①

回忆：4阶群 $G=\{e,a,b,c\}$

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

$a^2=b^2=c^2=e$

$ab=ba=c,\quad ac=ca=b,\quad cb=bc=a$

实例：$+:\ \underbrace{(\mathbb{Z}_2\times\mathbb{Z}_2)}_{G}\times\underbrace{(\mathbb{Z}_2\times\mathbb{Z}_2)}_{G}\longrightarrow\underbrace{\mathbb{Z}_2\times\mathbb{Z}_2}_{G}$

$(\bar m,\ \bar n),\ (\bar k,\bar l)\mapsto(\overline{m+k},\ \overline{n+l})$

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

$a+a=(\bar 1,\bar 0)+(\bar 1,\bar 0)=(\bar 1+\bar 1,\ \bar 0+\bar 0)$

$=(\bar 2,\bar 0)=(\bar 0,\bar 0)$

同理 $b+b=c+c=(\bar 0,\bar 0)$

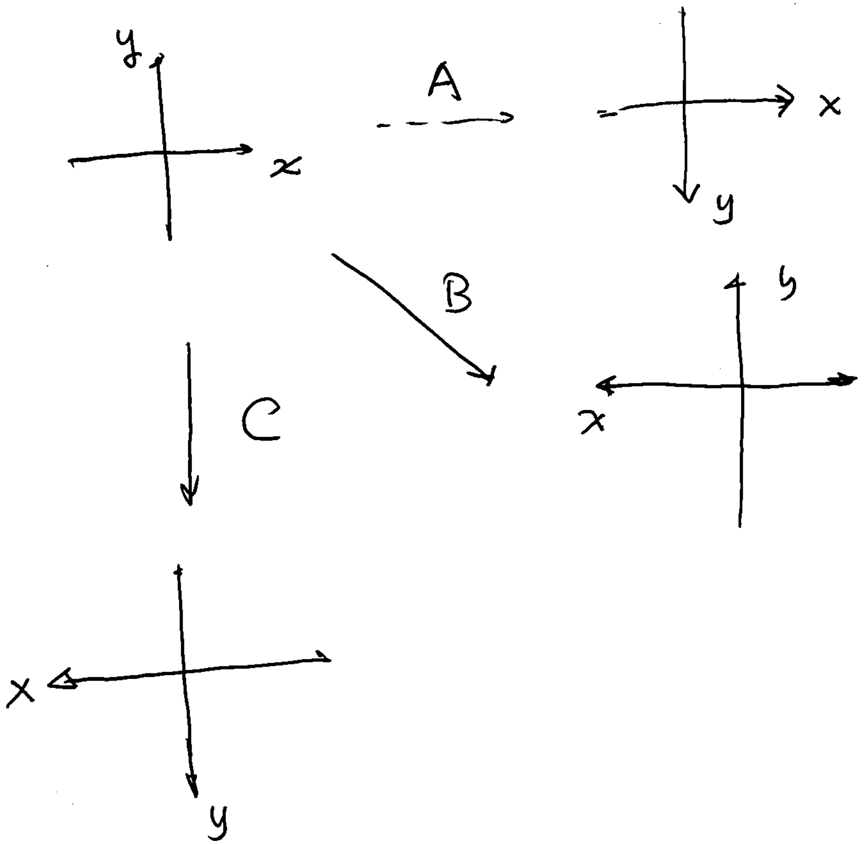
$b+c=(\bar 1,\bar 1)+(\bar 0,\bar 1)=(\bar 1+\bar 0,\ \bar 1+\bar 1)=(\bar 1,\bar 0)=a$

同理 $a+b=c,\quad a+c=b.$

$$G=\left(\left\{\underset{E}{\begin{pmatrix}1&0\\0&1\end{pmatrix}},\ \underset{A}{\begin{pmatrix}1&0\\0&-1\end{pmatrix}},\ \underset{B}{\begin{pmatrix}-1&0\\0&1\end{pmatrix}},\ \underset{C}{\begin{pmatrix}-1&0\\0&-1\end{pmatrix}}\right\},\ \cdot,\ E\right)$$

