信息安全数学基础

第七章　代数系统和群

7.1 代数系统

7.1 代数系统

代数系统也称为代数结构，是指定义了若干运算的集合，它通常有三部分组成：

（1）集合，也叫载体。

是由将要处理的对象构成，如整数、实数、函数、矩阵等。

（2）运算

定义在集合上，可能是一元运算、二元运算、也可能是多元运算，如函数求逆、矩阵求逆、整数相加及相乘等。

（3）集合上的特异元素。

例如整数集合 Z ，其上的运算+，常数0，构成一代数系统，记为$\langle Z,+,0\rangle$ 。有时为了简化，特异元素可以不写。有时把运算和特异元素都不写。

代数系统上的运算通常需要满足封闭性。设S是代数系统中的集合，$\circ$和Δ分别是S上的二元运算和一元运算，如果对$\forall a,b \in S$，有$a \circ b \in S$，则称S对$\circ$是封闭的。如果对$\forall a \in S$，有$\Delta a \in S$，则称S对Δ是封闭的。

常见的特异元素有单位元、零元和逆元。

定义1.1 设代数系统为 $\langle S,*\rangle$，其中 $*$ 是 S 上的二元运算，1 是 S 的元素，如果对 $\forall x\in S$，有 $1*x=x*1=x$，则称1是 S 关于 $*$ 的单位元。0是 S 中的元素，如果对 $\forall x\in S$，$0*x=x*0=0$，则称0是 S 的零元。

定理1.1 设代数系统 $\langle S,*\rangle$ 有单位元（零元），则单位元（零元）是唯一的。

证明 设1和 $1'$ 是单位元，则 $1=1*1'=1'$。零元的证明类似。证毕。

定义1.2 设代数系统 $\langle S,*\rangle$，$*$ 是 S 上的二元运算，1是S 关于 $*$ 的单位元。对 $x\in S$，如果存在 $y\in S$，使得 $x*y=y*x=1$，则称 y 是 x 的逆元，记为 $x^{-1}=y$。

定理1.2 在$\langle S,*\rangle$中，如果 $x\in S$ 有逆元，则逆元是唯一的。

证明 设 y_1,y_2 是 x 的逆元，即 $x*y_1=x*y_2=1$，则 $y_1=y_1*1=y_1*(x*y_2)=(y_1*x)*y_2=1*y_2=y_2$。 证毕。

定义1.3 设 $A=\langle S,*,\Delta,k\rangle$ 是一代数系统，如果

（1）$S'\subseteq S$ ；

（2）S' 对 $*$ 和 Δ 封闭；

（3）$k\in S'$；

则称 $A'=\langle S',*,\Delta,k\rangle$ 是 A 的子代数。

一些代数系统在结构上非常相似或结构上一致，用同态或同构来刻画两个代数结构的相似或一致。

定义1.4 设$A=\langle S,*,\Delta,k\rangle$和$A'=\langle S',*',\Delta',k'\rangle$是具有相同构成成分的2个代数系统，$h$ 是一个函数。如果

（1）$h:S\to S'$；

（2）对$\forall a,b\in S$，有$h(a*b)=h(a)*'h(b)$；

（3）对$\forall a\in S$，有$h(\Delta a)=\Delta' h(a)$；

（4）$h(k)=k'$；

则称 h 是A到A'的同态，$\langle h(S),*',\Delta',k'\rangle$ 称 A 为 h 在下的同态像。如果 h 是单射，则称之为单同态；如果 h 是满射，则称之为满同态。如果 h 是双射（也称一一映射），则称同构，此时称 A和 A'是同构的，同构的两个代数系统结构上完全相同，因此有完全相同的性质。

7.2 群

7.2 群

定义2. 1 设代数系统 $\langle G,\cdot\rangle$ 满足以下性质：

（1）封闭性；

（2）结合律，即对 $\forall a, b, c \in G$，有$(a\cdot b)\cdot c = a\cdot(b\cdot c)$ ；

（3）有单位元；

（4）任一元素都有逆元；

则称 $\langle G,\cdot\rangle$ 是群。若仅满足（1）（2）两条，则称 $\langle G,\cdot\rangle$ 是半群。若其中元素个数（记为 $|G|$ ）有限，则称为有限群，否则称为无限群。 $|G|$ 称为群的阶数。

若运算还满足交换律，即对$\forall a,b\in G$，有 $a\cdot b=b\cdot a$ ，则称$\langle G,\cdot\rangle$是交换群或Abel群。

由逆元的定义容易推出逆元有如下性质：

（1）$(a^{-1})^{-1}=a$ ；

（2）若 a,b 均可逆，则 $a\cdot b$ 可逆，且 $(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}$ ；

（3）若a可逆，则 a^n 可逆，$(a^n)^{-1}=(a^{-1})^n\overset{\text{记为}}{=}a^{-n}$ ；其中 $a^n=a\cdot a\cdots a(n\text{个}a)$。

a^n 称为元素的幂运算，有以下性质：

设 $m,n\in Z$ ，（1）$a^m\cdot a^n=a^{m+n}$；（2）$(a^n)^m=a^{mn}$。

例2.1 全体非0实数 R^* 对通常的乘法运算满足封闭性、结合律、单位元是1，$\forall a \in R^*$ 的逆元是 $a^{-1}=\dfrac{1}{a}$，因此 $\langle R^*,\cdot\rangle$ 形成群，且是交换群。同样地，全体非0有理数 Q^*，非0复数集 C^* 在通常的乘法下，也形成交换群。

例2.2 有理数集 Q，实数集 R 和复数集 C 对通常意义下的加法构成交换群，单位元是0，a 的逆元是 $-a$。

例2.3 $\langle Z,+\rangle$ 构成交换群，单位元是0，a 的逆元是 $-a$。

设 $Z^*=Z-\{0\}$，$\langle Z^*,\cdot\rangle$ 满足封闭性，结合律，有单位元1，但除了1以外，每一元素都无逆元，因此不构成群。

例2.4 $Z_n=\{0,1,\cdots,n-1\}$，在其上定义加法如下：

$a+_n b=(a+b)\bmod n$。

封闭性是显然的。

结合性： 对 $\forall a,b,c\in Z_n$：

$(a+_n b)+_n c=((a+b)\bmod n+c)\bmod n=(a+b+c)\bmod n$，

$a+_n(b+_n c)=(a+(b+c)\bmod n)\bmod n=(a+b+c)\bmod n$，

所以 $(a+_n b)+_n c=a+_n(b+_n c)$。

单位元是0，因为对 $\forall a\in Z_n, a+_n 0=(a+0)\bmod n=a$。

逆元，对 $\forall a \in Z_n, a^{-1} = n - a$ 。这是因为 $a +_n (n-a) = (a+(n-a)) \bmod n = 0$ 。

