第 6 章 商群

为了深入探讨群的结构，需要进一步研究子群的作用.

6.1 陪群与Lagrange定理

定义 6.1. $\boldsymbol{H}$是$\boldsymbol{G}$的子群. 在$\boldsymbol{G}$上定义模$\boldsymbol{H}$同余关系，$\forall a, b \in \boldsymbol{G}$，如果$a * b^{'} \in \boldsymbol{H}$，则称$a$与$b$**模**$H$**同余**，记作$a \equiv b(\mathrm{mod}\ \boldsymbol{H})$.

定理 6.1. 模$\boldsymbol{H}$同余关系是$\boldsymbol{G}$上的等价关系. 对于$\boldsymbol{G}$中的元素a，a所在的等价类为

$$\boldsymbol{H}a = \{h * a | h \in \boldsymbol{H}\},$$

称为$\boldsymbol{G}$中$\boldsymbol{H}$的右陪集，元素a是陪集$\boldsymbol{H}a$的代表元.

证明 任取$a \in \boldsymbol{G}$，$a * a^{'} = e \in \boldsymbol{H}$，故$a \equiv a(\mathrm{mod}\boldsymbol{H})$. 模$\boldsymbol{H}$同余关系是自反的. 如果$a, b \in \boldsymbol{G}$，$a \equiv b(\mathrm{mod}\boldsymbol{H})$，即$a * b^{'} \in \boldsymbol{H}$. 因$\boldsymbol{H}$是群，$(a * b^{'})^{'} = b * a^{'} \in \boldsymbol{H}$. 故$b \equiv a(\mathrm{mod}\boldsymbol{H})$. 模$\boldsymbol{H}$同余关系是对称的. 如果$a, b, c \in \boldsymbol{G}$，$a \equiv b(\mathrm{mod}\boldsymbol{H})$，$b \equiv c(\mathrm{mod}\boldsymbol{H})$，即$a * b^{'} \in \boldsymbol{H}$，$b * c^{'} \in \boldsymbol{H}$. $\boldsymbol{H}$是$\boldsymbol{G}$的子群，$\boldsymbol{H}$对群$\boldsymbol{G}$的运算$*$封闭，$(a * b^{'}) * (b * c^{'}) = a * c^{'} \in \boldsymbol{H}$，故$a \equiv c(\mathrm{mod}\ \boldsymbol{H})$. 模$\boldsymbol{H}$同余关系是传递的. 综上分析知模$\boldsymbol{H}$同余关系是$\boldsymbol{G}$上的等价关系.

$\boldsymbol{G}$中的元素a的等价类，

$$\begin{aligned}[a] &= \{b | b \in G, b * a^{'} \in \boldsymbol{H}\} \\ &= \{h * a | h \in \boldsymbol{H}\} = \boldsymbol{H}a.\end{aligned}$$

显然$a \in \boldsymbol{H}a$，a是该等价类的代表元.

模$\boldsymbol{H}$同余关系有如下性质：

1° $\boldsymbol{H}e = \boldsymbol{H}$;

2° $a \equiv b(\mathrm{mod}\ \boldsymbol{H}) \Longleftrightarrow \boldsymbol{H}a = \boldsymbol{H}b$;

3° $a \in \boldsymbol{H} \Longleftrightarrow \boldsymbol{H}a = \boldsymbol{H}$.

例 6.1. 非零有理数乘法群$\langle \boldsymbol{Q}^{*},\bullet\rangle$，$\boldsymbol{H}=\{-1,1\}\subset\boldsymbol{Q}^{*}$，是该乘法群的子群. $\boldsymbol{Q}^{*}$中元素a所在的右陪集$\boldsymbol{H}a=\{a,-a\}$. 当$a\equiv b\,(\mathrm{mod}\ \boldsymbol{H})$时，$b=\pm a$，显然$\boldsymbol{H}a=\boldsymbol{H}b$.

例 6.2. 三次二面体群$\langle \boldsymbol{D}_3,\bullet\rangle$，$\boldsymbol{H}=\{\rho_0,\rho_1,\rho_2\}$是$\boldsymbol{D}_3$的子群，因$\rho_i\in\boldsymbol{H}$，$0\leqslant i\leqslant 2$，故$\boldsymbol{H}\rho_0=\boldsymbol{H}\rho_1=\boldsymbol{H}\rho_2=\boldsymbol{H}$. 又因$\mu_i*\mu_j^{'}\in\boldsymbol{H}$，$1\leqslant i,j\leqslant 3$，故$\boldsymbol{H}\mu_1=\boldsymbol{H}\mu_2=\boldsymbol{H}\mu_3=\{\mu_1,\mu_2,\mu_3\}$. $\boldsymbol{H}$有两个不同的右陪集$\boldsymbol{H}$和$\boldsymbol{H}\mu_1$，$\boldsymbol{D}_3=\boldsymbol{H}\cup\boldsymbol{H}\mu_1$且$\boldsymbol{H}\cap\boldsymbol{H}\mu_1=\varnothing$.

例 6.3. $\boldsymbol{G}$是以g为生成元的9阶循环群，$\boldsymbol{G}=\{g^0,g^1,\cdots,g^8\}$，$g^9=e$. $\boldsymbol{H}=\{g^0,g^3,g^6\}$是$\boldsymbol{G}$的3阶子群.

$$\begin{aligned}\boldsymbol{H}g^0=\boldsymbol{H}g^3=\boldsymbol{H}g^6&=\{g^0,g^3,g^6\}=\boldsymbol{H},\\ \boldsymbol{H}g^1=\boldsymbol{H}g^4=\boldsymbol{H}g^7&=\{g^1,g^4,g^7\},\\ \boldsymbol{H}g^2=\boldsymbol{H}g^5=\boldsymbol{H}g^8&=\{g^2,g^5,g^8\}.\end{aligned}$$

$\boldsymbol{H}$有三个不同的右陪集$\boldsymbol{H}$，$\boldsymbol{H}g$，$\boldsymbol{H}g^2$. $\boldsymbol{G}=\boldsymbol{H}\bigcup\boldsymbol{H}g\bigcup\boldsymbol{H}g^2$，且这些右陪集两两非交.

对于群$\boldsymbol{G}$的子群$\boldsymbol{H}$也可以定义它的左陪集，先在$\boldsymbol{G}$上定义等价关系. $\forall a,b\in\boldsymbol{G}$,

$$a\equiv b\,(\mathrm{mod}\ \boldsymbol{H})\Longleftrightarrow a^{'}*b\in\boldsymbol{H}.$$

$\boldsymbol{G}$中元素a所在的等价类$[a]=\{b|b\in\boldsymbol{G},a^{'}*b\in\boldsymbol{H}\}=\{a*h|h\in\boldsymbol{H}\}=a\boldsymbol{H}$，称为$a$所在的左陪集.

