第3章 群

3.1 对称群

1: (1) $\sigma=(1732)(4)(58)(6)=(1732)(58)(4)(6)$ 偶置换. $(4-1)+(2-1)=4$

$\tau=(1354)(2)(687)=(1354)(687)(2)$ 奇置换. $(4-1)+(3-1)=5$

(2) $\sigma^{-1}=(1237)(58)$ 偶置换.

$\tau^{-1}=(1453)(678)$ 奇置换.

$\sigma\tau=(47)(6)(12)(38)$ 奇置换.

$\tau\sigma=(1684)(23)(57)$ 奇置换.

$\sigma\tau\sigma^{-1}=(7284)(603)$ 奇置换

$\tau\sigma\tau^{-1}=(47)(3652)$ 偶置换.

← 映射复合

2. $\sigma=(14235)(1345)=(154)(23)$ 奇置换. $=(14)(15)(23)$

$\sigma^{-1}=(23)^{-1}(154)^{-1}=(23)(145)$ 奇置换. $=(23)(15)(14)$

$=(15)(14)(23)$

3 (1) $\sigma=(147)(789)(392)(356)(39)$

$=(1478956)(23)$ $7-1+2-1=7$ 奇置换.

(2) $\sigma=(1293)(24)(67985)(47)$

$=(1243)(56798)$ $4-1+5-1=7$ 奇置换.

4 $\sigma=(123)(45)$

$\sigma^2=(123)(45)(123)(45)=(132)(4)(5)$

$\sigma^3=\sigma^2\cdot\sigma=(132)(123)(45)=(45)$

$\sigma^4=\sigma^3\cdot\sigma=(45)(123)(45)=(123)$

$\sigma^5=\sigma^4\cdot\sigma=(123)(123)(45)=(132)(45)$

$\sigma^6=\sigma^5\cdot\sigma=(132)(45)(123)(45)=(1)$.

5: (1) 证明：S_n中长为s的轮换为$(a_1 a_2 \cdots a_s)$

故a_1有n种选择，a_2有$n-1$种选择…，a_s有$n-s+1$种选择.

但有s倍的重复（因为轮换）

故有 $\frac{n\cdot(n-1)\cdots(n-s+1)}{s}$ 个s长轮换.

(2) 证明：在S_n $(n\geq 4)$中，形如$(a_1 a_2)(a_3 a_4)$的不相交对换.

有 $\frac{n(n-1)(n-2)(n-3)}{2\cdot 2\cdot 2} = \frac{n(n-1)(n-2)(n-3)}{8}$ 个

□

6: 证明：由 $m_1 \geq m_2 \geq \cdots \geq m_s \geq 1$. $k_1, \cdots, k_s \geq 1$.

$k_1 m_1 + k_2 m_2 + \cdots + k_s m_s = n$.

考虑轮形 $(m_1, \cdots, m_1, m_2, \cdots, m_2, m_s, \cdots, m_s)$的$n$元置换.

这n个位置，随意放数1到n，不能放重复的数，共$n!$个可能.

想在前m_1个位置（第一个轮换）有m_1种方式表示同一个轮换.

同理第二个轮换有m_1种方式表示同一个轮换 ……

故总数中要除以 $(m_1^{k_1} m_2^{k_2} \cdots m_s^{k_s})$.

又前k_1个轮换之间不相交，可以有$k_1!$个排序表示同一个置换.

同理，中间k_2个轮换亦是，等等.

故n元置换的共轭数为 $\frac{n!}{m_1^{k_1} m_2^{k_2} \cdots m_s^{k_s} \cdot (k_1)!(k_2)!\cdots(k_s)!}$

□

7: (1) $\tau^{-1} = (25)(34)$ $\sigma^{-1} = (25)(153)$

$\tau\sigma\tau^{-1} = (25)(34)(135)(25)(25)(34) = (25)(34)(135)(34) = (1425)$

$\sigma\tau\sigma^{-1} = (135)(25)(25)(34)(25)(153) = (135)(34)(25)(153) = (12)(54)$

(2) $\tau\sigma\tau^{-1} = (3152)$

$\sigma\tau\sigma^{-1} = (35)$

(3) $\tau\sigma\tau^{-1} = (2153)$

$\sigma\tau\sigma^{-1} = (153)$

□

8、参考例 3.1.2.

(1) $\sigma=(159)(2)(3)(4)(6)(7)(8)=$

$\alpha_i\sigma\alpha_i^{-1}$

$=(\alpha_i(1)\alpha_i(5)\alpha_i(9))(\alpha_i(2))(\alpha_i(3))(\alpha_i(4))(\alpha_i(6))(\alpha_i(7))(\alpha_i(8))$

$\alpha_1=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&4&2&3&5&8&6&7&9\end{pmatrix}$

$\alpha_2=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&6&7&8&5&2&3&4&9\end{pmatrix}$

(2) $\alpha_1=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&1&5&3&4&9&6&7&8\end{pmatrix}$ $\alpha_2=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&6&7&9&4&1&3&5&8\end{pmatrix}$

(3). $(\alpha_2(1)\alpha_2(2))(\alpha_2(3)\alpha_2(5))$

$(\alpha_2(1)\alpha_2(2))(\alpha_2(3)\alpha_2(5))(\alpha_2(7)\alpha_2(9))(\alpha_2(4))(\alpha_2(6))(\alpha_2(8))$

$\alpha_1=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&4&5&6&1&3&8&7&9\end{pmatrix}$

$\alpha_1=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&4&5&1&6&3&8&7&9\end{pmatrix}$ $\alpha_2=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&4&8&3&9&1&5&7&6\end{pmatrix}$

(4)

$\alpha_1=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&5&2&9&6&4&3&7&8\end{pmatrix}$ $\alpha_2=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&5&2&9&6&8&3&4&7\end{pmatrix}$

9. 都是

$\alpha=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$ $\alpha=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}$ $\alpha=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$

$I=(234)=(342)=(423)$

10: $\alpha=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$, $\alpha=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$, $\alpha=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$.

11: 证明: 由偶置换的定义可知两个偶置换的乘积仍为偶置换，故 A_n 具有封闭性

由 S_n 群，故 A_n 具有结合律，由偶置换的逆元仍为偶置换，故 A_n 中的元具有逆元

单位元 (1) 是偶置换 $(1)\in A_n$

故 A_n 成群

12: 证明：B_n 为 S_n 中全体奇置换组成的集合，则 A_n, B_n 均为有限集.

~~由 $L_{(12)}: \alpha \mapsto (12)\alpha$~~

由 $L_{(12)}: B_n \longrightarrow A_n$

$\alpha \longmapsto (12)\alpha$

显然若 $\alpha \in B_n$ 则 $(12)\alpha$ 为偶置换，即 $(12)\alpha \in A_n$

若 $\alpha_1, \alpha_2 \in B_n$ 且 $\alpha_1 \neq \alpha_2$，则有 $(12)\alpha_1 \neq (12)\alpha_2$，(若否由 $(12)^{-1}(12)\alpha_1 = (12)^{-1}(12)\alpha_2$ $\Rightarrow \alpha_1 = \alpha_2$，矛盾)

故 $L_{(12)}$ 为单射. ~~又由于 A_n, B_n 均为有限集，故 $L_{(12)}$ 为满射~~ (不能使用有限集间)

因此 $L_{(12)}$ 为双射.

此时 $|S_n| = |A_n| + |B_n| = |A_n| + |A_n| = 2|A_n| \Rightarrow |A_n| = \frac{|S_n|}{2}$.

对 $\forall \beta \in A_n$

$(12)^{-1}\beta \in B_n$

$s.t.\ L_{(12)}((12)^{-1}\beta) = (12)(12)^{-1}\beta = \beta \in A_n$

故 $L_{(12)}$ 为满射.

13. $5 = 1+1+1+1+1$

$5 = 2+1+1+1$

$5 = 2+2+1$

$5 = 3+1+1$

$5 = 3+2$

$5 = 4+1$

$5 = 5$

$5! = |S_5| = 120$, $|A_5| = 60$.

[作业例 3.1.4]

3.2 子群、生成子群

1. (1) 证明: $(m\mathbb{Z},+)\leq(\mathbb{Z},+)$ $m\in\mathbb{Z}_{\geq 0}$.

显然 $0\in(m\mathbb{Z},+)$, 故 $(m\mathbb{Z},+)$ 非空

对 $\forall a=mz_1, b=mz_2\in m\mathbb{Z}$, 有 $a+b=m(z_1+z_2)\in m\mathbb{Z}$

$-a=m(-z_1)\in m\mathbb{Z}$, 故 $(m\mathbb{Z},+)\leq(\mathbb{Z},+)$

(2) 证明: $A_n<S_n$ $\because |A_n|<|S_n|$ (当 S_n 中存在奇置换. $n\geq 2$)

显然, 由 A_n 与 S_n 的定义, 有 A_n 成群. $A_n\subseteq S_n$.

且 $A_n\neq S_n$ 故 $A_n<S_n$.

或利用子群判别法.

$\forall a,b\in A_n$. 则 a,b 仍为偶置换, a^{-1} 仍为偶置换

故 $ab\in A_n$, $a^{-1}\in A_n$ 因此 $A_n<S_n$

(3) 证明: 显然有 $K_4\subseteq S_4$, K_4 非空.

由 $(12)(34)\cdot(13)(24)=(14)(23)$ $[(12)(34)]^2=[(13)(24)]^2=[(14)(23)]^2=|$

$(12)(34)\cdot(14)(23)=(13)(24)$

$(13)(24)\cdot(14)(23)=(12)(34)$

故对 $\forall a,b\in K_4$, $ab\in K_4$, $a^{-1}\in K_4$ 故 $K_4<S_4$ $\#K_4=4$

28

2. 证明: 设 S 为 G 的全体有限阶元构成的集合.

因为 $e\in S$ 故 S 非空.

对 $\forall a,b\in S$, 存在 $m,n\in\mathbb{Z}_{>0}$, s.t. $a^m=e$, $a^n=e$.

故有 $(ab)^{mn}=e$ (G 为交换群), $(a^{-1})^m=e$.

$\Rightarrow ab\in S$, $a^{-1}\in S$ 因此 $S\leq G$.

2

3. 证明: 显然 $e\in C_G(g)$ 故 $C_G(g)$ 非空 $C_G(g)\leq G$.

$\forall a,b\in C_G(g)$, $abg=agb=gab$ 故 $ab\in C_G(g)$

$a^{-1}g=a^{-1}gaa^{-1}=a^{-1}aga^{-1}=ga^{-1}$ 故 $a^{-1}\in C_G(g)$

因此 $C_G(g)\leq G$

由对 $\forall a\in Z(G)\Leftrightarrow$ 对 $\forall g\in G$ 有 $ag=ga\Leftrightarrow \forall g\in G$, $a\in C_G(g)\Leftrightarrow a\in\bigcap_{g\in G}C_G(g)$ 得证 ■

③

4: 由 习题 3.1.10, $\sigma=(123)\in S_4$

满足 $\alpha\in S_4$, $\alpha\sigma\alpha^{-1}=\sigma$ 的所有 α 为 (1), (123), (132).