交换律也是显然的。

所以 $\langle Z_n, +_n \rangle$ 构成交换群。

设 $Z_n^* = Z_n - \{0\}$ ，定义乘法如下：$a \times_n b = (a \cdot b) \bmod n$ 。

$\times_n$ 满足封闭性、结合律、单位元是1。但有些元素没有逆元，比如 n 的真因子 d 没有逆元，否则存在 $d' \in Z_n^*$ ，使得 $d \times_n d' = 1$，即 $d \cdot d' \equiv 1 \bmod n$，则存在 $q \in Z$ ，使得 $dd' = 1 + qn$，得 $d \mid 1$ ，矛盾。

例2.5 设 $A=\{a \mid a\in Z_n^*,(a,n)=1\}$，即 A 是模 n 的简化剩余系构成的。对 $\forall a\in A, a^{-1}$ 存在，交换律显然，所以 $\langle A,\times_n\rangle$ 是交换群。

例2.6 设 p 为素数，$Z_p^*=Z_p-\{0\}=\{1,\cdots,p-1\}$ 上的运算定义如下：

$$a\times_p b=(a\cdot b)\bmod p$$

显然 Z_p^* 中每一个元素都有逆元，$\langle Z_p^*,\times_p\rangle$ 是交换群。

例2.7 实数域 R 上的全体 $n\times n$ 可逆矩阵构成的集合在矩阵的乘法运算下构成群。因为封闭性、结合律显然，单位元为单位矩阵，每个矩阵的逆元为其逆矩阵。然而矩阵乘法无交换性，该群不是交换群。

例2.8　设有限集合 $M \neq \Phi, M$ 上的双射函数称为M上的置换。

假设 $M=\{1,2,\cdots,n\}$，置换可表示为 $\sigma=\begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix}$，其中 $\{i_1,\cdots,i_n\}$ 是 $\{1,2,\cdots,n\}$ 的一个排列，所以共有 $n!$ 个置换，记置换的集合为 S，定义 S 上的复合运算 $\circ$ 如下：

设 $\sigma_1,\sigma_2 \in S, a \in M$，则 $\sigma_1 \circ \sigma_2(a)=\sigma_1(\sigma_2(a))$。

$\langle S,\circ\rangle$构成群：

因为封闭性和结合性是显然的，单位元是恒等置换，即 $\sigma_0=\begin{bmatrix}1&2&\cdots&n\\1&2&\cdots&n\end{bmatrix}$，$\sigma=\begin{bmatrix}1&2&\cdots&n\\i_1&i_2&\cdots&i_n\end{bmatrix}$ 的逆元 $\sigma^{-1}=\begin{bmatrix}i_1&i_2&\cdots&i_n\\1&2&\cdots&n\end{bmatrix}$。

然而，$\circ$ 不满足交换律，比如$M=\{1,2,3\}$上的置换 $\sigma_1=\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}$，$\sigma_2=\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}$，$\sigma_1\circ\sigma_2=\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}$，$\sigma_2\circ\sigma_1=\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}$。$\sigma_1\circ\sigma_2\neq\sigma_2\circ\sigma_1$。

如果置换σ将$\{1,2,\cdots,n\}$中的一部分元素$\{i_1,\cdots,i_k\}$变为 $\sigma(i_1)=i_2$，$\cdots$，$\sigma(i_{k-1})=i_k$，$\sigma(i_k)=i_1$，而保持其他元素不变，则称该置换为轮换，记为$(i_1,i_2,\cdots,i_k)$。

任一置换都可写成一些轮换的乘积，例如

$$\sigma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix}=(2,5,4)(1,6,3)$$

回忆一下第6章元素的指数(阶)的概念。给定模数 $n\geq 1,(a,n)=1$，满足$a^d\equiv 1 \bmod n$的最小的 d 称为 a 对模 n 的阶。

把这一概念推广到群，同样有元素阶的概念。

定义2.2 设$\langle G,*\rangle$是群，$a\in G$，如果存在$n\in N$，使得$a^n=e$（其中e为G的单位元），则a称的阶是有限的，最小的n称为a的阶，记为$\delta(a)$。如果不存在这样的n，则称a的阶是无限的。

阶的性质和第6章阶的性质一样，证明类似，总结如下：

定理2.1 设$\langle G,*\rangle$是群，$a\in G$，

（1）$a^k\equiv e$当且仅当$\delta(a)\mid k$；

（2）$\delta\left(a^{-1}\right)=\delta(a)$；

（3）$\delta\left(a^k\right)=\dfrac{\delta(a)}{\left(k,\delta(a)\right)}$。

下面介绍循环群，它是最重要的一种群。

定义2.3　设$\langle G,*\rangle$是群，如果存在$g \in G$，对$\forall a \in G$，存在$i \in Z$，使得$a = g^i$，则称$\langle G,*\rangle$是循环群，称g为$\langle G,*\rangle$的生成元。将循环群$\langle G,*\rangle$记为$\langle g\rangle$。

显然，循环群是交换群。

定理2.2 设$\langle G,*\rangle$是由$g\in G$ 生成的有限循环群,$|G|=n$，则有

（1）$g^n=e$, 且n 是使 $g^n=e$的最小正整数，即$\delta(g)=n$ ；

（2）$G=\{g,g^2,\cdots,g^n=e\}$。

证明 （1）设正整数$m<n$，使得$g^m=e$，则对任一$g^k\in G$，设 $k=qm+r, 0\le r<m, g^k=\left(g^m\right)^q*g^r=g^r$，这意味着$G$中任一元素都可写成$g^r$的形式，但$r<m$，所以$|G|<m$与$|G|=n$矛盾。

（2）设 $A=\{g,g^2,\cdots,g^n=e\}$，则显然$\forall a\in A$有$a\in G$，即$A\subseteq G$。又知A中元素全不相同，否则若有$g^i=g^j\ (1\le i,j\le n)$。不妨设$i>j$，则 $g^{i-j}=e, i-j<n$ 与n的最小性矛盾，所以$|A|=n=|G|$，所以$A=G$。证毕。

由定理2.2知,n阶循环群中任一生成元的阶也为n。

循环群的定义

定义 93

设 G 是群, 如果存在 $a \in G$, 使得 $G = \langle a \rangle$, 则称 G 为**一个循环群** (cyclic group), 并称 a 为 G 的**一个生成元** (generator). 当 G 的元素个数无限时, 称 G 为**无限循环群**; 当 G 的元素个数为 n 时, 称 G 为 n **阶循环群**.