$A^2=B^2=C^2=E\qquad AB=C=BA,\quad AC=CA=B,$

$BC=CB=A$



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

$G=\{e, b, \underset{a}{\underset{\|}{b^2}}, \underset{c}{\underset{\|}{b^3}}\}$

$(\mathbb{Z}_4, +, 0)$ $\qquad \mathbb{Z}_2 = \{\underset{e}{\underset{\|}{\bar{0}}}, \underset{b}{\underset{\|}{\bar{1}}}, \underset{a}{\underset{\|}{\bar{2}}}, \underset{c}{\underset{\|}{\bar{3}}}\}$

$b+b=\bar{1}+\bar{1}=\bar{2}=a$

$b+b+b=\bar{1}+\bar{1}+\bar{1}=\bar{3}=c$

$$G=\left\{\underset{E}{\underset{\|}{\begin{pmatrix}1&0\\0&1\end{pmatrix}}}, \underset{A}{\underset{\|}{\begin{pmatrix}-1&0\\0&-1\end{pmatrix}}}, \underset{B}{\underset{\|}{\begin{pmatrix}0&-1\\1&0\end{pmatrix}}}, \underset{C}{\underset{\|}{\begin{pmatrix}0&1\\-1&0\end{pmatrix}}}\right\}$$

$(G, \cdot, E)$

$$B^2=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=A$$

$$B^3=AB=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}0&1\\-1&0\end{pmatrix}=C$$

$(\mathbb{Z}_2\times\mathbb{Z}_2, +, (\bar{0},\bar{0}))$ 和 $(\mathbb{Z}_4, +, \bar{0})$ ②

好像不是一回事.

§2.2 群同态与群同构

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

群: $\varphi: G \longrightarrow H$ 映射

如果 $\forall g_1, g_2 \in G$

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

则称 φ 是从 G 到 H 的同态.

如果 φ 还是单射. 则称 φ 是单同态

φ 还是满射, 则称 φ 是满同态

φ 还是双射. 则称 φ 是同构

如果 G 和 H 之间有一个群同构. 则将

G 和 H 是同构的. 记为 $G \simeq H$.

引理 2.4 设 $(G,*,e)$ 和 $(H,\star,\varepsilon)$ 是两个群. $\varphi: G\to H$ 是群同态

则.
(i) $\varphi(e)=\varepsilon$
(ii) $\forall g\in G,\ \varphi(g^{-1})=\varphi(g)^{-1}$
(iii) 如果 φ 是同构. 则 $\varphi^{-1}: H\to G$ 也是同构.

证: (i) $\varphi(e)=\varphi(e*e)=\varphi(e)\star\varphi(e)$

$$\varphi(e)\star\varphi(e)^{-1}=[\varphi(e)\star\varphi(e)]\star\varphi(e)^{-1}$$
$$=\varphi(e)\star(\varphi(e)\star\varphi(e)^{-1})$$
$$\varepsilon=\varphi(e)\star\varepsilon=\varphi(e)$$

(ii) ~~$\varepsilon=\varphi(g)$~~ 由 (i)

$$\varepsilon=\varphi(e)=\varphi(g*g^{-1})=\varphi(g)\star\varphi(g^{-1})$$
$$\varphi(g)^{-1}\star\varepsilon=\varphi(g)^{-1}\star(\varphi(g)\star\varphi(g^{-1}))$$
$$=(\varphi(g)^{-1}\star\varphi(g))\star\varphi(g^{-1})$$
$$=\varepsilon\star\varphi(g^{-1})$$
$$\varphi(g)^{-1}=\varphi(g^{-1})$$

(iii) 设 $h_1,h_2\in H$. 则存在 $g_1,g_2\in G$ 使得 $\varphi(g_1)=h_1$, $\varphi(g_2)=h_2$