故 $C_{S_4}((123))=\{(1),(132),(123)\}$ □

④

5: 由 G 的中心 $Z(G)$ 的定义. 若 $Z(G)=G$, 则显然有 G 是交换群.

$\Rightarrow$ 若 G 是交换群. 由 $Z(G)\leq G$. 若 $Z(G)<G$. 则存在 $x\in G\setminus Z(G)$

且存在 $g\in G$ 使得 $xg\neq gx$ 但这与 G 是交换群矛盾 故 $Z(G)=G$ □

⑤

6: 证明: 由 $GL(n,K)$ 是全体满秩的 $n\times n$ 实矩阵组成的集合 $(n\geq 2)$.

对矩阵乘法组成的群.

由高代: 与所有 n 阶方阵可交换的矩阵只有数量矩阵.

故 $Z(GL(n,K))=\{kE \mid k\neq 0, k\in K, E$ 是单位矩阵$\}$. □

⑥

7. 证明: 由 H 是 G 的子群. 故有 $H^2\subseteq H$, $H^{-1}\subseteq H$.

由 $H=He=H\{e\}\subseteq HH=H^2$ 故 $H^2=H$

对 $\forall h\in H$, 有 $h^{-1}\in H$ 则 $\forall h=(h^{-1})^{-1}\in H^{-1}$ 故 $H^{-1}=H$ □

⑦

8. 证明: $\Leftarrow$ 若 $H\subseteq K$ 或 $K\subseteq H$. 则显然 $H\cup K\subseteq G$.

$\Rightarrow$ 反证. 若 $H\not\subseteq K$ 或 $K\not\subseteq H$ 均不成立

则存在 $a\in K\setminus H$, $b\in H\setminus K$.

则 $a\cdot b\in H\cup K$. 则 $a\cdot b\in H$ 或 $a\cdot b\in K$.

若 $a\cdot b\in H$ 则 $a\cdot b\cdot b^{-1}\in H\Rightarrow a\in H$ 矛盾

若 $a\cdot b\in K$ 则 $a^{-1}\cdot a\cdot b\in K\Rightarrow b\in K$ 矛盾.

故有 $H\subseteq K$ 或 $K\subseteq H$

再由 H, K 均为 G 的子群.

故有 $H\leq K$ 或 $K\leq H$ □

⑧

9: (1). 由 $\langle M\rangle$ 是包含 M 且由 M 生成的子群. $\langle M\rangle$ 对逆与乘法封闭, $e\in G\langle M\rangle$,
显然有 $T\subseteq\langle M\rangle$.

(2). 显然 T 是 G 的非空子集, 且 T 中任意两个元素的乘积仍属于 T,
T 中元素的逆元仍属于 T. 故 $T\leq G$.

(3). ~~由可知 $T\leq G$~~,
由 T 的定义, 显然有 $M\subseteq T$. 又 T 是 G 的子群. 故 $\langle M\rangle\subseteq T$
由 (1) 知 $\langle M\rangle=T$.

⑨

10: 证明: 由 $S_3=\{(1),(12),(13),(23),(123),(132)\}$

故 $S_3=\langle(12),(123)\rangle$

且 $o(123)=3$ $o(12)=2$ $(12)\cdot(123)(12)^{-1}=(12)(123)(12)$
$=(132)=(123)^{-1}$

由例 3.2.7 得 $S_3\cong D_{2\times3}=D_6$.

⑩

11: 证明: 显然有 $\langle-1\rangle\leq(\mathbb{Z},+)$.

且对 $\forall a\in(\mathbb{Z},+)$ 都有 $a=(-a)\cdot(-1)\in\langle-1\rangle$

故 $\langle-1\rangle=\langle\mathbb{Z},+\rangle$

⑪

12 证明: 由 $a=(a^{-1})^{-1}$ 故 $a\in\langle a^{-1}\rangle$ 因此 $\langle a\rangle\subseteq\langle a^{-1}\rangle$

由 $a^{-1}\in\langle a\rangle$ 故 $\langle a^{-1}\rangle\subseteq\langle a\rangle$

故 $\langle a\rangle=\langle a^{-1}\rangle$

⑫

13: 证明: 由 $G=\langle a,b\rangle$, 且 $ab=ba$.

故显然有 $G=\langle a,b\rangle=\{a^mb^m\mid m,n\in\mathbb{Z}\}$

对 $\forall x=a^{n_1}b^{m_1}$, $y=a^{n_2}b^{m_2}\in G$

故 $xy=a^{n_1}b^{m_1}\cdot a^{n_2}b^{m_2}=a^{n_2}b^{m_2}\cdot a^{n_1}b^{m_1}=yx$

故 G 是交换群

(13)

14: 假设 Q 是循环群. 即 $Q=\langle a\rangle$, $a\in Q$.

由 $\frac{a}{2}\in Q$, 但 $\frac{a}{2}$ 不是 a 的整数倍, 故 $\frac{a}{2}\notin\langle a\rangle$, 矛盾

因此 Q 的加法群不是循环群.

(14)

15: (1) 法①. $\bar{8}$, $\bar{8}+\bar{8}=\bar{5}$, $\bar{3}+\bar{8}=\bar{11}$, ... 至到出现重复

可得 $\langle\bar{8}\rangle=\mathbb{Z}/13\mathbb{Z}$.

法②. 由 $o(\bar{8})=n\le 13$. $n\cdot\bar{8}=\bar{0}\Rightarrow\overline{8n}=\bar{0}=\overline{13}$

得 $13\mid 8n$ 由 $(13,8)=1\Rightarrow 13\mid n$ 故 $n=13$

因此 $\langle\bar{8}\rangle=\mathbb{Z}/13\mathbb{Z}$

(2) $\bar{8}$, $\bar{8}\cdot\bar{8}=\bar{12}$, $\bar{12}\times\bar{8}=\bar{5}$, $\bar{5}\times\bar{8}=\bar{1}$,

故 $\langle\bar{8}\rangle=\{\bar{1},\bar{5},\bar{8},\bar{12}\}$

(15)

16. (1) $\bar{3}+\bar{3}=\bar{0}$ $6\cdot\bar{1}=\bar{0}$

$o(\bar{3})=2$ $o(\bar{1})=6$

(2) $o(\bar{1})=1$, $o(\bar{2})=4$, $o(\bar{3})=2$, $o(\bar{4})=2$

(16)

17. (1) $\sigma=(12345)$ $o(\sigma)=5$

(2) $\sigma=(123)(45)$ $o(\sigma)=2\times3=6$.

(3) $\sigma=(23)(45)$ $o(\sigma)=2$

(17)

18 证明: 由 $A=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ $A^2=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ $A^3=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$

$A^4=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ 故 $o(A)=4$

$B=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$ $B^2=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}\begin{pmatrix}0&1\\-1&-1\end{pmatrix}=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}$ $B^3=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\-1&-1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$

$AB=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\-1&-1\end{pmatrix}=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 故 $(AB)^2=\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&2\\0&1\end{pmatrix}$ ... 归纳

$(AB)^n=\begin{pmatrix}1&n\\0&1\end{pmatrix}$ 故 $o(AB)=\infty$ $(AB)^3=\begin{pmatrix}1&3\\0&1\end{pmatrix}\begin{pmatrix}1&3\\0&1\end{pmatrix}=\begin{pmatrix}1&6\\0&1\end{pmatrix}$

(中)

(18)

19：证明：

(3)：已知：$o(a)=n$，$o(b)=m$，$ab=ba$ $(m,n)=1$ $\Rightarrow o(ab)=mn$.

设 $o(ab)=k$，由 $(ab)^{mn}=a^{mn}b^{mn}=e$ 得 $k\mid mn$ （由第(1)部分）

由 $e=(ab)^{kn}=a^{kn}b^{kn}=b^{kn}$ 故 $m\mid kn$ 由 $(m,n)=1$ $\Rightarrow m\mid k$

同理 $e=(ab)^{km}=a^{km}b^{km}=a^{km}$ 故 $n\mid km$ 由 $(n,m)=1$ $\Rightarrow n\mid k$

由 $(m,n)=1$ 得 $mn\mid k$ 因此 $k=mn$ （m,n,k 均为正整数）。□

(4)：令 $o(ab)=s$.

由 $(ab)^{[m,n]}=(ab)^{\frac{mn}{(m,n)}}=(ab)^{m\cdot\frac{n}{(m,n)}}=a^{\frac{mn}{(m,n)}}=e$

故 $s\mid [m,n]$

由 $(ab)^s=e$ 得 $a^sb^s=e$ （$\because ab=ba$）

由 $a^s\in\langle a\rangle$，$b^s\in\langle b\rangle$，且 $\langle a\rangle\cap\langle b\rangle=\{e\}$

故 $a^s=e$，$b^s=e$ （若不然 e，假设 $a^s\neq e$ 则由 $a^sb^s=e$ 得 $b^s=a^{-s}\in\langle b\rangle$
但 $a^{-s}\in\langle a\rangle$ 故 $b^s\in\langle b\rangle\cap\langle a\rangle$ 故 $b^s=e$
故 $a^s=e$ 矛盾）

故 $m\mid s$，$n\mid s$

因此 $\frac{mn}{(m,n)}\mid s$ 故 $[m,n]\mid s$ 由 $s,[m,n]$ 均为正整数，因此 $s=[m,n]$。□

20：证明：

(1)：由 $\sigma=(a_1a_2\cdots a_L)$ 则 $\sigma^L=(a_1a_2\cdots a_L)^L=e$

且对任意 $1\le m<L$ 有 $\sigma^m(a_1)=a_{m+1}\neq a_1$ 故 $o(\sigma)=L$

(2) 由(1)可得 $o(\sigma_1)=k$，$o(\sigma_2)=L$ 且 $\sigma_1\sigma_2=\sigma_2\sigma_1$，$\langle\sigma_1\rangle\cap\langle\sigma_2\rangle=\{(1)\}$.
由命题 3.2.6(4) 有 $o(\sigma_1\sigma_2)=[k,L]$

(3)、数学归纳法：当 $r=1$ 时 (1) 已证，当 $r=2$ 时 (2) 已证.
假设当 $r=m$ 时成立，现考虑 $r=m+1$ 时.

设 $\sigma=\sigma_1\sigma_2\in G$ σ_1 是 m 个不相交轮换的乘积 σ_2 是 n_{m+1} 长的轮换.