定理 6.2. $\boldsymbol{H}$是群$\boldsymbol{G}$的子群，$\boldsymbol{H}$的所有左陪集集合$\boldsymbol{S}_L=\{a\boldsymbol{H}|a\in\boldsymbol{G}\}$和所有右陪集集合$\boldsymbol{S}_R=\{\boldsymbol{H}a|a\in\boldsymbol{G}\}$是等势的.

证明 令$f:\boldsymbol{S}_L\to\boldsymbol{S}_R$，$f(a\boldsymbol{H})=\boldsymbol{H}a^{'}$. 这里首先要说明该映射与代表元选取无关，即若$a\boldsymbol{H}=b\boldsymbol{H}$，必有$\boldsymbol{H}a^{'}=\boldsymbol{H}b^{'}$. 由$a\boldsymbol{H}=b\boldsymbol{H}$知$a^{'}*b\in\boldsymbol{H}$，$\boldsymbol{H}$是群，$(a^{'}*b)^{'}=b^{'}*(a^{'})^{'}\in\boldsymbol{H}$从而$\boldsymbol{H}a^{'}=\boldsymbol{H}b^{'}$. 显然$f$是满射. 如果$a_1\boldsymbol{H},a_2\boldsymbol{H}\in\boldsymbol{S}_L$都是$\boldsymbol{H}a$的原像，$f(a_1\boldsymbol{H})=f(a_2\boldsymbol{H})=\boldsymbol{H}a$，得出$\boldsymbol{H}a_1^{'}=\boldsymbol{H}a_2^{'}$，故有$(a_1^{'})*(a_2^{'})^{'}=a_1^{'}*a_2\in\boldsymbol{H}$. 由此可知$a_1\boldsymbol{H}=a_2\boldsymbol{H}$. 这说明$f$是单射.

综上分析，在$\boldsymbol{S}_L$和$\boldsymbol{S}_R$之间存在一个双射，故$\boldsymbol{S}_L$与$\boldsymbol{S}_R$等势.

注意:在定理6. 2证明中定义的映射是$f(a\boldsymbol{H}) = \boldsymbol{H}a'$，而不是$\boldsymbol{H}a$. 后者它不是映射. 当$a\boldsymbol{H} = b\boldsymbol{H}$时，不能保证$\boldsymbol{H}a = \boldsymbol{H}b$.

定义 6.2. *群$\boldsymbol{G}$关于它的子群$\boldsymbol{H}$的左(右)陪集个数叫做$\boldsymbol{H}$在$\boldsymbol{G}$中的**指数**，记为$[\boldsymbol{G} : \boldsymbol{H}]$.*

定理 6.3. ***(Lagrange定理)***

若$\boldsymbol{G}$是有限群，$\boldsymbol{H}$是$\boldsymbol{G}$的子群，那么

$$|\boldsymbol{G}| = [\boldsymbol{G} : \boldsymbol{H}]|\boldsymbol{H}|.$$

证明 $\boldsymbol{H}a$是$\boldsymbol{G}$中$\boldsymbol{H}$的一个右陪集. 定义映射$f : \boldsymbol{H} \to \boldsymbol{H}a$，$f(h) = h * a$，显然$f$是双射. $\boldsymbol{G}$是有限群，$\boldsymbol{H}$是$\boldsymbol{G}$的子群，所以$\boldsymbol{H}$也是有限群，得出$|\boldsymbol{H}| = |\boldsymbol{H}a|$. 由定理6. 1知，$\boldsymbol{G}$中$\boldsymbol{H}$的右陪集全体构成$\boldsymbol{G}$的一个分划，令$\boldsymbol{G}$关于子群$\boldsymbol{H}$的右陪集个数$[\boldsymbol{G} : \boldsymbol{H}] = k$，$k$个不同的右陪集的代表元分别为$a_1, a_2, \cdots, a_k$，那么$\boldsymbol{G} = \boldsymbol{H}a_1 \bigcup \boldsymbol{H}a_2 \cdots \bigcup \boldsymbol{H}a_k$，其中$\boldsymbol{H}a_i \bigcap \boldsymbol{H}a_j = \varnothing, (i \neq j)$. 从而

$$\begin{aligned} |\boldsymbol{G}| &= |\boldsymbol{H}a_1| + |\boldsymbol{H}a_2| + \cdots + |\boldsymbol{H}a_k| \\ &= k \bullet |\boldsymbol{H}| = [\boldsymbol{G} : \boldsymbol{H}] \bullet |\boldsymbol{H}| \end{aligned}$$

由此定理可以得到两个非常有用的推论.

推论 6.1. *有限群$\boldsymbol{G}$中元素的阶是$|\boldsymbol{G}|$ 的因子.*

证明 在有限群中所有元素的阶必然是有限的. 设$\boldsymbol{G}$中元素a的阶为m，令$\boldsymbol{H} = \{a^0, a^1, \cdots, a^{m-1}\}$，显然$\boldsymbol{H}$是$\boldsymbol{G}$的$m$阶子群. 由Lagrange定理知$|\boldsymbol{G}| = [\boldsymbol{G} : \boldsymbol{H}] \bullet |\boldsymbol{H}| = [\boldsymbol{G} : \boldsymbol{H}] \bullet m$，故$m \mid |\boldsymbol{G}|$.

推论 6.2. *素数阶群都是循环群.*

证明 设$\boldsymbol{G}$是p阶群，p是素数，它的因子只有1和p. 由推论6. 1知$\boldsymbol{G}$中的元素的阶是1或p. 显然群$\boldsymbol{G}$的单位元的阶为1，非单位元元素a的阶为p，从而$\boldsymbol{G} = \langle a \rangle$.

例 6.4. *证明4阶群$\boldsymbol{G}$或者是4阶循环群$\boldsymbol{C}_4$或者是Klein-4群$\boldsymbol{K}_4$.*

证明 4阶群$\boldsymbol{G}$中元素的阶可能为1,2,4. 如果$\boldsymbol{G}$中包括4阶元a，那么$\boldsymbol{G}=\langle a\rangle=\{a^0,a^1,a^2,a^3\}$，即$\boldsymbol{G}$是4阶循环群$\boldsymbol{C}_4$. 如果$\boldsymbol{G}$中没有4阶元，那么除单位元$e$外，其他元素均是2阶元，即$\boldsymbol{G}=\{e,a,b,c\}$，$a^2=b^2=c^2=e$. 由前面的习题知该群必是交换群. $a*b$不能是a,b,e，否则推出$b=e$，$a=e$，$a=b$. 从而$a*b=c$. 同理可知$a*c=b$，$b*c=a$. 据此得出该群的乘法表:

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

故$\boldsymbol{G}$是Klein-4群$\boldsymbol{K}_4$.

