第三章　正规子群和群的同态与同构

§1　群同态与同构的简单性质

一、主要内容

1. 在群 G 到 $\overline{G}$ 的同态映射 φ 之下,元素的象及逆象的特征:

$$\varphi(a^{-1})=\varphi(a)^{-1}\ (a\in G),\quad \varphi(e)=\overline{e}.$$

但是,$\overline{G}$ 的单位元 $\overline{e}$ 的所有逆象(即教材第三章§3 所说的同态核 $\mathrm{Ker}\,\varphi$)作成 G 的一个正规子群(当然包含 G 的单位元 e).若 $\overline{e}$ 的逆象只有 e,即 $\mathrm{Ker}\,\varphi=\{e\}$ 时,φ 为单射.

2. 在群 G 到 $\overline{G}$ 的同态映射 φ 之下,子群的象和逆象的特征:

1) 当 $H\leqslant G$ 时,$\varphi(H)\leqslant\overline{G}$,且 $H\sim\varphi(H)$;

2) 当 $\overline{H}\leqslant\overline{G}$ 时,$\varphi^{-1}(\overline{H})\leqslant G$.

3. 本节例 3 利用 Lagrange 定理与子群乘积的阶证明了,在同构意义下 6 阶群只有两个:一个是 6 阶循环群,另一个是三次对称群 S_3.

二、释疑解难

1. 对于群同态映射 φ,有时不必要求是满射,有时又必须要求

是满射.例如教材本节定理 1 中的同态映射必须是满射,而定理 2 和定理 3 的同态映射 φ 则不要求是满射.原因很简单:因为定理 1 中的同态映射 φ 若不是满射,则 $\overline{G}$ 中必有元素没有逆象,从而 φ 以及群 G 中元素的性质对它们不会产生任何影响,此时 $\overline{G}$ 当然就不一定作成群;然而定理 2 和定理 3 的情形可就不同了:因为这时 $\overline{G}$ 也是群,而且在同态映射 φ (不一定是满射)之下单位元必有逆象,而子群必含单位元,从而 $\overline{G}$ 的子群 $\overline{H}$ 必有逆象,不会是空集.

例 1 设 G 为非零有理数乘群,$\overline{G}$ 为全体有理数对乘法作成的幺半群.则

$$\varphi: 正有理数 \longrightarrow 1,\ 负有理数 \longrightarrow -1$$

是 G 到 $\overline{G}$ 的一个同态映射(不是满射),但 G 是群而 $\overline{G}$ 却不是群.

例 2 设 G 如上例,$\overline{G}$ 为有理数集对

$$a \circ b = a^2 \quad (\forall\ a, b \in \overline{G})$$

作成的代数系统.则

$$\varphi: x \longrightarrow 1 \quad (\forall\ x \in G)$$

显然为 G 到 $\overline{G}$ 的一个同态映射(不是满射).虽然 G 是群,但 $\overline{G}$ 对∘不仅不是群,连半群也不是(因为其代数运算不满足结合律).

2. 关于教材例 3,若利用第三章 § 6 定理 3 (若 $|G| = pn$,则群 G 有 p 阶元)的结论,则其证明可大为简化.现在本节是利用前面已学过的知识来证明,这也是 Lagrange 定理和已知结论

$$|KN| = \frac{|K| \cdot |N|}{|K \cap N|}$$

的一种应用.这样做虽然稍麻烦一点,但也很有意义.

三、习题 3.1 解答

1. 设 H 是群 G 的一个子群,$a \in G$.证明:

$$aHa^{-1} \leqslant G \quad 且\ H \cong aHa^{-1}.$$

证 在 aHa^{-1} 中任取两元素 ah_1a^{-1}, ah_2a^{-1},其中 $h_1, h_2 \in H$.但 H 是子群,故 $h_1h_2^{-1} \in H$.从而

$$(ah_1a^{-1})(ah_2a^{-1})^{-1}=a(h_1h_2^{-1})a^{-1}\in aHa^{-1}.$$

因此，$aHa^{-1}\leqslant G$.

又由于易知 $\varphi: h\longrightarrow aha^{-1}\ (\forall h\in H)$是子群 H 到 aHa^{-1} 的同构映射，故

$$H\cong aHa^{-1}.$$

2. 在群的同态映射下，一个元素与其象的阶是否一定相等？在同构映射下如何？

解　在同态映射下，元素与其象的阶不一定相等. 例如，设 G 为非零有理数乘群，$\overline{G}=\{1,-1\}$ 为对普通乘法作成的群. 则易知

$$\sigma: x\longrightarrow 1\quad 与\quad \tau: 正有理数\longrightarrow 1，负有理数\longrightarrow -1$$

都是群 G 到 $\overline{G}$ 的同态映射(σ 不是满射，τ 是满射). 但 $\overline{G}$ 中 1 的阶是 1，-1 的阶是 2，而 G 中除去± 1 外的元素的阶均无限.

若 φ 是群 G 到 $\overline{G}$ 的同构映射，则任何元素与其象的阶都相同. 这是因为，对任意 $a\in G$ 有

$$\varphi(a)^m=\varphi(a^m)=\overline{e}\Longleftrightarrow a^m=e.$$

3. 问：$\varphi(A)=A^{\mathrm{T}}$ (A^{T} 为 A 的转置方阵)是否为一般线性群 $GL_n(F)$ $(n>1)$的自同构？又$\sigma(A)=(A^{-1})^{\mathrm{T}}$ 呢？

解　φ 显然是 $GL_n(F)$的双射变换，但不是自同构：因为一般

$$(AB)^{\mathrm{T}}=B^{\mathrm{T}}A^{\mathrm{T}}\neq A^{\mathrm{T}}B^{\mathrm{T}},\quad 即\ \varphi(AB)\neq\varphi(A)\cdot\varphi(B).$$

又$\sigma: A\longrightarrow(A^{-1})^{\mathrm{T}}$ 显然是双射变换且

$$\begin{aligned}\sigma(AB)&=[(AB)^{-1}]^{\mathrm{T}}=(B^{-1}A^{-1})^{\mathrm{T}}\\&=(A^{-1})^{\mathrm{T}}\cdot(B^{-1})^{\mathrm{T}}=\sigma(A)\cdot\sigma(B),\end{aligned}$$

故σ 是群 $GL_n(F)$的自同构.

4. 先证明本节例 3 中 6 阶群 G 的元素 $ba=ab^2$，再各给出 G 与 S_3 的乘法表，并由此指出 φ 是群 G 到三次对称群 S_3 的同构映射.

证　由于 $G=\{e,a,b,b^2,ab,ab^2\}$ 且$|a|=2$，$|b|=3$，故易知 ba 不等于 e,a,b,b^2. 又 $ba\neq ab$ (因若 $ab=ba$，则$|ab|=6$，从而 G 为 6 阶循环群，这与 G 不是循环群的假设矛盾). 因此，$ba=ab^2$. 由此可

得 G 的乘法表如下：

$\cdot$	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	b	a	ab	b^2	e

再把 S_3 中六个置换按顺序(1),(12),(123),(132),(23),(13)列出乘法表(略去),即可知 φ 是 G 到 S_3 的同构映射.因此,$G\cong S_3$.

5. 证明:4 阶群 G 若不是循环群,则必与 Klein 四元群同构.

证　因为 $|G|=4$,G 又不是循环群,从而 G 无 4 阶元.于是由 Lagrange 定理知,G 中除单位元 e 外每个元素的阶均为 2.因此,若令

$$G=\{e,a,b,c\},$$

则映射

$$\varphi:\quad e\longrightarrow(1),\ b\longrightarrow(34),a\longrightarrow(12),\ c\longrightarrow(12)(34)$$

是 G 到 Klein 四元群 $K_4=\{(1),(12),(34),(12)(34)\}$ 的同构映射.因此,$G\cong K_4$.

6. 设 G 是正有理数乘群,$\overline{G}$ 是整数加群.证明:

$$\varphi:\ 2^n\cdot\frac{b}{a}\longrightarrow n$$

是群 G 到 $\overline{G}$ 的一个同态满射,其中 a,b 是互素的正奇数,n 是整数.

证　显然 φ 是群 G 到群 $\overline{G}$ 的满射.

又由于当 $(ab,2)=1$,$(cd,2)=1$ 时显然有

$$(abcd,2)=1,$$

且
$$\varphi\left(2^n\cdot\frac{b}{a}\cdot 2^m\cdot\frac{d}{c}\right)=\varphi\left(2^{n+m}\cdot\frac{bd}{ac}\right)=n+m$$
$$=\varphi\left(2^n\cdot\frac{b}{a}\right)\varphi\left(2^m\cdot\frac{d}{c}\right),$$
故 φ 是正有理数乘群 G 到整数加群 $\overline{G}$ 的一个同态满射.

§2　正规子群和商群

一、主要内容

1. 正规子群定义、性质和例子.性质主要有:

1) 设 $N\leqslant G$.则
$$N\trianglelefteq G\Longleftrightarrow aNa^{-1}\subseteq N\quad(\forall\, a\in G)$$
或
$$N\trianglelefteq G\Longleftrightarrow axa^{-1}\in N\quad(\forall\, a\in G,\, x\in N).$$

2) 正规子群在同态满射下的象和逆象均仍为正规子群.

3) 正规子群与子群之积是子群;正规子群与正规子群之积是正规子群.

2. 商群定义及商群的一个应用(Cauchy 定理:pn 阶交换群必有 p 阶子群,其中 p 为素数).

3. 介绍由正规子群来界定的两类群:哈密顿群和单群.这是两类在群论研究中占很重要地位的群.

二、释疑解难

1. 教材在本节所举的例子中,应该十分注意 S_4 及 $S_n\,(n\neq 4)$ 的正规子群的状况.因为这涉及 S_2, S_3 及 S_4 都是可解群(参考本节习题第 8 题),而当 $n\geqslant 5$ 时 S_n 不是可解群.这种名称来源于一般的二、三、四次代数方程都有求根公式,即可根式解,但一般的五次和五次以上的代数方程都没有求根公式,即不可根式解.

2. 若 $N\trianglelefteq G$,则对群 G 中任意元素 a,b 都有
$$(aN)(bN)=abN.$$

这是在教材中已经证明了的.对此也可以采取以下证法:

任取 $x\in(aN)(bN)$,并令

$$x=an_1\cdot bn_2\quad(n_1,n_2\in N).\tag{1}$$

由于 $N\trianglelefteq G$,从而 $n_1b\in Nb=bN$.于是令

$$n_1b=bn_3\quad(n_3\in N).$$

由(1)得

$$\begin{aligned}x&=a(n_1b)n_2=a(bn_3)n_2\\&=ab\cdot n_3n_2\in abN.\end{aligned}$$

因此,$(aN)(bN)\subseteq abN$.

反之,任取 $x\in abN$,则类似可证 $x\in(aN)(bN)$.故又有

$$abN\subseteq(aN)(bN).$$

因此,$(aN)(bN)=abN$.

这种证法是最原始的一种证法,当然不如教材中的证法简单.其所以简单,是由于利用了子集乘法的性质 $(AB)C=A(BC)$ 以及 $Nb=bN$ 和 $N^2=N$.

3. 在本教材中,共有三个定理(本节定理 5、§6 定理 3 及 §8 定理 1)涉及 pn(p 是素数)阶群 G 必有 p 阶子群.从表面上看,这三个定理似有重复之感.实际上三者互相联系紧密,而且其中任何一个都不能由另一个所代替.这是因为,本节定理 5 是假设 G 为交换群,而 §6 定理 3 并不假设 G 为交换群,但在证明中要用到本节定理 5;又 §8 定理 1 (即第一 Sylow 定理)又要用到 §6 定理 3.因此,三者密不可分,而且哪一个也不是多余的.对此,示意如下:

pn 阶交换群必有 p 阶子群(本节定理 5)$\longrightarrow$
凡 pn 阶群必有 p 阶子群(§6 定理 3)$\longrightarrow p^sm$ 阶
群必有 $p^i(i=0,1,\cdots,s)$ 阶子群(§8 定理 1).

4. 李型单群是李代数中谢瓦莱单群和单扭群的统称,它们是一些由矩阵作成的群.

三、习题 3.2 解答

1. 证明：群 G 的任意个正规子群的交还是 G 的一个正规子群.

证 略.

2. 证明：指数是 2 的子群必是正规子群.

证法Ⅰ 设 G 是群且 $N \leqslant G$，$(G:N)=2$.则有

$$G=N \cup aN, \quad N \cap aN=\varnothing.$$

任取 $n \in N$，$x \in G$，若 $x \in N$，则当然 $xnx^{-1} \in N$；

若 $x \notin N$，则必 $x \in aN$，从而可令

$$x=an_1 \quad (n_1 \in N).$$

设若 $xnx^{-1} \notin N$，则必 $xnx^{-1} \in aN$，从而可令

$$xnx^{-1}=an_2 \quad (n_2 \in N),$$

即 $an_1nn_1^{-1}a^{-1}=an_2$，从而 $a=n_2^{-1}n_1nn_1^{-1} \in N$，矛盾.故必 $xnx^{-1} \in N$.因此，$N \trianglelefteq G$.

证法Ⅱ 令 N 与 G 为如上所设.则任取 $x \in G$，当 $x \in N$ 时当然有

$$xN=Nx=N.$$

当 $x \notin N$ 时，则由于 $(G:N)=2$，故

$$G=N \cup xN=N \cup Nx,$$

从而也有 $xN=Nx$，故 $N \trianglelefteq G$.

3. 证明：若群 G 的 n 阶子群有且只有一个，则此子群必为 G 的正规子群.

证 设 $H \leqslant G$ 且 $|H|=n$.则对 G 中任意元素 a，易知 aHa^{-1} 也是 G 的一个 n 阶子群.

但由题设，G 的 n 阶子群只有一个，故

$$aHa^{-1}=H \quad (\forall a \in G),$$

从而 $H \trianglelefteq G$.

4. 设 $H \trianglelefteq G$，且 $(G:H)=m$.证明：对群 G 中任意元素 a 都

有 $a^m \in H$.

证 由于 $H \trianglelefteq G$,且$(G: H)=m$,故商群 G/H 是一个 m 阶群.于是对 G 中任意元素 a,商群 G/H 中元素 $aH=\bar{a}$都满足方程

$$x^m=\bar{e} \quad (\bar{e}=H \text{ 是 } G/H \text{ 的单位元}).$$

于是$\bar{a}^m=(aH)^m=a^m H=H$.因此 $a^m \in H$.

5. 设 H, K 是群 G 的两个正规子群,且二者的交为$\{e\}$.证明:H 与 K 中的元素相乘时可换.

证 任取 $a\in H, b\in K$.则因 $H \trianglelefteq G, K \trianglelefteq G$,故

$$aba^{-1}b^{-1} \in H\cap K=\{e\}.$$

从而 $aba^{-1}b^{-1}=e, ab=ba$.

6. 设 H 是包含在群 G 的中心内的一个子群.证明:当 G/H 是循环群时,G 是交换群.

证 首先,由于子群 H 含于群 G 的中心,故显然 $H \trianglelefteq G$.

当 G/H 是循环群,且 $G/H=\langle aH\rangle$ 时,令

$$xH, yH \in\langle aH\rangle, \quad \text{且 } xH=(aH)^s, yH=(aH)^t.$$

则 $xH=a^s H, yH=a^t H$,于是有 $h_1, h_2 \in H$ 使

$$x=a^s h_1, \quad y=a^t h_2.$$

由于 H 中元素同 G 中任何元素可交换,故

$$xy=(a^s h_1)(a^t h_2)=(a^t h_2)(a^s h_1)=yx,$$

即 G 是交换群.

7. 设 G 是群,$N \trianglelefteq G$.证明:如果 N 及商群 G/N 都是周期群,则 G 也是周期群.

证 任取 $a\in G$,则 $aN\in G/N$.但因为商群 G/N 是周期群,故有正整数 m 使

$$(aN)^m=a^m N=N, \quad \text{即 } a^m \in N.$$

又因为 N 也是周期群,故又有正整数 n 使

$$(a^m)^n=a^{mn}=e,$$

从而 a 的阶有限,即 G 是一个周期群.