注 93.1

由循环群的定义易见以下结论:

(1) 如果 $G = \langle a \rangle$ 是 n 阶循环群, 则 $G = \left\{e, a, a^2, a^3, \cdots, a^{n-1}\right\}$. 显然有 $\operatorname{ord} a = n$ 并且 $a^{k+tn} = a^k a^{tn} = a^k e = a^k$, 其中 $k, t \in \mathbb{Z}$. 进一步, 对任意 $k, l \in \mathbb{Z}$, 若有 $a^k = a^l$, 则 $a^{k-l} = e$. 由定理 *49* 第 *(2)* 条知 $n \mid k - l$, 于是 $a^k = a^l \Leftrightarrow n \mid k - l$.

(2) 如果 G 为无限循环群, 则由定理 *33* 知 $G = \left\{e, a, a^{-1}, a^2, a^{-2}, a^3, a^{-3}, \cdots\right\}$, 并且 $\operatorname{ord} a = \infty$. 对任意 $k, l \in \mathbb{Z}$, 若有由 $a^k = a^l$, 则 $a^{k-l} = e$, 于是 $k = l$.

例2.9 （1）$\langle z,+\rangle$ 是无限循环群，1和-1是生成元。

（3）$\langle z_k,+_k\rangle$ 是有限循环群，其中 $+_k$ 定义为 $a+_k b=(a+b)\bmod k$。

例如$k=4$时，运算如表2.1所示，1和3是生成元。

表2.1 z_4上的$+_4$运算

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

7.3 子群和群同态

7.3 子群和群同态

将子代数的概念用于群，就得到子群的定义。

定义3.1 设$\langle G, * \rangle$是群，H是G的非空子集。如果H在运算$*$下也构成群，则称$\langle H, * \rangle$是$\langle G, * \rangle$的子群。

当$H=\{e\}$和$H=G$时，$\langle H, * \rangle$都是$\langle G, * \rangle$的子群，称为$\langle G, * \rangle$的平凡子群。除此之外的子群叫非平凡子群。

例 $\langle Z,+\rangle$ 是群，令 $nZ=\{nk\mid k\in Z\}$，则$\langle nZ,+\rangle$ 是$\langle Z,+\rangle$的非平凡子群。（证明见下一页PPT）

按照定义3.1，要判断$\langle H,*\rangle$是$\langle G,*\rangle$ 的子群，需要判断$\langle H,*\rangle$满足群的4个条件，即运算的封闭性、运算的结合性，有单位元，每个元素有逆元。然而按照以下定理，4个条件的判断可合并成一个。

例 21

设 m 是一个整数，令
$$H = \{mz \mid z \in \mathbb{Z}\},$$
则 H 为整数加群 $\mathbb{Z}$ 的子群. 这个群称为由 m 所生成的子群，常记作 $m\mathbb{Z}$ 或 $\langle m \rangle$.

证明: (1) 因为 $0 = m \times 0 \in H$, 所以 H 非空.

(2) 对任意的 $mx, my \in H$, 有 $mx + my = m(x + y) \in H$, 所以 H 关于 $\mathbb{Z}$ 的运算封闭.

(3) 因为结合律对 $\mathbb{Z}$ 成立，所以对 H 也成立.

(4) 因为 $0 \in H$ 且对任意的 $mx \in H$, $0 + mx = mx + 0 = mx$, 所以 0 为 H 的零元.

(5) 对 $mx \in H$, 有 $-mx = m(-x) \in H$, 且 $(-mx) + mx = mx + (-mx) = 0$, 所以 $-mx$ 为 mx 的负元.

从而由子群的定义知，$H < G$.

定理3.1 设H是G的非空子集,$\langle H,*\rangle$是$\langle G,*\rangle$的子群的充要条件是对$\forall a,b\in H$，有$a*b^{-1}\in H$。

证明 必要性显然。

充分性：H是G的非空子集,H中运算的结合性可从G中继承下来。$H\neq\Phi$，存在$a\in H$，由条件得$e=a*a^{-1}\in H$，即H中有单位元。对$\forall a\in H$，由$e\in H$及条件得$a^{-1}=e*a^{-1}\in H$。又对$\forall a,b\in H,b^{-1}\in H,a*b=a*\left(b^{-1}\right)^{-1}\in H$，即运算具有封闭性。

综上,$\langle H,*\rangle$是$\langle G,*\rangle$的子群。 证毕。

定理 24

设 G 为群, H 是 G 的子群, 则

(1) 群 G 的单位元 e 是 H 的单位元;
(2) 对任意的 $a \in H$, a 在 G 中的逆元 a^{-1} 就是 a 在 H 中的逆元.

证明: (1) 以 e' 表示 H 的单位元, e' 当然也是 G 的元素, 则

$$e'e' = e' = e'e,$$

由定理 17 知群 G 有消去律, 于是 $e' = e$.

(2) 以 a' 表示 a 在 H 中的逆元, 则

$$aa' = e' = e = aa^{-1}.$$

同样由 G 的消去律得 $a' = a^{-1}$.

定理3.2 设 H_1, H_2 都是 G 的子群，则 $H_1 \cap H_2$是G 的子群。

证明 对 $\forall a,b \in H_1 \cap H_2$, $a,b \in H_1$ ，得 $a*b^{-1} \in H_1$。$a,b \in H_2$ 得 $a*b^{-1} \in H_2$，

所以 $a*b^{-1} \in H_1 \cap H_2$ ，即 $H_1 \cap H_2$是 G 的子群。

证毕。

定理3.2的结论可推广到多个子群。

注 30.1

群 G 的两个子群的并集不一定是 G 的子群. 例如在整数加群 $\mathbb{Z}$ 中, 令 $H_1 = \{2z \mid z \in \mathbb{Z}\}$, $H_2 = \{3z \mid z \in \mathbb{Z}\}$, 则易验证 $H_1, H_2 < \mathbb{Z}$, 但是 $2+3 \notin H_1 \cup H_2$.