~~$\varphi^{-1}(h_1\star h_2)=?$~~

则 $\varphi(g_1*g_2)=h_1\star h_2 \Rightarrow$
$$\varphi^{-1}\circ\varphi(g_1*g_2)=\varphi^{-1}(h_1\star h_2)$$
$$\varphi^{-1}(h_1\star h_2)=g_1*g_2=\varphi^{-1}(h_1)*\varphi^{-1}(h_2)\ \square$$

~~注: 由(ii)的证明可知~~
~~设 G 是群. $g,h\in G$.~~
~~如果 $gh=e$ 或 $hg=e$. 则 $h=g^{-1}$.~~

例: 自然投射
$$\pi: \mathbb{Z}\to\mathbb{Z}_n$$
是从 $(\mathbb{Z},+,0)$ 到 $(\mathbb{Z}_n,+,\bar{0})$ 的群同态: $\forall\ a,b\in\mathbb{Z}$
$$\pi(a+b)=\overline{a+b}=\bar{a}+\bar{b}=\pi(a)+\pi(b).$$
$\square$

例：证明：

$(\mathbb{Z}_2, +, \bar{0})$ 与 $(\{1,-1\}, \cdot, 1)$

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

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

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

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

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

$\boxtimes$

φ 显然是双射.

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

证：假设 $\varphi: \mathbb{Z}_2\times\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$ 是同构. 则 $\exists\, (\bar{m},\bar{n}) \in \mathbb{Z}_2\times\mathbb{Z}_2$ 使得 $\varphi((\bar{m},\bar{n})) = \bar{1} \in \mathbb{Z}_4$

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

$\therefore (\bar{m},\bar{n}) = (\bar{1},\bar{0})$, 或 $(\bar{0},\bar{1})$, 或 $(\bar{1},\bar{1})$

同时在 $\mathbb{Z}_2\times\mathbb{Z}_2$ 中 $(\bar{m},\bar{n}) + (\bar{m},\bar{n}) = (\bar{0},\bar{0})$

$\Rightarrow \bar{1}+\bar{1} = \varphi((\bar{m},\bar{n})+(\bar{m},\bar{n})) =$
$= \varphi(\bar{0},\bar{0}) = \bar{0}$

即在 $\mathbb{Z}_4$ 中 $\bar{1}+\bar{1} = \bar{0}$. 但 $\bar{1}+\bar{1} = \bar{2} \neq \bar{0}$.
$\rightarrow\leftarrow$

引理2.5 设 $(G, *, e)$, $(H, \star, \varepsilon)$, $(K, \diamond, \lambda)$ 是三个群. $\varphi: G \to H$, $\psi: H \to K$ 是两个群同态. 则 $\psi\circ\varphi$ 是 G 到 K 的同态.

证：

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

证：设 $g_1, g_2 \in G$

$\psi\circ\varphi(g_1 * g_2)$
$= \psi(\varphi(g_1) \star \varphi(g_2))$
$= \psi\circ\varphi(g_1) \diamond \psi\circ\psi(g_2)$

$\boxtimes$

命题 2.1 群同构"$\simeq$"是等价关系

证: 设 G, H, K 是三个群

$G \to G$ 的恒同映射显然是群同构, 于是 $G \simeq G$, 自反性成立.