8. 设 G 是群,$G_i\,(0\leqslant i\leqslant k)$为其子群且

$$e=G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{k-1} \trianglelefteq G_k = G, \qquad (1)$$

则称此为群 G 的正规群列.若群 G 有正规群列(1)且诸商群

$$G_1/G_0,\quad G_2/G_1,\quad \cdots,\quad G_k/G_{k-1}$$

又都是交换群时,则称 G 为可解群.证明:对称群 S_2, S_3 及 S_4 都是可解群.

证　因为 $e \trianglelefteq S_2$,而 $S_2/e \cong S_2$ 是交换群,故 S_2 是可解群.

又令 $H=\{(1),(123),(132)\}$,则由本节教材例 1 知:

$$e \trianglelefteq H \trianglelefteq S_3, \quad 且\ H/e, S_3/H\ 均可换.$$

故 S_3 是可解群.

再由本节教材例 3 知:

$$e \trianglelefteq K_4 \trianglelefteq A_4 \trianglelefteq S_4.$$

而且 K_4/e、A_4/K_4、S_4/A_4 又都是交换群,故 S_4 是可解群.

注　因为当 $n \geqslant 5$ 时 A_n 是单群,故只有

$$e \trianglelefteq A_n \trianglelefteq S_n.$$

但是 $A_n/e \cong A_n$ 是非交换群,故此时 S_n 不是可解群.

§3　群同态基本定理

一、主要内容

1. 在同构意义下,每个群能而且只能与其商群同态.即指以下两点:

1) 设 $N \trianglelefteq G$,则 $G \sim G/N$ $(\tau: a \longrightarrow aN)$且 $\mathrm{Ker}\tau = N$;

2) 反之,若 $G \overset{\tau}{\sim} \overline{G}$,则 $N=\mathrm{Ker}\tau \trianglelefteq G$ 且 $G/N \cong \overline{G}$.

2. 在同态映射下,循环群的同态象是循环群.

3. 若 $G \sim \overline{G}$,则群 G 的所有包含核的子群同 $\overline{G}$ 的所有子群间有一个保持包含关系的双射.

二、释疑解难

1. 设 $N \trianglelefteq G$,则称 $\tau: a \longrightarrow aN\ (\forall a \in G)$为群 G 到商群的自

然同态.应注意,除自然同态外,G到G/N可能还有别的同态.

例1　$N=\{(1),(12)\}\trianglelefteq G=\{(1),(12),(34),(12)(34)\}$.又

$$G/N=\{N,(34)N\}.$$

易知　φ: $(1),(34)\longrightarrow N$,　$(12),(12)(34)\longrightarrow(34)N$

也是G到商群G/N的同态满射,但它不是自然同态.

2. 应注意,教材中推论1的逆定理不成立.即若有限群$\overline{G}$的阶整除有限群G的阶,则不一定有$G\sim\overline{G}$.

例2　设$\overline{G}$为三次对称群S_3,G为12次单位根乘群,则$|\overline{G}|=6$整除$|G|=12$.但是不可能有$G\sim\overline{G}$,因为G是交换群,其同态象必为交换群,但S_3不是交换群.

3. 教材定理3中的$G\sim\overline{G}$必须强调是满同态.若不是满同态,则定理3应改述为:若φ是群G到群$\overline{G}$的一个同态映射,则当G为循环群时同态象$\varphi(G)$也是循环群.

4. 教材定理4的两个条件“φ是满同态”和“G的含K的所有子群”不能少.

1) 例如,设G为任意群,$\overline{G}$为2阶群.则显然

$$\varphi:\ x\longrightarrow\bar{e}\quad(\forall\ x\in G,\ \bar{e}\text{为}\ \overline{G}\ \text{的单位元})$$

是G到$\overline{G}$的同态映射(但不是满射),而$\mathrm{Ker}\,\varphi=G$.从而G的包含核的子群只有一个即G本身.但$\overline{G}$有两个子群,显然二者间不能建立双射.

2) 又例如,设$|G|>1$,$|\overline{G}|=1$,则

$$\varphi:\ x\longrightarrow\bar{e}\quad(\forall\ x\in G)$$

是群G到$\overline{G}$的同态满射,且核$K=\mathrm{Ker}\,\varphi=G$.若不强调“含$K$”的所有子群,则$G$至少有两个子群$\{e\}$及$G$.但$\overline{G}$只有一个子群即$\overline{G}$本身,二者间显然也不能建立双射.

三、习题3.3解答

1. 设群$G\sim\overline{G}$,且同态核是K.证明:G中二元素在$\overline{G}$中有相同的象,当且仅当它们在K的同一陪集中.

证　设 φ 是群 G 到群 $\overline{G}$ 的一个同态映射，且核为 K，又 G 中元素 x 在 φ 之下的象表示为 $\overline{x}$，即 $\overline{x}=\varphi(x)$。则对任意 $a,b\in G$，若 $\overline{a}=\overline{b}$，则

$$\overline{a}\,\overline{b}^{-1}=\overline{e},\quad \overline{ab^{-1}}=\overline{e},\quad ab^{-1}\in K,$$

即 G 中元素 a 与 b 在 K 的同一陪集中。

反之，倒推回去即得。

注　本题原设 $G\sim\overline{G}$，但实际上对同态映射可不要求是满射。

2. 证明：单群的同态象是单群或单位元群(即只含一个元素的群)。

证　设 G 是单群，且 φ 是 G 到群 $\overline{G}$ 的一个同态满射。又设 $\overline{N}\trianglelefteq\overline{G}$ 且 $\varphi^{-1}(\overline{N})=N\trianglelefteq G$。但 G 是单群，故

$$N=G\quad 或\quad N=\{e\}.$$

当 $N=G$ 时，$\overline{N}=\overline{G}$；当 $N=\{e\}$ 时，$\overline{N}=\{\overline{e}\}$。即 $\overline{G}$ 是单群或单位元群。

3. 设 N 是群 G 的一个正规子群，又 $N\subseteq H\leqslant G$。证明：H 在 G 到 G/N 的自然同态下的象为 H/N。

证　设 φ 为群 G 到商群 G/N 的自然同态，则对 G 中任意元素 x 有 $\varphi(x)=xN$。由题设知，N 也是 H 的正规子群。故若 $a\in H$，则 $\varphi(a)=aN\in H/N$。从而 $\varphi(H)\subseteq H/N$。

又显然 $H/N\subseteq\varphi(H)$。故 $\varphi(H)=H/N$。

4. 证明：

1) 无限循环群与任何循环群同态；

2) 两个有限循环群 G 与 $\overline{G}$ 同态 $\Longleftrightarrow |\overline{G}|\;\big|\;|G|$。

证　1) 设 $G=\langle a\rangle$ 是无限循环群，$\overline{G}=\langle b\rangle$ 是任一循环群，定义

$$\varphi:\ G\longrightarrow\overline{G},\ a^k\longrightarrow b^k,\ k\in\mathbf{Z}.$$

因为 $G=\langle a\rangle$ 是无限循环群，所以 $|a|=\infty$，从而

$$a^k=a^l\Longleftrightarrow k=l.$$

于是，若 $a^k=a^l$，则 $\varphi(a^k)=\varphi(a^l)$，故 φ 是无限循环群 G 到循环群

$\overline{G}$ 的映射.

又易知 φ 是满射且保持运算,因此 $G\sim\overline{G}$.

2) 设 $G=\langle a\rangle$, $\overline{G}=\langle b\rangle$ 是两个有限循环群且

$$|a|=m,\quad |b|=n.$$

设 $G\sim\overline{G}$,且 ψ 为其一同态满射,则 $G/\mathrm{Ker}\,\psi\cong\overline{G}$.但由于

$$|\overline{G}|=|G/\mathrm{Ker}\,\psi|$$

整除 $|G|$,故 $|\overline{G}|\;\big|\;|G|$.

反之,设 $|\overline{G}|\;\big|\;|G|$,即 $n|m$.定义:

$$\varphi:\ G\longrightarrow\overline{G},\quad a^s\longrightarrow b^r.$$

其中 $s=nq+r$, $q,r\in\mathbf{Z}$ 且 $0\leqslant r<n$.

任取 $a^x, a^y\in\langle a\rangle$,且令

$$x=nq_1+r_1,\quad y=nq_2+r_2,\quad 0\leqslant r_1, r_2<n.$$

当 $a^x=a^y$,即

$$a^{x-y}=a^{n(q_1-q_2)+(r_1-r_2)}=e,$$

亦即 $n|[n(q_1-q_2)+r_1-r_2]$时,必有 $n|(r_1-r_2)$,但是

$$0\leqslant|r_1-r_2|<n,$$

故 $r_1-r_2=0$,即 $r_1=r_2$.从而

$$\varphi(a^x)=b^{r_1}=b^{r_2}=\varphi(a^y),$$

故 φ 是从 G 到 $\overline{G}$ 的映射.又易知 φ 是满射且保持运算,因此,$G\sim\overline{G}$.

5. 证明:有理数加群 $\mathbf{Q}_+$ 与非零有理数乘群 $\mathbf{Q}^*$ 不同构.

证法 I 反证法.

若不然,设加群 $\mathbf{Q}_+$ 与乘群 $\mathbf{Q}^*$ 同构且 φ 为其一同构映射,则令 $\varphi(a)=-1$ $(a\in\mathbf{Q}_+)$,于是

$$\varphi\left(\frac{a}{2}\right)^2=\varphi\left(\frac{a}{2}\right)\varphi\left(\frac{a}{2}\right)=\varphi\left(\frac{a}{2}+\frac{a}{2}\right)=\varphi(a)=-1.$$

即有有理数$\frac{a}{2}$其平方等于-1.这是不可能的,因此,$\mathbf{Q}_+$ 与 $\mathbf{Q}^*$ 不同

构.

证法Ⅱ　反证法.

若不然,设 $\mathbb{Q}_+ \cong \mathbb{Q}^*$,且 φ 为其一同构映射,则由于 0 是 $\mathbb{Q}_+$ 的零元而 1 是 $\mathbb{Q}^*$ 的单位元,故必

$$\varphi(0)=1. \tag{1}$$

又由于 $-1\in\mathbb{Q}^*$,故有 $x\in\mathbb{Q}_+$ 使 $\varphi(x)=-1$.于是

$$\varphi(2x)=\varphi(x+x)=\varphi(x)\varphi(x)=(-1)\cdot(-1)=1. \tag{2}$$

但 φ 是单射,故由(1)与(2)知,$2x=0$, $x=0$.那么

$$\varphi(0)=-1.$$

这与(1)矛盾.故 $\mathbb{Q}_+$ 与 $\mathbb{Q}^*$ 不同构.

§4　群的同构定理

一、主要内容

1. 本节主要介绍了群的三个同构定理.它们是:

1) $G \overset{\varphi}{\sim} \overline{G}$, $\mathrm{Ker}\,\varphi \subseteq N \trianglelefteq G \Longrightarrow G/N \cong \varphi(G)/\varphi(N)$;

2) $H \leqslant G$, $N \trianglelefteq G \Longrightarrow H\cap N \trianglelefteq H$, $HN/N \cong H/(H\cap N)$;

3) $N \trianglelefteq G$, $\overline{H} \leqslant G/N \Longrightarrow G$ 有惟一子群 $H \supseteq N$ 使 $\overline{H}=H/N$;

若 $\overline{H} \trianglelefteq G/N \Longrightarrow$ 有惟一的 $H \trianglelefteq G$ 使 $\overline{H}=H/N$ 且

$$G/H \cong (G/N)/(H/N).$$

2. 借助同构定理,作为例子证明了以下两个结论:

1) $H, K \trianglelefteq G \Longrightarrow G/HK \cong (G/H)/(HK/H)$;

2) $S_4/K_4 \cong S_3$　(K_4 为 Klein 四元群).

二、释疑解难

1. 第一同构定理还有另一证法,见本节习题第 4 题,此外还应注意第一同构定理中的两个条件:

1) φ 必须是满同态.

因若不然,设 G 为任意群,$\overline{G}$ 为 2 阶群,则 φ: $x \longrightarrow \overline{e}\ (\forall\ x \in G)$ 是 G 到 $\overline{G}$ 的一个同态映射(但不是满射).此时 $\mathrm{Ker}\,\varphi = N = G$,而 $\overline{N} = \{\overline{e}\}$,从而 G/N 为 1 阶群,而 $\overline{G}/\overline{N}$ 为 2 阶群,二者当然不会同构.

2) G 的正规子群 N 必须包含核 $\mathrm{Ker}\,\varphi$.

因若不然,例如设 G 是 6 阶循环群,$\overline{G} = \{\overline{e}\}$ 是单位元群,则

$$\varphi:\ x \longrightarrow \overline{e}\quad (\forall\ x \in G)$$

是满同态,且 $\mathrm{Ker}\,\varphi = G$.现取 G 的一个 2 阶子群 $N \nsupseteq \mathrm{Ker}\,\varphi$,则此时 G/N 为 3 阶群,而 $\overline{G}/\overline{N}$ 为 1 阶群,二者当然不能同构.

因此,“φ 是满同态”与“G 的正规子群 N 包含核”这两个条件都不能少.

2. 关于第二同构定理的说明.

1) 条件要求:$H \leqslant G$, $N \trianglelefteq G$.由此可得

$$H \cap N \trianglelefteq H, \qquad N \trianglelefteq HN.$$

(应注意,一般 $H \cap N \ntrianglelefteq N$, $H \ntrianglelefteq HN$.读者作为练习可自己举例).而且商群 $H/(H \cap N)$ 与 $(HN)/N$ 同构.再结合教材中所画的示意图,从而不难记住这个定理.

2) 关于本定理的证明,教材中是先证

$$\varphi:\ x \longrightarrow xN\quad (\forall\ x \in H)$$

是 H 到 HN/N 的同态满射,再证 $\mathrm{Ker}\,\varphi = H \cap N$ (因为证明容易,教材中省略),故而得

$$H/(H \cap N) \cong HN/N. \tag{1}$$

对此也可以采取另一种证法如下:令

$$\tau:\ x(H \cap N) \longrightarrow xN\quad (\forall\ x \in H).$$

可以证明,τ 是商群 $H/(H \cap N)$ 到 HN/N 的一个同构映射(此证明留给读者).因此可直接得(1).

至于定理的结论写成

$$H/(H \cap N) \cong HN/N \quad 或 \quad HN/N \cong H/(H \cap N),$$

这是无关紧要的,因为同构关系具有对称性.

3. 第三同构定理说明商群中子群的特征.简言之,商群中的子群仍为一种商群;且商群之商群可类似于普通分数那样$\left(\frac{b}{a}=\frac{b}{c}\Big/\frac{a}{c}\right)$进行约分.

三、习题 3.4 解答

1. 设群 $G\sim\overline{G}$, $\overline{N}\trianglelefteq\overline{G}$, N 是 $\overline{N}$ 的逆象.证明:

$$G/N\cong\overline{G}/\overline{N}.$$

证　设 φ 是群 G 到群 $\overline{G}$ 的同态满射,由题设知:

$$\operatorname{Ker}\varphi\subseteq N=\varphi^{-1}(\overline{N})\trianglelefteq G,$$

且 $\varphi(N)=\varphi[\varphi^{-1}(\overline{N})]=\overline{N}$.于是由第一同构定理即得证.

2. 设 H,K 是群 G 的两个子群,又 $K'\trianglelefteq K$.证明:

1) $H\cap K'\trianglelefteq H\cap K$;

2) $(H\cap K)/(H\cap K')$与 K/K' 的一个子群同构.

证　1) $H\cap K'\leqslant H\cap K$ 显然.又设

$$a\in H\cap K',\quad x\in H\cap K,$$

则由于 $x,a\in H$,又 $H\leqslant G$,故 $xax^{-1}\in H$.

又由于 $a\in K'$, $x\in K$,而 $K'\trianglelefteq K$,故又有

$$xax^{-1}\in K'.$$

从而,$xax^{-1}\in H\cap K'$.因此,$H\cap K'\trianglelefteq H\cap K$.

2) 易知

$$\varphi:\ x(H\cap K')\longrightarrow xK'\quad(x\in H\cap K)$$

是群$(H\cap K)/(H\cap K')$到 K/K' 的单同态,故由同态基本定理知:

$$(H\cap K)/(H\cap K')\cong\varphi((H\cap K)/(H\cap K'))\leqslant K/K'.$$

3. 设 G 是群,又 $K\leqslant H\trianglelefteq G$, $K\trianglelefteq G$.证明:若 G/K 是交换群,则 G/H 也是交换群.