例 6.5. *$\boldsymbol{G}$是6阶群，$\boldsymbol{G}$至少含有一个3阶子群.*

证明 $\boldsymbol{G}$是6阶群. $\boldsymbol{G}$中元素的阶可能是1，2，3，6. 如果$\boldsymbol{G}$中有3阶元a，那么$\langle a\rangle$就是$\boldsymbol{G}$的3阶子群. 如果$\boldsymbol{G}$中有6阶元a，那么$\langle a^2\rangle$为3阶子群. 下面证明$\boldsymbol{G}$中不可能既无3阶元也无6阶元. 也就是说$\boldsymbol{G}$中不可能除掉单位元e外都是2阶元. 用反证法，假设$\boldsymbol{G}=\{e,a,b,c,d,f\}$，且$a^2=b^2=c^2=d^2=f^2=e$. 由于$a*b$不可为a,b,e，取$\boldsymbol{K}=\{e,a,b,a*b\}$，其中$a*b\in\{c,d,f\}$，显然$\boldsymbol{K}$是Klein-4群. 而$\boldsymbol{K}\subseteq\boldsymbol{G}$. 故$\boldsymbol{K}$是$\boldsymbol{G}$的子群. $|\boldsymbol{K}|=4$. 而$4\nmid 6$，与Lagrange定理矛盾. 故不可. 综上知六阶群必有三阶子群.

6.2 正规子群与商群

本节介绍一类特殊的子群—正规子群.

定义 6.3. *$\boldsymbol{H}$是群$\boldsymbol{G}$的子群. 如果对所有的$\boldsymbol{G}$中元素g 和$\boldsymbol{H}$中元素h都有$g'*h*g\in\boldsymbol{H}$，那么称$\boldsymbol{H}$是$\boldsymbol{G}$的***正规子群***，并记为$\boldsymbol{H}\lhd\boldsymbol{G}$.*

定理 6.4. *$\boldsymbol{H}$是群$\boldsymbol{G}$的子群. $\boldsymbol{H}$是$\boldsymbol{G}$的正规子群当且仅当对$\boldsymbol{G}$中任意元素g，$\boldsymbol{H}g=g\boldsymbol{H}$.*

证明 若$\boldsymbol{H}$是$\boldsymbol{G}$的正规子群. 任取$x \in g\boldsymbol{H}$，存在$h_1 \in \boldsymbol{H}$使$x = g * h_1$. 而$x = (g^{'})^{'} * h_1 * g^{'} * g$，由正规子群的定义，$(g^{'})^{'} * h_1 * g^{'} \in \boldsymbol{H}$，故$x \in \boldsymbol{H}g$，于是$g\boldsymbol{H} \subseteq \boldsymbol{H}g$. 反过来，任取$y \in \boldsymbol{H}g$，存在$h_2 \in \boldsymbol{H}$使$y = h_2 * g$，而$y = g * g^{'} * h_2 * g$，由正规子群的定义$g^{'} * h_2 * g \in \boldsymbol{H}$，故$y \in g\boldsymbol{H}$. 于是$\boldsymbol{H}g = g\boldsymbol{H}$. 综上知，$\boldsymbol{H}g = g\boldsymbol{H}$.

又若对$\boldsymbol{G}$中任意元素g均有$\boldsymbol{H}g = g\boldsymbol{H}$，任取$h_3 \in \boldsymbol{H}$，必存在$h_4 \in \boldsymbol{H}$使$h_3 * g = g * h_4$，于是$g^{'} * h_3 * g = h_4 \in \boldsymbol{H}$，从而$\boldsymbol{H}$是$\boldsymbol{G}$的正规子群.

例 6.6. 三次二面体$\boldsymbol{D}_3$的子群$\boldsymbol{H} = \{\rho_1, \rho_2, \rho_3\}$是正规子群，

$$\begin{aligned}
&\rho_0\boldsymbol{H} = \rho_1\boldsymbol{H} = \rho_2\boldsymbol{H} = \boldsymbol{H}\rho_0 = \boldsymbol{H}\rho_1 = \boldsymbol{H}\rho_2 = \{\rho_0, \rho_1, \rho_2\}, \\
&\mu_1\boldsymbol{H} = \mu_2\boldsymbol{H} = \mu_3\boldsymbol{H} = \boldsymbol{H}\mu_1 = \boldsymbol{H}\mu_2 = \boldsymbol{H}\mu_3 = \{\mu_1, \mu_2, \mu_3\}.
\end{aligned}$$

$\widetilde{\boldsymbol{H}}$是$\boldsymbol{D}_3$的子群，但不是正规子群. 例如

$$\mu_2\widetilde{\boldsymbol{H}} = \{\mu_2, \rho_1\}，\ \widetilde{\boldsymbol{H}}\mu_2 = \{\mu_2, \rho_2\}.$$

$\mu_2\widetilde{\boldsymbol{H}} \neq \widetilde{\boldsymbol{H}}\mu_2$.

例 6.7. 指数为*2*的子群是正规子群.

证明 $\boldsymbol{H}$是群$\boldsymbol{G}$的子群且$[\boldsymbol{G}:\boldsymbol{H}] = 2$，即$\boldsymbol{G} = \boldsymbol{H} \bigcup \boldsymbol{H}a_1$，其中$a_1 \notin \boldsymbol{H}$，并且$\boldsymbol{H} \bigcap \boldsymbol{H}a_1 = \varnothing$. 我们任取群$\boldsymbol{G}$的元素$a$，有两种可能性：若$a \in \boldsymbol{H}$，由于$a\boldsymbol{H} = \boldsymbol{H}$，$\boldsymbol{H}a = \boldsymbol{H}$，故$a\boldsymbol{H} = \boldsymbol{H}a$；若$a \notin \boldsymbol{H}$，$\boldsymbol{G} = \boldsymbol{H} \bigcup \boldsymbol{H}a = \boldsymbol{H} \bigcup a\boldsymbol{H}$. $\boldsymbol{H}a = \boldsymbol{G} - \boldsymbol{H} = a\boldsymbol{H}$. 所以不管是哪种情况均有$a\boldsymbol{H} = \boldsymbol{H}a$. $\boldsymbol{H}$是$\boldsymbol{G}$的正规子群.

显然交换群的任何子群都是正规子群.

下面研究在$\boldsymbol{G}$中$\boldsymbol{H}$的所有右陪集构成的集合上的运算及相应的代数结构.

定义 6.4. $\boldsymbol{A}$，$\boldsymbol{B}$是群$\boldsymbol{G}$的非空子集，定义

$$\boldsymbol{A} \bullet \boldsymbol{B} = \{a * b | a \in \boldsymbol{A}, b \in \boldsymbol{B}\}.$$

该运算符满足结合律. 任取$x \in \boldsymbol{A} \bullet (\boldsymbol{B} \bullet \boldsymbol{C})$，存在$a \in \boldsymbol{A}$，$b \in \boldsymbol{B}$，$c \in \boldsymbol{C}$使$x = a*(b*c)$. 群$\boldsymbol{G}$中乘法满足结合律$x = (a*b)*c$，故$x \in (\boldsymbol{A} \bullet \boldsymbol{B}) \bullet \boldsymbol{C}$. 从而$\boldsymbol{A} \bullet (\boldsymbol{B} \bullet \boldsymbol{C}) \subseteq (\boldsymbol{A} \bullet \boldsymbol{B}) \bullet \boldsymbol{C}$. 同理也可证明$(\boldsymbol{A} \bullet \boldsymbol{B}) \bullet \boldsymbol{C} \subseteq \boldsymbol{A} \bullet (\boldsymbol{B} \bullet \boldsymbol{C})$. 最后得到$\boldsymbol{A} \bullet (\boldsymbol{B} \bullet \boldsymbol{C}) = (\boldsymbol{A} \bullet \boldsymbol{B}) \bullet \boldsymbol{C}$.