故 $o(\sigma_1)=[n_1,n_2,\cdots,n_m]$，$o(\sigma_2)=n_{m+1}$，由 (2) 得 $o(\sigma)=[o(\sigma_1),o(\sigma_2)]$
$=[n_1,n_2,\cdots,n_{m+1}]$ □(5)

(20) 设 S_6 中4阶元素的轮形为 $(n_1, n_2, \cdots, n_r)$

由20题知 要么 $[n_1, n_2, \cdots, n_r] = 4$

故4阶的轮形为 $(4,2)$, $(4,1,1)$.

再由 习题3.1.6, 轮形为

$$(m_1 \cdots m_1, m_2 \cdots m_2, \cdots m_s \cdots m_s) \quad (k_1 m_1 + \cdots + k_s m_s = n)$$

的 n 元置换的个数为 $\dfrac{n!}{m_1^{k_1} \cdots m_s^{k_s} (k_1)! \cdots (k_s)!}$

故 阶为4的6元素置换的个数为 $\dfrac{6!}{4 \cdot 2!} + \dfrac{6!}{4 \times 2} = 90 + 90 = 180$ □

(21) 设 S_n 中的元素 轮形为 $(n_1, n_2, \cdots, n_r)$

$[n_1, n_2, \cdots, n_r] = 10$ 轮形为 $(5,2)$ 的元素 阶为10,

不存在阶为11, 14的元素

(22)

(23) S_8 中所有6阶元素可能的轮形

$$\begin{cases} [n_1, n_2, \cdots, n_r] = 6 \\ n_1 + n_2 + \cdots + n_r = 8 \end{cases}$$

(6,1,1), (3,2,1,1), (3,2,2). (6,2) □

(24) 解. S_5 中所有的轮的轮形为 (5), (4,1), (3,2), (3,1,1), (2,2,1), (2,1,1,1), (1,1,1,1,1)

故 S_5 中含有 n 阶元素, n 的集合为 $\{1, 2, 3, 4, 5, 6\}$

(25) S_7 中所有可能的轮形为 (7), (6,1), (5,2), (5,1,1) (4,1,1,1), (4,3), (4,2,1)

(3,3,1), (3,2,2), (3,2,1,1,) (3,1,1,1) (2,2,2,1), (2,2,1,1,1)

(2,1,1,1,1) (1,1,1,1,1,1,1)

故 n 的取值为 $\{1, 2, 3, 4, 5, 6, 7, 10, 12\}$ □

证: (1). 证明: 由 $\varphi: G \to H$ 为同构映射, 故 H 中的单位元为 $\varphi(e)$.

对任意正整数 n. $\forall g \in G$, $g^n = e \Leftrightarrow [\varphi(g)]^n = \varphi(g^n) = \varphi(e)$.

因此 $o(g) = o(\varphi(g))$

若 $o(g) = m$, $g^m = e$

$\varphi(g^m) = \varphi(gg\cdots g) = \varphi(e)$

若 $\varphi(g)$ 的阶 $n < m$

$\varphi(g)^n = \varphi(g^n) = \varphi(e)$

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

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

$\varphi(g)^{m-n} = \varphi(e)$

$\varphi(g)$ 的阶 $m-n < n$ 矛盾 $[\varphi(g)]^m = \varphi(g^m) \neq \varphi(e)$

(2). 由 $(\mathbb{Z}_{12}, +)$ 中有 $o(\bar{7}) = o(\bar{5}) = 4$, 但 K_4 中不存在4阶元素, K_4 中只有1, 2阶元素

故 $(\mathbb{Z}_{12}, +) \not\cong K_4$. 由 Q_8 是四元数群, 只有一个阶为2的元素 $-E$, (见P34页)

D_8 中有大于1个的阶为2的元素: a^2, b, ab, a^2b, a^3b. 故 $D_8 \not\cong Q_8$ □ (6)

26 证明：乘法群 R^* 中的有限阶元素为 ± 1，

乘法群 C^* 中的有限阶元素为 $\pm 1, \pm i$

故 R^* 与 C^* 不同构.

$a^4=1$

$(-i)(-i)=-1$

$a^4=1 \Rightarrow (\pm 1)^2$

$\pm$

$a^4=1$ $e^{\frac{2k\pi}{4}}$ $k=0,1,2,3$

$e^{\frac{2\pi}{2}}=-1$

$e^{\pi}=$

27 证明：由 $f_x: G \to G$ $(x \in G)$

$g \mapsto xgx^{-1}$ $\forall g$

对 $\forall g_1, g_2 \in G$，若 $g_1=g_2 \Leftrightarrow xg_1=xg_2 \Leftrightarrow xg_1x^{-1}=xg_2x^{-1}$

故 f_x 是映射，且是单射.

对 $\forall g \in G$，有 $x^{-1}gx \in G$ 使得 $f_x(x^{-1}gx)=x\cdot(x^{-1}gx)x^{-1}=g$

故 f_x 是满射.

且对 $\forall g_1, g_2 \in G$，$f_x(g_1g_2)=xg_1g_2x^{-1}=xg_1x^{-1}xg_2x^{-1}=f_x(g_1)\cdot f_x(g_2)$

故 f_x 保持运算，因此 f_x 是 G 的一个自同构.

28 由题 3.2.26，有 $o(g)=o(xgx^{-1})$ □

29：由 $D_{2n}=\langle a,b\rangle=\{e, a, a^2, \cdots, a^{n-1}, b, ba, ba^2, \cdots, ba^{n-1}\}$

$=\langle a, b \mid a^n=1, b^2=1, bab^{-1}=a^{-1}\rangle$.

(1). 由 a 为逆时针旋转 $\frac{2\pi}{n}$，由元素阶的定义，有 $o(a)=n$.

b 为反射，故 $o(b)=2$.

$\langle a\rangle=\{e, a, a^2, \cdots, a^{n-1}\}$，$\langle b\rangle=\{e, b\}$.

(2) 当 n 为奇数时，D_{2n} $(n\geq 3)$ 中的二阶元素为 $\{b, ba, \cdots, ba^{n-1}\}$ 共 n 个.

由 $bab^{-1}=a^{-1}$ 得 $ba=a^{-1}b \Rightarrow aba=b$.

对 $\forall ba^i$ $(i\leq n-1)$ 有 $(ba^i)^2=ba^iba^i=ba^{i-1}ba^{n-1}=\cdots=b^2=e$

当 n 是偶数时，D_{2n} $(n\geq 3)$ 中的二阶元素为 $\{b, ba, \cdots, ba^{n-1}, a^{\frac{n}{2}}\}$ 共 $n+1$ 个.

(3)：由 $D_{2n}=\langle a,b\rangle$ 故显然有 $\langle b, ba^{n-1}\rangle \subseteq \langle a,b\rangle = D_{2n}$.

对 $\forall b, ba^{n-1} \in \langle b, ba^{n-1}\rangle$ 故 $b^{-1}\cdot ba^{n-1}=a^{n-1} \in \langle b, ba^{n-1}\rangle$

故 $(a^{n-1})^2=a^{n-2} \in \langle b, ba^{n-1}\rangle$ $a^1=e$

故 $a^{n-3}, \cdots, a \in \langle b, ba^{n-1}\rangle$ 故 $\langle a,b\rangle \subseteq \langle b, ba^{n-1}\rangle$

因此 $D_{2n}=\langle b, ba^{n-1}\rangle$

□

30: (1) 证明: 由 $a \in G$ $o(a)=n$

故 $a^n = e$ 两边同时乘 a^{-1} 得 $a^{n-1} = a^{-1}$

(2) 证明: $\Rightarrow$ 由 $H \leq G$, 显然有 $H^2 \subseteq H$.

$\Leftarrow$ 由 $H^2 \subseteq H$. 故 H 中的元素对乘法满足封闭性.

且 $e \in H^2 \subseteq H$, H 非空.

由 $|H|$ 是有限数, 故对 $\forall a \in H$, $o(a) = n < \infty$

(元素的阶整除群的阶)

故 $a^{n-1} = a^2 \cdot a^2 \cdots a^2 \cdot a^* = a^{-1} \in H$ $(*=2或1)$ 由(1). 单元 $\in H$

故 $H \leq G$

31: 由 $K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$

$(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

定义映射 $\varphi: (\mathbb{Z}/8\mathbb{Z})^* \longrightarrow K_4$

$\bar{1} \longmapsto (1)$

$\bar{3} \longmapsto (12)(34)$

$\bar{5} \longmapsto (13)(24)$

$\bar{7} \longmapsto (14)(23)$

可验证 φ 是保持运算的双射, 故 $(\mathbb{Z}/8\mathbb{Z})^* \cong K_4$

32: $\mathbb{Z}/m\mathbb{Z} = \langle \bar{1} \rangle$ 由命题 3.2.8.

$\mathbb{Z}/m\mathbb{Z}$ 有 $\varphi(m)$ 个生成元 $\{\bar{a} \mid 1 \leq a \leq m-1, (a,m)=1\}$

33: 由 $(r,n)=d$, 故存在 $s,t \in \mathbb{Z}$, 使得 $sr+tn=d$

由 $a^r \in \langle a^r \rangle \Rightarrow a^{rs} \in \langle a^r \rangle$ 又由 $a^{tn} = e$ 故 $a^{rs} \cdot a^{tn} = a^d \in \langle a^r \rangle$

($a^{rs} \in \langle a^r \rangle$, $a^{tn} \in \langle a^r \rangle$)

故 $\langle a^d \rangle \subseteq \langle a^r \rangle$

又由于 $a^r = a^{d \cdot \frac{r}{d}} \in \langle a^d \rangle$ $\left(\frac{r}{d} \in \mathbb{Z}\right)$ 故 $\langle a^r \rangle \subseteq \langle a^d \rangle$

因此 $\langle a^r \rangle = \langle a^d \rangle$

34: (1) 由定理3.2.3, 循环群的子群仍为循环群.

且存在 $d \in \mathbb{Z}_{\geq 0}$, 使得 $H = \langle a^d \rangle$. 注 $H \neq (e)$

若 H 不是无穷阶的, 则存在正整数 n, 使得 $(a^d)^n = e$, $a^{dn} = e$.

与 $O(a) = \infty$ 矛盾. 故除掉平凡子群外都是无穷阶的

(2): 由命题3.2.8 若 $|G| = m$, 则 G 有 $\varphi(m)$ 个生成元 $\{a^r \mid 1 \leq r \leq m-1, (r, m) = 1\}$.

由定理3.2.3 循环群 G 的子群 H 一定形如 $H = \langle a^t \mid t \in \mathbb{Z}_{\geq 0} \rangle$

设 $\langle t, m \rangle = d$ 则 $1 \leq d \leq m$.

由习题3.2.33 有 $\langle a^t \rangle = \langle a^d \rangle$, $1 \leq d \leq m$.