证　任取 $x,y\in G$,由于 G/K 可换,故

$$xK\cdot yK=yK\cdot xK,\quad 即\ xyK=yxK.$$

从而$(xy)^{-1}(yx)\in K\leqslant H$.因此,

$$(xy)^{-1}(yx)\in H,\quad xyH=yxH.$$

即 $xH\cdot yH=yH\cdot xH$,G/H 也是交换群.

4. 题设如定理 1. 证明:σ: $x\longrightarrow\varphi(x)\overline{N}$ 是群 G 到商群 $\overline{G}/\overline{N}$的满同态,且其核 $\mathrm{Ker}\,\sigma=N$.从而 $G/N\cong\overline{G}/\overline{N}$.

证 因为φ 是满同态,故σ 显然是 G 到 $\overline{G}/\overline{N}$ 的一个满射;又由于

$$\varphi(ab)\overline{N}=\varphi(a)\varphi(b)\overline{N}=\varphi(a)\overline{N}\cdot\varphi(b)\overline{N},$$

即$\sigma(ab)=\sigma(a)\sigma(b)$,故$\sigma$ 是群 G 到 $\overline{G}/\overline{N}$ 的一个同态满射.于是

$$G\sim\overline{G}/\overline{N}.$$

下面再证 $\mathrm{Ker}\,\sigma=N$.

首先,任取 $x\in N$,则$\varphi(x)\in\overline{N}$,于是在$\sigma$ 之下

$$x\longrightarrow\varphi(x)\overline{N}=\overline{N},$$

故 $x\in\mathrm{Ker}\,\sigma$, $N\subseteq\mathrm{Ker}\,\sigma$;

其次,任取 $c\in\mathrm{Ker}\,\sigma$,则在σ 之下有

$$c\longrightarrow\varphi(c)\overline{N}=\overline{N},$$

即$\varphi(c)\in\overline{N}$.但是 $\overline{N}=\varphi(N)$,故有 $x\in N$ 使

$$\varphi(x)=\varphi(c)\quad 或\quad \varphi(x^{-1}c)=\overline{e},$$

其中$\overline{e}$是 $\overline{G}$ 的单位元.于是

$$x^{-1}c\in\mathrm{Ker}\,\varphi\subseteq N,\quad c\in N,$$

即又有 $\mathrm{Ker}\,\sigma\subseteq N$,因此 $\mathrm{Ker}\,\sigma=N$.

既然同态 $G\sim\overline{G}/\overline{N}$ 的核是 N,于是由群同态基本定理知,

$$G/N\cong\overline{G}/\overline{N}.$$

5. 设 G 是一个群,又 $H_1\leqslant G$, $H_2\trianglelefteq G$, $N\trianglelefteq G$.证明:如果$|H_1|$以及$|H_2|$与$(G:N)$均有限,且

$$(|H_i|,(G:N))=1\quad(i=1,2).$$

则 $H_1H_2\leqslant N$.

证 因为由群第二同构定理知:

$$H_i/(H_i\cap N)\cong H_iN/N\leqslant G/N\quad(i=1,2),$$

故$(H_iN: N)=(H_i: H_i\cap N)$整除$(G: N)$.又由 Lagrange 定理知:

$$|H_i|=|H_i\cap N|(H_i: H_i\cap N),$$

从而$(H_iN: N)$也整除$|H_i|$.因此,$(H_iN: N)$整除$(|H_i|,(G: N))=1$.这只有$(H_iN: N)=1$,即 $H_iN=N$,从而 $H_i\leqslant N$,$H_1H_2\leqslant N$.

6. 设 G是群,$N\vartriangle G$.如果当 $N\leqslant H\vartriangle G$时必有 $N=H$,则称 N 是 G 的一个<u>极大正规子群</u>.证明:

$$N \text{ 是 } G \text{ 的极大正规子群} \Longleftrightarrow G/N \text{ 是单群}.$$

证　设φ是群 G 到商群 G/N 的自然同态.

1) 设 N 是 G 的极大正规子群,下证:G/N 是单群.

任取 $K/N\trianglelefteq G/N$,且 $K/N\neq\{N\}$,则

$$\varphi^{-1}(K/N)\trianglelefteq G.$$

因为 $N\in K/N$,而φ是自然同态,故$\varphi^{-1}(N)=N$,从而

$$N\subseteq\varphi^{-1}(K/N).$$

又因为 $K/N\neq\{N\}$,故 $N\neq\varphi^{-1}(K/N)$,即

$$N\subset\varphi^{-1}(K/N).$$

但 N 是群 G 的极大正规子群,因此

$$\varphi^{-1}(K/N)=G.\quad 故\ K/N=G/N.$$

即 G/N 只有平凡正规子群,从而为单群.

2) 设 G/N 是单群.下证:N 是 G 的极大正规子群.

设 $N\subset K\trianglelefteq G$,则

$$\varphi(K)\trianglelefteq G/N.$$

但因 $N\subset K$,故$\varphi(K)\neq\{N\}$;又因 G/N 是单群,故

$$\varphi(K)=G/N.$$

任取 $a\in G$,由于$\varphi(K)=G/N=\varphi(G)$,故存在 $k\in K$ 使

$$\varphi(a)=\varphi(k),\quad \varphi(ak^{-1})=N,$$

从而 $ak^{-1}\in\operatorname{Ker}\varphi=N\subset K$,故 $a=ak^{-1}\cdot k\in K$,$G\subseteq K$.于是 $K=G$.即 N 是 G 的极大正规子群.

§5 群的自同构群

一、主要内容

1. 群的自同构群、内自同构群以及特征子群和全特征子群的定义和例子.

1) 群 G 的全体自同构关于变换的乘法作成一个群,称为 G 的自同构群,记为 Aut G.

2) 群 G 的全体内自同构

$$\sigma_a: x \longrightarrow axa^{-1} \quad (\forall\ x, a \in G)$$

作成 Aut G 的一个正规子群,称为 G 的内自同构群,记为 Inn G.

3) 设 $N \leqslant G$.若对群 G 的每个自同构 σ 都有

$$\sigma(N) \subseteq N,$$

则称 N 是 G 的一个特征子群.

4) 若对群 G 的每个自同态 Ψ 都有

$$\Psi(N) \subseteq N,$$

则称子群 N 为群 G 的一个全特征子群.

2. 群 G 的内自同构群 Inn G 与自同构群 Aut G 和其中心 C 间有以下重要关系:

$$G/C \cong \text{Inn } G \trianglelefteq \text{Aut } G.$$

二、释疑解难

1. 教材中曾经指出,要从已知群定出其自同构群,一般而言,是非常困难的,这由教材中所举出的例子即可说明这一点.但是,对有些群却可定出其自同构群的一些性质,就本教材而言,主要有:

1) 定理 2 指出,从循环群可定出其自同构群的阶.

2）从教材本节例 1 和上节例 2 知：

$$\mathrm{Aut}\ K_4 \cong S_3 \cong S_4 / K_4 .$$

从而 Klein 四元群 K_4 的自同构群是非常清楚的，它是一个 6 阶非交换群，而且其元素的阶以及子群和正规子群的状况都很清楚.

3）本节习题第 6 题指出，无中心群的自同构群仍是一个无中心群，从而由教材第二章 §6 定理 6 可知，当 $n\geqslant 3$ 时，S_n 的自同构群是一个无中心群.

2. 群 G 中元素 a 与 b 确定同一个内自同构（即 $\sigma_a=\sigma_b$）的充要条件是：

$$aC=bC \quad (a^{-1}b\in C).$$

即 a 与 b 在同一个（关于 C 的）陪集中.因此，有多少个关于 C 的陪集就有多少个 G 的内自同构，即 $|\mathrm{Inn}\ G|=(G:C)$.其实这一点也是同构 $\mathrm{Inn}\ G\cong G/C$ 的直接结果，即

$$|\mathrm{Inn}\ G|=|G/C|=(G:C).$$

3. 群 G 的自同构群显然是 G 上对称群 $S(G)$（G 的全体双射变换关于变换乘法作成的群）的一个子群，即

$$\mathrm{Aut}\ G\leqslant S(G).$$

从而可知，当 $|G|=n$ 时，$\mathrm{Aut}\ G\leqslant S_n$.于是

$$|\mathrm{Aut}\ G| \,\Big|\, n!.$$

进一步，由于群的每个自同构都保持单位元 e 不变，因此，实际上更有

$$\mathrm{Aut}\ G\leqslant S_{n-1}. \quad 从而\ |\mathrm{Aut}\ G| \,\Big|\, (n-1)!.$$

4. 由于

$$全特征子群\subset 特征子群\subset 正规子群,$$

故特征子群是一类特殊的正规子群，而全特征子群又是一类特殊的特征子群.

我们知道，正规子群是不可传递的，即正规子群的正规子群不一定是原群的正规子群.但是，对于特征子群和全特征子群来说，

却是可以传递的.即若 G_1 是群 G_2 的(全)特征子群,又 G_2 是群 G_3 的(全)特征子群,则 G_1 必是 G_3 的(全)特征子群.这个证明并不难,留给读者作为练习.

三、习题 3.5 解答

1. 证明:阶数≤7 的循环群的自同构群都是循环群.

证 由定理 2 知,n 阶循环群的自同构群是一个$\varphi(n)$阶群,然而

$$\varphi(1)=\varphi(2)=1,\quad \varphi(3)=\varphi(4)=\varphi(6)=2,$$

故 1、2、3、4、6 阶循环群的自同构群显然都是循环群.

5 阶循环群$\langle a\rangle$ 的自同构群是一个$\varphi(5)=4$ 阶群.但易知

$$\tau:\ x\longrightarrow x^3\quad (\forall\ x\in\langle a\rangle)$$

是$\langle a\rangle$ 的一个自同构,且$|\tau|=4$.即 4 阶群中有 4 阶元,故 5 阶循环群的自同构群也是一个循环群.

7 阶循环群$\langle b\rangle$ 的自同构群是一个$\varphi(7)=6$ 阶群.但易知

$$\sigma:\ x\longrightarrow x^5$$

是$\langle b\rangle$ 的一个自同构,且$|\sigma|=6$.即 6 阶群中有 6 阶元,故 7 阶循环群的自同构群也是一个循环群.

注 问:8 阶循环群的自同构群是循环群吗? 它与 Klein 四元群有何关系? (可参阅习题 4.12 第 16 题)

2. 证明:非交换群的自同构群不能是循环群.

证 设 G 是一个非交换群,Aut G 是 G 的自同构群,Inn G 是 G 的内自同构群,则由定理 4 知,

$$G/C\cong \mathrm{Inn}\ G,$$

其中 C 为群 G 中心.但由于 G 是非交换群,由习题 3.2 第 6 题知,G/C 不是循环群,从而 Inn G 不是循环群.由于循环群的子群是循环群,因此,Aut G 不是循环群.

3. 证明:若群 G 的自同构群是一个单位元群(即 G 只有恒等自同构),则 G 必为交换群且每个元素都满足方程 $x^2=e$.

证　因为$|\mathrm{Aut}\ G|=1$，从而$|\mathrm{Inn}\ G|=1$．但由定理4，

$$\mathrm{Inn}\ G\cong G/C\quad(C\text{为}G\text{的中心}),$$

从而$|G/C|=1$．故$G=C$是交换群．据此又易知

$$\tau:\ a\longrightarrow a^{-1}\quad(\forall a\in G)$$

是群G的自同构，从而τ是G的恒等自同构．于是对G中任意元a都有$a^{-1}=a$，即$a^2=e$，得证．

4. 证明：任何非交换单群G必与其内自同构群$\mathrm{Inn}\ G$同构．

证　因为中心$C\trianglelefteq G$，而G是非交换单群，故只有$C=\{e\}$．从而由定理4知：

$$\mathrm{Inn}\ G\cong G/C\cong G.$$

因此，$G\cong\mathrm{Inn}\ G$．

5. 设N是群G的一个子群．证明：N是G的特征子群，当且仅当对G的每个自同构σ都有$\sigma(N)=N$．

证　若对G的每个自同构σ都有$\sigma(N)=N$，当然$\sigma(N)\subseteq N$，故N是G的特征子群．

反之，设N是G的一个特征子群，而σ是G的任一自同构，则有$\sigma(N)\subseteq N$．又因σ^{-1}也是G的自同构，故又有

$$\sigma^{-1}(N)\subseteq N,\quad \sigma[\sigma^{-1}(N)]\subseteq\sigma(N).$$

从而$N\subseteq\sigma(N)$．因此，$\sigma(N)=N$．

6. 证明：若G是一个无中心群，则其自同构群$\mathrm{Aut}\ G$也是一个无中心群．

证　任取$\tau\in\mathrm{Aut}\ G$，但τ不是恒等自同构，则有$a\in G$使

$$\tau(a)=b\neq a,$$

如果τ属于$\mathrm{Aut}\ G$的中心，则τ必与群G的每个自同构可换，从而与G的内自同构σ_a可换：

$$\tau\sigma_a=\sigma_a\tau,$$

于是对任意$x\in G$，令$x=\tau(y)$，则有

$$\tau\sigma_a(y)=\sigma_a\tau(y)\ \text{或}\ \tau(aya^{-1})=\sigma_a(x),$$

$$\tau(a)\tau(y)\tau(a)^{-1}=axa^{-1},$$

$$bxb^{-1}=axa^{-1},\ (a^{-1}b)x=x(a^{-1}b),$$

即 $a^{-1}b$ 是 G 的中心元素.但 G 是无中心群,故

$$a^{-1}b=e,\quad b=a,$$

矛盾.因此,Aut G 也是无中心群.

§6　共轭关系与正规化子

一、主要内容

1. 群中子集的共轭(特别是元素的共轭、子群的共轭)定义,和由此得到的共轭子集类(特别是共轭元素类和共轭子群类)以及群的类等式等概念.

2. 正规化子 $N(S)$ 与中心化子 $C(S)$ 的定义和性质.其性质有:

$$N(S)\leqslant G,\quad H\leqslant N(H),\quad C(H)\trianglelefteq N(H).$$

其中 S 是群 G 的子集,而 $H\leqslant G$.

3. 正规化子的作用(刻画一个共轭类中成员的个数)和一个应用(Cauchy 定理:pn 阶群有 p 阶子群).

二、释疑解难

1. 二元素是否共轭同此二元素所在的群的范围有关.就是说,设

$$a,b\in H\leqslant G,$$

则若 a 与 b 在 H 中共轭,当然在 G 中一定共轭;但是,当 a 与 b 在 G 中共轭时,则在 H 中不一定共轭.

例 1　交代群 A_4 中的元素(123)与(132)在 S_4 中共轭,因为有 $(12)\in S_4$ 使

$$(12)(123)(12)^{-1}=(132);$$

但是在 A_4 中不共轭,因为易知 A_4 有 4 个共轭类:

$\{(1)\}$, $\{(12)(34),(13)(24),(14)(23)\}$,
$\{(123),(134),(142),(243)\}$, $\{(132),(143),(124),(234)\}$.
从而可知,(123)与(132)在 A_4 中不共轭.

另外,群 S_4(参考习题 3.9 第 30 题)及 A_4 的类等式分别为:

$$|S_4| = 1+3+6+6+8,\quad |A_4| = 1+3+4+4.$$

2. 群的类等式有很多应用,教材中本节定理 3 (Cauchy 定理)的证明就是一个例子.下面再举一例.

例 2 证明:交代群 A_4 没有 6 阶子群.

证 反证法.设若 A_4 有 6 阶子群 H,则$(A_4: H)=2$.从而 H 是 A_4 的正规子群.但是,

H 是 A_4 的正规子群 $\Longleftrightarrow$ H 是 A_4 的若干个共轭类的并

(一般也成立,读者自证)而 A_4 的类等式为

$$|A_4| = 1+3+4+4,$$

由于 4 个数 1,3,4,4 中任几个的和也不会是 6,矛盾.因此,A_4 无 6 阶子群.

3. 若 $H\leqslant G$,则必 $H\subseteq N(H)$ (实际是 $H \trianglelefteq N(H)$).但是,对群 G 的子集 S 却不一定有 $S\subseteq N(S)$.

例 3 子集 $S=\{(12),(13)\}\subset S_3$.但易知

$$N(S)=\{(1),(23)\}.\quad 故\ S\not\subseteq N(S).$$

此外还有 $S\not\subseteq C(S)=\{(1)\}$.即使 S 是子群也不一定有 $S\subseteq C(S)$.