定理 6.5. $\boldsymbol{N}$是群$\boldsymbol{G}$的正规子群，$\langle \{\boldsymbol{N}g | g \in \boldsymbol{G}\}, \bullet \rangle$是群，称为$\boldsymbol{G}$模$\boldsymbol{N}$的**商群**，记为$\boldsymbol{G}/\boldsymbol{N}$.

证明 首先研究两个正规子群的右陪集怎样做乘法.

$$\boldsymbol{N}g_1 \bullet \boldsymbol{N}g_2 = \{(n_1 * g_1) * (n_2 * g_2) | n_1, n_2 \in \boldsymbol{N}\}.$$

因$\boldsymbol{N}$是$\boldsymbol{G}$的正规子群，对于$\boldsymbol{G}$中元素g_1，有$g_1\boldsymbol{N} = \boldsymbol{N}g_1 . g_1 * n_2 \in g_1\boldsymbol{N}$，那么存在$n_3 \in \boldsymbol{N}$使$g_1 * n_2 = n_3 * g_1$，代入上式，

$$\begin{aligned} \boldsymbol{N}g_1 \bullet \boldsymbol{N}g_2 &= \{n_1 * (n_3 * g_1) * g_2 | n_1, n_2 \in \boldsymbol{N}\} \\ &= \{n * (g_1 * g_2) | n \in \boldsymbol{N}\} \\ &= \boldsymbol{N}g_1 * g_2. \end{aligned}$$

这里定义的正规子群右陪集间的乘法运算与右陪集代表元的选取无关. 这是因为，如果$\boldsymbol{N}g_1 = \boldsymbol{N}a_1$，$\boldsymbol{N}g_2 = \boldsymbol{N}a_2$，即$g_1 * a_1', g_2 * a_2' \in \boldsymbol{N}$，那么

$$(g_1 * g_2) * (a_1 * a_2)' = g_1 * (g_2 * a_2') * a_1'.$$

令$n_1 = g_2 * a_2'$，$n_1 * a_1' = a_1' * n_2$，$n_3 = g_1 * a_1'$

$$(g_1 * g_2) * (a_1 * a_2)' = n_3 * n_2 \in \boldsymbol{N}.$$

于是$\boldsymbol{N}g_1 * g_2 = \boldsymbol{N}a_1 * a_2$.

在集合$\{\boldsymbol{N}g | g \in \boldsymbol{G}\}$上的乘法运算显然是封闭的. 并且满足结合律. $\boldsymbol{N} = \boldsymbol{N}e$是单位元，$\boldsymbol{N}g'$是$\boldsymbol{N}g$的逆元. 所以$\langle \boldsymbol{N}g | g \in \boldsymbol{G}, \bullet \rangle$是群.

当$\boldsymbol{G}$是有限群时，$\boldsymbol{G}$模$\boldsymbol{N}$的商群$\boldsymbol{G}/\boldsymbol{N}$中的元素个数就是$\boldsymbol{N}$在$\boldsymbol{G}$中的指数，故

$$|\boldsymbol{G}/\boldsymbol{N}| = |\boldsymbol{G}|/|\boldsymbol{N}|.$$

例 6.8. 整数加群$\langle \boldsymbol{Z}, + \rangle$是交换群. 每个子群都是正规子群. $\boldsymbol{Z}$模正规子群$\langle n \rangle = \{kn | k \in \boldsymbol{Z}\} = n\boldsymbol{Z}$的商群.

$$\boldsymbol{Z}/n\boldsymbol{Z} = \{n\boldsymbol{Z}, 1+n\boldsymbol{Z}, \cdots, (n-1)+n\boldsymbol{Z}\}.$$

若映射$f: \boldsymbol{Z}/n\boldsymbol{Z} \to \boldsymbol{Z}_n$，$f(i+n\boldsymbol{Z}) = [i]$，显然$f$是双射，故

$$\boldsymbol{Z}/n\boldsymbol{Z} \cong \boldsymbol{Z}_n.$$

例 6.9. 三次二面体$\boldsymbol{D}_3$中，子群$\boldsymbol{H} = \{\rho_0, \rho_1, \rho_2\}$的指数为2. $\boldsymbol{H}$是$\boldsymbol{D}_3$的正规子群，$\boldsymbol{D}_3$模$\boldsymbol{H}$ 的商群

$$\boldsymbol{D}_3/\boldsymbol{H} = \{\boldsymbol{H}, (12)\boldsymbol{H}\}$$

是2阶循环群.

例 6.10. $\boldsymbol{G}$是有限交换群. 素数p是$|\boldsymbol{G}|$的因子，那么群$\boldsymbol{G}$中必有一个p阶元.

证明 我们对群$\boldsymbol{G}$的阶数进行归纳证明. 当$|\boldsymbol{G}| = 2$时，$\boldsymbol{G} = \{e, a\}$且$a^2 = e$. 素数$2 \mid |\boldsymbol{G}|$. a是2阶元，命题成立. 假设$|\boldsymbol{G}| < k$时，命题成立. 现设$|\boldsymbol{G}| = k$，某素数$p|k$. 任取$\boldsymbol{G}$的某个非单位元素g，它的阶为t，显然$t|k$且$t > 1$. 如果$p|t$，即$t = rp$，则g^r 是$\boldsymbol{G}$中的p阶元. 如果$p \nmid t$，考虑$\boldsymbol{G}$模正规子群$\langle g\rangle$的商群$\boldsymbol{G}/\langle g\rangle$.

$$|\boldsymbol{G}/\langle g\rangle| = |\boldsymbol{G}|/t < |\boldsymbol{G}| = k,$$

$\boldsymbol{G}/\langle g\rangle$仍是有限交换群. 由于$p|k$，$p \nmid t$，故$p \mid |\boldsymbol{G}/\langle g\rangle|$. 由归纳假设知在$\boldsymbol{G}/\langle g\rangle$中有$p$阶元$a\langle g\rangle$. 假设$a$在$\boldsymbol{G}$中的阶为$u$，显然有$(a\langle g\rangle)^u = \langle g\rangle$. 从而$p|u$. 由前面讨论知，$a^{u/p}$是$\boldsymbol{G}$的$p$阶元. 命题对$|\boldsymbol{G}| = k$ 也成立.