对若 $(d, m) = 1$. 则由命题3.2.8(上面) $\langle a^d \rangle = G = \langle a^1 \rangle$

故 G 的全部子群为 $\{\langle a^d \rangle \mid d \mid m, 1 \leq d \leq m\}$

显然有 $\langle a^d \rangle = \{a^d, a^{2d}, \cdots, a^{(\frac{m}{d}-1)d}, a^{\frac{m}{d} \cdot d} = e\}$

即 $|\langle a^d \rangle| = \frac{m}{d}$

□

35: 由 $\mathbb{Z}/m\mathbb{Z} = \langle \bar{1} \rangle$, $|\mathbb{Z}/m\mathbb{Z}| = m$

由习题3.2.34得. $\mathbb{Z}/m\mathbb{Z}$ 的全部子群为 $\{\langle \bar{d} \rangle \mid d \mid m, 1 \leq d \leq m\}$

□

36

37

3.3 陪集、拉格朗日定理

1. 类似引理3.3.1

证明：(1). $a = ea \in Ha$

(2). 若 $Ha = H$，则 $ea = a$ $a = ea \in Ha = H$.

反之若 $a \in H$，因为 $H \leq G$，则 $Ha \subseteq H \cdot H = H$

由于 $a^{-1} \in H$ 所以 $Ha^{-1} \subseteq H$ 两边右乘 a，得 $H \subseteq Ha$ 故 $Ha = H$.

(3). $Ha = Hb \Leftrightarrow$ ~~$Haa^{-1} = Hba^{-1}$~~

$\Leftrightarrow Hab^{-1} = Hbb^{-1} \Leftrightarrow H = Hab^{-1}$

$\Leftrightarrow ab^{-1} \in H$

$\Leftrightarrow ab^{-1} \cdot b \in Hb \Leftrightarrow a \in Hb$ □

2. 证明：$a + 3\mathbb{Z} = b + 3\mathbb{Z} \Leftrightarrow a - b \in 3\mathbb{Z}$. ∵ $a + 3\mathbb{Z} = 3\mathbb{Z} + a$. $\forall a \in \mathbb{Z}$

所有加法陪集 $0 + 3\mathbb{Z}$，$1 + 3\mathbb{Z}$，$2 + 3\mathbb{Z}$

3. 证明：(1) well defined + 单射

$a_1H = a_2H \Leftrightarrow a_2^{-1}a_1 \in H$

$\Leftrightarrow Ha_2^{-1}a_1 = H$

$\Leftrightarrow Ha_2^{-1} = Ha_1^{-1}$

{ 良定义：原像相同 $\Rightarrow$ 像相同
  单射： $\Leftarrow$

(2) 满射：显然，对 $\forall Hb$，存在 $b^{-1} \in G$，使得 $\rho(b^{-1}H) = Hb$

得证

4. 证明 由拉格朗日定理及推论3.3.1.

对任意 $a \in G$ $o(a) \mid |G| = n$ 若 $o(a) = m$

即 $m \mid n$，$a^m = e$ 故 $a^n = a^{m \cdot \frac{n}{m}} = e$ □

5. 证明：群 $(\mathbb{Z}/p\mathbb{Z})^\times$ 乘法群 $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, 3, \cdots, p-1\}$ (因为 p 是素数)

(因为 $\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times$，$(a, p) = 1$. 由 c.d.s.t. $ac + dp = 1$

$a^{-1} = c \mod p$)

对 $\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times$，$1 \leq a \leq p-1$，$(a, p) = 1$

设 $o(a) = m$ 故由拉格朗日定理 $o(a) = m \mid p-1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$

故 $a^{p-1} \equiv a^{m \cdot \frac{p-1}{m}} \equiv 1^{\frac{p-1}{m}} \equiv 1 \mod p$ $\Rightarrow$ 费马 ①

⇒集.

现对任与p互素的整数a. 做代除法且 $1 \le r \le p-1$.

有 $a = q \cdot p + r$ $\quad 1 \le r \le p-1$ $\quad (a, p) = 1 \Rightarrow (r, p) = 1$

故 $a^{p-1} \equiv (q \cdot p + r)^{p-1} \equiv \sum_{i=0}^{p-1} \binom{p-1}{i} \cdot [q \cdot p]^i \cdot r^{p-1-i} \mod p$

$\equiv r^{p-1} \quad (\text{当 } i=0) \mod p$

由上述讨论有 $a^{p-1} \equiv r^{p-1} \equiv 1 \mod p$

$(1 \le r \le p-1)$

6. 证明: 在 $G_1 \cap G_2$ 中任一个元素 a, 则 $o(a) \mid |G_1|$ 且 $o(a) \mid |G_2|$

由 $(|G_1|, |G_1|) = 1$, 故 $o(a) = 1$ 因此 $a = e$.

故 $G_1 \cap G_2 = \{e\}$

7. 证明: 若 $G \neq \{e\}$ 设 G 无非平凡子群.

对 $\forall a \in G$, $a \neq e$, 则 $\langle a \rangle \le G$ 故 $\langle a \rangle = G$

因此 G 为循环群. (只有两类)

若 $o(a) = \infty$, 则 $G \cong \mathbb{Z}$, 但在 $(\mathbb{Z}, +)$ 中, $n\mathbb{Z} \le G$, 矛盾

若 $o(a) = p$. 则 $G \cong \mathbb{Z}_p$ (有限群)

设 $\mathbb{Z}_p$ 的循环子群为 $\langle b \rangle$ $b \in \mathbb{Z}_p$ 而 $\mathbb{Z}_p$ 无非平凡循环子群.

故 $\mathbb{Z}_p = \langle b \rangle$ 故 $(b, p) = 1$ 对 $\forall 1 \le b \le p-1$ 因此 p 是素数.

故 G 是素数阶循环群

8. 证明: 设 $H \le S_3$, 由拉格朗日定理 $|H| \mid |S_3| = 3! = 6$

故 $|H|$ 可能的值为 1, 2, 3, 6. 若 $|H| = 1$ 则 $H = \{e\}$

若 $|H| = 6$ 则 $H = S_3$

若 $|H| = 2$. 则 $H = \langle (12) \rangle$, $\langle (13) \rangle$, $\langle (23) \rangle$

若 $|H| = 3$ 则 $H = \langle (123) \rangle = \langle (132) \rangle = A_3$ (交错群)

注: $S_3 = \{(1), (12), (13), (23), (123), (132)\}$

9: 证明: 由 $|S_4|=4!=24 \Rightarrow |A_4|=\frac{24}{2}=12$.

设 $H\leq A_4$. 则由拉格朗日定理 $|H|\mid|A_4|$.

$|H|$可能的值为 1, 2, 3, 4, 6, 12. (A_4没有6阶子群)

若$|H|=1$, 则 $H=\{e\}$ 若$|H|=12$, 则 $H=A_4$.

若$|H|=2$ 则 $H=\{\langle(12)(34)\rangle;\langle(13)(24)\rangle;\langle(14)(23)\rangle$

若$|H|=3$ 则 $H=\langle(123)\rangle;\langle(124)\rangle;\langle(134)\rangle;\langle(234)\rangle$

若$|H|=4$ 则 $H=V_4=\{(1),(12)(34),(14)(23),(13)(24)\}$.

□

注: $A_4=\{(1),(12)(34),(14)(23),(13)(24),(123),(132),(124),(142),(134),(143),(234),(243)\}$.

10: 证明: 由习题3.37: 除平凡子群外无其他真子群的非平凡群本为素数阶循环群.

故由 $|G|=2p$ p是素数 设 $H\leq G$ $H\neq e$, G.

则 $|H|$可能的值为 2, p.

若$|H|=p$, 则结论成立.

若$|H|=2$, 则 H为对换群.

证明: 设 $e\neq a\in G$. 若 $o(a)=2p$, 则 G为$2p$阶循环群

则取 $H=\langle a^2\rangle$, 则 H是G的一个p阶子群.

若 $o(a)=p$ 则 $H=\langle a\rangle$ 是G的一个p阶子群.

若{G中不含有p阶元素 / 且不含有2阶元素} 则由拉格朗日定理

对$\forall e\neq a\in G$, 有 $o(a)\mid 2p$ 且 $o(a)=2$.

则对$\forall a,b\in G$, $a^2=e$, $b^2=e$, $(ab)^2=e$

则 $H=\langle a,b\rangle=\{e,a,b,ab\}$ 是一个4阶子群. 但 $4\nmid 2p$ (p为奇素数)

(或者) 则 G中存在一个p阶子群

□

11: 由 $H=\langle(1234)\rangle \leq S_4$ $S_3 \leq S_4$ 故有 $S_3H \subseteq S_4$

且 $\#H=|H|=4$ $|S_3|=3!=6$

由 $H \cap S_3=\{e\}$ ($\because S_3$ 是固定数字4的子群)

故由定理3.3.4 有 $|S_3H|=\frac{|S_3|\cdot|H|}{|S_3\cap H|}=4\cdot 6=24$

又 $\because |S_4|=4!=24$ $S_3H \subseteq S_4$

因此 $S_4=S_3H$

□

12: 证明:

(1) 15阶群中至多有一个5阶子群. (证明与例3.3.3类似)

若不然, 设 $H_1 \leq G$, $H_2 \leq G$ 为两个5阶子群. 且 $H_1 \neq H_2$.

则由 $H_1 \cap H_2 \leq G$ 有 $|H_1 \cap H_2| \mid 5$ 故有 $|H_1 \cap H_2|=1$.

($H_1 \neq H_2$)

由 $|H_1H_2|=\frac{|H_1|\cdot|H_2|}{|H_1\cap H_2|}=25>|G|$ ($=15$), 但 $H_1H_2 \leq G$ 矛盾.

因此 G 至多有一个5阶子群

(2) 对 $\forall a \in G$, 若则 $o(a)=1, 3, 5, 15$.

若 $a \neq e$, 则当 $o(a)=5$ 时 有 $o(a^3)=\frac{15}{(3,15)}=5$

若 $o(a)=3$ 时 则 a 即为一个3阶元素.

若 $o(a)=5$ 时 则 $|\langle a\rangle|=5$. 则任取一个 $G\setminus\langle a\rangle$ 中的元素 $b \neq e$.

由(1) G 中至多有一个5阶子群, 故 $o(b)=3$ 或 15. 此时 G 中必有3阶元素.

□

13: 证明: 自反性: $a \sim a$ (因为 $a=a\cdot e$, $e \in H$)

对称性: 若 $a \sim b$ 则 $\exists h \in H$ 有 $a=bh$ 则 $ah^{-1}=b$ 即 $b \sim a$.

传递性: 若 $a \sim b$, $b \sim c$ 则 $\exists h_1 \in H$, $h_2 \in H$ 有 $a=bh_1$, $b=ch_2$ 则 $a=ch_2h_1$

故 $a \sim c$

因此 "$\sim$" 为等价关系.

且 a 所在等价类为 $\bar{a}=\{b \mid \exists h \in H, 使得 a=bh\}$

$=\{b \mid 对 \forall h \in H, s.t.\ ah^{-1}=b\}$

$=\{ah \mid 对 h \in H\}=aH$

□ (4)

12(续). 对 pq 阶群，p, q $(p<q)$ 为素数.