例如,$H=\{(1),(123),(132)\}\leqslant S_3$,但易知 $C(H)=\{(1)\}$,故

$$H\not\subseteq C(H).$$

另外应注意,教材定理 6 指出:$C(H)\trianglelefteq N(H)$,其中 H 是子群.其实对群的任何非空子集 S 均有 $C(S)\trianglelefteq N(S)$.因为定理 6 的证明并未用到 H 是子群的条件.这一点教材也明确指出来了.之所以定理 6 假设 H 是子群,是因为今后遇到最多的是这种情况.

4. 对任二共轭的有限子群来说,由于二者包含的元素个数相等,当然不可能其中一个是另一个的真子群.但对无限子群来说,

这种情况却可能发生.

例 4 令 $G=S(\mathbf{Z})$,即整数集 $\mathbf{Z}$ 上的对称群.再令

$$M=\{(12),(23),\cdots,(n,n+1),\cdots\}\subset S(\mathbf{Z}),\quad H=\langle M\rangle.$$

现在取 G 中元素

$$a=(\cdots,-k,\cdots,-2,-1,0,1,2,\cdots,k,\cdots),$$

则易知:$a(n,n+1)a^{-1}=(n+1,n+2)$(其中 n 为正整数).从而

$$aHa^{-1}\subseteq H.$$

但是,$(12)\notin aHa^{-1}$,故 $aHa^{-1}\subset H$.即 H 的共轭子群 aHa^{-1} 是 H 的真子群.

三、习题 3.6 解答

1. 试分别写出四次单位根乘群 U_4 和四次对称群 S_4 的类等式.并说明理由.

解 略.

2. 证明:群中子集的共轭关系是一个等价关系.

证 略.

3. 证明:

1) 若 C_1,C_2 是群 G 的两个共轭元素类,则乘积 C_1C_2 是 G 的一些共轭元素类的并集;

2) 若 C_1 是群 G 的一个共轭元素类,则 $C_1^{-1}=\{x^{-1}\mid x\in C_1\}$,更一般地 C_1^m(m 为任意整数)也是 G 的一个共轭元素类.

证 1) 任取 $x\in C_1C_2$,则令

$$x=x_1x_2,\quad 其中\ x_1\in C_1,\ x_2\in C_2.$$

若群 G 中元素 y 与 x 共轭,且设

$$x=aya^{-1},\quad 其中\ a\in G.$$

因为 C_1,C_2 都是 G 的共轭元素类,故

$$a^{-1}x_1a\in C_1,\quad a^{-1}x_2a\in C_2.$$

于是有

$$y=a^{-1}xa=a^{-1}(x_1x_2)a=a^{-1}x_1a\cdot a^{-1}x_2a\in C_1C_2.$$

即凡与 C_1C_2 中元素共轭的元素必属于 C_1C_2 .因此, C_1C_2 是 G 中一些共轭元素类的并集.

注　应留意,但不能证明 C_1C_2 中任二元素必共轭.

2) 任取 $x, y\in C_1^m$,并令

$$x = x_1^m,\quad y = y_1^m,\quad 其中\ x_1, y_1\in C_1 .$$

由于 C_1 是 G 的一个共轭元素类,故有 $b\in G$ 使 $x_1 = by_1b^{-1}$.从而有

$$x_1^m = (by_1b^{-1})^m = by_1^mb^{-1} .$$

即 $x = byb^{-1}$.亦即 C_1^m 中任二元素必共轭.

其次,设 $x\in C_1^m$, $x = x_1^m$ ($x_1\in C_1$) 且 x 与 y 共轭,令 $x = CyC^{-1}$ ($C\in G$) .则因 C_1 是共轭元素类,故

$$y = C^{-1}xC = C^{-1}x_1^mC = (C^{-1}x_1C)^m\in C_1^m .$$

即凡与 C_1^m 中元素共轭的元素都属于 C_1^m .

因此, C_1^m 是群 G 的一个共轭元素类.

特别,当 $m = -1$ 时即得 C_1^{-1} 是 G 的一个共轭元素类.

4. 设 a 是群 G 的一个元素.证明:

$$\langle a\rangle \trianglelefteq N(a)\leqslant N(\langle a\rangle) .$$

证　显然 $\langle a\rangle\subseteq N(a)$.又对任意 $x\in N(a)$ 有

$$xa^mx^{-1} = a^m\in\langle a\rangle ,\quad 故\ \langle a\rangle \trianglelefteq N(a) .$$

又显然 $N(a)\subseteq N(\langle a\rangle)$,故 $N(a)\leqslant N(\langle a\rangle)$.因此

$$\langle a\rangle \trianglelefteq N(a)\leqslant N(\langle a\rangle) .$$

5. 证明: S_n 的所有对换构成一个共轭类.

证　任取 S_n 中的一个对换 (ij) ,而 $\pi(ij)\pi^{-1}$ 为与 (ij) 共轭的任意一个置换,其中 π 是一个 n 次置换,则由第二章 § 6 定理 5 知,

$$\pi(ij)\pi^{-1} = (\pi(i)\pi(j))$$

也是 S_n 的一个对换.

反之,设 (ij) 与 (st) 为 S_n 的任两个对换,则任取 S_n 中一个置换 π 使 $\pi(i) = s, \pi(j) = t$ (显然这样的置换是存在的),则

$$\pi(ij)\pi^{-1} = (\pi(i)\pi(j)) = (st) ,$$

即(ij)与(st)共轭.因此,S_n的全体对换作成一个共轭类.

注　由于S_n中对换的个数显然就是n个元素中每取两个的组合数(因为$(ij)=(ji)$),故由此可知S_n共有

$$C_n^2=\frac{n(n-1)}{2}$$

个对换.

6. 设G是有限群,且$H<G$.证明:

$$G\neq\bigcup_{x\in G}xHx^{-1}.$$

证　因G是有限群,故可设$(G:N(H))=k$,且由推论2知

$$x_1Hx_1^{-1},\quad x_2Hx_2^{-1},\quad\cdots,\quad x_kHx_k^{-1}$$

是与H共轭的全部子群,从而$\bigcup_{x\in G}xHx^{-1}=\bigcup_{1}^{k}x_iHx_i^{-1}$.

设若$G=\bigcup_{x\in G}xHx^{-1}$,则由于$H<G$,故$k>1$且由于

$$H\leqslant N(H),$$

从而有

$$|G|=\left|\bigcup_{x\in G}xHx^{-1}\right|=\left|\bigcup_{1}^{k}x_iHx_i^{-1}\right|$$
$$<k|H|\leqslant(G:N(H))\cdot|N(H)|=|G|,$$

矛盾.因此,$\bigcup_{x\in G}xHx^{-1}\subset G$,即二者不能相等.

*§7　群的直积

一、主要内容

1. 群的外直积和内直积的定义与关系.

2. 群G是n个子群$G_1,G_2,\cdots,G_n$的内直积的充要条件;n阶循环群是s个阶为$p_i^{k_i}$的循环群的直积,其中

$$n=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s},\quad p_1,\cdots,p_s\text{ 为互异素数}.$$

3. 可分解群与不可分解群的定义和例子.

1) n次对称群、有理数加群和无限循环群都是不可分解群.

2) n阶循环群是不可分解群 $\Longleftrightarrow$ n为素数的方幂.

二、释疑解难

1. 群的内直积在不同的书中常有不同的表述形式.常见的大体上有以下四种形式,分别称其为定义 1,2,3,4.

定义 1 称群 G 为其子群 $G_1, G_2, \cdots, G_n$ 的(内)直积,若

1) $G_i \trianglelefteq G, \quad i=1,2,\cdots,n$;

2) $G=G_1G_2\cdots G_n$;

3) $G_1G_2\cdots G_{i-1}\cap G_i=e$[①], $\quad i=2,3,\cdots,n$.

定义 2 称群 G 为其子群 $G_1, G_2, \cdots, G_n$ 的(内)直积,若

1) $G=G_1G_2\cdots G_n$;

2) G中每个元素表为 $G_1, G_2, \cdots, G_n$ 中元素之积是惟一的;

3) G_i 中元素与 $G_j\,(i\neq j)$中元素可换.

定义 3 称群 G 为其子群 $G_1, G_2, \cdots, G_n$ 的(内)直积,若

1) $G_i \trianglelefteq G, \quad i=1,2,\cdots,n$;

2) $G=G_1G_2\cdots G_n$;

3) G中每个元素表为 $G_1, G_2, \cdots, G_n$ 中元素之积是惟一的.

定义 4 称群 G 为其子群 $G_1, G_2, \cdots, G_n$ 的〈内〉直积,若

1) $G=G_1G_2\cdots G_n$;

2) $G_1G_2\cdots G_{i-1}G_{i+1}\cdots G_n\cap G_i=e, \quad i=2,3,\cdots,n$;

3) G_i 中元素与 G_j 中元素可换$(i\neq j)$.

当然,以上四种定义是等价的.教材采用定义 1,而把定义 2 作为等价的定理,即定理 3.

应注意,定义 1 中的条件 2)、3)或定义 2 中的条件 1)、2)或定义 3 中的条件 2)、3)或定义 4 中的条件 1)、2),均可合并为一个条

① 与教材保持一致,一个是只由单位元 e 作成的子群$\{e\}$,简记为 e.

件如下:

4) G 中每个元素都可惟一地表为 $G_1, G_2, \cdots, G_n$ 中元素之积.

另外,定义 1 中的条件 3)与定义 4 中的条件 2)也可互相代替.

证明如下:

任取 $x \in G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_n \cap G_i$,则

$$x \in G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_n, \quad x \in G_i .$$

令 $x = x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_n (x_j \in G_j)$. 由于教材已证明定义 1 与定义 2 等价,故得

$$e = x_1 x_2 \cdots x_{i-1} x^{-1} x_{i+1} \cdots x_n .$$

由于元素表示法惟一,故 $x^{-1} = e, x = e$. 即定义 4 的条件 2)成立.

反之,由定义 4 也可推出定义 1 中的条件 3).

2. 群直积的重要意义.

1) 利用直积,可以由已知的群构造出一些新的群.

2) 反过来,如果一个群 G 可以分解成一些(正规)子群的直积,那么群 G 的结构决定于每个直积因子的结构.只要每个直积因子研究清楚了,那么群 G 也就清楚了.例如,教材本章 §9 指出,有限交换群就是一类研究清楚了的群类,因为有限交换群基本定理指出:每个阶大于 1 的有限交换群都可惟一地分解为素幂阶循环群的直积.而素幂阶循环群是完全清楚的一类群.

3) 再举一个简单例子说明这个问题.

例 1　设 G 是一个阶大于 1 的有限群,且每个元素都满足方程 $x^2 = e$. 则

$$G \cong C_2 \times C_2 \times \cdots \times C_2 .$$

其中 C_2 为 2 阶循环群.

证　由习题 2.1 第 6 题知, G 是一个交换群且其中除 e 外每个元素的阶均为 2. 因此, G 中每个元素 $a = a^{-1}$.

现在假设 $a_1, a_2, \cdots, a_n$ 为 G 的一个元素个数最少的生成系.于是 G 中每个元素都可表示成

$$a_1^{s_1} a_2^{s_2} \cdots a_n^{s_n} \quad (s_i = 0 \text{ 或 } 1).$$

而且这种表示法是惟一的.因若

$$a_1^{s_1} a_2^{s_2} \cdots a_n^{s_n} = a_1^{t_1} a_2^{t_2} \cdots a_n^{t_n} \quad (t_i = 0 \text{ 或 } 1),$$

不妨假设 $s_1 \neq t_1$,则 $a_1^{t_1 - s_1} = a_2^{s_2 - t_2} a_3^{s_3 - t_3} \cdots a_n^{s_n - t_n}$.从而可知 a_2, a_3,…,a_n 也是 G 的一个生成系.这与 a_1,a_2,…,a_n 是元素个数最少的生成系矛盾.

又由于 $|G| > 1$,故 a_1,a_2,…,a_n 中不能有 e.即每个 a_i 都是 2 阶元.从而 $\langle a_i \rangle \cong C_2$.因此

$$G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle \cong C_2 \times C_2 \times \cdots \times C_2.$$

由此顺便得出这种群的阶 $|G| = 2^n$.

这就是说,研究这种群可转化为研究 2 阶循环群.因此这种群完全在我们的掌握之中.

3. 定理 5 说明,完全可分解群的任何正规子群都是其直积因子.但这一结论对非完全可分解群不再成立.

例 2　三次对称群 S_3 是不可分解群,当然就不是完全可分解群.S_3 的非平凡正规子群只有

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

它当然不是群 S_3 的直积因子.

例 3　设 $G = \langle a \rangle$ 为 12 阶循环群.它是交换群,从而每个子群都是正规子群.但是,其非平凡子群共有 4 个:

$$H_2 = \{e, a^6\}, \qquad H_3 = \{e, a^4, a^8\},$$

$$H_4 = \{e, a^3, a^6, a^9\}, \qquad H_6 = \{e, a^2, a^4, a^6, a^8, a^{10}\}.$$

$H_2 \trianglelefteq G$,但是 H_2 显然不是 G 的直积因子,因为

$$H_2 \cap H_6 = H_2 \neq e.$$

4. 一个群不是可分解群就必然是不可分解群.另外,不要误认为不可分解群就一定简单,而可分解群就一定复杂.例如,n 次对称群、有理数加群和无限循环群等都是不可分解群,但它们并不比可分解群例如 C_6,C_{10},C_{15}(6,10,15 阶循环群)简单.

5. 直积的概念也可以推广到任意个群上去.

设 Ω 为任一指标集(有限或无限、可数或不可数), G_i (对每个 $i\in\Omega$) 为群.则加氏积

$$G=\{(\cdots,a_i,\cdots)\mid i\in\Omega\}$$

对运算

$$(\cdots,a_i,\cdots)(\cdots,b_i,\cdots)=(\cdots,a_ib_i,\cdots)$$

作成一个群,称为一切群 G_i $(i\in\Omega)$ 的(外)直积.记为

$$G=\prod_{i\in\Omega}G_i.$$

当 Ω 有限时,就得到教材中所说的直积.

6. 当 $G_1, G_2, \cdots, G_n$ 为交换群且代数运算用加号表示(即每个 G_i 都是加群)时,这时的“直积”称为“直和”,并用符号

$$G_1\oplus G_2\oplus\cdots\oplus G_n$$

表示.

三、习题 3.7 解答

1. 设群 $G=G_1\times G_2\times\cdots\times G_n$.证明:当 $i\neq j$ 时,

$$G_i\cap G_j=e.$$

证　因为 $i\neq j$,不妨设 $i<j$.则由 $G=G_1\times G_2\times\cdots\times G_n$ 得

$$G_i\cap G_j\subseteq G_1G_2\cdots G_i\cdots G_{j-1}\cap G_j=e.$$

故 $G_i\cap G_j=e$.

2. 证明:定理 3 中的“每个元素表示法惟一”可改为“单位元表示法惟一”.

证　若每个元素表示法惟一,则当然单位元表示法惟一.反之,若单位元表示法惟一,任取 $a\in G$,令

$$a=a_1a_2\cdots a_n=b_1b_2\cdots b_n\quad(a_i,b_i\in G_i).$$

则 $e=a_1b_1^{-1}\cdot a_2b_2^{-1}\cdot\cdots\cdot a_nb_n^{-1}$,其中 $a_ib_i^{-1}\in G_i$.但因 e 表示法惟一,故

$$a_ib_i^{-1}=e,\quad a_i=b_i\quad(i=1,2,\cdots,n).$$

即 G 中任何元素都表示法惟一.

3. 设群 $G=G_1\times G_2$, $G=G_1\times G_2$. 证明：$G_1\cong G_1$.

证 因为 $G=G_1\times G_2=G_1\times G_2$，故由后面第 6 题知：

$$G_1\cong G/G_2,\quad G/G_2\cong G_1.$$

从而 $G_1\cong G_1$.

4. 设群 $G=G_1\times G_2\times\cdots\times G_n$. 证明：

$$\varphi_i: a_1a_2\cdots a_n\longrightarrow a_i\quad(a_i\in G_i)$$

是群 G 到 G_i 的满同态.

证 因为是直积，群中每个元素表示法惟一，故显然 φ_i 是群 G 到群 $G_i(i=1,2,\cdots,n)$ 的满射.