一般地，n阶群$\boldsymbol{G}$，对n的因子d，在$\boldsymbol{G}$中不一定有d阶子群. 例如:全体四元偶置换构成$\boldsymbol{A}_4$，$|\boldsymbol{A}_4| = 12$. 6是12的因子，但$\boldsymbol{A}_4$没有6阶子群，这是因为$\boldsymbol{A}_4$中有1个1阶元，8个3阶元，3个2阶元. 若$\boldsymbol{H}$是$\boldsymbol{A}_4$的6阶子群，因2阶元只有3个. 故$\boldsymbol{H}$中至少有1个3阶元，不妨假设是$(a,b,c) \in \boldsymbol{H}$. 3阶元的逆元仍是3阶元，故3阶元必须成对出现. 单位元$e \in \boldsymbol{H}$，所以$\boldsymbol{H}$中至少有一个2阶元，不妨假设是$(ab)(cd) \in \boldsymbol{H}$. 由$(a,b,c) \in \boldsymbol{H}$，$(ab)(cd) \in \boldsymbol{H}$推出$(abc)' = (acb) \in \boldsymbol{H}$，$(abc)(ab)(cd) = (acd) \in \boldsymbol{H}$，$(acd)' = (adc) \in \boldsymbol{H}$，$(ab)(cd)(abc) = (bdc) \in \boldsymbol{H}$，$(bdc)' = (bcd) \in \boldsymbol{H}, \cdots$，$\boldsymbol{H}$中的元素个数已超过6个，与$\boldsymbol{H}$是$\boldsymbol{A}_4$的6阶子群矛盾. 所以$\boldsymbol{A}_4$没有6阶子群.

6.3 群的同态

本节继续讨论两个群的关系.

定义 6.5. *在群$\langle \boldsymbol{G}_1, *\rangle$和$\langle \boldsymbol{G}_2, \bullet\rangle$之间存在映射$f: \boldsymbol{G}_1 \to \boldsymbol{G}_2$，对任意$a, b \in \boldsymbol{G}_1$，$f(a * b) = f(a) \bullet f(b)$，则称$f$是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的***同态映射***(简称**同态**). 如果f是满射(单射，双射)，则称f是***满同态映射(单一同态映射，同构映射)***.*

若f是从群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的同态映射，$\boldsymbol{G}_1$，$\boldsymbol{G}_2$单位元分别为e_1和e_2，那么$f(e_1) = e_2$. 对任意$a \in \boldsymbol{G}$，$f(a^{'}) = (f(a))^{'}$. 此结论证明方法与群同构映射相应性质证明方法相同.

定义 6.6. *f是从群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射，f的**核**是$\boldsymbol{G}_1$中通过f映到$\boldsymbol{G}_2$的单位元e_2的那些元素组成的集合，记为$Kerf$，*

$$Kerf = \{a | a \in \boldsymbol{G}_1, f(a) = e_2\}.$$

.

定理 6.6. *f是从群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射.*
1° $Kerf$是群$\boldsymbol{G}_1$的正规子群.
2° f为单射而且仅当$Kerf = \{e_1\}$.

证明

1° f是从群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射. 由于$f(e_1) = e_2$，$e_1 \in \mathrm{Ker}f$，所以$\mathrm{Ker}f$是$\boldsymbol{G}_1$的非空子集. 任取$g_1, g_2 \in \mathrm{Ker}f$，$f(g_1) = f(g_2) = e_2$，而

$$f(g_1 * g_2) = f(g_1) \bullet f(g_2) = e_2 \bullet e_2 = e_2,$$
$$f(g_1^{'}) = (f(g_1))^{'} = e_2^{'} = e_2.$$

故$g_1 * g_2 \in \mathrm{Ker}f$，$g_1^{'} \in \mathrm{Ker}f$从而$\mathrm{Ker}f$是$\boldsymbol{G}_1$的子群，任取$g \in \boldsymbol{G}_1$，$k \in \mathrm{Ker}f$，

$$\begin{aligned} f(g^{'} * k * g) &= (f(g))^{'} \bullet f(k) \bullet f(g) \\ &= (f(g))^{'} \bullet e_2 \bullet f(g) = e_2, \end{aligned}$$

故$g^{'}*k*g\in \mathrm{Ker}f$.$\mathrm{Ker}f$是$\boldsymbol{G}_1$的正规子群.

2° 当f为单射时，只有e_1的像为e_2，故$\mathrm{Ker}f=\{e_1\}$，反过来，当$\mathrm{Ker}f=\{e_1\}$时，如果存在$g_2\in \boldsymbol{G}_2$，它有两个不同的原像$g_{11},g_{12}\in \boldsymbol{G}_1$，$g_{11}\neq g_{12}$，$f(g_{11})=f(g_{12})=g_2$.

$$f(g_{11}*g_{12}^{'})=f(g_{11})\bullet(f(g_{12}))^{'}=g_2\bullet g_2^{'}=e_2.$$

那么$g_{11}*g_{12}^{'}\in \mathrm{Ker}f=\{e_1\}$，即$g_{11}*g_{12}^{'}=e_1$. 从而得到$g_{11}=g_{12}$，矛盾. 这说明如果$\boldsymbol{G}_2$中的元素有原像，那么原像是唯一的，所以$f$是单射.

例 6.11. $\boldsymbol{G}_1$和$\boldsymbol{G}_2$是任意两个群，令$f:\boldsymbol{G}_1\to\boldsymbol{G}_2$，对任意$g\in\boldsymbol{G}_1$，$f(g)=e_2$. 任取$g_1,g_2\in\boldsymbol{G}_1$，

$$f(g_1*g_2)=e_2=e_2\bullet e_2=f(g_1)\bullet f(g_2),$$

f是群同态映射. $\mathrm{Ker}f=\boldsymbol{G}_1$，我们称这个特殊的同态映射为零同态映射.

例 6.12. $\boldsymbol{G}_1=\langle\boldsymbol{Z},+\rangle$，$\boldsymbol{G}_2=\langle\boldsymbol{C},\bullet\rangle$，令$f:\boldsymbol{Z}\to\boldsymbol{C}$. $f(m)=\mathrm{i}^m$. $f(k+l)=\mathrm{i}^{k+l}=\mathrm{i}^k\bullet\mathrm{i}^l=f(k)\bullet f(l)$. f是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的同态映射. $\mathrm{Ker}f=\{n|\mathrm{i}^n=1\}=\{4m|m\in\boldsymbol{Z}\}$. f的像集$\mathrm{Im}f=\{1,-1,\mathrm{i},-\mathrm{i}\}$.