设 $G \simeq H$. 则存在群同构

$\varphi: G \to H$

由引理2.3 (iii). $\varphi^{-1}: H \to G$ 也是群同构

于是 $H \simeq G$. (对称性成立)

设 $G \simeq H$, $H \simeq K$. 则存在群同构

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

$\psi \circ \varphi$ 也是群同态. 且是双射, $\Rightarrow$ 同构

于是: $G \simeq K$. 传递律成立. ∎

<u>群论的基本问题:</u> 给定一类群. 求这类群在"$\simeq$"下的等价类

一阶群: 都同构于 $(\{0\}, +, 0)$

二阶群 - - - - $(\mathbb{Z}_2, +, \bar{0})$

三阶群 - - - - $(\mathbb{Z}_3, +, \bar{0})$

四阶群 或同构于 $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0}))$ 或

同构于 $(\mathbb{Z}_4, +, \bar{0})$

五阶群 都同构于 $(\mathbb{Z}_5, +, \bar{0})$

<u>六阶群</u> $S_3 = \{e, (12), (13), (23), (123), (213)\}$

$$(12)(13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (213)$$

$$(13)(12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$$

$(12)(13) \neq (13)(12)$. S_3 是非交换群.

§2.3 子群与生成元

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 (subgroup).

引理2.~~5~~ 设 $(G, *, e)$ 是群

(i) 设 $g, h \in G$. 如果 $g*h=e$ 则 $h=g^{-1}$

(ii) 设 $g \in G$. 则 $(g^{-1})^{-1}=g$

(iii) $(g*h)^{-1}=h^{-1}*g^{-1}$

证: (i) $g*h=e \Rightarrow g^{-1}*(g*h)=g^{-1}*e$

$\Rightarrow (g^{-1}*g)*h=g^{-1}*e \Rightarrow e*h=g^{-1}$

$\Rightarrow h=g^{-1}$

(ii) $(g^{-1})^{-1}*g^{-1}=e=g*g^{-1}$

$\Rightarrow (g^{-1})^{-1}=g$ （消去律） $\square$

(iii) 自己验证

记号: 设 G 是群. $x \in G$

$x^0=e$, $\forall n \in \mathbb{Z}$. $n<0$

$x^n = \underbrace{x^{-1} * \cdots * x^{-1}}_{-n}$ $\quad nx = \underbrace{(-x)+\cdots+(-x)}_{-n}$

从此以后我们~~可能~~在不会混淆的前提下. 用 xy 代替 $x*y$.

~~命题~~ 2.2 设 G 是群. e 是其单位元

设 $H \subset G$. H 非空. 如果 $\forall h_1, h_2 \in H$ $h_1 h_2^{-1} \in H$. 则 H 是子群.

证: 设 $h \in H$. 则 $hh^{-1} \in H \Rightarrow e \in H$

H 有单位元

$eh^{-1} \in H \Rightarrow h^{-1} \in H$. 即 H 中的元素可逆

设 $h_1, h_2 \in H$. 则 $h_2^{-1} \in H$

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

即 G 中的乘法是 H 上的二元运算

结合律显然 $\square$

例: 设 $\mathbb{E}$ 是所有偶数的集合

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

验证: 偶数相减仍为偶数

例: 设 $A_n = \{\sigma \in S_n \mid \varepsilon_\sigma = 1\}$

A_n 是 S_n 的子群.

验证: $\sigma \in A_n \Rightarrow \sigma = (i_1 j_1) \cdots (i_{2k}, j_{2k})$

$\sigma^{-1} = (i_{2k}, j_{2k}) \cdots (i_1, j_1) \in A_n$

设 $\sigma, \tau \in A_n$. $\sigma\tau^{-1} \in A_n$. $\square$

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

$U_n(\mathbb{Z}) = \{ A \in GL_n(\mathbb{R}) \mid$ A 中的元素为整数 且 $|A|=1 \}$

证明：$U_n(\mathbb{Z})$，$GL_n(\mathbb{Q})$ 都是 $GL_n(\mathbb{R})$ 的子群

证：设 $A \in GL_n(\mathbb{R})$，则

$$A^{-1} = \frac{1}{|A|} A^*$$

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

$A \in U_n(\mathbb{Z}) \Rightarrow A^{-1} \in U_n(\mathbb{Z})$

由此可知 $A, B \in GL_n(\mathbb{Q})$ $\quad AB^{-1} \in GL_n(\mathbb{Q})$

$A, B \in U_n(\mathbb{Z})$，$AB^{-1} \in U_n(\mathbb{Z})$

由命题2.2. $GL_n(\mathbb{Q})$，$U_n(\mathbb{Z})$ 是子群.

