) = (mn)(ab)$

证: 情形1. $m>0, n>0$

由定理3.1 $(ma)(nb) = \left(\sum_{i=1}^{m} a\right)\left(\sum_{j=1}^{n} b\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} ab$

$= (mn)ab$

情形2. $m=0$ 或 $n=0$. 不妨设 $m=0$

则 $ma = 0_R$ [符号约定]

$(ma)(nb) = 0_R(nb) = 0_R$

$(mn)ab = 0\, ab = 0_R$ [符号约定]

情形3. $m>0$, $n<0$

$nb = (-n)(-b)$ $\quad (ma)(nb) = (ma)[(-n)(-b)]$

$= [m(-n)][a(-b)]$ ← [情形1]

$= (-mn)(a(-1_R)b) = (-mn)(a(-1_R)(-1_R)(-1_R)b)$

$= (-mn)(a(-1_R)b) = (-mn)(-ab)$

$= mn(ab)$ [符号约定]

自己分析 $m<0, n>0$. $\quad m<0, n<0$ □