定理 6.7. *f是群$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的一个同态映射.*

1° 若$\boldsymbol{H}_1\leqslant\boldsymbol{G}_1$，则$f(\boldsymbol{H}_1)\leqslant\boldsymbol{G}_2$，特别地$f(\boldsymbol{G}_1)\leqslant\boldsymbol{G}_2$;

2° 若$\boldsymbol{H}_1\lhd\boldsymbol{G}_1$，则$f(\boldsymbol{H}_1)\lhd\boldsymbol{G}_1$;

3° 若$\boldsymbol{H}_2\leqslant f(\boldsymbol{G}_1)$，则$f^{-1}(\boldsymbol{H}_2)\leqslant\boldsymbol{G}_1$;

4° 若$\boldsymbol{H}_2\lhd f(\boldsymbol{G}_1)$，则$f^{-1}(\boldsymbol{H}_2)\lhd\boldsymbol{G}_1$且$\boldsymbol{G}_1/f^{-1}(\boldsymbol{H}_2)\cong f(\boldsymbol{G}_1)/\boldsymbol{H}_2$.

证明 这里只证2°，3°，其他留作练习题.

2° $\boldsymbol{H}_1$是$\boldsymbol{G}_1$的正规子群，由1°知$f(\boldsymbol{H}_1)\leqslant\boldsymbol{G}_2$. 而$f(\boldsymbol{H}_1)\subseteq f(\boldsymbol{G}_1)\subseteq\boldsymbol{G}_2$，$f(\boldsymbol{G}_1)$为群，故$f(\boldsymbol{H}_1)$是$f(\boldsymbol{G}_1)$的子群. 任取$y\in f(\boldsymbol{G}_1)$，$x\in f(\boldsymbol{H}_1)$，存在$g\in\boldsymbol{G}_1$，$h\in\boldsymbol{H}_1$使$f(g)=y$，$f(h)=x$.

$$y^{'}\bullet x\bullet y=f(g^{'})\bullet f(h)\bullet f(g)=f(g^{'}*h*g).$$

由于$\boldsymbol{H}_1$是$\boldsymbol{G}_1$的正规子群，$g^{'}*h*g\in\boldsymbol{H}_1$，故$y^{'}\bullet x\bullet y\in f(\boldsymbol{H}_1)$，$f(\boldsymbol{H}_1)$是$f(\boldsymbol{G}_1)$的正规子群.

3° $\boldsymbol{H}_2$是$f(\boldsymbol{G}_1)$的子群. $f^{-1}(\boldsymbol{H}_2)=\{x|x\in\boldsymbol{G}_1, f(x)\in\boldsymbol{H}_2\}\subseteq\boldsymbol{G}_1$，$f(e_1)=e_2\in\boldsymbol{H}_2$，显然$e_1\in f^{-1}(\boldsymbol{H}_2)$.$f^{-1}(\boldsymbol{H}_2)$是$\boldsymbol{G}_1$的非空子集. 若$x_1,x_2\in f^{-1}(\boldsymbol{H}_2)$，存在$h_1,h_2\in\boldsymbol{H}_2$，使$f(x_1)=h_1$，$f(x_2)=h_2$.

$$\begin{aligned}
&f(x_1*x_2)=f(x_1)\bullet f(x_2)=h_1\bullet h_2\in\boldsymbol{H}_2,\\
&f(x_1^{'})=(f(x_1))^{'}=h_1^{'}\in\boldsymbol{H}_2.
\end{aligned}$$

可知$x_1*x_2\in f^{-1}(\boldsymbol{H}_2)$，$x_1^{'}\in f^{-1}(\boldsymbol{H}_2)$. 从而$f^{-1}(\boldsymbol{H}_1)$是$\boldsymbol{G}_1$的子群.

定理 6.8. f是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射，对任意$a\in\boldsymbol{G}_1$，$f^{-1}(f(a))=aKerf$.

证明 任取$a\in\boldsymbol{G}_1$，f是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的群同态映射，$f(a)\in\boldsymbol{G}_2$. 由f^{-1}定义知$f^{-1}(f(a))=\{x|x\in\boldsymbol{G}_1, f(x)=f(a)\}$. 任取$x\in f^{-1}(f(a))$，$f(a^{'}*x)=f(a^{'})\bullet f(x)=(f(a))^{'}\bullet f(a)=e_2$，故$a^{'}*x\in\mathrm{Ker}f$，即$x\in a\mathrm{Ker}f$. 从而得到$f^{-1}(f(a))\subseteq a\mathrm{Ker}f$. 又任取$y^{'}\in a\mathrm{Ker}f$，存在$k\in\mathrm{Ker}f$使$y=a*k$，$f(y)=f(a)\bullet f(k)=f(a)\bullet e_2=f(a)$，所以$y\in f^{-1}(f(a))$. 又得出$a\mathrm{Ker}f\subseteq f^{-1}(f(a))$. 综上分析知

$$f^{-1}(f(a))=a\mathrm{Ker}f.$$

这个定理说明了，若f是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的满同态，则$\boldsymbol{G}_2$中每个元素的原像集正好是f的同态核$\mathrm{Ker}f$的一个陪集. 据此，我们可以在$\boldsymbol{G}_1/\mathrm{Ker}f$和$\boldsymbol{G}_2$之间建立起一个一一对应关系.

定理 6.9. ***(群同态基本定理)***

群$\boldsymbol{G}_1$的任何商群都是$\boldsymbol{G}_1$的同态像. 若$\boldsymbol{G}_2$是$\boldsymbol{G}_1$的同态像，则$\boldsymbol{G}_1/Kerf\cong\boldsymbol{G}_2$.

证明 设$\boldsymbol{H}$是群$\boldsymbol{G}_1$的正规子群. 定义$\varphi:\boldsymbol{G}_1\to\boldsymbol{G}_1/\boldsymbol{H}$，$\varphi(a)=a\boldsymbol{H}$. 显然$\varphi$是满同态映射，$\varphi(\boldsymbol{G}_1)=\boldsymbol{G}_1/\boldsymbol{H}$，这就证明了群$\boldsymbol{G}_1$的任何商群都是$\boldsymbol{G}_1$的同态像.

若$\boldsymbol{G}_2$是$\boldsymbol{G}_1$的同态像，即$f:\boldsymbol{G}_1\to\boldsymbol{G}_2$，$f(\boldsymbol{G}_1)=\boldsymbol{G}_2$. 定义$\tilde{f}:\boldsymbol{G}_1/\mathrm{Ker}f\to\boldsymbol{G}_2$，$\tilde{f}(a\mathrm{Ker}f)=f(a)$. 首先说明$\tilde{f}$是映射，就是说如果$a_1\mathrm{Ker}f=a_2\mathrm{Ker}f$，

那么$a_1^{'} * a_2 \in \mathrm{Ker}f$. 而$(f(a_1))^{'} \bullet f(a_2) = f(a_1^{'} * a_2) = e_2$，得出$f(a_1) = f(a_2)$，即映射$\tilde{f}$与代表元选取无关.