定义3.2 设 $\langle G,*\rangle$ 和 $\langle H,\cdot\rangle$ 是2个群，映射 $h:G\to H$ 称为从 $\langle G,*\rangle$ 到 $\langle H,\cdot\rangle$ 的群同态，如果对 $\forall a,b\in G$，有 $h(a*b)=h(a)\cdot(b)$。

类似于定义1.4，群同态同样有单一同态、满同态、同构。

和定义1.4比较，可见定义3.2中省去了两条：

$$h(e_G)=e_H\ ,\ h(a^{-1})=[h(a)]^{-1}。$$

这里 e_G 和 e_H 分别是 $\langle G,*\rangle$ 和 $\langle H,\cdot\rangle$ 的单位元。这是由于群的结构，这两条已经在定义3.2中蕴含了：

$h(e_G)=h(e_G*e_G)=h(e_G)\cdot h(e_G)$，两边同乘 $h(e_G)$ 的逆元得 $h(e_G)=e_H$ 。

$h(a)\cdot h(a^{-1})=h(a*a^{-1})=h(e_G)=e_H$，所以 $h(a^{-1})=[h(a)]^{-1}$。

同态的性质

定理 79

设 ϕ 是群 G 到群 G' 的同态映射, e 与 e' 分别是 G 与 G' 的单位元, $a \in G$, 则

(1) ϕ 将 G 的单位元映到 G' 的单位元, 即 $\phi(e) = e'$;
(2) ϕ 将 a 的逆元映到 $\phi(a)$ 的逆元, 即 $\phi\left(a^{-1}\right) = (\phi(a))^{-1}$;
(3) 设 n 是任一整数, 则 $\phi\left(a^{n}\right) = (\phi(a))^{n}$;
(4) 如果 $\operatorname{ord} a$ 有限, 则 $\operatorname{ord} \phi(a) \mid \operatorname{ord} a$.

证明

(1) 因 e 与 e' 分别是 G 与 G' 的单位元, 所以对 $\forall a \in G$ 有

$$\phi(a)e' = \phi(a) = \phi(ae) = \phi(a)\phi(e),$$

从而由消去律得

$$e' = \phi(e),$$

即 $\phi(e)$ 为 G' 的单位元.

(2) 直接计算可得

$$\phi(a)\phi\left(a^{-1}\right) = \phi\left(aa^{-1}\right) = \phi(e) = e' = \phi(a)(\phi(a))^{-1}.$$

由消去律得

$$\phi\left(a^{-1}\right) = (\phi(a))^{-1},$$

即 $\phi\left(a^{-1}\right)$ 为 $\phi(a)$ 的逆元.

证明 (续)

(3) 当 $n=0$ 时,

$$\phi\left(a^{0}\right)=\phi(e)=e'=(\phi(a))^{0}.$$

当 $n>0$ 时,

$$\begin{aligned}\phi\left(a^{n}\right)=\phi\left(a^{n-1}a\right)=\phi\left(a^{n-1}\right)\phi(a)\\ =\cdots=(\phi(a))^{n-1}\phi(a)=(\phi(a))^{n}.\end{aligned}$$

当 $n<0$ 时,

$$\begin{aligned}\phi\left(a^{n}\right)=\phi\left(\left(a^{-1}\right)^{-n}\right)=\left(\phi\left(a^{-1}\right)\right)^{-n}\\ =\left(\phi(a)^{-1}\right)^{-n}=(\phi(a))^{n}.\end{aligned}$$

(4) 设 ord $a=r$, 则

$$(\phi(a))^{r}=\phi\left(a^{r}\right)=\phi(e)=e',$$

所以 $\operatorname{ord}\phi(a)\mid\operatorname{ord}a$.

定理3.3 设 h 是 $\langle G,*\rangle$ 到 $\langle H,\cdot\rangle$ 的群同态，则 $\langle h(G),\cdot\rangle$ 是 $\langle H,\cdot\rangle$ 的子群，称之为 $\langle G,*\rangle$ 的同态像，其中 $h(G)=\{h(a)\mid a\in G\}$。

证明 对 $\forall x,y\in h(G)$，存在 $a,b\in G$，使得 $x=h(a),y=h(b)$，$x\cdot y^{-1}=h(a)\cdot h(b)^{-1}=h(a)\cdot h(b^{-1})=h(a*b^{-1})\in h(G)$。由定理3.1，$\langle h(G),\cdot\rangle$ 是 $\langle H,\cdot\rangle$ 的子群。 证毕。

例3.2 证明每一个k阶循环群$\langle G,*\rangle$都同构于$\langle Z_k, +_k\rangle$。

证明 取$\langle G,*\rangle$的生成元a，由定理2.2，$G=\langle a, a^2, \cdots, a^k=e\rangle$。作映射$h: Z_k \to G, h(i)=a^i\ (0 \le i \le k-1)$，显然$h$是单一的、满射的。

对$\forall i, j \in Z_k$，$h(i +_k j) = h((i+j) \bmod k) = a^{(i+j) \bmod k} = a^i * a^j = h(i) * h(j)$。

所以$\langle G,*\rangle$和$\langle Z_k, +_k\rangle$同构。

例3.3 证明有限群$\langle G,*\rangle$的运算表（例如表2.1）中，每一行和列都是G的元素的一个置换。将这种置换构成的集合记为P，其上的复合运算记为$\Diamond$，证明$\langle P,\Diamond\rangle$是群，且与$\langle G,*\rangle$同构。

证明 设$a\in G$，首先证明运算表中a对应的行中，G中的元素最多出现一次。反证，设$k\in G$在a对应的行中出现了2次，即$k=a*b_1=a*b_2$，两边同乘以a^{-1}得$b_1=b_2$，矛盾。

再证明$\forall k \in G$ 必在a对应的行中出现。因为$k = a*(a^{-1}*b)$，而$a^{-1}*b \in G$，k 出现在a的行中$a^{-1}*b$列。

所以a对应的行是G的元素的一个置换。列的情况类似。

下面证明$\langle P,\Diamond\rangle$ 是群。设a对应的行置换为p_a，即$p_a(x)=a*x$，$\forall a,b \in G,\ p_a \Diamond p_b(x) = p_a(p_b(x)) = a*(b*x) = p_{a*b}(x)$，所以$P_a \Diamond P_b = P_{a*b}$。