又因为是直积，G_i 与 $G_j(i\neq j)$ 中元素相乘可以交换，从而

$$\begin{aligned}&\varphi_i(a_1a_2\cdots a_i\cdots a_n\cdot b_1b_2\cdots b_i\cdots b_n)\\&=\varphi_i(a_1b_1\cdot a_2b_2\cdot\cdots\cdot a_ib_i\cdot\cdots\cdot a_nb_n)=a_ib_i\\&=\varphi_i(a_1a_2\cdots a_n)\cdot\varphi_i(b_1b_2\cdots b_n)\quad(a_i,b_i\in G_i).\end{aligned}$$

故 $G\sim G_i$.

5. 设 G_1, G_2 是两个群. 证明：$G_1\times G_2\cong G_2\times G_1$.

证 由于是直积，元素表示法惟一，故易知

$$\varphi: a_1a_2\longrightarrow a_2a_1\quad(a_i\in G_i)$$

是 $G_1\times G_2$ 到 $G_2\times G_1$ 的同构映射，因此，$G_1\times G_2\cong G_2\times G_1$.

6. 设群 G 是其子群 G_1 与 G_2 的直积，即

$$G=G_1\times G_2.$$

证明：$G/G_1\cong G_2$，$G/G_2\cong G_1$.

证 因为 $G=G_1\times G_2$，故

$$G/G_1=\{aG_1\mid a\in G_2\}.$$

现定义：$\varphi: G/G_1\longrightarrow G_2,\quad aG_1\longrightarrow a$.

由 $G_1\cap G_2=\{e\}$ 知，对 $aG_1, bG_1\in G/G_1\ (a,b\in G_2)$ 有

$$\begin{aligned}aG_1=bG_1&\Longleftrightarrow a^{-1}b\in G_1\Longleftrightarrow a^{-1}b\in G_1\cap G_2\\&\Longleftrightarrow a^{-1}b=e\Longleftrightarrow a=b.\end{aligned}$$

又因为

$$\varphi(aG_1\cdot bG_1)=\varphi(abG_1)=ab=\varphi(aG_1)\varphi(bG_1),$$

故 φ 为同构映射，因此 $G/G_1 \cong G_2$.

同理可证，$G/G_2 \cong G_1$.

注　本题也可利用同构定理证明，即

$$G/G_1 = G_1G_2/G_1 \cong G_2/G_1 \cap G_2 = G_2/\{e\} \cong G_2.$$

7. 设群 $G = G_1 \times G_2$，且 $N \trianglelefteq G_1$. 证明：$N \trianglelefteq G$.

证　任取 $x \in G$，则由 $G = G_1 \times G_2$ 知，存在 $x_1 \in G_1$，$x_2 \in G_2$，使 $x = x_1x_2 = x_2x_1$，且由于 $N \trianglelefteq G_1$，故有

$$x_2N = Nx_2.$$

再由 $N \trianglelefteq G_1$ 知，$x_1N = Nx_1$，故

$$xN = (x_1x_2)N = x_1Nx_2 = N(x_1x_2) = Nx,$$

即 $N \trianglelefteq G$.

8. 设 $G_1, G_2, \cdots, G_n$ 是群 G 的正规子群且 $G = G_1G_2\cdots G_n$. 证明：

$$G_1G_2\cdots G_{i-1} \cap G_i = e \Longleftrightarrow G \text{ 中每个元素表示法惟一}.$$

证　设 $G_1G_2\cdots G_{i-1} \cap G_i = e$，　$i = 2, 3, \cdots, n$，又 $a \in G$ 且

$$a = a_1a_2\cdots a_n = b_1b_2\cdots b_n \quad (a_j, b_j \in G_j). \tag{1}$$

如果 a 的表示法不惟一，设 $a_i \neq b_i$，$a_{i+1} = b_{i+1}$，$\cdots$，$a_n = b_n$. 但由于 $G_j \trianglelefteq G$，故 $G_1G_2\cdots G_{i-1} \trianglelefteq G$，从而由(1)可得

$$(b_1\cdots b_{i-1})^{-1}(a_1\cdots a_{i-1}) = b_ia_i^{-1} \in G_1\cdots G_{i-1} \cap G_i = e.$$

从而 $b_ia_i^{-1} = e$，$a_i = b_i$，矛盾.

反之，设 G 中每个元素表示法惟一，令

$$x_i = x_1x_2\cdots x_{i-1} \in (G_1G_2\cdots G_{i-1} \cap G_i),$$

其中 $x_j \in G_j$. 则得 $e = x_1x_2\cdots x_{i-1}x_i^{-1}$. 从而

$$x_1 = x_2 = \cdots = x_{i-1} = x_i^{-1} = e, \quad x_i = e.$$

即 $G_1G_2\cdots G_{i-1} \cap G_i = e$. 得证.

注　这里每个 G_i 都必须是正规子群. 否则，例如三次对称群 S_3 的子群

$$G_1 = \{(1), (12)\}, G_2 = \{(1), (13)\}, G_3 = \{(1), (23)\},$$

有 $S_3 = G_1G_2G_3$ 且

$$G_1 \cap G_2 = G_1 G_2 \cap G_3 = e,$$

但 S_3 中元素表示方法不惟一.

* §8 Sylow 定理

一、主要内容

1. Sylow p-子群和重陪集定义,以及一个群关于两个子群的重陪集分解的概念.

2. 三个 Sylow 定理.设 $|G| = p^s m$ (p 是素数, $p\nmid m$)

1) 第一 Sylow 定理(存在性和包含性). 对群 G 的每个 $p^i(i=0,1,\cdots,s-1)$阶子群 H,总有 G 的 p^{i+1} 阶子群 K 存在使 $H \trianglelefteq K$.从而 G 有 Sylow p-子群.

2) 第二 Sylow 定理(共轭性). 群 G 的所有 Sylow p-子群恰好是 G 的一个共轭子群类.

3) 第三 Sylow 定理(计数定理). 若群 G 的 Sylow p-子群共有 k 个,则

$$k \mid |G|, \quad 且 \quad p \mid k-1.$$

3. p-群定义和有限群是 p-群的充要条件.

二、释疑解难

1. 三个 Sylow 定理对于 Sylow p-子群的讨论相当详尽和完美.从其存在性、相互关系以及计数都给予了完满而彻底的回答.在群论中,对一个问题的研究能得到如此圆满解决虽然也有一些,但为数并不太多.特别是,由 Sylow 定理还可以推演出关于群的一些重要结论.就本教材来说,至少有以下四点:

1) pq (p,q 是互异素数) 阶群当 $p\nmid q-1$ 且 $q\nmid p-1$ 时,必为循环群.

由此可知,凡阶为 15,33,35,51,65,69,…的群都是循环群.

此前我们曾经证明了:pq 阶交换群必为循环群;又当 $p<q$ 时,pq 阶群 G 有惟一的 q 阶正规子群,从而不是单群.但对其 p 阶子群的状况由第三 Sylow 定理可知:若其 p 阶子群(它就是 G 的 Sylow p-子群)的个数为 k,则

$$k \Bigm| |G| = pq, \quad 且 \quad p \mid k-1.$$

由此易推知,只有 $k=1$ 或 q.当 $k=1$ 时,其 p 阶子群就是 G 的一个正规子群.也就是说,此时 G 要么有一个 p 阶正规子群,要么有 q 个 p 阶子群.例如,$6=2\cdot 3$ 阶交换群(当然是循环群)有一个 2 阶(正规)子群,而 6 阶非交换群 S_3 有 3 个 2 阶子群,等等.

2) 利用 Sylow 定理还可以确定一些群是不是单群.例如,196 阶群、200 阶群都不是单群 (参考本节习题第 7 题及教材例 4);又 np (p 是素数且 $n<p$) 阶群不是单群 (参考习题第 2 题),从而可知凡 6,10,14,15,20,21,28,…阶群都不是单群.

3) 任何有限交换群都是其所有 Sylow 子群的直积.这使我们讨论有限交换群可以转化为讨论素幂阶交换群(或循环群).

4) 利用 Sylow 定理证明了:对有限交换群来说,Lagrange 定理的逆定理成立.这当然是一个很重要的结论.

2. 第二 Sylow 定理是说,有限群 G 的所有 Sylow p-子群恰好是一个共轭子群类.由于共轭子群必同构;又若一个子群与一个 Sylow p-子群同构,它必然也是一个 Sylow p-子群,因此,G 的所有 Sylow p-子群不仅是一个共轭子群类,而且也是一个同构子群类.

3. p-群有很多重要性质.例如:

1) 有限群 G 是 p-群 $\Longleftrightarrow$ $|G|$ 是 p 的方幂.

2) 阶大于 1 的有限 p-群的中心 $\supset \{e\}$.

3) p^2 阶群必为交换群.

4) 如果有限 p-群 G 只有一个指数为 p 的子群,则 G 必为循

环群.

5) p^n 阶群对每个 $i=1,2,\cdots,n-1$,都至少有一个 p^i 阶的正规子群.

三、习题 3.8 解答

1. 试求出四次交代群 A_4 的所有 Sylow 子群.

解 因为 $|A_4|=2^2\cdot 3$,故 A_4 有 Sylow 2-子群(阶为 4)和 Sylow 3-子群(阶为 3).

又因为 Klein 四元群

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

显然是 A_4 的一个 Sylow 2-子群,而 $K_4 \trianglelefteq S_4$,从而 $K_4 \trianglelefteq A_4$,故 K_4 是 A_4 的惟一的 Sylow 2-子群.

由 A_4 的一切 3-循环(阶为 3)生成的子群,显然是 A_4 的全部 Sylow 3-子群,共有 4 个,它们是:

$$\langle(123)\rangle,\ \langle(124)\rangle,\ \langle(134)\rangle,\ \langle(234)\rangle.$$

2. 设 G 是 np 阶群(p 是素数).证明:若 $n<p$,则 G 有 p 阶正规子群.

证 因为 $n<p$,故 G 的 Sylow p-子群是 p 阶循环群 C_p.设这样的子群共有 k_p 个,则由 Sylow 定理知:

$$k_p=ps+1,\quad k_p\mid np,\quad 即(ps+1)\mid np.$$

但因$(ps+1,p)=1$,故$(ps+1)\mid n$.又因 $n<p$,故必 $s=0$, $k_p=1$.因此对 G 中任何元素 a 都有 $aC_pa^{-1}=C_p$,从而 C_p 是 G 的 p 阶正规子群.

3. 设 G 是一个有限群,P 是 G 的一个 Sylow p-子群,H 是 G 的一个 p 子群.证明:若 $H\subseteq N(P)$,则 $H\subseteq P$.

证 因为 $H\subseteq N(P)$,故对任意 $a\in H$,都有 $aP=Pa$.从而 $HP=PH$,因此

$$HP\leqslant G \quad 且 \quad a^{-1}Pa=P.$$

现任意取 $ab\in HP(b\in P)$,由 $a^{-1}ba\in P$ 知,

$$(ab)^2 = abab = a^2(a^{-1}ba)b = a^2 b_1 b = a^2 b_2,$$

其中 $b_1 = a^{-1}ba, b_2 = b_1 b \in P$.再对 m 用归纳法易知

$$(ab)^m = a^m b_m \quad (b_m \in P). \qquad (1)$$

又因 H 为 p-子群,故 a 的阶为 p 的方幂 p^r,从而由(1)知:

$$(ab)^{p^r} = a^{p^r} b_0 = eb_0 = b_0 \in P.$$

同样,由 P 为 p-子群知 b_0 的阶为 p 的方幂,从而知 ab 的阶为 p 的方幂,即 HP 为 p-子群.但子群 $HP \supseteq P$,而 P 是 G 的 Sylow p-子群,所以必有 $HP = P$,于是 $H \subseteq P$.

4. 设 K 是群 G 的一个有限正规子群,P 是 K 的一个 Sylow p-子群.证明:$G = N(P)K$.

证 任取 $x \in G$,则由于 $P \leqslant K \trianglelefteq G$,故

$$xPx^{-1} \leqslant xKx^{-1} = K \quad (\forall\ x \in G).$$

但 P 是有限群 K 的一个 Sylow p-子群,故 xPx^{-1} 也是 K 的一个 Sylow p-子群.于是,由 Sylow 定理知,P 与 xPx^{-1} 在 K 中共轭.即有 $k \in K$ 使

$$xPx^{-1} = kPk^{-1}, \quad (k^{-1}x)P = P(k^{-1}x),$$

于是 $k^{-1}x \in N(P)$,从而

$$x \in K \cdot N(P), \quad G \subseteq K \cdot N(P), \quad G = K \cdot N(P).$$

又由于 $K \trianglelefteq G$ 及 $K \cdot N(P) = N(P)K$,因此

$$G = N(P)K.$$

5. 设 P 是有限群 G 的一个 Sylow p-子群.证明:若 G 有子群 H 包含 $N(P)$,则 $N(H) = H$.

证 因为 H 是子群,故 $H \subseteq N(H)$.下证 $N(H) \subseteq H$.

任取 $a \in N(H)$,则 $aH = Ha$ 或 $aHa^{-1} = H$.但是

$$P \trianglelefteq N(P) \subseteq H,$$

故
$$aPa^{-1} \subseteq aHa^{-1} = H.$$

从而 P 与 aPa^{-1} 也是 H 的 Sylow p-子群,因而由 Sylow 定理知,P 与 aPa^{-1} 在 H 中共轭,即存在 $h \in H$ 使

$$h(aPa^{-1})h^{-1}=P \text{ 或 } (ha)P(ha)^{-1}=P,$$

$$P(ha)=(ha)P.$$

因此,$ha\in N(P)$.但是 $N(P)\subseteq H$,$h\in H$,从而 $a\in H$,$N(H)\subseteq H$.故

$$N(H)=H.$$

6. 证明:有限群 G 必有一个最大的正规 p-子群 H.即 H 是 G 的正规 p-子群,又若 K 也是 G 的正规 p-子群,则必 $K\subseteq H$.

证 若 G 无阶数大于 1 的正规 p-子群,则显然 G 的单位元群就是 G 的最大正规 p-子群.

若 G 有阶数大于 1 的正规 p-子群,则 G 的一切正规子群之积仍为正规子群,且由下面第 8 题知,也是一个 p-子群.因此,它是 G 的最大正规 p-子群.

7. 证明:196 阶群 G 必有一个阶大于 1 的 Sylow 子群,它是 G 的一个正规子群.

证 由于 $|G|=196=2^2\cdot 7^2$,令 P 是 G 的一个 Sylow 7-子群,与其共轭的子群个数 $k=7q+1$ 应是 196 的因数.但 $196=2^2\cdot 7^2$ 的正因数只有 1,2,4,7,14,28,49,98,196,这只有 $q=0$,即 $k=1$.因此 P 是 G 的惟一的 Sylow p-子群.从而 P 是 G 的一个阶大于 1 的 Sylow 子群且是 G 的正规子群.

8. 设 H, K 是群 G(不一定有限)的两个 p-子群,且 $K\trianglelefteq G$.证明:HK 也是 G 的一个 p-子群.

证法 I 因为 $H\leqslant G$, $K\trianglelefteq G$,故 $HK\leqslant G$.又由群同构定理知:

$$H/(H\cap K)\cong HK/K.$$

但 H 为 p-子群,故 $H/(H\cap K)$ 为 p-子群,从而 HK/K 为 p-子群.任取 $a\in HK$,则 $aK\in HK/K$.设 aK 的阶为 p^s,则

$$a^{p^s}K=(aK)^{p^s}=K,\ a^{p^s}\in K.$$

但 K 也是 p-子群,设 a^{p^s} 的阶为 p^t,从而

$$\left(a^{p^s}\right)^{p^t}=a^{p^{s+t}}=e.$$

于是 a 的阶是 p 的方幂,即 HK 为 p-子群.

证法Ⅱ　由于 $H\leqslant G$, $K\trianglelefteq G$,故 $HK\leqslant G$.再任取 $hk\in K$,其中 $h\in H$, $k\in K$.由于 $K\trianglelefteq G$,故对 G 中任意元素 x 都有

$$Kx=xK. \tag{1}$$

因 H 是 p-子群,设 $|h|=p^s$,例如 $|h|=3$ 时,由(1)有

$$\begin{aligned}(hk)^3&=h(kh)(kh)k=h\cdot hk_1\cdot kh\cdot k=h^2(k_1k)h\cdot k\\&=h^2\cdot hk_2\cdot k=h^3\cdot k_3=k_3,\end{aligned}$$

其中 $k_1,k_2\in K$ 且 $k_3=k_2k\in K$.因此一般地有

$$(hk)^{p^s}=h^{p^s}k'=k'\in K.$$

但 K 也是 p-子群,设 $|k'|=p^t$,于是有

$$(hk)^{p^{s+t}}=(k')^{p^t}=e.$$

即 hk 的阶是 p 的方幂.因此,HK 也是 G 的 p-子群.