定义：设 G 是群，$S \subset G$ 非空

定义

$$\langle S \rangle = \{ x_1^{k_1} \cdots x_n^{k_n} \mid k_1, \dots k_n \in \mathbb{Z}, n \in \mathbb{Z}^+ \}$$

称 $\langle S \rangle$ 是 G 中由 $x_1, \dots x_n$ 生成的子群

验证：$\langle S \rangle$ 是子群．设 $x_1, \dots x_p, y_1 \dots y_q \in S$ ⑦

$$(x_1^{k_1} \cdots x_p^{k_p})(y_1^{l_1} \cdots y_q^{l_q})^{-1}$$

$$= (x_1^{k_1} \cdots x_p^{k_p})(y_q^{-l_q} \cdots y_1^{-l_1}) \quad \text{(引理2.1)}$$

$$= x_1^{k_1} \cdots x_p^{k_p} y_q^{-l_q} \cdots y_1^{-l_1} \in \langle S \rangle.$$

（广义结合律）

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

注：当 $S = \{x_1, \dots x_s\}$ 时 $\langle S \rangle = \langle x_1, \dots x_s \rangle$

例．$(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0})) = \langle (\bar{0}, \bar{1}), (\bar{1}, \bar{0}) \rangle$

$\mathbb{Z}_4 = \langle \bar{1} \rangle$ $\quad$ 于是 $\mathbb{Z}_2 \times \mathbb{Z}_2$，$\mathbb{Z}_4$

不可能同构

例：$GL_n(\mathbb{R}) = \langle S \rangle$，其中

S 是所有n阶初等矩阵的集合．

$GL_n(\mathbb{Q})$ 由所有n阶有理数域上的初等矩阵生成

回42　群中的消去律

设 G 是群，$a,b,c\in G$

如果 $ab=ac$ 或 $ba=ca$

则 $b=c$.

因为 a 可逆 所以 a^{-1} 存在

$$a^{-1}(ab)=a^{-1}(ac)\Rightarrow \cancel{b=}$$

$$(a^{-1}a)b=(a^{-1}a)c\Rightarrow b=c$$

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

设 G 由一个元素 x 生成

$$G=\{x^k \mid k\in\mathbb{Z}\}$$

$+$

$$\langle 1\rangle=\{k\cdot 1 \mid k\in\mathbb{Z}\}$$

$$=\{1+\cdots+1 \mid k\in\mathbb{Z}\}$$

$$=\{k \mid k\in\mathbb{Z}\}$$

$$=\mathbb{Z}.$$

§2.4. 循环群.

定义：设 G 是由一个元素生成的群.

则称 G 是循环群.

定义：设 G 是群，$g \in G$（单位元 e）. 如果存在正整数 k，使得 $g, g^2, \ldots, g^{k-1}$ 都不等于 e 而 $g^k = e$. 则称 k 是 G 的阶. 记为 $\mathrm{ord}(g)$. 如果这样的正整数不存在，则称 g 的无穷阶的，记为 $\mathrm{ord}(g) = +\infty$.

例：S_n 中 σ 的阶与以前定义的相同

例 设 G 是群，$g \in G$

证明 $\mathrm{card}(\langle g \rangle) = \mathrm{ord}(g)$

证：情形1. 设 g $\mathrm{ord}(g) = \infty$

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

若 $g^{k_1} = g^{k_2}$ $\quad k_1 \le k_2$

则 $g^{-k_1} g^{k_1} = g^{-k_1} \cdot g^{k_2}$

$$\Rightarrow g^{k_2 - k_1} = e \Rightarrow k_2 = k_1$$

（e → 单位元）

于是 $\mathrm{card}(\langle g \rangle) = \infty$.