由于 $P_a \Diamond P_{a^{-1}} = P_{a*a^{-1}} = P_e$ 为恒等置换得 $(P_a)^{-1} = P_{a^{-1}}$。$P_a \Diamond P_b^{-1} = P_a \Diamond P_{b^{-1}} = P_{a*b^{-1}} \in P$，所以 $\langle P,\Diamond\rangle$ 是群。

最后证明$\langle P,\Diamond\rangle$和$\langle G,*\rangle$同构：

做映射$h:G\to P, h(a)=p(a)$，h显然是双射函数。

且$h(a*b)=p_{a*b}=P_a\Diamond P_b=h(a)\Diamond h(b)$，这就证明了同构。证毕。

例3.2表明对任何群的研究都可归结于对置换群的研究。如果置换群研究清楚了，一切有限群就都清楚了，可见置换群的重要性。但经验告诉我们，研究置换群并不比研究抽象群容易。所以不得不直接研究抽象群。

定义3.3 设 h 是从 $\langle G,*\rangle$ 到 $\langle H,\cdot\rangle$ 的群同态，如果 $K\subseteq G$ 中每一元素都被映射成 H 的单位元 e_H，再没有其他元素映射到 e_H，则称 K 为同态 h 的核，记为 $\ker(h)=\{a\mid a\in G,h(a)=e_H\}$。

易知：$\{e_H\}$ 是 G 的正规子群。从而由定理84第(4)条知核 $\ker(h)$ 是 G 的正规子群。

定理3.4 $\ker(h)$是$\langle G,*\rangle$的子群，且h是单同态的充要条件是$\ker(h)=\{e\}$，其中e是G中的单位元。

证明 设$a,b\in\ker(h)$，即$h(a)=e_H,h(b)=e_H$，从而

$$h(a*b^{-1})=h(a)\cdot h(b^{-1})=h(a)\cdot h(b)^{-1}=e_H\cdot e_H^{-1}=e_H$$

所以$a*b^{-1}\in\ker(h)$，即$\ker(h)$是$\langle G,*\rangle$的子群。

若h是单射，则由$h(a)=e_H=h(e)$得$a=e$，即$\ker(h)=\{e\}$。

反过来，如果$\ker(h)=\{e\}$，对$\forall a,b\in G,h(a)=h(b)$，则有$h(a*b^{-1})=h(a)\cdot h(b^{-1})=h(a)\cdot h(b)^{-1}=e_H$，所以$a*b^{-1}\in\ker(h)$。即$a*b^{-1}=e$，所以$a=b$，即是$h$单射的。证毕。

(原) 象集

定义 83

设 ϕ 为群 G 到群 G' 的映射, A, B 分别为 G 与 G' 的非空子集. 记

$$\phi(A) = \{\phi(x) \mid x \in A\},$$

$$\phi^{-1}(B) = \{x \in G \mid \phi(x) \in B\},$$

则 $\phi(A)$ 与 $\phi^{-1}(B)$ 分别是 G' 与 G 的非空子集 ($\phi^{-1}(B)$ 仅仅是一个集合的记号, 并不表示映射 ϕ 是可逆的). $\phi(A)$ 与 $\phi^{-1}(B)$ 分别称为子集 A 与 B 在 ϕ 下的象集与原象集.

同态的性质

定理 84

设 ϕ 是群 G 到 G' 的同态映射, H 与 K 分别是 G 与 G' 的子群, 则

(1) $\phi(H)$ 是 G' 的子群;
(2) $\phi^{-1}(K)$ 是 G 的子群;
(3) 如果 H 是 G 的正规子群, 则 $\phi(H)$ 是 $\phi(G)$ 的正规子群;
(4) 如果 K 是 G' 的正规子群, 则 $\phi^{-1}(K)$ 是 G 的正规子群.

证明: (1) 对任意的 $h_1, h_2 \in H$, 有 $h_1 h_2^{-1} \in H$, 所以

$$\phi(h_1)(\phi(h_2))^{-1} = \phi(h_1)\phi\left(h_2^{-1}\right) = \phi\left(h_1 h_2^{-1}\right) \in \phi(H),$$

所以 $\phi(H)$ 是 G' 的子群.

证明 (续)

(2) 对任意的 $a, b \in \phi^{-1}(K)$, 有 $\phi(a), \phi(b) \in K$, 则

$$\phi\left(ab^{-1}\right) = \phi(a)\phi\left(b^{-1}\right) = \phi(a)\phi(b)^{-1} \in K,$$

于是 $ab^{-1} \in \phi^{-1}(K)$, 所以 $\phi^{-1}(K)$ 是 G 的子群.(3) 由 (1) 知, $\phi(H)$ 是 $\phi(G)$ 的子群. 又对任意的 $a' \in \phi(G), h' \in \phi(H)$, 存在 $a \in G, h \in H$ 使得 $\phi(a) = a', \phi(h) = h'$, 则 $aha^{-1} \in H$. 于是

$$a'h'a'^{-1} = \phi(a)\phi(h)(\phi(a))^{-1} = \phi(a)\phi(h)\phi\left(a^{-1}\right)$$

$$= \phi\left(aha^{-1}\right) \in \phi(H),$$

所以 $\phi(H)$ 是 $\phi(G)$ 的正规子群.(4) 由 (2) 知, $\phi^{-1}(K)$ 是 G 的子群. 又对任意的 $a \in G, h \in \phi^{-1}(K)$, 则 $\phi(h) \in K$, 而 K 是 G' 的正规子群, 故

$$\phi\left(aha^{-1}\right) = \phi(a)\phi(h)\phi(a)^{-1} \in K.$$

从而 $aha^{-1} \in \phi^{-1}(K)$, 所以 $\phi^{-1}(K)$ 是 G 的正规子群.

同构的性质

定理 80

设 ϕ 是群 G 到 G' 的同构映射, e 与 e' 分别是 G 与 G' 的单位元, 则 ϕ 是可逆映射, 且 ϕ 的逆映射 ϕ^{-1} 是群 G' 到群 G 的同构映射.

证明: ϕ 是群 G 到 G' 的一一映射, 所以 ϕ 是可逆的映射, 且其逆映射 ϕ^{-1} 是 G' 到 G 的一一映射. 下面证明 ϕ^{-1} 为同态映射.