则 G 有 p 阶元素，且至多有一个 q 阶子群.

证明：① 至多有一个 q 阶子群.

若不然存在两个 H_1, H_2 则 $|H_1 \cdot H_2| = q^2 > pq$ 矛盾.

$(H_1 H_2 \subseteq G, |G| = pq)$. □

② 对 $\forall a \neq e, a \in G$ 设 $o(a)$ 可能取值 p, q, pq.

若 ⟨1⟩ $o(a) = pq$ 则 $o(a^q) = p$

⟨2⟩ $o(a) = p$ 则结论成立.

⟨3⟩ 若 $o(a) = q$. 则任取 $b \in G \setminus \langle a \rangle$, $b \neq e$.

故 $o(b) = pq$ 或 p 由 ⟨1⟩, ⟨2⟩ 都结论成立. □

3.4 正规子群与商群

1. 共轭关系：$a \sim b \Leftrightarrow a$与$b$在$G$中共轭 $\Leftrightarrow \exists g \in G$, s.t. $a = gbg^{-1}$

(1) 自反性：$a \sim a$ ($\because a = eae^{-1}$)

(2) 对称性：$a \sim b$ 则 $\exists g \in G$. s.t $a = gbg^{-1}$ 故 $b = g^{-1}a(g^{-1})^{-1}$

由 $g^{-1} \in G$ 故 $b \sim a$.

(3) 传递性：$a \sim b$, $b \sim c$ 则 $\exists g_1, g_2 \in G$. s.t. $a = g_1 b g_1^{-1}$, $b = g_2 c g_2^{-1}$

故 $a = g_1 b g_1^{-1} = g_1 g_2 c g_2^{-1} g_1^{-1} = g_1 g_2 c (g_1 g_2)^{-1}$

故 $a \sim c$

因此共轭关系是等价关系.

2. 证明：$\Rightarrow$ 若 $C(a) = \{a\}$, 则 对任意的 $g \in G$. 都有 $gag^{-1} = a$.

即 $ga = ag$, 因此 $a \in Z(G)$.

$\Leftarrow$ 若 $a \in Z(G)$. 则 对 $\forall g \in G$, 都有 $ag = ga$ 即 $gag^{-1} = a$.

因此 $C(a) = [a]$

3. 证明. 设 $o(ab) = m$, $o(ba) = n$ 则 $(ab)^m = (ab)^{m+1} \cdot ab = e$

故 $(ab)^{m+1} = b^{-1}a^{-1}$ 因此 $(ba)^m = b(ab)^{m+1} \cdot a$

$= bb^{-1}a^{-1}a = e$

因此 $n \mid m$, 同理有 $m \mid n$ (m, n 均为正整数)

故 $m = n$

4. 证明：① 子群：(1) 封闭性：对 $\forall ah_1a^{-1}, ah_2a^{-1} \in aHa^{-1}$.

有 $ah_1a^{-1} \cdot ah_2a^{-1} = ah_1h_2a^{-1} \in aHa^{-1}$

(2) 逆元 $\in aHa^{-1}$. 对 $\forall aha^{-1}$ 有 $(aha^{-1})^{-1} = ah^{-1}a \in aHa^{-1}$

② 同构：定义 $\varphi: H \longrightarrow aHa^{-1}$

$h \longmapsto aha^{-1}$

① $h_1 = h_2 \Leftrightarrow ah_1 = ah_2 \Leftrightarrow ah_1a^{-1} = ah_2a^{-1}$ 故 φ 定义合理且为单射.

② 对 $\forall b \in aHa^{-1}$ 则 $\exists$ 唯一 $h \in H$ 有 $b = aha^{-1}$ 故 $\varphi(h) = b$ ∴ φ 为满射.

③ 保持运算 $\varphi(h_1h_2) = ah_1h_2a^{-1} = ah_1a^{-1} \cdot ah_2a^{-1} = \varphi(h_1)\varphi(h_2)$ 故 φ 是同构映射. □

(续) 由 φ 是同构映射，故有 $|aHa^{-1}|=H$

5. 证明：对 $\forall g\in G$ 构造集合 $H(g)=\{ghg^{-1}\mid h\in H\}$

则由 $\forall ghg^{-1}\cdot gh_2g^{-1}=gh_1h_2g^{-1}\in H(g)$

取 $ghg^{-1}, gh_2g^{-1}\in H(g)$ 则

$\Leftrightarrow$ 由 $ghg^{-1}\in H(g)$ $(ghg^{-1})^{-1}=gh^{-1}g\in H(g)$

故 $H(g)\leq G$ 是 G 的子群 $\#H(g)=n$ ($ghg^{-1}=gh_2g^{-1}\Leftrightarrow h_1=h_2$ 消去律)

由 G 只有一个 n 阶子群，故 $H(g)=H$.

故对 $\forall ghg^{-1}\in H(g)$ 有 $ghg^{-1}\in H$

由命题 3.4.2 得 $H\trianglelefteq G$.

6. 证明：由 $K\trianglelefteq G$ 则对 $\forall a\in G$ 有 $aka^{-1}\in K$ $\forall k\in K$ (命题 3.4.2)

故对 $\forall b\in H\subseteq G$ 有 $bkb^{-1}\in K$ 因此 $K\trianglelefteq H$.

7. 证明：由 $H_1\trianglelefteq G$, $H_2\trianglelefteq G$

显然有 $H_1\cdot H_2\leq G$.

对 $\forall g\in G$ 有 $gH_1g^{-1}=H_1$ $gH_2g^{-1}=H_2$.

故 $(gH_1g^{-1})(gH_2g^{-1})=gH_1H_2g^{-1}=H_1H_2$ 故 $H_1H_2\trianglelefteq G$.

8. 证明：由 $Z(G)=\{x\in G\mid xg=gx\mid \forall g\in G\}\leq G$

对 $\forall h\in H$, 对 $\forall g\in G$ 由 $h\in H\leq Z(G)$

有 $hg=gh$ 故 $ghg^{-1}=h\in H$

故 $H\trianglelefteq G$

9: 证明: 对任意的 $a, b \in G$

由 $G/Z(G)$ 是循环群. 设 $G/Z(G) = \langle x \rangle$

故 $\bar{a} = x^{n_1}$ $\bar{b} = x^{n_2}$ $G \langle x \rangle$

$\in \langle x \rangle$

故 ~~$a = x^{n_1}$~~ 存在 $m_1, m_2 \in Z(G)$

使得 $a = x^{n_1} \cdot m_1$ $b = x^{n_2} \cdot m_2$

因此 $a \cdot b = x^{n_1} \cdot m_1 \cdot x^{n_2} m_2 = x^{n_1+n_2} \cdot m_1 m_2 = x^{n_2} \cdot m_2 \cdot x^{n_1} \cdot m_1 = b \cdot a$. ∎

10: 证明: 由 $|K| = 2$, 设 $K = \{e, a\}$

由 $K \trianglelefteq G$, 则对 $\forall b \in G$ 有 $bK = Kb$.

故 $\{eb, ba\} = \{eb, ab\}$ $\Rightarrow ab = ba$.

由 $e \in Z(G)$ (显然) 且 $a \in Z(G)$ [$ab = ba$, 对 $\forall b \in G$]

故 $K \leq Z(G)$ ∎

[二阶正规子群并不全在中心]

11: 证明: S_3 的正规子群: $\{(1)\}$, A_3, S_3.

(1) 共轭 σ 与 τ 在 S_n 中共轭, $\Leftrightarrow$ σ 与 τ 的轮形相等.

(2) $H \trianglelefteq G$, $\Leftrightarrow$ H 一定由 G 的若干完整的共轭类组成

S_3 中元素可能的轮形有 $(1,1,1)$, $(2,1)$, (3).

(3) → $C((123)) = \{(123), (132)\}$

$(2,1)$ → 共轭类 $C((2,1)) = \{(12), (13), (23)\}$

$(1,1,1)$ → 共轭类 $C((1)) = \{(1)\}$

$|S_3| = 6$. 设 S_3 的正规子群为 H. 则 $|H| \mid 6$ $\Rightarrow$ $|H|$ 可能为 $1, 2, 3, 6$.

由 H 由若干共轭类组成 故 $C(1)$, $C(1) \cup C(123)$, $C(1) \cup C(123) \cup C(12)$.

即: $\{(1)\}$, A_3, S_3 为 S_3 的所有正规子群

S_4 的正规子群: $\{(1)\}$, K_4, A_4, S_4.

(续): S_4 中元素可能的轮形 (1,1,1,1)、(2,1,1)、(2,2)、(3,1)、(4).

共5个共轭类:

① $C((1)) = \{(1)\}$

② $C((12)) = \{(12), (13), (14), (23), (24), (34)\}$

③ $C((12)(34)) = \{(12)(34), (13)(24), (14)(23)\}$

④ $C((123)) = \{(123), (132), (124), (142), (134), (143), (234), (243)\}$

⑤ $C((1234)) = \{(1234), (1243), (1324), (1342), (1423), (1432)\}$

$|S_4| = 4! = 24$, $|H| \mid 24$ $|H|$ 可能为 1, 2, 3, 4, 6, 8, 12, 24.

故 S_4 的A正规子群可能为

①, ①④, ①③④, ①②③④⑤

$\{(1)\}$, K_4, A_4, S_4

12: 证明: 对任给的 $g_1H, g_2H \in G/H$, $g_1, g_2 \in G$.

则 $g_1H \cdot g_2H = g_1g_2H = g_2g_1H = g_2H \cdot g_1H$

故 G/H 是交换群

13. 证明:

$|A_4| = 12$, $A_4 = \{(1), (12)(34), (13)(24), (14)(23),$
$(123), (132), (124), (142), (134), (143), (234), (243)\}$

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

$A_4/K_4 = \{\overline{(1)}, \overline{(123)}, \overline{(132)}\}$ 满足交换律, 得证

14. 证明: $\forall a, b \in H$, $ab \in H$, $a^{-1} \in H$. (H 非空) $\Rightarrow H \leq S_4$.

	(1)	(12)	(34)	(12)(34)
(1)	(1)	(12)	(34)	(12)(34)
(12)	(12)	(1)	(12)(34)	(34)
(34)	(34)	(12)(34)	(1)	(12)
(12)(34)	(12)(34)	(34)	(12)	(1)

考虑 K_4 的A运算与右表对应关系.

$\varphi: H \to K$

$(1) \mapsto (1)$

$(12) \mapsto (12)(34)$

$(34) \mapsto (13)(24)$

$(12)(34) \mapsto (14)(23)$

显然 φ 是双射

且对 $\forall a, b \in H$ 有

$\varphi(a)\varphi(b) = \varphi(ab)$ 故 $H \cong K_4$

但 $H \not\trianglelefteq S_4$. 例: $(123)(12) = (23)(123)$ $(23)(12)(123)^{-1} = (28)$

15: 证明: $m\mathbb{Z} \cong \mathbb{Z}$.