情形2. 设 $\mathrm{ord}(g) = k > 0$

断言. $e, g, g^2, \ldots, g^{k-1}$ 两两不同

断言的证明：设 $g^i = g^j$. $i, j \in \{0, 1, \ldots, k-1\}$, $j \geq i$

则 $g^{j-i} = e \Rightarrow j = i$. 断言成立

$$\Rightarrow \mathrm{card}(\langle g \rangle) \geqslant k.$$

设 $a \in \langle g \rangle$. 则 $\exists\, n \in \mathbb{Z}$，使得

$$~~a^n = g~~ \quad a = g^n$$

由整数除法 $n = qk + r$ $\quad r \in \{0, 1, \ldots, k-1\}$

$$a = g^n = g^{qk+r} = (g^k)^q \cdot g^r = e^q \cdot g^r = g^r \in \{e, g, g^2, \ldots, g^{k-1}\}$$

于是 $\langle g \rangle = \{e, g, g^2, \ldots, g^{k-1}\}$ $\square$

命题2.3 设 G 是循环群且 $\mathrm{card}(G)=\infty$. 则

$$G \simeq (\mathbb{Z}, +, 0)$$

证: 设 $G=\langle g\rangle=\{g^k \mid k\in\mathbb{Z}\}$

$$\varphi:\ G \longrightarrow \mathbb{Z}$$
$$g^k \longmapsto k$$

$\because \forall k, l\in G$, $k\neq l$. $g^k\neq g^l$. $\therefore$ φ 是良定义的

且 φ 是双射. 设 $a, b\in G$

$\exists\, m, n\in\mathbb{Z}$ 使得 $a=g^m$, $b=g^n$

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

$= m+n=\varphi(g^m)+\varphi(g^n)=\varphi(a)+\varphi(b)$

于是 φ 是同态, 从而是同构 $\square$

命题2.4 设 G 是 n 阶循环群

则 $G\simeq(\mathbb{Z}_n, +, \overline{0})$

证: 设 $G=\langle g\rangle$ 因为 G 有限

所以 $\mathrm{ord}(g)=k<\infty$ (见上例 ~~情形~~ 1)

由情形2可知 $k=n$ 且

$$G\simeq\{e, g, \cdots, g^{n-1}\}$$

$$\varphi:\ G\longrightarrow\mathbb{Z}_n$$
$$g^i\longmapsto\overline{i}$$

$i=0, 1, \cdots, n-1$. 由上例情形2的断言

φ 是良定义的. φ 是双射

设 $a, b\in G$. $\exists\, i, j\in\{0, 1, \cdots, n-1\}$ 使得

$a=g^i$, $b=g^j$

$\varphi(ab)=\varphi(g^i g^j)=\varphi(g^{i+j})=\overline{i+j}$

$=\overline{i}+\overline{j}=\varphi(g^i)+\varphi(g^j)$ $\square$

于是 φ 是同构 $\square$

§2.5 Cayley 定理

设 G 是群. $T_G = \{ f: G \to G \mid f \text{ 是双射} \}$

则 $(T_G, \circ, id_G)$ 是群.

定理2.1　G 同构于 T_G 的某个子群.

引理2.5. 设 G, H 是两个群

$\varphi: G \to H$ 是群同态. 则

$im(\varphi)$ ~~[illegible]~~ 是 H 的子群.

证: 设 $h_1, h_2 \in im(\varphi)$, 则存在

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

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = h_1 \varphi(g_2^{-1})$$
$$= h_1 h_2^{-1} \quad (\text{引理}2.3)$$

~~和 $\varphi(g_2^{-1})\varphi(g_2) = \varphi(g_2^{-1} g_2) = \varphi(e) = e$~~

~~(e 是 G 的~~

$\Rightarrow h_1 h_2^{-1} \in im(\varphi)$

$\Rightarrow im(\varphi)$ 是子群　□

定理2.1 的证明

由引理2.3 $\forall g \in G$ 左平移

$$L_g \in T_G$$

$$\varphi: G \longrightarrow T_G$$
$$g \longmapsto L_g$$

设 $g_1, g_2 \in G$

若 $\varphi(g_1) = \varphi(g_2)$. 则 $L_{g_1} = L_{g_2}$

$L_{g_1}(e) = L_{g_2}(e)$,　e 是 G 的单位.