* §9　有限交换群

一、主要内容

1. 有限交换群基本定理:任何阶大于1的有限交换群 G,都可以惟一分解为素幂阶循环群的直积.

这些循环群的阶的全体,称为群 G 的初等因子组.

2. 有限交换群的不变因子定理:任何阶大于1的有限交换群 G,都可以惟一地分解为

$$G=\langle b_1\rangle\times\langle b_2\rangle\times\cdots\times\langle b_m\rangle,$$

其中 $|b_i|>1\,(i=1,2,\cdots,m)$ 且 $|b_i|\,\big|\,|b_{i+1}|\,(i=1,2,\cdots,m-1)$.

这些循环群的阶的全体,即$\{|b_1|,|b_2|,\cdots,|b_m|\}$称为群 G 的不变因子组.

3. 阶大于1的二有限交换群 G_1 与 G_2 同构的充要条件:

$$G_1\cong G_2\Longleftrightarrow \text{二者有相同的初等因子组}$$

$\Longleftrightarrow$ 二者有相同的不变因子组.

二、释疑解难

1. 有限交换群基本定理的逆定理显然成立.因此,该定理与其逆定理合起来可表述为:

群 G 可分解为素幂阶循环群的直积 $\Longleftrightarrow$ G 为有限交换群.

2. 交换群的基.

定义　设 $a_1, a_2, \cdots, a_m$ 是交换群 G 的一组元素.如果由

$$a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m} = e$$

必有

$$a_1^{k_1} = a_2^{k_2} = \cdots = a_m^{k_m} = e,$$

则称元素 $a_1, a_2, \cdots, a_m$ 是无关的.G 的一组无关的生成元称为 G 的一基.

交换群中元素无关很类似于域上线性空间中一组向量线性无关;交换群的基又类似于线性空间的基.特别是,当交换群的代数运算改用加号时,这种类似程度就更加接近.所不同的只是,普通所说的线性空间都是数域或域上的线性空间,而交换群则是整数环(系数是整数)上的“线性空间”,或者更正确地说,是整数环上的“模”.

教材定理 1 中的$\{a_1, a_2, \cdots, a_n\}$以及定理 3 中的$\{b_1, b_2, \cdots, b_m\}$都是各该交换群 G 的基.

3. 有限生成的交换群.

具有有限个生成元的交换群(不一定是有限群,例如无限循环群),称为有限生成的交换群.有限交换群是一种特殊的有限生成交换群.有限生成交换群有以下重要的结构定理:

有限生成交换群的基本定理:每一个有限生成的交换群 G 都可以惟一地分解为以下循环群的直积:

$$G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle \times \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_m \rangle,$$

其中 $n \geqslant 0, |a_i| = \infty$; $m \geqslant 0, |b_j|$ 均有限且 $|b_j| \mid |b_{j+1}|$ $(j = 1,$

$2, \cdots, m-1)$.

显然$\{a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_m\}$为群 G 的一基.

又当 $n=0$ 时,以上定理就变成教材中的定理 3 (不变因子定理).

4. 为什么把教材定理 1 (有限交换群基本定理)中的素数幂 $p_i^{a_i}$ $(i=1,2,\cdots,n)$ 叫做初等因子,而把定理 3 (不变因子定理) 中的$|b_j|$ $(j=1,2,\cdots,m)$ 叫做不变因子?

大概读者已经觉察到 (甚至已经完全明白) 关于有限交换群的初等因子、不变因子,同高等代数中λ-矩阵的初等因子和不变因子是何等的类似.在高等代数中,每个 $m\times n$ 的λ-矩阵 $A(\lambda)$ 都可经过初等变换化为惟一的标准形,标准形的主对角线上全体非零多项式就是 $A(\lambda)$ 的不变因子.次数大于零的不变因子的标准分解式中,全体不可约多项式的方幂就是 $A(\lambda)$ 的初等因子.关于λ-矩阵的初等因子和不变因子有以下基本而重要的事实:

1) 两个 $m\times n$ λ-矩阵等价的充要条件是,二者有相同的秩和初等因子.

2) 两个 $m\times n$ λ-矩阵等价的充要条件是,二者有相同的不变因子.

3) $A(\lambda)$ 的初等因子和不变因子都是惟一确定的.由 $A(\lambda)$ 的秩和初等因子可以求不变因子,反之由不变因子 (从理论上说) 也可求初等因子.

λ-矩阵按等价分类,而有限交换群按同构分类.二者相应的概念和联系,有以下对应关系:

λ-矩阵　　有限交换群

标准形——不变因子分解式

不变因子——不变因子

初等因子——初等因子

等价——同构

等价的充要条件——同构的充要条件.

三、习题 3.9 解答

1. 证明：对任意素数 $p_1, p_2, \cdots, p_m$ 和任意正整数 $k_1, k_2, \cdots, k_m$，总存在有限交换群，其初等因子组为：

$$\{p_1^{k_1}, p_2^{k_2}, \cdots, p_m^{k_m}\}. \tag{1}$$

证　令 $t_i = p_i^{k_i}\,(i=1,2,\cdots,m)$．则显然群

$$G = C_{t_1}\times C_{t_2}\times\cdots\times C_{t_m}$$

即为初等因子组是(1)的有限交换群．

2. 设 p 是素数．试给出同构意义下的所有 p^4 阶交换群．

解　因为 p^4 阶交换群的初等因子组共有五种，即

$$\{p^4\},\ \{p, p^3\},\ \{p^2, p^2\},\ \{p, p, p^2\},\ \{p, p, p, p\},$$

故互不同构的全部 p^4 阶交换群为：

$$C_{p^4},\ C_p\times C_{p^3},\ C_{p^2}\times C_{p^2},\ C_p\times C_p\times C_{p^2},\ C_p\times C_p\times C_p\times C_p.$$

3. 给出同构意义下的所有 108 阶交换群．

解　因为 $108 = 2^2\cdot 3^3$，故 108 阶交换群的初等因子组共有六种，即

$$\{2^2, 3^3\},\quad \{2^2, 3, 3^2\},\quad \{2^2, 3, 3, 3\},$$
$$\{2, 2, 3^3\},\quad \{2, 2, 3, 3^2\},\quad \{2, 2, 3, 3, 3\}.$$

因此相应地，得互不同构的全部 108 阶交换群共有六个，即

$$C_4\times C_{27},\quad C_4\times C_3\times C_9,\quad C_4\times C_3\times C_3\times C_3,$$
$$C_2\times C_2\times C_{27},\quad C_2\times C_2\times C_3\times C_9,\quad C_2\times C_2\times C_3\times C_3\times C_3.$$

4. 设 G 是阶大于 1 的有限交换群．证明：若除 e 外其余元素的阶都相同，则 G 必为素幂阶群．

证　若有互异素数 p, q 使 $pq \mid |G|$，则由本章 §2 定理 5(或本章 §6 定理 3 以及 Sylow 定理)知，G 有 p 阶与 q 阶元素，这与题设矛盾．因此，$|G|$ 必为素数 p 的方幂．

注　还可知这个相同的阶为 p．因为任取 $e\neq a\in G$，且设 $|a| = p^s$．则 $\left|a^{p^{s-1}}\right| = p$．但由假设

$$|a| = \left| a^{p^{s-1}} \right|, \quad 即\ p^s = p, \quad 从而\ s = 1.$$

即 G 中任何非 e 元素的阶都是 p.另外由证明可知,本题不需假设 G 交换.

5. 设 G 是有限交换群.证明:G 是循环群的充要条件是,$|G|$ 是 G 中所有元素的阶的最小公倍.

证 设 G 为 n 阶循环群,则 G 当然有 n 阶元素,而 G 中别的元素的阶都是 n 的因数,因此,n 是 G 的所有元素的阶的最小公倍.

反之,设 n 是 n 阶交换群 G 中所有元素的阶的最小公倍,则由习题 2.7 第 12 题知,在 n 阶群 G 中有 n 阶元素.从而可知 G 是循环群.

6. 用 C_k 表示 k 阶循环群.证明:

$$C_{m_1} \times C_{m_2} \times \cdots \times C_{m_n} \cong C_{m_1 m_2 \cdots m_n}$$

当且仅当正整数 $m_1, m_2, \cdots, m_n$ 两两互素.

证 1) 对 n 用归纳法.当 $n = 1$ 时显然.当 $n = 2$ 时,只用证 $C_{m_1} \times C_{m_2}$ 中含有 $m_1 m_2$ 阶元素即可.

令 a 是 C_{m_1} 的一个生成元,b 是 C_{m_2} 的一个生成元,则

$$(a, b) \in C_{m_1} \times C_{m_2},$$

且
$$(a, b)^{m_1 m_2} = (a^{m_1 m_2}, b^{m_1 m_2}) = (e_1, e_2).$$

其中 e_1 是 C_{m_1} 的单位元,e_2 是 C_{m_2} 的单位元.

又若 $(a, b)^s = (e_1, e_2)$,则 $(a^s, b^s) = (e_1, e_2)$,$a^s = e_1$,$b^s = e_2$,从而 $m_1 | s$,$m_2 | s$.但是 $(m_1, m_2) = 1$,故

$$m_1 m_2 | s.$$

因此 (a, b) 的阶是 $m_1 m_2$.而由于

$$|C_{m_1} \times C_{m_2}| = |C_{m_1}| \cdot |C_{m_2}| = m_1 m_2,$$

故 $C_{m_1} \times C_{m_2}$ 是 $m_1 m_2$ 阶循环群.由于凡同阶循环群都同构,故 $C_{m_1} \times C_{m_2} \cong C_{m_1 m_2}$.

假设对 $n - 1$ 成立,即有

$$C_{m_1}\times C_{m_2}\times\cdots\times C_{m_{n-1}}\cong C_{m_1m_2\cdots m_{n-1}}.$$

而 $C_{m_1}\times\cdots\times C_{m_{n-1}}\times C_{m_n}\cong(C_{m_1}\times\cdots\times C_{m_{n-1}})\times C_{m_n}$,故

$$C_{m_1}\times\cdots\times C_{m_{n-1}}\times C_{m_n}\cong C_{m_1m_2\cdots m_{n-1}}\times C_{m_n}.$$

又因 $m_1, m_2, \cdots, m_n$ 两两互素,故

$$(m_1m_2\cdots m_{n-1}, m_n)=1.$$

再由上面所证 $n=2$ 的情形知,

$$C_{m_1m_2\cdots m_{n-1}}\times C_{m_n}\cong C_{m_1m_2\cdots m_{n-1}m_n}.$$

故

$$C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}\cong C_{m_1m_2\cdots m_n}.$$

2) 反之,设 $C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}$ 是循环群,则由于其阶为 $m_1m_2\cdots m_n$,故其必有阶为 $m_1m_2\cdots m_n$ 的元素(即其生成元的阶).

如果 $m_1, m_2, \cdots, m_n$ 不两两互素,不妨设

$$(m_1, m_2)=d>1,\quad m_1=dm_1',\quad m_2=dm_2',$$

则 $dm_1'm_2'm_3\cdots m_n<m_1m_2m_3\cdots m_n$ 且对 $C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}$ 中任意元素 $(a_1, a_2, \cdots, a_n)$ 有

$$(a_1, a_2, \cdots, a_n)^{dm_1'm_2'm_3\cdots m_n}=(e_1, e_2, \cdots, e_n),$$

这与 $C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}$ 中有阶为 $m_1m_2\cdots m_n$ 的元素矛盾.故 $m_1, m_2, \cdots, m_n$ 必两两互素.

7. 设 G 是群, $H\leqslant G$.证明:如果关于 H 的任意两个左陪集的乘积仍是一个左陪集,则 $H\trianglelefteq G$.

证 任取 $a\in G$,则由于 H 的任两左陪集之积仍是一个左陪集,故可设

$$aH\cdot a^{-1}H=cH.$$

但由于 $H\leqslant G$,故 $e=ae\cdot a^{-1}e\in aH\cdot a^{-1}H$,即 $e\in cH$.令

$$e=ch\quad(h\in H),$$

则 $c=h^{-1}\in H$, $cH=H$,即 $aH\cdot a^{-1}H=H$.故对任意 $x\in H$,有

$$axa^{-1}=ax\cdot a^{-1}e\in aH\cdot a^{-1}H=H.$$

因此, $H\trianglelefteq G$.

8. 举例指出,存在群 G, C 为其中心,而商群 G/C 的中心的阶大于 1.

解　例如四元数群

$$G=\{1,i,j,k,-1,-i,-j,-k\},$$

其中心 $C=\{1,-1\}$.然而易知商群为

$$G/C=\{C,iC,jC,kC\},$$

且 G/C 是一个交换群,因此,G/C 的中心即自身,其阶为 $4>1$.

9. 设 G 是群,$N\trianglelefteq G$,$|N|=m$,$(m,n)=1$.证明:若 $|a|=n$,则 aN 在商群 G/N 中的阶也是 n;反之,若 aN 的阶是 n,则在 G 中有 n 阶元素 b 使

$$bN=aN.$$

证　因为 $|a|=n$,故

$$(aN)^n=a^nN=eN=N.$$

又设 $(aN)^r=N$,则 $a^rN=N$,$a^r\in N$.但是 $|N|=m$,故

$$a^{rm}=e.$$

由 $|a|=n$ 知,$n\mid rm$.但由题设 $(m,n)=1$,故 $n\mid r$,即在商群 G/N 中元素 aN 的阶也是 n.

反之,若 aN 的阶是 n,由于 $(m,n)=1$,故存在整数 s,t 使

$$ms+nt=1. \tag{1}$$

令

$$b=a^{ms}=a^{1-nt}=a\cdot a^{-nt}. \tag{2}$$

由于 aN 的阶是 n,故

$$(aN)^n=a^nN=N,\quad a^n\in N.$$

从而由(2)知

$$a^{-1}b=a^{-nt}=(a^n)^{-t}\in N,\quad bN=aN.$$

又因为 $|N|=m$,$a^n\in N$,故 $(a^n)^m=e$.从而

$$b^n=(a^{ms})^n=e.$$

又若 $b^r=a^{msr}=e$,则

$$(aN)^{msr}=eN=N.$$

但 aN 的阶是 n,故 $n\mid msr$.又由(1)知 $(n,ms)=1$,故 $n\mid r$.从而 b 的阶是 n.

10. 称群 G 中元素 $a^{-1}b^{-1}ab$ 为 G 中元素 a 与 b 的<u>换位元</u>,记

为 $a \circ b$.证明:

1) 由 G 中所有换位元生成的子群 K 是 G 的一个正规子群;

2) G/K 是交换群;

3) 若 $N \trianglelefteq G$,且 G/N 可换,则 $N \supseteq K$.

证 1) 设 φ 是群 G 的任一自同态,于是对 G 中任二元素 a, b 有

$$\begin{aligned}\varphi(a \circ b) &= \varphi(a^{-1}b^{-1}ab) = \varphi(a^{-1})\varphi(b^{-1})\varphi(a)\varphi(b) \\ &= \varphi(a)^{-1}\varphi(b)^{-1}\varphi(a)\varphi(b) = \varphi(a) \circ \varphi(b).\end{aligned}$$

任取 $x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k} \in K$,即其中 $x_1, \cdots, x_k$ 都是 G 的换位元,而 $m_1, m_2, \cdots, m_k$ 为整数,则由上面知,$\varphi(x_1), \cdots, \varphi(x_k)$ 均仍为换位元,故

$$\varphi\left(x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k}\right) = \varphi(x_1)^{m_1}\varphi(x_2)^{m_2}\cdots\varphi(x_k)^{m_k} \in K,$$

即 $\varphi(K) \subseteq K$.因此,K 是 G 的一个全特征子群.从而 K 是 G 的一个正规子群.

2) 任取 $a, b \in G$,则由于 $ab = ba(a \circ b)$,故

$$aK \cdot bK = (ab)K = (ba)(a \circ b)K = baK = bK \cdot aK,$$

即 G/K 是交换群.