定义 $\varphi: \mathbb{Z} \to m\mathbb{Z}$

$k \mapsto mk \quad \forall k \in \mathbb{Z}$.

则 φ 是双射, 且保持运算 (见例 2.1.9).

同理 $n\mathbb{Z} \cong \mathbb{Z}$, $m\mathbb{Z} \cong n\mathbb{Z} \cong \mathbb{Z}$.

~~由 $|\mathbb{Z}/m\mathbb{Z}| = m \neq n = |\mathbb{Z}/n\mathbb{Z}|$ 故 $\mathbb{Z}/m\mathbb{Z}$~~

由 $|\mathbb{Z}/m\mathbb{Z}| = m \neq n = |\mathbb{Z}/n\mathbb{Z}|$ 故 $\mathbb{Z}/m\mathbb{Z} \not\cong \mathbb{Z}/n\mathbb{Z}$ □

16: 证明: 由 p, q 均为素数.

故 G 中唯一的 p 阶子群和 q 阶子群 均为循环群. 设为 ~~$\langle x \rangle$~~

$\langle x \rangle$, $\langle y \rangle$ ~~$(x^p = 1, y^q = 1)$~~ $o(x) = p$ $o(y) = q$

且 $y \notin \langle x \rangle$ $x \notin \langle y \rangle$.

由 ~~B~~ 则 $\langle xy \rangle \leq G$.

由拉格朗日定理 (子群的阶整除群的阶)

故 G 的子群最多为 $\{e\}$, $\langle x \rangle$, $\langle y \rangle$, G.

若 $\langle xy \rangle = \{e\}$, 则 由 $xy = e$ $x = y^{-1}$, 矛盾 ($o(x) \neq o(y)$) ($y = x^{-1} \in \langle x \rangle$)

若 $\langle xy \rangle = \langle x \rangle$ 则 $xy \in \langle x \rangle$ 设 $xy = x^n$ $y = x^{n-1} \in \langle x \rangle$ 矛盾 对某个 n

同理 $\langle xy \rangle \neq \langle y \rangle$

故 $\langle xy \rangle = G$ 因此 G 是循环群 □

3.5. 同态、同态基本定理.

1. $\langle a\rangle = \{a, a^2, a^3, e\}$

故 $o(a)=4$

K_4 中所有非单位元的阶均为 2. 故 $K_4 \not\cong \langle a\rangle$.

4阶群的所有同构型：K_4 与 4阶循环群

由元素的阶整除群的阶（拉格朗日定理）

对任意 $a\in G$，则 $o(a)=1, 2, 4$.　　$\#G=4$

若 G 中含有4阶元素. 则 $G \cong$ 4阶循环群.

若 G 中不含4阶元素 则 $o(a)=2, 1$. 此时 $G\cong K_4$.

2. (1). $\varphi: (\mathbb{Z},+) \longrightarrow (\mathbb{Z},+)$

$n \longmapsto 2n$

$\varphi(n_1+n_2) = 2(n_1+n_2) = 2n_1+2n_2 = \varphi(n_1)+\varphi(n_2)$

但对 $n_1\neq n_2$ 显然 $\varphi(n_1)=2n_1\neq 2n_2=\varphi(n_2)$ 故 φ 是单同态

但 φ 不是满射，例 $5\in(\mathbb{Z},+)$ 但不存在原像.

$\ker\varphi = \{0\}$

□

(2). $\varphi: GL(2,K) \longrightarrow K^*$

$A=\begin{pmatrix}a&b\\c&d\end{pmatrix} \longmapsto ad-bc$.　　设 $A_1=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ $A_2=\begin{pmatrix}x&y\\z&w\end{pmatrix}$

$\varphi(A_1A_2) = \varphi\begin{pmatrix}ax+bz & ay+bw\\ cx+dz & cy+dw\end{pmatrix}$　　$A_1A_2=\begin{pmatrix}ax+bz & ay+bw\\ cx+dz & cy+dw\end{pmatrix}$

$= (ax+bz)(cy+dw)-(cx+dz)(ay+bw)$

$= axcy+axdw+bzcy+bzdw-acxy-bcxw-dzay-dzbw$

$= (ad-bc)(xw-zy) = \varphi(A_1)\varphi(A_2)$

由 $A_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\varphi(A_1)=1$　　$A_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\varphi(A_2)=1$. 但 $A_1\neq A_2$

故 φ 不是单同态

对 $\forall\, m\in(K^*,\times)$ 则 $\exists A=\begin{pmatrix}m&0\\0&1\end{pmatrix}$ $\varphi(A)=m$ 故 φ 是满同态 ■

$\ker\varphi = \{A \in GL(2,R) \mid ad-bc=1\}$

$= SL(2,R)$ 全体行列式等于1的2×2实矩阵组成的集合. □

(3) $\pi: G \to G/H = \bar{G}$

$a \mapsto aH = \bar{a}$

$\pi(a_1a_2) = \overline{a_1a_2} = \overline{a_1}\,\overline{a_2} = \overline{a_2}\,\overline{a_1} = \bar{a}_2\cdot\bar{a}_1 =$

$= \overline{a_1a_2} = \bar{a}_1\cdot\bar{a}_2 = \pi(a_1)\cdot\pi(a_2)$

且显然不是满的.

故不是满的群同态.

且 $\pi(a) = \bar{e} = H \Leftrightarrow a \in H$. $\ker\pi = H$ □

3. 证明:

(必) 对 $\forall a,b \in G$,

$\varphi(a)=\varphi(b) \Leftrightarrow \varphi(a)\varphi(b)^{-1}=e \Leftrightarrow \varphi(ab^{-1})=e \Leftrightarrow ab^{-1}\in H \Leftrightarrow b \in aH$.

$\varphi(a)=\varphi(b) \Leftrightarrow \varphi(b)^{-1}\varphi(a)=e \Leftrightarrow \varphi(b^{-1}a)=e \Leftrightarrow b^{-1}a\in H \Leftrightarrow b\in aH$ □

4. (1) 证明: $\forall \sigma_1\ \sigma_2 \in G$

若 $\sigma_1\ \sigma_2$ 同为偶置换/奇置换. 则 $sgn(\sigma_1\sigma_2) = 1 = sgn(\sigma_1)\,sgn(\sigma_2)$

若 $\sigma_1\ \sigma_2$ 一偶一奇 则 $sgn(\sigma_1\sigma_2) = -1 = sgn(\sigma_1)\cdot sgn(\sigma_2)$

故 sgn 为 $G \to \{1,-1\}$ 的同态 □

(2) $\ker sgn$ 为 G 中所有偶置换组成的集合.

由同态基本定理 $G/\ker sgn \cong \{1,-1\}$

故 $|G/\ker sgn| = 2 = \dfrac{|G|}{|\ker sgn|}$. 由(2) 知 $\ker sgn$ 为 G 中所有偶置换组成的集合.

故 G 中奇置换与偶置换各占一半 □

S_n 中有奇置换

5: (1) 由 $\varphi: G \to G_1$　　$G \cong G_1$

对 $\forall a_1, b_1 \in \varphi(H)$，由 φ 是同构映射，则存在 $a, b \in H$，使得

$a_1 = \varphi(a)$，$b_1 = \varphi(b)$　且 $ab^{-1} \in H$

故 $a_1 \cdot b_1^{-1} = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(ab^{-1}) \in \varphi(H)$

故 $\varphi(H) \leq G_1$

且由 φ 限制到 H 上有 $H \cong \varphi(H)$，或定义 $\psi = \varphi|_H : H \to \varphi(H)$

$a \mapsto \varphi(a)$

是你指定的双射.

(2) 若 $H \trianglelefteq G$，由上面知 $\varphi(H) \leq G_1$

对 $\forall c_1 \in G_1$ 又因 φ 满，$\exists c \in G$，使得 $\varphi(c) = c_1$

故 $G_1 \cdot \varphi(H) = \varphi(c) \cdot \varphi(H) = \varphi(cH) = \varphi(Hc) = \varphi(H)\varphi(c) = \varphi(H)c_1$

故 $\varphi(H) \trianglelefteq G_1$

(2). 记 S 为 G 的子群集合，S_1 为 G_1 的子群集合

定义 $\psi: S \to S_1$

$H \mapsto \varphi(H)$　由 $H \in S$ 则 $\varphi(H) \in S_1$，故 ψ 为映射

由(1)的讨论，若 $H_1 \neq H_2$ 则由 φ 是群同构映射 故 $\varphi(H_1) \neq \varphi(H_2)$

对任意 $M \in S_1$ 则 $\varphi^{-1}(M) \in S$，由 φ 是 $G \to G_1$ 的群同构，

故 $\varphi^{-1}(M)$ 是 G 的一个子群，故 $\psi(\varphi^{-1}(M)) = M$.

故 ψ 是双射，且由(1) 正规子群对应正规子群.

6: (1) 若 G 是交换群，$\varphi: G \to G_1$ 满同

G_1 不一定是交换群，记 $G = C_n = \langle a \rangle$　$G_1 = D_{2n}$.

$\varphi: C_n \to D_n = \{e, a, a^2, \cdots, a^{n-1}, b, ba, \cdots, ba^{n-1}\}$

$a^k \mapsto a^k$　$k = 0, 1, \cdots n-1$.　D_n 不交换.

若 φ 是满同，则 G_1 是交换群.

(2) $\varphi: G \to \{e\}$ 平凡同态　不一定.

$\pi: S_4 \to S_4/K_4$ 交换群.　是3,5,4.

7: 类似于例题 3.5.2.

对任意正整数 l，同构 φ 满足 $\varphi(a^l)=\varphi(a)^l$.

所以 $\varphi: \langle a\rangle \to \langle b\rangle$ 由 $\varphi(a)$ 完全确定.

由题 $o(\varphi(a)) \mid o(a)=8$ 又由拉格朗日定理 $o(\varphi(a)) \mid |\langle b\rangle|=12$.

即是 $3.5.1(3)$

故 $o(\varphi(a))$ 可能的值为 $1, 2, 4$. 于是 $\varphi(a)$ 可能为 b^0, b^3, b^6, b^9.

(1) 若 $\varphi(a)=b^0$, 则 φ 为平凡同态 $\ker\varphi=\langle a\rangle$

(2) 若 $\varphi(a)=b^3$ 则 $\varphi: \langle a\rangle \to \langle b\rangle$

$a^0, a^4 \to b^0$

$a, a^5 \to b^3$

$a^2, a^6 \to b^6$

$a^3, a^7 \mapsto b^9$.