$g_1 e = g_2 e \Rightarrow g_1 = g_2$

于是 φ 是单射

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

$\forall a \in G$　$L_{g_1 g_2}(a) = (g_1 g_2) a = g_1 (g_2 a)$

$= g_1 (L_{g_2}(a)) = L_{g_1}(L_{g_2}(a)) = L_{g_1} \circ L_{g_2}(a)$

$\Rightarrow L_{g_1 g_2} = L_{g_1} \circ L_{g_2}$

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

φ 是群同态; 令

$$\psi: G \longrightarrow im(\varphi) \quad \text{是群同构}$$
$$g \longmapsto L_g$$

□

<u>注:</u> n 阶群 G 同构于 S_n 的一个子群.

注: Lagrange 定理: 设 G 是 n 阶群

H 是 G 的子群. 则

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

特别地: $\forall g \in G \quad \mathrm{ord}(g) \mid \mathrm{card}(G)$.

命题 2.5 设 G 是群, $a \in G$

$$I_a: \begin{aligned} G &\longrightarrow G \\ g &\longmapsto a g a^{-1} \end{aligned}$$

是同构 (自同构). 称 I_a 是关于 a 的共轭映射

<u>证:</u> $$\varphi: \begin{aligned} G &\longrightarrow G \\ g &\longmapsto a^{-1} g a \end{aligned}$$

$I_a \circ \varphi(g) = I_a(a^{-1}ga) = a(a^{-1}ga)a^{-1} = g$

$\varphi \circ I_a(g) = g \quad \Rightarrow \quad I_a$ 是双射

$g_1, g_2 \in G$

$$\begin{aligned} I_a(g_1 g_2) &= a(g_1 g_2) a^{-1} \\ &= (a g_1)(a^{-1} a)(g_2 a^{-1}) \\ &= (a g_1 a^{-1})(a g_2 a^{-1}) = I_a(g_1) I_a(g_2) \end{aligned}$$ ☒

pre. Ex. 9, 10, 11

引理 2.7 设 $(i_1, \cdots, i_r) \in S_n$. 则 $\forall \pi \in S_n$

$$\pi (i_1, \cdots, i_r) \pi^{-1} = (\pi(i_1), \cdots, \pi(i_r))$$

<u>证:</u> $j \in \{\pi(i_1), \cdots, \pi(i_r)\}$ 则 $\exists!\ k \in \{i_1, \cdots, i_r\}$

使得 $j = \pi(i_k)$

$$(\pi(i_1), \cdots, \pi(i_r))(j) = \begin{cases} \pi(i_{k+1}), & k < r \\ \pi(i_1), & k = r \end{cases}$$

$$\pi(i_1, \cdots, i_r)\pi^{-1}(j) = \pi(i_1, \cdots, i_r)(i_k) = \begin{cases} \pi(i_{k+1}), & k < r \\ \pi(i_1), & k = r \end{cases}$$

若 $j \notin \{\pi(i_1), \cdots, \pi(i_r)\}$

$(\pi(i_1), \cdots, \pi(i_r))(j) = j$

$\pi\,(\cancel{\pi i_1} i_1, \cdots, i_r)\,\pi^{-1}(j) = \pi \circ \pi^{-1}(j) = j$. ☒