证明 (续)

对任意的 $a', b' \in G'$, 由于可逆映射是满映射, 所以存在 $a, b \in G$, 使

$$\phi(a) = a', \quad \phi(b) = b'.$$

于是, $\phi^{-1}(a') = a$, $\phi^{-1}(b') = b$, 并且

$$\begin{aligned}
\phi^{-1}(a'b') &= \phi^{-1}(\phi(a)\phi(b)) \\
&= \phi^{-1}(\phi(ab)) \\
&= \left(\phi^{-1} \circ \phi\right)(ab) \\
&= ab \\
&= \phi^{-1}(a')\,\phi^{-1}(b'),
\end{aligned}$$

这就证明了 ϕ^{-1} 是 G' 到 G 的同构映射.

同构的性质

注 81.1

设群 G 与 G' 同构. 如果 G 是交换群, 则 G' 也是交换群; 如果 G 是有限群, 则 G' 也是有限群且 $|G| = |G'|$.

群的同构是一个等价关系, 即

(1) $G \cong G$ (反身性);

(2) 若 $G \cong G'$, 则 $G' \cong G$ (对称性);

(3) 若 $G \cong G', G' \cong G''$, 则 $G \cong G''$ (传递性), 其中 G, G', G'' 都是群.

证明

(1) 见例 76.

(2) 由定理 80 立即可证. (3) 设 ϕ 是 G 到 G' 的同构映射, ψ 是 G' 到 G'' 的同构映射. 由映射复合的性质知 $\psi \circ \phi$ 是 G 到 G'' 的一一映射. 又对任意的 $x, y \in G$ 有

$$\begin{aligned}(\psi \circ \phi)(xy) &= \psi(\phi(xy)) \\ &= \psi(\phi(x)\phi(y)) \\ &= \psi(\phi(x))\psi(\phi(y)) \\ &= (\psi \circ \phi)(x)(\psi \circ \phi)(y).\end{aligned}$$

所以 $\psi \circ \phi$ 是 G 到 G'' 的同构映射, 从而 $G \cong G''$.

7.4 正规子群和商群

7.4 正规子群和商群

设$\langle H,*\rangle$是群$\langle G,*\rangle$的子群，对$\forall a\in G$，构造集合$aH=\{a*h\mid h\in H\}$。aH称为由a确定的子群$\langle H,*\rangle$的左陪集，a称为左陪集aH的表示元素。类似地$Ha=\{h*a\mid h\in H\}$为右陪集。

例4.1 设 $n\in N$，则$H=nZ$是$\langle Z,+\rangle$的子群，对$\forall a\in Z$，

$$a+H=a+nZ=\{a+kn\mid k\in Z\}$$

就是nZ的左陪集，且$a+H=H+a$。

下面只讨论左陪集的性质，右陪集的性质类似。

定理4.1 设 $\langle H,*\rangle$ 是 $\langle G,*\rangle$ 的子群，则

（1）对 $\forall a\in G, aH=\{c\mid c\in G$ 且 $c^{-1}*a\in H\}$；

（2）对 $\forall a,b\in G, aH=bH$ 的充要条件是 $b^{-1}*a\in H$；

（3）对 $\forall a,b\in G$，$aH\cap bH=\Phi$ 的充要条件是 $b^{-1}*a\notin H$；

（4）对 $\forall a\in H$，有 $aH=H=Ha$；

证明 （1）设$H'=\{c\,|\,c\in G, c^{-1}*a\in H\}$，要证 $aH=H'$。对$\forall c\in aH$，存在$h\in H$，使得 $c=a*h$，从而$c^{-1}*a=h^{-1}\in H$，$c\in H'$，所以 $aH\subseteq H'$。反过来，对$\forall c\in H'$，有 $c^{-1}*a\in H$，存在$h_1\in H$，使得$c^{-1}*a=h_1$，从而$c=a*h^{-1}\in aH$，所以$H'\subseteq aH$。得$aH=H'$。

（2）设$aH=bH$，则$b=b*e^{-1}\in bH=aH$，所以存在$h_1\in H$，使得$b=a*h_1$，从而$b^{-1}*a=h_1^{-1}\in H$。反过来，设$b^{-1}*a\in H$，存在$h_2\in H$，使得$b^{-1}*a=h_2$，$a=b*h_2$，$b=a*h_2^{-1}$。对$\forall c\in aH$，存在$h_3\in H$，使得$c=a*h_3=b*(h_2*h_3)\in bH$，所以$aH\subseteq bH$。对$\forall c\in bH$，存在$h_4\in H$，使得$c=b*h_4=a*\left(h_2^{-1}*h_4\right)\in aH$。所以$bH\subseteq aH$。

综上，$aH=bH$。

（3）**必要性**：反证 若 $b^{-1}*a\in H$ ，则由（2）$aH=bH$ ，$aH\cap bH\neq\Phi$，矛盾。

充分性：反证，若 $aH\cap bH\neq\Phi$ ，则存在 $r\in aH\cap bH$ ，$r=a*h_1=b*h_2$，$b^{-1}*a=h_2*h_1^{-1}\in H$ 与 $b^{-1}*a\notin H$ 矛盾。

（4）在（2）中取 $b=e$ ，则 $b^{-1}*a=a\in H$ ，由（2） $aH=eH=H$ 。 证毕。

由定理4.1可见，H 的任意2个左陪集要么完全一样，要么不相交。

定理4.2 设$\langle H,*\rangle$是$\langle G,*\rangle$的子群，则G可以表示成H的所有左陪集的并，即$G=\bigcup\limits_{a\in G} aH$。

证明 对$\forall a\in G$，$a=a*e\in aH$，所以$G\subseteq aH\subseteq \bigcup\limits_{a\in G} aH$。

反过来，对$\forall b\in \bigcup\limits_{a\in G} aH$，存在$a\in G$，使得$b\in aH$，进而存在$h\in H$，使得$b=a*h\in G$，所以$\bigcup\limits_{a\in G} aH\subseteq G$。从而得$\bigcup\limits_{a\in G} aH=G$。证毕。

定理4.3 设$\langle H, *\rangle$是$\langle G, *\rangle$的子群，则H的任意陪集的大小（基数）是相等的。

证明 设$h_1, h_2 \in H, h_1 \neq h_2$，则$a * h_1 \neq a * h_2$，否则两边同乘$a^{-1}$，得$h_1 = h_2$，矛盾。所以$H$中不同元素对应$aH$中的不同元素，$|aH| = |H|$。证毕。