任取$y \in \boldsymbol{G}_2 = f(\boldsymbol{G}_1)$，存在$a \in \boldsymbol{G}_1$使$y = f(a)$，那么$a\mathrm{Ker}f \in \boldsymbol{G}_1/\mathrm{Ker}f$是$y$的原像. 又若$a_1\mathrm{Ker}f, a_2\mathrm{Ker}f \in \boldsymbol{G}_1/\mathrm{Ker}f$都是$y \in f(\boldsymbol{G}_1)$的原像，那么$f(a_1) = f(a_2)$. 而$f(a_1^{'} * a_2) = (f(a_1))^{'} \bullet f(a_2) = e_2$，故$a_1^{'} * a_2 \in \mathrm{Ker}f$，即$a_1\mathrm{Ker}f = a_2\mathrm{Ker}f$. 由上面分析知$\tilde{f}$是双射.

$$\begin{aligned}\tilde{f}(a\mathrm{Ker}f \bullet b\mathrm{Ker}f) = \tilde{f}&((a * b)\mathrm{Ker}f)\\ &= f(a * b) = f(a) \bullet f(b)\\ &= \tilde{f}(a\mathrm{Ker}f) \bullet \tilde{f}(b\mathrm{Ker}f).\end{aligned}$$

故$\tilde{f}$保持运算，是群同构映射. 最后得到

$$\boldsymbol{G}_1/\mathrm{Ker}f \cong f(\boldsymbol{G}_1)$$

例 6.13. $\boldsymbol{H}$是群$\boldsymbol{G}$的正规子群. 令$\varphi : \boldsymbol{G} \to \boldsymbol{G}/\boldsymbol{H}$，$\varphi(a) = a\boldsymbol{H}$，称$\varphi$为自然同态. φ的同态核

$$\begin{aligned}Ker\varphi &= \{x | x \in \boldsymbol{G}, \varphi(x) = \boldsymbol{H}\}\\ &= \{x | x \in \boldsymbol{G}, x\boldsymbol{H} = \boldsymbol{H}\} = \boldsymbol{H}.\end{aligned}$$

例 6.14. 令$\boldsymbol{G}_1 = \langle \boldsymbol{Z}, + \rangle$，$\boldsymbol{G}_2 = \langle a \rangle = \{a^0, a^1, \cdots, a^{n-1}\}$且$a^n = e$. 定义$f : \boldsymbol{Z} \to \langle a \rangle$，$f(m) = a^m$，$f$是从$\boldsymbol{G}_1$到$\boldsymbol{G}_2$的满同态映射，它的同态核

$$Kerf = \{m | m \in \boldsymbol{Z}, a^m = a^0\} = \{kn | k \in \boldsymbol{Z}\} = n\boldsymbol{Z}.$$

由群同态基本定理知

$$\boldsymbol{Z}/n\boldsymbol{Z} \cong \langle a \rangle.$$

而$\boldsymbol{Z}/n\boldsymbol{Z} \cong \boldsymbol{Z}_n$，所以$\langle a \rangle \cong \boldsymbol{Z}_n$. 我们再次得到“$n$阶循环群同构于模$n$同余类群”这个结论.

例 6.15. 用同态基本定理证明定理*6. 7*中的*4°*.

证明 已知$\boldsymbol{H}_2$是$f(\boldsymbol{G}_1)$的正规子群. 定义$\tilde{f} : \boldsymbol{G}_1 \to f(\boldsymbol{G}_1)/\boldsymbol{H}_2$.$\tilde{f}(a) = f(a)\boldsymbol{H}_2$. 由于$f : \boldsymbol{G}_1 \to f(\boldsymbol{G}_1)$是满同态映射，易知$\tilde{f}$也是满同态映射.

$$\begin{aligned}\mathrm{Ker}\tilde{f} &= \{x|x \in \boldsymbol{G}_1, f(x)\boldsymbol{H}_2 = \boldsymbol{H}_2\}\\ &= \{x|x \in \boldsymbol{G}_1, f(x) \in \boldsymbol{H}_2\} = f^{-1}(\boldsymbol{H}_2),\end{aligned}$$

由定理6. 6知$f^{-1}(\boldsymbol{H}_2)$是$\boldsymbol{G}_1$的正规子群. 再由群同态基本定理知

$$\boldsymbol{G}_1/f^{-1}(\boldsymbol{H}_2) \cong f(\boldsymbol{G}_1)/\boldsymbol{H}_2.$$

定理 6.10. $\boldsymbol{H}$，$\boldsymbol{K}$均是群$\boldsymbol{G}$的正规子群，且$\boldsymbol{K} \subseteq \boldsymbol{H}$，那么

$$\boldsymbol{G}/\boldsymbol{H} \cong \frac{\boldsymbol{G}/\boldsymbol{K}}{\boldsymbol{H}/\boldsymbol{K}}.$$

证明 $\boldsymbol{K}$是群$\boldsymbol{G}$的子群. $\boldsymbol{K}$对于$\boldsymbol{G}$中的运算构成群. $\boldsymbol{K} \subseteq \boldsymbol{H}$，$\boldsymbol{H}$对于$\boldsymbol{G}$中的运算也构成群，从而$\boldsymbol{K}$也是$\boldsymbol{H}$的子群. 任取$h \in \boldsymbol{H} \subseteq \boldsymbol{G}$，$k \in \boldsymbol{K}$，由于$\boldsymbol{K}$是$\boldsymbol{G}$的正规子群，$h' * k * h \in \boldsymbol{K}$，所以$\boldsymbol{K}$是$\boldsymbol{H}$的正规子群，从而$\boldsymbol{H}/\boldsymbol{K}$是群.

令$f : \boldsymbol{G}/\boldsymbol{K} \to \boldsymbol{G}/\boldsymbol{H}$，$f(a\boldsymbol{K}) = a\boldsymbol{H}$，容易证明$f$与代表元选取无关，$f$是映射，并且是满射.

$$\begin{aligned}f(a\boldsymbol{K} \bullet b\boldsymbol{K}) &= f(a * b\boldsymbol{K}) = a * b\boldsymbol{H} = a\boldsymbol{H} \bullet b\boldsymbol{H}\\ &= f(a\boldsymbol{K}) \bullet f(b\boldsymbol{K}),\end{aligned}$$

f是满同态映射，它的同态核

$$\begin{aligned}\mathrm{Ker}f &= \{a\boldsymbol{K}|a\boldsymbol{K} \in \boldsymbol{G}/\boldsymbol{K}, f(a\boldsymbol{K}) = \boldsymbol{H}\}\\ &= \{a\boldsymbol{K}|a\boldsymbol{K} \in \boldsymbol{G}/\boldsymbol{K}, a\boldsymbol{H} = \boldsymbol{H}\}\\ &= \{a\boldsymbol{K}|a \in \boldsymbol{H}\} = \boldsymbol{H}/\boldsymbol{K}.\end{aligned}$$

由同态基本定理知

$$\frac{\boldsymbol{G}/\boldsymbol{K}}{\boldsymbol{H}/\boldsymbol{K}} \cong \boldsymbol{G}/\boldsymbol{H}.$$

习题

1. $\boldsymbol{H}$是交换群$\boldsymbol{G}$的子群，证明$\boldsymbol{H}$的每个左陪集也是一个右陪集.