P128.9

证明：$S_n = \langle (12), (13), \cdots (1n) \rangle$

由第一章 $S_n = \langle \{ (ab) \mid a, b \in \{1, \cdots n\}, a \neq b \} \rangle$

于是只要证明：$(ab) \in \langle (12), (13), \cdots (1n) \rangle$

即可　设 $\pi = (1a)$

$\pi (ab) \pi^{-1} = (\pi(a), \pi(b)) = (1b)$

$\Rightarrow (ab) = \pi^{-1} (1b) \pi = (1a)(1b)(1a) \in \langle (12), (13), \cdots (1n) \rangle$

P128.10　证明 $S_n = \langle (12), (123 \cdots n) \rangle$

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

由 Ex 9. 只要证：

$(12), (13), \cdots (1n) \in \langle \underbrace{(12), (23), \cdots (n-1, n)}_{H} \rangle$

(12) ✓

$(12)(23)(12)^{-1} = (23) \Rightarrow (13) = (12)(23)(13) \in H$

设 $(1i) \in H$. $2 \leq i < n$

$(1i)(i, i+1)(1i)^{-1} = (1, i+1) \Rightarrow$

$(1, i+1) = (1i)(i, i+1)(1i) \in H$ (归纳假设

断言成立

只要证：$(i, i+1) \in \langle (12), (12 \cdots n) \rangle$

$i = 1, 2, \cdots n-1$

$i=1$. 显然

设 $i < n-1$ 且 $(i, i+1) \in \langle (12), (12 \cdots n) \rangle$

$(12 \cdots n)(i, i+1)(12 \cdots n)^{-1} = ((12 \cdots n)(i), (12 \cdots n)(i+1))$

$= (i+1, i+2). \in \langle (12), (12 \cdots n) \rangle$

于是 $(12), \cdots (n-1, n) \in \langle (12), (12 \cdots n) \rangle$

$\Rightarrow H \subset \langle (12), (12 \cdots n) \rangle$

$\Rightarrow S_n \subset \langle (12), (12 \cdots n) \rangle \subset S_n$

$\Rightarrow S_n = \langle (12), (12 \cdots n) \rangle$ ☒

P128.11　证明 $A_n = \langle (123), (124), \cdots (12n) \rangle$

$(n \geq 3)$

证：注意到 $(abc)(abd) = (ac)(bd)$

于是 A_n 可以由所有3个数的循环生成

我们只要证：任何一个3-循环属于

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

$(2km)(k l m)(2km)^{-1} = (m l 2) = (2ml)$

$(12 \cdot)(2ml)(12 \cdot)^{-1} = ($

$m, l \notin \{1, 2\}$

设 $\sigma=(k\,m\,l)$ $\quad k<m<l$, $k\neq 1, m\neq 2$.

$(1\,2\,k)(1\,2\,m)(1\,2\,k)^{-1}=(2\,k\,m)\in H$

$(2\,k\,m)(2\,k\,l)(2\,k\,m)^{-1}=(k\,m\,l)\in H$ ☒

§3. 环 (Ring)

设集合 R 上有两个运算 +、·，有两个特别的元素 $0,1\in R$

如果 $(R,+,0)$ 是交换群

$(R,\cdot,1)$ 是含幺半群

且 $\forall a,b,c\in R$

$a(b+c)=ab+ac$

$(b+c)a=ba+ca$

则称 R 是环（含幺环）

注：书上要求 $(R,\cdot)$ 是半群时为简单起见，我们只考虑 $(R,\cdot)$ 是含幺半群的情形。

环的等价定义：

设 R 是集合，$0,1\in R$ 且 $0\neq 1$，+、· 是 R 上的两个二元运算

如果 $\forall a,b,c\in R$

(R_1) $a+b=b+a$

$(a+b)+c=a+(b+c)$

$a+0=0+a=a$

$\forall a\in R$，$\exists d\in R$ 使得 $a+d=d+a=0$

(R_2) $(ab)c=a(bc)$

$a\cdot 1=1\cdot a=a$

(R_3) $a(b+c)=ab+ac$

$(b+c)a=ba+ca$

则称 R 是一个环，记为 $(R,+,0,\cdot,1)$