3) 因为 G/N 是交换群,则对任意 $a, b \in G$,有

$$aN \cdot bN = bN \cdot aN, \quad (ab)N = (ba)N,$$

从而 $a \circ b = a^{-1}b^{-1}ab \in N$.即 G 中任二元素的换位元都属于 N,因此 $K \subseteq N$.

注 一般称 K 为群 G 的<u>换位子群</u>或<u>导群</u>,并用 G 表示.另外由以上证明可知,G 不仅是群 G 的正规子群,而且还是 G 的一个全特征子群.

11. 设 H, K 是群 G 的两个有限正规子群,并且 $(|H|, |K|) = 1$.证明:如果商群 G/H 和 G/K 都是交换群,则 G 也是交换群.

证 因为 $H \cap K \leqslant H$, $H \cap K \leqslant K$,而 H 与 K 又都是有限子群,故

$$|H \cap K| \,\Big|\, |H|, \quad |H \cap K| \,\Big|\, |K|,$$

从而 $|H\cap K| \mid (|H|,|K|)$.但由题设 $(|H|,|K|)=1$,故

$$|H\cap K|=1,\quad H\cap K=\{e\}.$$

任取 $a,b\in G$,则由于商群 G/H 和 G/K 都是交换群,故

$$abH=baH,\quad abK=baK.$$

即 $a^{-1}b^{-1}ab\in H$, $a^{-1}b^{-1}ab\in K$,从而

$$a^{-1}b^{-1}ab\in H\cap K=\{e\},\ a^{-1}b^{-1}ab=e,\ ab=ba.$$

即 G 是交换群.

12. 设 k 是一个奇数.证明:$2k$ 阶群 G 必有一个 k 阶子群.

证 由 Cayley 定理知,$2k$ 阶群 G 与 G 上的一个 $2k$ 阶 $2k$ 次置换群 $\overline{G}$ 同构.

由于 G 是偶数阶群,G 必含有 2 阶元,令 a 是 G 的任意一个 2 阶元.再任取 $x_1\in G$,于是易知

$$x_1\neq ax_1.$$

再从 G 中取 $x_2\notin\{x_1,ax_1\}$,则由于 $a^{-1}=a$,故易知

$$ax_2\neq x_2,\ ax_2\neq x_1,\ ax_2\neq ax_1;$$

如此下去,由于 $|G|=2k$,故可得

$$G=\{x_1,x_2,\cdots,x_k,ax_1,ax_2,\cdots,ax_k\}.$$

又由于

$$a^2=e,\ a(ax_i)=a^2x_i=x_i\quad(i=1,2,\cdots,k),$$

故

$$\begin{aligned}\tau_a&=\begin{pmatrix}x_1&x_2&\cdots&x_k&ax_1&ax_2&\cdots&ax_k\\ax_1&ax_2&\cdots&ax_k&x_1&x_2&\cdots&x_k\end{pmatrix}\\&=(x_1,ax_1)(x_2,ax_2)\cdots(x_k,ax_k)\in\overline{G}.\end{aligned}$$

但 k 是奇数,于是 $\overline{G}$ 含有奇置换.从而由第二章 §6 例 3 知,$\overline{G}$ 中奇偶置换各半.又因 $|\overline{G}|=2k$,故其 k 个偶置换作成 G 的一个子群,即 $\overline{G}$ 有 k 阶子群,从而 G 也有 k 阶子群.

13. 设 G 是一个阶大于 1 的有限 p-群.证明:G 的中心 C 的阶大于 1.

证 设 $|G|=p^m$.将 G 分解为共轭元素类的并:

$$G = G_1 \cup G_2 \cup \cdots \cup G_t, \quad G_i \cap G_j = \varnothing\,(i \neq j).$$

其中 $G_1 = \{e\}$.由于每个$|G_i|$都是 p^m 的因数,因此每个$|G_i|$必是 1 或素数 p 的方幂.但是

$$|G_1| + |G_2| + \cdots + |G_t| = |G| = p^m,$$

且$|G_1| = 1$,故至少还有一个 r 使$|G_r| = 1$.于是 G_r 只含有一个元素 $a \neq e$,从而 $a \in C$.因此,$|C| > 1$.

14. 证明:p^2 阶群必是交换群,其中 p 是一个素数.

证　设 G 是一个阶为 p^2 的群,C 是 G 的中心,则 C 是 G 的正规子群,因此$|C| \mid p^2$.但由上题知$|C| > 1$,故必

$$|C| = p \text{ 或 } p^2.$$

若$|C| = p$,则商群 G/C 的阶为素数 p,从而是循环群.于是由习题 3.2 第 6 题知,G 是交换群.因此 $C = G$,这与 G 是 p^2 阶群矛盾.故$|C| = p^2$,即 $G = C$ 是交换群.

15. 证明:群 G 的子集 S 的中心化子 $C(S)$等于 S 中各元素的正规化子的交.

证　由于

$$C(S) = \{x \in G \mid x \text{ 与 } S \text{ 中每个元素可换}\},$$

$$N(a) = \{y \in G \mid ya = ay\}, \quad a \in S,$$

故可知

$$\bigcap_{a \in S} N(a) = \{z \mid z \in G, \text{对 } \forall\, a \in S \text{ 都有 } az = za\},$$

从而

$$\bigcap_{a \in S} N(a) \subseteq C(S).$$

又任取 $x \in C(S)$,当然 $x \in \bigcap_{a \in S} N(a)$,故

$$C(S) \subseteq \bigcap_{a \in S} N(a).$$

因此

$$C(S) = \bigcap_{a \in S} N(a).$$

16. 证明:如果有限 p-子群 G 只有一个指数为 p 的子群,则 G 是一个循环群.

证 设 $|G| = p^n$,并对 n 用数学归纳法.

当 $n=1$ 时结论显然.假定对 $k<n$ 时结论成立,下证对 $|G| = p^n$ 时结论成立.

设 C 是 G 的中心,由第 13 题知 $|C| >1$,故 $|G/C| < p^n$.而由题设 G 只有一个指数为 p 的子群 H,再由于易知

$$(G/C:\ H/C) = p \Longleftrightarrow (G:\ H) = p,$$

从而商群 G/C 只能有一个指数为 p 的子群.于是由归纳假设,G/C是循环群.从而由习题 3. 2 第 6 题知,G 是交换群.

因此,G 是有限交换 p-群,根据基本定理,设

$$G=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_s\rangle,$$

其中 $|a_i| = p^{k_i}$ $(i=1,2,\cdots,s)$.如果 $s>1$,则$\langle a_1\rangle$ 与$\langle a_2\rangle$ 均有惟一的指数为 p 的子群$\langle a_1^p\rangle$ 与$\langle a_2^p\rangle$.于是

$$\langle a_1^p\rangle\times\langle a_2\rangle\times\cdots\times\langle a_s\rangle \quad 与 \quad \langle a_1\rangle\times\langle a_2^p\rangle\times\langle a_3\rangle\times\cdots\times\langle a_s\rangle$$

便是 G 的两个指数为 p 的子群,与题设矛盾.故必 $s=1$,即 G 为循环群.

17. 证明:n 阶群的自同构群是有限群,且其阶是$(n-1)!$ 的一个因数.

证 设 G 是一个 n 阶群,且 $G=\{e, a_2,\cdots, a_n\}$.

任取$\sigma\in \mathrm{Aut}\ G$,因为$\sigma(e)=e$,又$\sigma$ 为双射,故σ 在集合

$$S=\{a_2, a_3,\cdots, a_n\}$$

上的限制$\sigma|_S$ 是 S 上的一个置换,从而

$$\sigma|_S\in S_{n-1},$$

其中 S_{n-1} 为集合 S 上的 $n-1$ 次对称群.又易知

$$\varphi:\sigma\longrightarrow\sigma|_S$$

是 G 的自同构群 $\mathrm{Aut}\ G$ 到 S_{n-1} 的一个单射.

又任取$\sigma,\tau\in\mathrm{Aut}\ G$, $x\in G$,由于$\sigma|_S$ 与σ 对于 G 中元素 x 的象是一致的,即$\sigma|_S(x)=\sigma(x)$,故易知φ 是一个同态映射.从而φ 是 $\mathrm{Aut}\ G$ 到 S_{n-1} 的一个单同态映射.因此

$$\mathrm{Aut}\ G \cong \varphi(\mathrm{Aut}\ G) \leqslant S_{n-1}.$$

于是由 Lagrange 定理知,$|\mathrm{Aut}\ G|$ 是 $|S_{n-1}| = (n-1)!$ 的一个因数.

18. 设 G_1, G_2 是两个群.证明:若 $G_1 \cong G_2$,则

$$\mathrm{Aut}\ G_1 \cong \mathrm{Aut}\ G_2.$$

再举例指出反之不成立.

证 由题设:$G_1 \cong G_2$,且设 φ 为其一个同构映射.任取 $\sigma_1 \in \mathrm{Aut}\ G_1$,下证:

$$\sigma_2: \varphi(x_1) \longrightarrow \varphi(\sigma_1(x_1)) \quad (x_1 \in G_1)$$

是 G_2 的一个自同构.

事实上,任取 $x_2 \in G_2$,令 $\varphi(x_1) = x_2$,则 $\varphi(\sigma_1(x_1))$ 是由 x_2 完全确定的 G_2 中的一个元素.反之,任取 $y_2 \in G_2$,令

$$\varphi(y_1) = y_2, \quad y_1 \in G_1, \sigma_1(x_1) = y_1,$$

于是 $\varphi(x_1) \in G_2$,且

$$\sigma_2(\varphi(x_1)) = \varphi(\sigma_1(x_1)) = \varphi(y_1) = y_2,$$

即 σ_2 是 G_2 到 G_2 的一个满射.

类似可证 σ_2 是单射.从而为双射.

最后,由于对 G_1 中任意元素 x_1, y_1 有

$$\begin{aligned}\sigma_2[\varphi(x_1)\varphi(y_1)] &= \sigma_2[\varphi(x_1 y_1)]\\ &= \varphi[\sigma_1(x_1 y_1)] = \varphi[\sigma_1(x_1)\sigma_1(y_1)]\\ &= \varphi[\sigma_1(x_1)]\cdot\varphi[\sigma_1(y_1)] = \sigma_2[\varphi(x_1)]\cdot\sigma_2[\varphi(y_1)],\end{aligned}$$

故 σ_2 是群 G_2 的一个自同构,即 $\sigma_2 \in \mathrm{Aut}\ G_2$.

易知 $\Psi: \sigma_1 \longrightarrow \sigma_2$ 是 $\mathrm{Aut}\ G_1$ 到 $\mathrm{Aut}\ G_2$ 的一个映射.又任取 $\tau_2 \in \mathrm{Aut}\ G_2$,令

$$\tau_1: x_1 \longrightarrow \varphi^{-1}[\tau_2(\varphi(x_1))].$$

则可证 $\tau_1 \in \mathrm{Aut}\ G_1$,且对任意 $x_2 \in G_2$,令 $\varphi(x_1) = x_2$,有

$$\varphi[\tau_1(x_1)] = \varphi\varphi^{-1}[\tau_2(x_2)] = \tau_2(x_2) = \tau_2[\varphi(x_1)],$$

即在 Ψ 之下,τ_1 是 τ_2 的逆象,故 Ψ 为满射.

类似可证 Ψ 为单射,从而为双射.

又对$\sigma_1,\tau_1\in \mathrm{Aut}\ G_1$,令

$$\sigma_2:\varphi(x_1)\longrightarrow\varphi[\sigma_1(x_1)],\quad \tau_2:\varphi(x_1)\longrightarrow\varphi[\tau_1(x_1)].$$

于是

$$\begin{aligned}\sigma_2\tau_2(\varphi(x_1))&=\sigma_2[\varphi(\tau_1(x_1))]\\&=\varphi[\sigma_1(\tau_1(x_1))]=\varphi[(\sigma_1\tau_1)(x_1)],\end{aligned}$$

即 Ψ 是 $\mathrm{Aut}\ G_1$ 与 $\mathrm{Aut}\ G_2$ 的一个同构映射,故

$$\mathrm{Aut}\ G_1\cong\mathrm{Aut}\ G_2.$$

反之,若 $\mathrm{Aut}\ G_1\cong\mathrm{Aut}\ G_2$,则不一定有 $G_1\cong G_2$.这由§5 推论 2 可知.

19. 设 P 是有限群 G 的一个 Sylow p-子群,$N\trianglelefteq G$.证明:

1) $P\cap N$ 是 N 的一个 Sylow p-子群;

2) PN/N 是 G/N 的一个 Sylow p-子群.

证 1) 令 $P_1=P\cap N$,则 P_1 显然是 p-子群.若能证明 P_1 在 N 中的指数不含因子 p,则 P_1 便是 N 的 Sylow p-子群.为此,下面来考察$(N:P_1)$.

因为由群同构定理知,$N/(P\cap N)\cong PN/N$,故

$$(N:P_1)=(N:P\cap N)=(PN:P),\tag{1}$$

$$(G:P)=(G:PN)(PN:P).\tag{2}$$

而 P 是 G 的 Sylow p-子群,故$(G:P)$不含因子 p.从而由(2)知,$(PN:P)$也不含因子 p.从而再由(1)知,$(N:P_1)$不含因子 p.得证.

2) 设$|G|=p^nst$,$|N|=p^mt$,$(p,st)=1$,则$|P|=p^n$,$|P\cap N|=p^r$,$r\leqslant m$.

由群的同构定理知:

$$|PN/N|=|P/(P\cap N)|=p^{n-r},\quad n-r\geqslant n-m.\tag{1}$$

但$|G/N|=p^{n-m}s$,$|PN/N|\ \big|\ |G/N|$,故

$$|PN/N|\leqslant p^{n-m},\ 即\ n-r\leqslant n-m.$$

从而由(1)知,$n-r=n-m$,即$|PN/N|=p^{n-m}$,亦即 PN/N 是

G/N的 Sylow p-子群.

20. 设 S_3 是 $M=\{1,2,3\}$ 上的三次对称群.证明:

$$\mathrm{Aut}\ S_3 \cong S_3.$$

证 S_3 共有三个 2 阶子群:

$$H_1=\{(1),(12)\},\quad H_2=\{(1),(13)\},\quad H_3=\{(1),(23)\}.$$

令 $M'=\{H_1,H_2,H_3\}$,且 S_3' 为 M' 上的三次对称群.则易知

$$\varphi:\tau \longrightarrow \begin{pmatrix} H_1 & H_2 & H_3 \\ \tau(H_1) & \tau(H_2) & \tau(H_3) \end{pmatrix} \quad (\forall \tau \in \mathrm{Aut}\ S_3)$$

是 $\mathrm{Aut}\ S_3$ 到 S_3' 的一个同态映射.又易知

$$\tau \in \mathrm{Ker}\varphi \Longleftrightarrow \tau \text{ 在 } S' \text{ 上引出恒等置换},$$

即 $\tau(H_i)=H_i(i=1,2,3)$,亦即 τ 把(12),(13),(23)分别变为自身.但因

$$S_3=\langle (12),(13),(23)\rangle,$$

故 τ 是 S_3 的恒等自同构.因此 φ 是单射.

又由 $|C(S_3)|=1$, $\mathrm{Inn}\ S_3\cong S_3/C(S_3)\cong S_3$,得

$$|\mathrm{Aut}\ S_3| \geqslant |\mathrm{Inn}\ S_3| = |S_3| = 6.$$

于是 φ 满同态,从而 φ 是同构映射, $\mathrm{Aut}\ S_3\cong S_3'\cong S_3$.

注 更一般地,当 $n\geqslant 3$,但 $n\neq 6$ 时, S_n 的自同构都是内自同构,而且

$$\mathrm{Aut}\ S_n \cong S_n.$$

21. 设 G 是一个有限群,且 $|G|=p^2q$,其中 p,q 是两个互异素数.证明: G 不是单群.

证 设 G 有 k_p 个 Sylow p-子群,有 k_q 个 Sylow q-子群,则由 Sylow 定理可知: $k_p\mid q$, $k_q\mid p^2$.但 p,q 是互异素数,故

$$k_p=1 \text{ 或 } q;\quad k_q=1,p,p^2.$$

1) 若 $k_p=1$,则 G 有惟一的 Sylow p-子群,它是 G 的非平凡正规子群,故此时 G 不是单群.

2) 若 $k_p=q$,则由于 $k_p\equiv 1 \pmod p$,故 $p\mid q-1$, $p<q$.