$\ker\varphi=\{a^0, a^4\}$

$\varphi(a^l)=b^{3l}=e$

$12 \mid 3l$

$4 \mid l$

$\Rightarrow l=0, 4$ □

(3) 若 $\varphi(a)=b^6$, 则 $\varphi(a) \to \langle b\rangle$

$a^0, a^2, a^4, a^6 \mapsto b^0$

$a, a^3, a^5, a^7 \mapsto b^6$.

$\ker\varphi=\{a^0, a^2, a^4, a^6\}$

(4) 若 $\varphi(a)=b^9$ 则 $\varphi: \langle a\rangle \to \langle b\rangle$

$a^0, a^4 \mapsto b^0$

$a, a^5 \mapsto b^9$

$a^2, a^6 \mapsto b^6$

$a^3, a^7 \mapsto b^3$.

$\ker\varphi=\{a^0, a^4\}$

8: 当然是 3.5.2, 即: 例 $3.5.1(2)$. 将 $GL(2,R)$ 改为 $GL(n,R)$ $n\geq 2$.

正确

再来一遍, 然后由群同态基本定理得 $GL(n,R)/SL(n,R) \cong R^*$, $n\geq 2$

□

3.6 同构定理

1. 由 $\pi^{-1}(\pi^*(M)) = \pi^{-1}(\pi(M)) = \pi^{-1}(M/H) = M$

~~由题 3.5.3 和 ker 有 π 不是满射~~

[由命题 1.1.1：π^* 是单射.]

2. 证明：因为 $S_3 \leq S_4$，$K_4 \trianglelefteq S_4$. 故 $S_3K_4 \leq S_4$

又因为 $S_3 \cap K_4 = \{(1)\}$. 则 $|S_3K_4| = \frac{|S_3|\cdot|K_4|}{|S_3 \cap K_4|} = 24 = |S_4|$

故 $S_4 = S_3K_4$

由第二同构定理. $S_4/K_4 = (S_3K_4)/K_4 \cong S_3/K_4 \cap S_3 = S_3/\{(1)\} = S_3$

3. 证明：由 $H \trianglelefteq G$，$K \leq G$. 则有 $HK \leq G$.

(1).

因 $H \cap K \trianglelefteq K$.

$KH/H \cong K/H \cap K$.

故 $\frac{|KH|}{|H|} = \frac{|K|}{|H \cap K|} \Rightarrow |KH| \cdot |H \cap K| = |H||K|$

故由拉格朗日定理 $|HK||G| = p\cdot|H|$ 由 $|HK| \geq |H|$

由 $K \neq H$ 故 $|HK| > |H|$ 故 $|HK| = p|H| = |G|$

(2)：由第二同构定理. $(KH)/H \cong K/(H \cap K)$

由 $G = HK$ 故 $G/H \cong K/(H \cap K)$

由 $|G:H| = p$ 为素数 素数阶群是循环群. 得证

4：(1) 由例 3.2.10：$\mathbb{Z}/6\mathbb{Z}$ 的所有子群为 $\{n\mathbb{Z}/6\mathbb{Z} \mid n \in \mathbb{Z}_{>0},\ n|6\}$. 得证.

(2) 由(1)与推论 3.6.1. $\mathbb{Z}/6\mathbb{Z}$ 的所有子群为 $\{(0), 3\mathbb{Z}/6\mathbb{Z}, 2\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}\}$

(3)：$3\mathbb{Z}/6\mathbb{Z} = \{3k+6\mathbb{Z} \mid k \in \mathbb{Z}\} = \{0+6\mathbb{Z}, 3+6\mathbb{Z}\} = \langle\overline{3}\rangle \cong C_2$.

同理 $2\mathbb{Z}/6\mathbb{Z} = \{0+6\mathbb{Z}, 2+6\mathbb{Z}, 4+6\mathbb{Z}\} = \langle\overline{2}\rangle \cong C_3$.

(4). 由支撑群 $\mathbb{Z}$ 的子群 $2\mathbb{Z}$，$3\mathbb{Z}$，$6\mathbb{Z}$，均为正规子群，$2\mathbb{Z} \trianglelefteq 6\mathbb{Z}$，$3\mathbb{Z} \trianglelefteq 6\mathbb{Z}$.

由同构第一定理 $(\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$，$(\mathbb{Z}/6\mathbb{Z})/(3\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}$

3.8 群的直积.

1. 证明:

(1)⇒(2): $\forall g \in G$ 由于 $G = G_1G_2$, 故存在 $g_1 \in G_1$, $g_2 \in G$. s.t. $g = g_1g_2$.

若存在 $h_1 \in G_1$, $h_2 \in G_2$ 使得 $g = g_1g_2 = h_1h_2$ 则

$g_1^{-1}h_1 = g_2h_2^{-1} \in G_1 \cap G_2 = \{e\}$.

故 $g_1 = h_1$, $g_2 = h_2$. 因此, g 的表示法唯一.

(2)⇒(3). $e \in G$ 显然成立.

(3)⇒(1) 对任给的 $g \in G_1 \cap G_2$, 由于 G_1 G_2 是 G 的子群, 故 $g^{-1} \in G_1 \cap G_2$.

于是 $e = g \cdot g^{-1} = e \cdot e$ 由条件. 单位元表示为 G_1 与 G_2 的元素的表示法唯一. 故 $g = e$. 因此 $G_1 \cap G_2 = \{e\}$

□

2. 证明: (1) ⇒ (2). $G_1 \cap G_2 = \{e\}$, $G_1 \trianglelefteq G$, $G_2 \trianglelefteq G$ 则 G_1 的元素与 G_2 的元素可交换

见 例3.4.5 p73页.

(2) ⇒ (1).

由 $G = G_1G_2$, 对 $\forall g \in G$. 存在 g_1 且 $\in G_1$ $g_2 \in G_2$ 使得 $g = g_1g_2$.

由 G_1 是 G 的子群. 对 $\forall h_1 \in G_1$.

则 $gh_1g^{-1} = g_1g_2h_1g_2^{-1}g_1^{-1}$ 由(2)

$= g_1h_1g_2g_2^{-1}g_1^{-1}$

$= g_1h_1g_1^{-1} \in G_1$

故 $G_1 \trianglelefteq G$ 同理 $G_2 \trianglelefteq G$ □

3. 与第1题同理可证.

□

4. 与第2题同理可证.

□

5. 证明: 构造映射 φ: $G_1 \times \cdots \times G_n \longrightarrow G_{i_1} \times \cdots \times G_{i_n}$

$$(x_1, \cdots, x_n) \longmapsto (x_{i_1}, \cdots, x_{i_n})$$

对 $(x_1, \cdots x_n), (y_1 \cdots y_n) \in G_1 \times \cdots \times G_n$

$$\begin{aligned}\varphi((x_1 \cdots x_n)\cdot(y_1 \cdots y_n)) &= \varphi((x_1y_1, \cdots, x_ny_n)) \\ &= (x_{i_1}y_{i_1}, \cdots, x_{i_n}y_{i_n}) \\ &= (x_{i_1}, \cdots x_{i_n})\cdot(y_{i_1}, \cdots y_{i_n}) \\ &= \varphi(x_1 \cdots x_n)) \cdot \varphi((y_1 \cdots y_n))\end{aligned}$$

故 φ 是同态. 且显然 φ 即单又满. 因此 φ 是一个同构. 得证 □

6. 证明: 由 P86 页例 3.3.2. 4阶群只有2个: 循环群 及 K_4.

由 $\#(G_1 \times G_2) = 4$. 且对 $\forall (a,b) \in G_1 \times G_2$ $(a,b)(a,b) = (a^2, b^2) = (e_1, e_2)$ 单位元.

故 $G_1 \times G_2$ 中元素阶 ≤ 2. 故 $G_1 \times G_2$ 不是循环群. 因此 $G_1 \times G_2 \cong K_4$.

所以4阶群的同构型是 C_4, $C_2 \times C_2$. □

7. 证明: 若 $n=1$ 时显然成立,

若 $n=2$ 时, 由命题 3.2.6 有 $o(a_1, a_2) = [o(a_1), o(a_2)]$

假设 $n-1$ 时. 有 $o(a_1 a_2 \cdots a_{n-1}) = [o(a_1), \cdots, o(a_{n-1})]$

现若 $G = G_1 \times \cdots \times G_n$ 时

$$\begin{aligned}o(a_1, \cdots, a_n) &\xrightarrow{\text{命题2.6(2)}} [o(a_1 a_2 \cdots a_{n-1}), o(a_n)] \\ &= [[o(a_1), \cdots, o(a_{n-1})], o(a_n)] \\ &= [o(a_1), \cdots, o(a_n)]\end{aligned}$$

□

8. 证明: 若 $(m,n)=1$. 则 $C_{mn} \cong C_m \times C_n$ (见例 3.8.1)

现若 $C_{mn} \cong C_m \times C_n$. 设 $(m,n) = d$. $\forall (a,b) \in C_m \times C_n$.

有 $(a,b)^{\frac{mn}{d}} = \left((a^m)^{\frac{n}{d}}, (b^n)^{\frac{m}{d}}\right) = (e_1, e_2)$ 其中 (e_1, e_2) 是 $C_m \times C_n$ 的单位元.

故 $o((a,b)) \leq \frac{mn}{d}$. 若 $d \neq 1$ 则 $o((a,b)) \leq \frac{mn}{d} < mn$ 由 (a,b) 是任取的.

故 $C_m \times C_n$ 中不存在 mn 阶元素. 故 $C_m \times C_n$ 不是 mn 阶循环群. 矛盾.

因此 $d = 1$. $(m,n) = 1$ □

10. 证明：$CF(p)$：有限域.

$\sigma : (V,+) \longrightarrow G$

$(x_1 \cdots x_n) \longmapsto (a^{x_1}, \cdots, a^{x_n})$

对$\forall$ $G_0 = C_p \times \cdots \times C_p = \{(a^{x_1}, \cdots, a^{x_n}) \mid a^{x_i} \leq p-1\}$

且 $V = \{(x_1 \cdots x_n) \mid 0 \leq x_i \leq p\}$ （p是素数）

故σ显然是双射.

且 $\forall (x_1 \cdots x_n), (y_1 \cdots y_n) \in (V,+)$

有 $\sigma((x_1 \cdots x_n) + (y_1 \cdots y_n)) = \sigma((x_1+y_1), \cdots, x_n+y_n))$

$= (a^{x_1+y_1}, \cdots, a^{x_n+y_n})$

$= (a^{x_1} \cdots a^{x_n}) \cdot (a^{y_1}, \cdots, a^{y_n})$

$= \sigma(x_1 \cdots x_n) \cdot \sigma(y_1 \cdots y_n)$

故σ是保持运算的双射. 故σ是同构

□

9. 证明：$\varphi : G \longrightarrow G/H \times G/K$

$g \longmapsto (gH, gK)$

若$g_1 \neq g_2$ 则 $(g_1H, g_1K) \neq (g_2H, g_2K)$

若否则 $g_1H = g_2H$, $g_1K = g_2K$

$g_1Hg_2^{-1} = H$ $g_1Kg_2^{-1} = K$ $H \cap K = \{e\}$

$\Rightarrow g_1 = g_2$

故φ是单射

φ是嵌入映射. $G/H \times G/K$的一个子集 $\cong G$

故G同构于$G/H \times G/K$的子群

□

3.9 群在集合上的作用

1. 证明：① G 是群，$\Omega = G$.