由定理4.2、定理4.3，H的所有左陪集G构成的一个划分，且划分的块大小相等，由此得到以下定理。

定理4.4（Lagrange定理）有限群的任意子群的阶数可整除群的阶数。

下面利用Lagrange定理证明循环群的几个重要性质。

定理4.5 循环群的子群是循环群。

证明 设H是循环群$G=\{g^i \mid i=1,\cdots\}$的子群，$k$ 是使得$g^k \in H$的最小正整数。对任一$a=g^i \in H$，令$i=qk+r(0 \le r < k)$，则$g^i=(g^k)^q g^r$，$g^r=g^i(g^{qk})^{-1} \in H$。所以 $r=0$，否则与k的最小性矛盾。所以$g^i=(g^k)^q$，H是由g^k生成的循环子群。证毕。

定理4.6 设G是n阶有限群，a是G中任一元素，那么$a^n=e$。

证明 设$H=\{e,a,a^2,\cdots,a^{r-1}\}$，其中$r$是$a$的阶，由定理3.1易证$\langle H,\cdot\rangle$是$\langle G,\cdot\rangle$的子群，由Lagarange定理，$|H|\,|\,|G|$，$r|n$，存在正整数$t$，使得$n=rt$。所以$a^n=(a^r)^t=e$。证毕。

定理4.7 素数阶的群是循环群，且任一与单位元不同的元素是生成元。

证明 设$\langle G,\cdot\rangle$是群，且$|G|=p$（p为素数）。任取$a\in G$，$a\neq e$，构造$H=\{e,a,a^2,\cdots\}$，易知H是G的子群（同定理4.6）。设$|H|=n$，则$n\neq1$。由Lagarange定理，$n\,|\,p$，所以$n=p$，$H=G$。所以G是循环群，a是生成元。证毕。

定理4.8 设a^k是n阶循环群$G=\langle a\rangle$中任一元素，那么

$$\delta\left(a^k\right)=\frac{n}{(k,n)}。$$

证明 由定理2.2，$\delta(a)=n$。以下证明类似于第6章定理1.3。证毕。

定理4.9 在n阶循环群$G=\langle a\rangle$中，a^k是生成元当且仅当$(k,n)=1$。

证明 由定理4.8直接得。证毕。

定义4.1 设$\langle H,*\rangle$是$\langle G,*\rangle$的子群，如果对 $\forall a \in G$ ，有 $aH = Ha$，则称$\langle H,*\rangle$是正规子群。

定义中 $aH = Ha$ 的是指对$\forall h_1 \in H$ ，都有$h_2 \in H$，使得 $a * h_1 = h_2 * a$ ，并不要求 $a * h_1 = h_1 * a$ 。

对正规子群来说，左陪集等于右陪集，可以简称为陪集。

显然，交换群的所有子群是正规子群，任一群的平凡子群是正规子群。

定理4.10　设$\langle H,*\rangle$是$\langle G,*\rangle$的子群，则下面结论等价。

（1）H是G的正规子群；

（2）对$\forall a\in G,\ aHa^{-1}=H$；

（3）对$\forall a\in G,\ aHa^{-1}\subseteq H$。

证明　$(1)\Rightarrow(2)\Rightarrow(3)$显然，下面证明$(3)\Rightarrow(1)$

对$\forall a\in G,\ h\in H$，由$aHa^{-1}\subseteq H$知，存在$h'\in H$，使得$a*h*a^{-1}=h'$，$a*h=h'*a\subseteq Ha$，所以$aH\subseteq Ha$。又由$a^{-1}\in G$，有$a^{-1}H\left(a^{-1}\right)^{-1}=a^{-1}Ha\subseteq H$。存在$h''\in H$，使得$a^{-1}*h*a=h''$，$h*a=a*h''\subseteq aH$，所以$Ha\subseteq aH$，所以$aH=Ha$。证毕。

在证明$aH=Ha$时，要证明2个集合aH和Ha互相包含，但由定理4.10，只需证明集合$aH^{-1}a$包含在H。

由正规子群可构造商群。

定理4.11 设 $\langle H,*\rangle$ 是 $\langle G,*\rangle$ 的正规子群，则如下构造的代数系统 $\langle G/H,\cdot\rangle$ 是群，称为群 G 对正规子群 H 的商群。其中 $G/H=\{aH \mid a\in G\}$，运算“ · ”定义为：$aH\cdot bH=(a*b)H$ 。

证明 封闭性显然，结合律由 G 中的结合律直接可得。单位元 $eH=H$，因为 $aH\cdot H=aH\cdot eH=(a*e)H=aH$ 。aH 的逆元是 $a^{-1}H$，因为 $aH\cdot a^{-1}H=(a*a^{-1})H=eH=H$。证毕。

例4.2 由例4.1知 $H\equiv nZ$ 是群 $<Z,+>$ 的正规子群，则 $\langle Z/H,\oplus\rangle$ 是 $\langle Z,+\rangle$ 对 H 的商群。其中 $Z/H=\{a+H \mid a\in Z\}$, $(a+H)\oplus(b+H)=(a+b)+H$ 。

定理4.12 设 h 是群 $\langle G,*\rangle$ 到群 $\langle H,\cdot\rangle$ 的同态，则 $\ker(h)$ 是 G 的正规子群。反过来，若 N 是 G 的正规子群，映射 $s:G\to G/N$，$s(a)=aN$ 是核为 N 的同态，称为 G 到 G/N 的自然同态。

证明 对 $\forall a\in G, b\in\ker(h), h(a*b*a^{-1})=h(a)\cdot h(b)\cdot h(a^{-1})=h(a)\cdot h(a^{-1})$ $=h(a*a^{-1})=h(e)=e'$，其中 e' 是 $\langle H,\cdot\rangle$ 的单位元，所以 $a*b*a^{-1}\in\ker(h)$，即 $a*\ker(h)*a^{-1}\subseteq H$ 。由定理4.10，$\ker(h)$ 是正规子群。

对 $\forall a,b\in G, s(a*b)=(a*b)N=(aN)\cdot(bN)=s(a)\cdot s(b)$，其中“·”是 G/N 上的运算，所以 s 是 G 到 G/N 的同态。

又 N 是 G/N 的单位元，由 $s(a)=N$ 得 $aN=N$ ，由定理4.1，$a\in N$ ，即 $\ker(s)=N$ 。

证毕。

定理 89 (群同态基本定理)

设 ϕ 是群 G 到群 G' 的满同态, $K = \operatorname{Ker}\phi$, 则

$$G/K \cong G'.$$

证明: 由定理 86 知, K 是 G 的正规子群, 所以有商群 G/K. 令

$$\begin{aligned} \tilde{\phi}: \quad G/K &\longrightarrow \quad G', \\ aK &\longmapsto \phi(a). \end{aligned}$$

(1) 如果 $aK = bK$, 则 $a^{-1}b \in K$, 于是 $\phi\left(a^{-1}b\right) = e'$, 所以 $\phi(a) = \phi(b)$, 即 $\widetilde{\phi}(aK) = \widetilde{\phi}(bK)$. 这说明, $\widetilde{\phi}$ 的定义与代表元的选取无关, 从而 $\widetilde{\phi}$ 为 G/K 到 G' 的映射.