若 $k_q=p$,则因 $k_q\equiv 1 \pmod q$,故 $q\mid p-1$.这与 $p<q$ 矛盾;若

$k_q = p^2$,则由于 $|G| = p^2 q$ 即 G 的 Sylow q-子群都是 q 阶元生成的循环群,而任二这种互异子群的交为 $\{e\}$,从而 G 共有

$$k_q(q-1) = p^2(q-1) = p^2 q - p^2$$

个 q 阶元.于是,G 的非 q 阶元共有 p^2 个.设 P 是 G 的一个 Sylow p-子群,则 $|P| = p^2$ 且 P 中元素都不是 q 阶的.于是 P 是 G 的惟一的 Sylow p-子群,这与 $k_p = q$ 也矛盾.

因此只有 $k_q = 1$,即 G 有惟一的 Sylow q-子群,它是 G 的非平凡正规子群.从而 G 不是单群.

22. 设 G 是有限群,且 $|G| = pqr$,其中 p, q, r 是互异素数.证明:G 不是单群.

证 不妨设 $p > q > r$,且 G 有 k_p 个 Sylow p-子群,k_q 个 Sylow q-子群,k_r 个 Sylow r-子群.若 $k_p > 1$, $k_q > 1$, $k_r > 1$,则由于任二不同的 Sylow p-子群的交是 $\{e\}$,因此 k_p 个 Sylow p-子群共含 $k_p(p-1)$个 p 阶元.同理,有 $k_q(q-1)$个 q 阶元,有 $k_r(r-1)$个 r 阶元.于是

$$|G| = pqr \geqslant 1 + k_p(p-1) + k_q(q-1) + k_r(r-1). \quad (1)$$

但是由 Sylow 定理知,$k_p \mid qr$.由于 p, q, r 是互异素数,且 $k_p > 1$,故只有

$$k_p = q,\ r,\ qr.$$

若 $k_p = q$,则由于 $p \mid k_p - 1$,故 $p \mid q-1$,这与 $p > q$ 矛盾;若 $k_p = r$,则同样有 $p \mid r-1$,这与 $p > r$ 矛盾.故只有

$$k_p = qr. \quad (2)$$

又因 $k_q \mid pr$, $q \mid k_q - 1$, $k_q > 1$, $q > r$,所以 $k_q \geqslant p$.

同理,$k_r \geqslant q$.于是由(1)及(2)知:

$$pqr \geqslant 1 + qr(p-1) + p(q-1) + q(r-1).$$

从而得 $0 \geqslant (p-1)(q-1)$,矛盾.故 k_p, k_q, k_r 中至少有一个为 1,从而 G 至少有一个非平凡正规子群,G 不是单群.

23. 证明:不存在 56 阶单群.

证 设 G 是任意一个 56 阶群.因为 $56 = 2^3 \cdot 7$,于是由 Sylow

定理知,G 的 Sylow 7-子群的个数 $k_7 \mid 56$ 且

$$k_7 \equiv 1 \pmod 7).$$

据此可得

$$k_7 = 1 \text{ 或 } 8.$$

若 $k_7 = 1$,则这惟一的 Sylow 7-子群是 G 的正规子群,且是非平凡的,从而 G 不是单群.

若 $k_7 = 8$,因为 G 的 Sylow 7-子群是7阶群,所以它们为循环群且任二个不同的 Sylow 7-子群之交只含有单位元,因此,这8个 Sylow 7-子群共占去 G 的49个元素,而 Sylow 7-子群与 Sylow 2-子群的交只含有单位元,故 G 只有一个 Sylow 2-子群.因而它就是 G 的正规子群,故 G 不是单群.

总之,不存在56阶单群.

24. 证明:凡455阶群必为循环群.

证　设 G 是一个455阶群.因为 $455 = 5 \cdot 7 \cdot 13$,所以由Sylow定理知,G 有阶是5,7,13的元素.设 G 的 Sylow 7-子群有 k_7 个,于是由 Sylow 定理知:

$$k_7 \mid 455 = 5 \cdot 7 \cdot 13, \text{ 且 } k_7 \equiv 1 \pmod 7).$$

据此可知必 $k_7 = 1$.即 G 的 Sylow 7-子群只有一个,用 P_7 表示,它是 G 的一个正规子群.

同理,G 的 Sylow 13-子群也只有一个,用 P_{13} 表示,它也是 G 的一个正规子群.从而 $P_7 P_{13}$ 是 G 的91阶正规子群.

又同理,根据 Sylow 定理,G 的 Sylow 5-子群的个数为1或91.如果有91个 Sylow 5-子群,则 G 共有 $91 \times 4 = 364$ 个5阶元素,而 $P_7 P_{13}$ 中包含91个阶与5互素的元,这两种元素共有455个,即 G 的全部元素.任取一个 Sylow 5-子群 P_5,则 $P = P_5 P_7$ 是 G 的一个35阶子群.因为

$$P_5 \triangle P, \quad P_7 \triangle P, \quad P_5 \cap P_7 = \{e\},$$

故 $P = P_5 \times P_7$.因此,P 是一个35阶循环群.从而 G 包含一个35阶元.但 G 的前面所有元中没有35阶元,矛盾.因此,G 只有一个

Sylow 5-子群 P_5.

又因为 P_5, P_7, P_{13} 都是 G 的互异的素幂阶循环群,故由上面第 6 题知,

$$G = P_5 \times P_7 \times P_{13}$$

是一个循环群.

25. 设 G 是一个有限非交换单群, p 是一个素数,且 $p \mid |G|$. 证明:G 的 Sylow p-子群的个数 $k > 1$.

证 令 P 是 G 的一个 Sylow p-子群.若 $|G| = p^m$,则根据群的类等式可知, G 的中心 C 的阶必大于 1.又因 G 不可换,故 $C \neq G$,即 C 是 G 的非平凡正规子群,这与 G 是单群矛盾.

因此,$|G|$ 至少有两个不同的素因子.于是

$$\{e\} \subset P \subset G.$$

这样,如果 P 是 G 的惟一的 Sylow p-子群,则 P 便是 G 的一个非平凡的正规子群,这与 G 是单群矛盾.故 G 的 Sylow p-子群的个数 $k > 1$.

26. 设 G 是一个有限群, $H \trianglelefteq G$, $K \trianglelefteq G$, 又 P 是 G 的一个 Sylow p-子群.证明:

1) $|P \cap HK| = \dfrac{|P \cap H| \cdot |P \cap K|}{|P \cap H \cap K|}$;

2) $P(H \cap K) = PH \cap PK$.

证 1) 设 $|G| = p^s m$, $p \nmid m$,其中 p 是素数,则 $|P| = p^s$.另设

$$|H| = p^\alpha a,\ |K| = p^\beta b,\ |H \cap K| = p^\gamma c, \qquad (1)$$

其中 $p \nmid a$, $p \nmid b$, $p \nmid c$.由于 $H \trianglelefteq G$, $K \trianglelefteq G$,故

$$H \cap K \trianglelefteq G,\quad HK \trianglelefteq G,$$

且由第 19 题知, $P \cap H$、$P \cap K$、$P \cap H \cap K$ 分别为 H、K、$H \cap K$ 的 Sylow p-子群.于是由(1)知:

$$|P \cap H| = p^\alpha,\ |P \cap K| = p^\beta,\ |P \cap H \cap K| = p^\gamma,$$

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = p^{\alpha+\beta-\gamma} \cdot d. \qquad (2)$$

其中 $d=\frac{ab}{c}$为正整数,且 $p\nmid d$.

又因 $P\cap HK$ 也是 HK 的 Sylow p-子群,故由(2)知

$$|P\cap HK|=p^{\alpha+\beta-\gamma}=\frac{|P\cap K|\cdot|P\cap K|}{|P\cap H\cap K|}. \qquad (3)$$

2) 再根据

$$|PHK|=\frac{|P|\cdot|HK|}{|P\cap HK|},\quad |P(H\cap K)|=\frac{|P|\cdot|H\cap K|}{|P\cap H\cap K|}$$

以及(3)可得

$$|PH\cap PK|=\frac{|PH|\cdot|PK|}{|PHK|}=\frac{|P|\cdot|H\cap K|}{|P\cap H\cap K|}$$
$$=|P(H\cap K)|.$$

但由于 G是有限群,且显然

$$P(H\cap K)\subseteq PH\cap PK,$$

因此,

$$P(H\cap K)=PH\cap PK.$$

27. 证明:当 $n\geqslant 3$ 时,全体 3-循环是交代群 A_n 的一个生成系.

证 $n=3$ 时,结论显然成立.因此下设 $n>3$.

由于 A_n 中每个元素都可表为偶数个对换之积,从而也就是一些形如

$$(ab)(cd) \text{ 或 } (ab)(ac)$$

的项之积.其中 a,b,c,d 是$\{1,2,\cdots,n\}$中互异的元素.但由于

$$(ab)(cd)=(abc)(bcd),\quad (ab)(ac)=(acb),$$

故 A_n 中的每个元素又都是一些 3-循环之积,即 A_n 由全体 3-循环生成.

28. 证明:当 $n\geqslant 5$ 时,n 次交代群 A_n 是一个单群,即其正规子群只有$\{(1)\}$及 A_n.

证 设$\{(1)\}\neq N\trianglelefteq A_n$.在 N 中任取元素$\tau\neq(1)$,且τ 是 N 中变动数码最多的一个置换.

1）若 τ 恰变动 4 个数码，这时 τ 必为二对换之积，因为恰变动 4 个数码的偶置换，别的可能性是不存在的. 现在不妨设

$$\tau=(12)(34).$$

因为 $n>4$，$N\triangle A_n$，取 $\sigma=(345)$，则易知

$$\tau_1=\sigma\tau\tau^{-1}=(12)(45)\in N,\quad \tau^{-1}\tau_1=(345)\in N.$$

这与 τ 是 N 中变动数码最多的置换矛盾.

2）设 τ 所变动的数码多于 4 个. 此时可分以下三种情形并取 $\sigma=(234)$ 可得：

①$\tau=(1234\cdots)\cdots$，$\tau_1=\sigma\tau\sigma^{-1}=(1342\cdots)\cdots\in N$；

②$\tau=(123)(4a\cdots)\cdots$，$\tau_1=\sigma\tau\sigma^{-1}=(134)(2\cdots)\cdots\in N$；

③$\tau=(12)(34\cdots)\cdots$，$\tau_1=\sigma\tau\sigma^{-1}=(13)(42)(56)\cdots\in N$.

其中显然 $\tau_1\neq\tau$，故 $\tau^{-1}\tau_1\neq(1)$. 在①与③情形下，由于对所有数码 $k>4$ 均有 $\tau^{-1}\tau_1(k)=k$，这与 τ 的取法矛盾；在②的情形下，$\tau^{-1}\tau_1$ 除 1,2,3,4, a 之外使其余数码都不变，即 $\tau^{-1}\tau_1$ 只变动五个数码，而此时 τ 所变动的数码多于 5 个，这与 τ 的取法也矛盾.

因此由 1）与 2）知，τ 只能变动三个数码，即 τ 是一个 3－循环，故由上题知，$N=A_n$.

29. 证明：当 $n\geqslant5$ 时，n 次对称群 S_n 不是可解群.

证　见习题 3. 2 第 8 题.

30. 若 n 次置换 π 是 a_1 个 1－循环、a_2 个 2－循环、…、a_n 个 n－循环（不相连循环且每个数码都出现）之积，则称 π 有循环结构

$$[1^{a_1},2^{a_2},\cdots,n^{a_n}].$$

证明：二 n 次置换 σ 与 τ 在 S_n 中共轭的充分与必要条件是 σ 与 τ 有相同的循环结构.

证　设 σ 与 τ 共轭，即存在 n 次置换 α 使

$$\sigma=\alpha\tau\alpha^{-1}.$$

设 $\tau=(i_1\ i_2\cdots i_s)(j_1\ j_2\cdots j_t)\cdots(k_1\ k_2\cdots k_m)$ 是不相连的循环之积（每个字母都出现）. 则由第二章 §6 定理 5 知，

$$\sigma=\alpha\tau\alpha^{-1}=(\alpha(i_1)\cdots\alpha(i_s))(\alpha(j_1)\cdots\alpha(j_t))\cdots(\alpha(k_1)\cdots\alpha(k_m))$$

显然仍为不相连的循环之积,即σ与τ有相同的循环结构.

反之,设σ与τ有相同的循环结构,且

$$\sigma=(i_1)(i_2)\cdots(i_s)\cdots(j_1 j_2\cdots j_t)\cdots,$$
$$\tau=(i'_1)(i'_2)\cdots(i'_s)\cdots(j'_1 j'_2\cdots j'_t)\cdots.$$

令

$$\alpha=\begin{pmatrix} i_1 & i_2 & \cdots & i_s & \cdots & j_1 & j_2 & \cdots & j_t & \cdots \\ i'_1 & i'_2 & \cdots & i'_s & \cdots & j'_1 & j'_2 & \cdots & j'_t & \cdots \end{pmatrix},$$

则

$$\alpha(i_1)=i'_1,\cdots,\alpha(i_s)=i'_s,\cdots,\alpha(j_1)=j'_1,\cdots,\alpha(j_t)=j'_t,\cdots$$

于是

$$\alpha\tau\alpha^{-1}=(\alpha(i_1))\cdots(\alpha(i_s))\cdots(\alpha(j_1)\cdots\alpha(j_t))\cdots$$
$$=(i'_1)\cdots(i'_s)\cdots(j'_1 j'_2\cdots j'_t)\cdots=\sigma.$$

即σ与τ共轭.

31. 设a是群G中一个阶为$m_1 m_2\cdots m_n$的元素.证明:若正整数$m_1,m_2,\cdots,m_n$两两互素,则a可惟一表示为

$$a=a_1 a_2\cdots a_n,$$

其中a_i都是a的方幂(从而可两两互换)且

$$|a_i|=m_i\quad(i=1,2,\cdots,n).$$

证 对n用数学归纳法.

1) 存在性

当$n=1$时显然,假设对$n-1$成立,下证对n成立.

令$k=m_1 m_2\cdots m_{n-1}$,则由于$m_1,m_2,\cdots,m_n$两两互素,故

$$(k,m_n)=1,$$

于是存在整数s,t使$ks+m_n t=1$.由此可得

$$a=a^{m_n t}\cdot a^{ks}=a'\cdot a_n,\tag{1}$$

其中$a'=a^{m_n t}$,$a_n=a^{ks}$.且易知

$$|a'|=m_1 m_2\cdots m_{n-1},\quad |a_n|=m_n.$$

于是由归纳假设,有

$$a'=a_1 a_2\cdots a_{n-1},\tag{2}$$

其中$|a_i|=m_i$,且a_i都是a'的方幂从而也是a的方幂($i=1,2,\cdots,n-1$).

将(2)式代入(1)式,得

$$a=a_1a_2\cdots a_{n-1}a_n.$$

其中$|a_i|=m_i$,且每个a_i都是a的方幂 ($i=1,2,\cdots,n$).

2) 惟一性

当$n=1$时显然.假定对$n-1$成立,下证对n成立.令

$$a=a_1a_2\cdots a_{n-1}a_n=b_1b_2\cdots b_{n-1}b_n,$$

其中$|a_i|=|b_i|=m_i$,且a_i与b_i都是a的方幂 ($i=1,2,\cdots,n$).再令

$$a'=a_1a_2\cdots a_{n-1},\quad b'=b_1b_2\cdots b_{n-1},$$

则由于$m_1,m_2,\cdots,m_{n-1}$两两互素,且a_i与b_i都是a的方幂,从而可换,故

$$|a'|=|b'|=k=m_1m_2\cdots m_{n-1}.$$

令

$$b'a'^{-1}=a_nb_n^{-1}=c \qquad (3)$$

于是有

$$c^k=(b'a'^{-1})^k=e,\quad c^{m_n}=(a_nb_n^{-1})^{m_n}=e.$$

但由于$m_1,m_2,\cdots,m_{n-1},m_n$两两互素,故$(k,m_n)=1$.从而由此易知$c=e$是群$G$的单位元.于是由(3)知

$$a'=b',\quad a_n=b_n.$$

即$a'=a_1a_2\cdots a_{n-1}=b_1b_2\cdots b_{n-1}$,$a_n=b_n$.因此由归纳假设知

$$a_i=b_i\quad(i=1,2,\cdots,n).$$