2. $\boldsymbol{H}$是$\boldsymbol{G}$的子群，a, b是$\boldsymbol{G}$中的元素，证明以下六个命题是等价的:

(1)$a' * b \in \boldsymbol{H}$; (2)$b' * a \in \boldsymbol{H}$; (3)$b \in a\boldsymbol{H}$;

(4)$a \in b\boldsymbol{H}$;　　(5)$a\boldsymbol{H} = b\boldsymbol{H}$;　　(6)$a\boldsymbol{H} \bigcap b\boldsymbol{H} \neq \varnothing$.

3. 写出$\boldsymbol{A}_4$中关于$\boldsymbol{H} = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$的左陪集分解与右陪集分解.

4. $\boldsymbol{H}$是群$\boldsymbol{G}$的指数为2的子群. 证明:对于$\boldsymbol{G}$的任意元素a必有$a^2 \in \boldsymbol{H}$, 若$\boldsymbol{H}$的指数为3，是否对$\boldsymbol{G}$的任意元素a有$a^3 \in \boldsymbol{H}$? 证明你的断言.

5. $\boldsymbol{H}$,$\boldsymbol{K}$是$\boldsymbol{G}$的两个子群，$[\boldsymbol{G} : \boldsymbol{H}] = m$，$[\boldsymbol{G}, \boldsymbol{K}] = n$，证明子群$\boldsymbol{H} \bigcap \boldsymbol{K}$在$\boldsymbol{G}$中的指数$\leqslant m \bullet n$.

6. 群$\boldsymbol{G}$的阶数为$p \bullet q$，其中p, q均为素数且$p < q$. 证明:群$\boldsymbol{G}$不可能有两个不同的q阶子群.

7. $\boldsymbol{H}$是$\boldsymbol{G}$的正规子群. 如果a和b属于$\boldsymbol{H}$的同一个陪集中，c和d属于$\boldsymbol{H}$的同一个陪集中，那么$a * c$和$b * d$属于$\boldsymbol{H}$的同一个陪集中.

8. $\boldsymbol{G}$是整数加群，$\boldsymbol{H} = \{mk | k \in \boldsymbol{Z}\}$. 商群$\boldsymbol{G}/\boldsymbol{H}$含有哪些元素? 它的单位元是什么? 写出该商群的乘法表.

9. 如果群$\boldsymbol{G}$中含有一个某阶子群，那么该群必是正规子群.

10. $\boldsymbol{H}_1$和$\boldsymbol{H}_2$是群$\boldsymbol{G}$的正规子群. 证明：$\boldsymbol{H}_1 \bigcap \boldsymbol{H}_2$，$\boldsymbol{H}_1 \bullet \boldsymbol{H}_2$ 也是$\boldsymbol{G}$的正规子群.

11. $\boldsymbol{H}_1, \boldsymbol{H}_2, \boldsymbol{N}$都是$\boldsymbol{G}$的正规子群，并且$\boldsymbol{H}_1 \subset \boldsymbol{H}_2$，证明$\boldsymbol{H}_1 \bullet \boldsymbol{N}$是$\boldsymbol{H}_2 \bullet \boldsymbol{N}$的正规子群

12. $\boldsymbol{H}$,$\boldsymbol{K}$都是群$\boldsymbol{G}$的正规子群并且$\boldsymbol{H} \bigcap \boldsymbol{K} = \{e\}$. 证明:对任意$h \in \boldsymbol{H}$, $k \in \boldsymbol{K}$，都有$h * k = k * h$.

13. 在$\boldsymbol{G} = \{f | f : \boldsymbol{Z} \to \boldsymbol{Z}/(2)\}$上定义运算$+$.

$$(f + g)(x) = f(x) + g(x).$$

证明：$\langle \boldsymbol{G}, + \rangle$是交换群，并且非零元素的阶为2.

14. 在非零实数乘法群中，如下定义的映射f中，哪些是同态映射，并且找出它的同态核.

(1)$f_1(x) = |x|$;　　(2)$f_2(x) = 2x$;　　(3)$f_3(x) = x^2$;

(4)$f_4(x) = \frac{1}{x}$;　　(5)$f_5(x) = -x$;　　(6)$f_6(x) = -\dfrac{1}{x}$.

15. 令$\boldsymbol{G} = \{\boldsymbol{A} | \boldsymbol{A} \in (\boldsymbol{Q})_n, |\boldsymbol{A}| \neq 0\}$，$\boldsymbol{G}$对于矩阵乘法构成群. $f : \boldsymbol{G} \to \boldsymbol{R}^*$，$f(\boldsymbol{A}) = |\boldsymbol{A}|$. 证明: f 是从群$\boldsymbol{G}$到非零实数乘群$\boldsymbol{R}^*$的同态映射. 求$f(\boldsymbol{G})$和$\mathrm{Ker} f$.

16. $\boldsymbol{G}$是交换群，k是取定的正整数. $f:\boldsymbol{G}\to\boldsymbol{G}$，$f(a)=a^k$. 证明:$f$是同态映射. 求出$f(\boldsymbol{G})$和$\mathrm{Ker}f$.

17. $\boldsymbol{G}=\langle a\rangle$是$n$阶循环群，$\boldsymbol{G}^{'}=\langle b\rangle$是$m$阶循环群，证明:

$$m|nk\Leftrightarrow\exists\varphi:\boldsymbol{G}\to\boldsymbol{G}^{'}\text{是同态映射并且}\varphi(a)=b^k.$$

18. $\boldsymbol{H}$是$\boldsymbol{G}$的正规子群，$[\boldsymbol{G}:\boldsymbol{H}]=m$. 证明:对于$\boldsymbol{G}$的任意元素$x,x^m\in\boldsymbol{H}$.

19. $\boldsymbol{H},\boldsymbol{K}$是$\boldsymbol{G}$的正规子群. 如果$\boldsymbol{G}/\boldsymbol{H}$，$\boldsymbol{G}/\boldsymbol{K}$是交换群，那么$\boldsymbol{G}/\boldsymbol{H}\bigcap\boldsymbol{K}$也是交换群.

20. 在群$\boldsymbol{G}$中，a,b是$\boldsymbol{G}$中的元素，称$a^{'}*b^{'}*a*b$为$\boldsymbol{G}$的换位元. 证明:

(1)$\boldsymbol{G}$的所有有限个换位元乘积构成$\boldsymbol{G}^{'}$，$\boldsymbol{G}^{'}$是$\boldsymbol{G}$的正规子群;

(2)$\boldsymbol{G}/\boldsymbol{G}^{'}$是交换群;

(3)若$\boldsymbol{N}$是$\boldsymbol{G}$的正规子群且$\boldsymbol{G}/\boldsymbol{N}$是交换群，那么$\boldsymbol{G}^{'}$是$\boldsymbol{N}$的子群.