定义 $x(g) = xgx^{-1}$ $\forall x \in G$, $\forall g \in G$.

由 (1) $e \in G$ $e(g) = ege^{-1} = g$ $\forall g \in \Omega = G$

(2) $x(y(g)) = x(ygy^{-1}) = xygy^{-1}x^{-1} = xyg(xy)^{-1} = (xy)(g)$

$\forall x, y \in G$, $\forall g \in \Omega = G$.

故是一个群作用.

② 由 $\forall x \in G$, $\sigma_x : G \to G$

$g \mapsto xgx^{-1}$

由 $g_1 = g_2 \Leftrightarrow xg_1 = xg_2 \Leftrightarrow xg_1x^{-1} = xg_2x^{-1}$ $\quad xgx^{-1} = h$ $g = x^{-1}hx$

故 σ_x 是良定的且是单射 对 $\forall h \in G$ 则存在 $g = x^{-1}hx \in G$

使得 $\sigma_x(x^{-1}hx) = x \cdot x^{-1}hx \cdot x^{-1} = h$ 故 σ_x 是满射.

故由 $\sigma_x(g_1g_2) = xg_1g_2x^{-1} = xg_1x^{-1} \cdot xg_2x^{-1} = \sigma_x(g_1) \cdot \sigma_x(g_2)$

故 σ_x 是自同构映射. 即 $\sigma_x \in Aut(G)$.

其余显然 □

2. 证明：对 $\forall i, j \in \{1, 2, \cdots n\}$ 有 $(ij) \in S_n$ 使得

$(ij) \circ i = j$ 故 S_n 在 $\{1, 2 \cdots n\}$ 上的自然作用是传递的.

点 1 处的定群 $G_1 = \{\sigma \in S_n \mid \sigma(1) = 1\}$

$= S_A$. $A = \{2, 3, \cdots, n\}$. □

3. 证明：由 n≥3. 设 $i \neq j \neq 1$.

则 $(1ij) \circ (1) = i$ 故 A_n 在集合 $\{1, 2, \cdots, n\}$ 上的作用是传递的.

$(1) \circ (1) = 1$

点 1 处的稳定子群为 $G_1 = \{\sigma \in A_n \mid \sigma \circ 1 = 1\}$

$= \{\sigma \mid \sigma$ 是在 $\{2, 3, \cdots, n\}$ 上的交错群$\}$

□

4. $C_G(g)=\{x\in G \mid xg=gx\}$

① $C_{A_4}((123))=\{x\in A_4 \mid x(123)=(123)x\}$

$=\{x\in A_4 \mid x(123)x^{-1}=(123)\}$

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

1 2 3

2 3 1

3 1 2

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ (记作 3,1,2)

$=\{(1),(123),(132)\}$

② $C_{A_4}((132))=\{x\in A_4 \mid x(132)=(132)x\}$

$=\{x\in A_4 \mid x(132)x^{-1}=(132)\}=\{(1),(123),(132)\}$

$\begin{pmatrix} x(1) & x(3) & x(2) \end{pmatrix}=(132)$

1 3 2

2 1 3

3 2 1

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

2 3 1 4

3 1 2 4

③ $C_{S_4}((123))=C_{A_4}((123))$, $C_{S_4}((132))=C_{A_4}((132))$.

5. $C(\sigma)=\{x\sigma x^{-1} \mid \forall x\in G\}$ 设 $\sigma=(12\cdots m)$

设 $|C(\sigma)|=m$.

$|C(\sigma)|=\dfrac{|S_n|}{|C_{S_n}(\sigma)|}\Rightarrow |C_{S_n}(\sigma)|=\dfrac{n!}{m}$

引用 习题3.1.6

与 σ 共轭的置换的轮换形为 $(m,\underbrace{1,\cdots,1}_{共n-m个})$

故 $|C(\sigma)|=\dfrac{n!}{m\cdot(n-m)!}$

$C_{S_n}(\sigma)=\{\tau \mid \tau\sigma\tau^{-1}=\sigma\}$

$=\langle\sigma\rangle\times S_A$ $A=\{m+1,\cdots,n\}$

设 $\tau\sigma\tau^{-1}=(\tau(1)\tau(2)\cdots\tau(m))(\tau(m+1))\cdots(\tau(n))$

$=(1,2,3,\cdots m)(m+1)\cdots(n)$

□

6. 证明：

$D_8 = \{ b^i a^j \mid i=0,1,\ j=0,1,2,3 \}$

且 $ba^{-k} = a^k b$

$$\left.\begin{aligned} (a^k)^{-1} a^i a^k &= a^i \\ (ba^k)^{-1} a^i ba^k &= a^{-i} \end{aligned}\right\} \ a^i \text{与} a^j \text{共轭当且仅当 } i+j=n$$

$$\left.\begin{aligned} (a^k)^{-1} ba^i a^k &= ba^{2k+i} \\ (ba^k)^{-1} ba^i ba^k &= ba^{2k-i} \end{aligned}\right\} \Rightarrow ba^i \text{与} ba^j \text{共轭当且仅当 } n \mid i \pm i + 2k.$$

故 D_8 的共轭类：$\{e\}$，$\{ba^2, b\}$，$\{ba, ba^3\}$，$\{a^2\}$，$\{a, a^3\}$

$C_e = D_8$　$C_b = \{1, b, a^2, a^2b\}$

$C_{ba} = \{ab, ba, a^2, 1\}$，　$C_{a^2} = D_8$

$C_a = \{a, a^2, a^3, 1\}$

7. S_4 由第是 3,4,1. 的元在 S_n 中共轭 $\Leftrightarrow$ 的元的轮形相等.

4 的分拆：
$$\begin{cases} 4 \\ 3\,1 \\ 2\,2 \\ 2\,1\,1 \\ 1\,1\,1\,1 \end{cases}$$

$\#C((1234)) = 4$　$\#C((1)(234)) = \frac{4!}{3} = 8$

$\#C((12)(34)) = \frac{4!}{2^2 2!} = 3$，$\#C((12)(3)(4)) = \frac{4!}{2 \cdot 2} = 6$，$\#C((1)(2)(3)(4)) = 1$

$S_{4(1234)} = \{\sigma \in S_4 \mid \sigma(1234)\sigma^{-1} = (1234)\}$

$= \{(1), (1234), (13)(24), (1432)\}$

$S_{4(1)(234)} = \{(1), (234), (243)\}$

$S_{4(12)(34)} = \{(1), (34), (12), (12)(34)\}$

$S_{4((12)(3)(4))} = \{(12), (1)\}$

$S_{4(1)} = \{(1)\}$

$\begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 2&3&4&1 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 3&4&1&2 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 4&1&2&3 \end{pmatrix}$

$\begin{pmatrix} 1&2&3&4 \\ 1&2&4&3 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 2&1&3&4 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 2&1&4&3 \end{pmatrix}$

$\begin{pmatrix} 1&2&3&4 \\ 1&3&4&2 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 1&4&2&3 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}$

$\begin{pmatrix} 1&2&3&4 \\ 1&2&3&4 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 1&2&4&3 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 2&1&3&4 \end{pmatrix}$
$\begin{pmatrix} 1&2&3&4 \\ 2&1&4&3 \end{pmatrix}$

8. 设 G 的中心为 $Z(G)$，则 $Z(G)$ 是 G 的极小正规子群. (推论 3.9.1)

设 $|Z(G)| = p$ 或 p^2.

若 $|Z(G)| = p$ 则 $Z(G)$ 是循环群. 令 $Z(G) = \langle a \rangle$

由 $|G/Z(G)| = p$. 即 $G/Z(G)$ 是循环群. 设 G 中任一元素 b 可以写成 $b = a^k$

$= \langle b \rangle$

注意 $a \in Z(G)$

故 G 是交换群. 而交换群的 p 阶子群是 G 的正规子群，故 $|Z(G)| = p$ 矛盾.

若 $|Z(G)| = p^2$，则 $Z(G) = G$，为交换群.

故 p^2 阶群交换.

同构型：① 若 G 中有 p^2 阶元素 则 G 是 p^2 阶循环群. $G \cong Z_{p^2}$.

② 若 G 中无 p^2 阶元素，那么除单位元 e 外，其余元素均是 p 阶的

(元素的阶整除群的阶)

(取 $a \in G$ $a \neq e$，那么存在 $b \notin \langle a \rangle$ 由 G 交换 $\langle a \rangle, \langle b \rangle$ 均为 G 的正规子群

故 $G = \langle a \rangle \times \langle b \rangle \cong Z_p \times Z_p$

且 $\langle a \rangle \cap \langle b \rangle = \{e\}$

$|\langle a \rangle \times \langle b \rangle| = p^2 = |G|$

□

9: 证明：由 $H \leq G$. O 是 H 的轨道

令 $O = \{m_1, m_2, \cdots, m_n\} \subseteq H$. 且 $H \cdot O = O$.

设 $\chi(O) = \{\chi m_1, \chi m_2, \cdots, \chi m_n\}$

故 $\chi H \chi^{-1} \cdot \chi(O) = \chi H \{\chi^{-1}\chi m_1, \chi^{-1}\chi m_2, \cdots, \chi^{-1}\chi m_n\} = \chi H_1 \cdot O$

故 $\chi(O)$ 是 $\chi H \chi^{-1}$ 的轨道 $= \chi \cdot (O)$

10: 证明：若否，存在两个 Ω 上的轨道 Ω_1 与 Ω_2 使得 $|\Omega_1| \neq |\Omega_2|$.

即取 $a \in \Omega_1$, $b \in \Omega_2$ $a, b \in \Omega$. 则 $|Na| \neq |Nb|$.

~~由对 $h_1 a = h_2 a$ 则 $a_1 = a_2$~~ 由于 G 在 Ω 上的作用是传递的. 故 $\exists g \in G$

$\exists h_1, h_2 \in N$. 使 $h_1 a = h_2 a$ $h_1 b \neq h_2 b$ $h_1 g a \neq h_2 g a$ 使 $ga = b$，此时 $a = g^{-1} b$

则 $h_1 g^{-1} b = h_2 g^{-1} b$ 由于 $N \trianglelefteq G$ 故 $hgh^{-1} \in N$

此时 不同存在 $h_1 g^{-1}, h_2 g^{-1} \in N$ 使 $h_1 g^{-1} b = h_2 g^{-1} b$ 与 $|Na| \neq |Nb|$ 矛盾

□