证明 (续)

(2) 对任意的 $a' \in G'$, 因为 ϕ 是满映射, 所以存在 $a \in G$ 使得 $\phi(a) = a'$. 从而

$$\widetilde{\phi}(aK) = \phi(a) = a',$$

因此, $\widetilde{\phi}$ 是 G/K 到 G' 的满映射.

(3) 如果 $\phi(a) = \phi(b)$, 则

$$\phi\left(a^{-1}b\right) = (\phi(a))^{-1}\phi(b) = e'.$$

于是 $a^{-1}b \in K$, 由此得 $aK = bK$. 所以 $\widetilde{\phi}$ 是 G/K 到 G' 的单映射.

(4) 对任意的 $aK, bK \in G/K$, 有

$$\widetilde{\phi}(aK \cdot bK) = \widetilde{\phi}(abK) = \phi(ab) = \phi(a)\phi(b)$$

$$= \widetilde{\phi}(aK)\widetilde{\phi}(bK).$$

所以

$$\widetilde{\phi}: \quad G/K \cong G'.$$

证明同构的基本步骤

应用群同态基本定理证明群的同构, 一般有以下五个步骤:

第一步 建立群 G 与群 G' 的元素之间的对应关系 ϕ, 并证明 ϕ 为 G 到 G' 的映射;

第二步 证明 ϕ 为 G 到 G' 的满映射;

第三步 证明 ϕ 为 G 到 G' 的同态映射;

第四步 计算同态的核 $\operatorname{Ker}\phi$;

第五步 应用群同态基本定理得 $G/\mathrm{Ker}\phi \cong G'$.

循环群的结构定理

定理 106

设 G 为循环群.

(1) 如果 $G = \langle a \rangle$ 是无限循环群, 则 $G \cong (\mathbb{Z}, +)$;
(2) 如果 $G = \langle a \rangle$ 是 n 阶循环群, 则 $G \cong (\mathbb{Z}_n, +)$.

证明: (1) 令

$$\phi : \mathbb{Z} \longrightarrow G,$$
$$k \longmapsto a^k, \quad \forall k \in \mathbb{Z}.$$

(i) 显然 ϕ 是 $\mathbb{Z}$ 到 G 的映射;

证明 (续)

(ii) 设 $k, l \in \mathbb{Z}$, 如果 $a^k = a^l$, 则由注 93.1 第 (2) 条得 $k = l$, 所以 ϕ 为 $\mathbb{Z}$ 到 G 的单映射; (iii) 对任意的 $a^k \in G$, 有 $k \in \mathbb{Z}$, 使 $\phi(k) = a^k$, 所以 ϕ 是 $\mathbb{Z}$ 到 G 的满映射; (iv) 对任意的 $k, l \in \mathbb{Z}$,

$$\phi(k+l) = a^{k+l} = a^k \cdot a^l = \phi(k) \cdot \phi(l),$$

所以 ϕ 是 $\mathbb{Z}$ 到 G 的同构映射. 因此, $G \cong (\mathbb{Z}, +)$. (2) 令

$$\begin{aligned} \phi: \quad \mathbb{Z}_n &\longrightarrow G, \\ \bar{k} &\longmapsto a^k, \quad \forall \bar{k} \in \mathbb{Z}_n. \end{aligned}$$

(i) 设 $\bar{k} = \bar{l}$, 则 $n \mid k - l$, 于是 $a^{k-l} = e$, 从而 $a^k = a^l$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的映射;

证明 (续)

(ii) 设 $\bar{k},\bar{l}\in\mathbb{Z}_n$, 如果 $\phi(\bar{k})=\phi(\bar{l})$, 即 $a^k=a^l$, 则 $n\mid k-l$, 从而 $\bar{k}=\bar{l}$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的单映射;

(iii) 对任意的 $a^k\in G$, 有 $\bar{k}\in\mathbb{Z}_n$, 使 $\phi(\bar{k})=a^k$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的满映射; (iv) 对任意的 $\bar{k},\bar{l}\in\mathbb{Z}_n$, 有

$$\phi(\bar{k}+\bar{l})=\phi(\overline{k+l})=a^{k+l}=a^k\cdot a^l=\phi(\bar{k})\cdot\phi(\bar{l}).$$

注 106.1

由定理 *106* 可知, 从同构的观点看, 循环群仅有两类, 即整数加群 $(\mathbb{Z},+)$ 和模 n 剩余类加群 $(\mathbb{Z}_n,+)$, 所以掌握了这两类群, 也就等于把一切循环群都弄清楚了.

定理4.14 $\langle Z,+\rangle$的每个子群$\langle H,+\rangle$是循环群，且有$H=\{0\}$或$H=kZ$，其中k是H中的最小正整数。如果$H\neq\{0\}$则H是无限的。

证明 若$H=\{0\}$，则结论显然成立。若$H\neq\{0\}$，则其中有非0整数$a\in H$，由H是群得$-a\in H$，即H中有正整数。设其中的最小正整数为k，对$\forall a\in H$，存在唯一的q,r，使得$a=qk+r$，其中$0\leqslant r<k$，由$r=a-qk$得$r\in H$，再由k的最小性得$r=0$，$a=qk\in kZ$，所以$H\subseteq kZ$。

又对$\forall a\in kZ$，存在$q\in Z$，使得$a=kq$。若$q>0$，则a为q个k的加法，若$q<0$，则$a=-(-q)k$，为$-q$个k的加法再取逆元。所以$a\in H$，即$kZ\subseteq H$。所以$H=kZ$，若$H\neq\{0\}$，则显然是无限的。证毕。