5-4 群与子群
(group & subgroup)

定义5-4.1设<G,*>是一个代数系统，其中G是非空集合，*是G上一个二元运算，如果

（1） 运算*是封闭的。

（2） 运算*是可结合的。

（3） 存在幺元e。

（4） 对于每一个元素x∈G,存在着它的逆元x^{-1}。

则称<G,*>是一个群。

例题1： 设**R={0°，60°，120°，180°，240°，300°}**表示在平面上几何图形绕形心顺时针旋转角度的六种可能情况，设★是**R**上的二元运算，对于**R**中任意两个元素**a**和**b,a★b**表示平面图形连续旋转**a**和**b**得到的总旋转角度。并规定旋转**360°**等于原来的状态，就看作没有经过旋转。验证**<R,★>**是一个群。

解：（见书**P191**）

定义5-4.2[有限群][无限群]

设<G,*>是一个群。如果G是有限集，那么称<G,*>为有限群，G中元素的个数通常称为该有限群的阶数，记为|G|；如果G是无限集，则称<G,*>为无限群。

例题2：试验证代数系统**<I,+>**是一个群，这里**I**是所有整数的集合，**+**是普通加法运算。

解：明显地，二元运算**+**在**I**上是封闭的且是可结合的。幺元是**0**对于任一**a**∈**A,**它的逆元是**-a**。所以**<I,+>**是一个群，且是一个无限群。

至此，我们可以概括地说：广群仅仅是一个具有封闭二元运算的非空集合；半群是一个具有结合运算的广群；独异点是具有幺元的半群；群是每个元素都有逆元的独异点。即有：

{群}⊆{独异点}⊆{半群}⊆{广群}

由定理**5-2.4**可知，群中任何一个元素的逆元必定是唯一的由群中逆元的唯一性，我们可以有以下几个定理。

定理5-4.1 群中不可能有零元。

证明**:**当群的阶为**1** 时**(|G|=1)**，它的唯一元素视作幺元。

设**|G|>1**且群**<G,*>**有零元θ。
那么群中任何元素$x \in G$,都有$x * \theta = \theta * x = \theta \neq e$,
所以，零元θ就不存在逆元，这与**<G,*>**是群相矛盾。

定理5-4.2设<G,*> 是一个群，对于$a,b\in G$,必存在唯一的$x\in G$,使得$a*x=b$。

证明：设a的逆元是a^{-1}，令$x=a^{-1}*b$

则 $a*x=a*(a^{-1}*b)$

$=(a*a^{-1})*b$

$=e*b$

$=b$

若另有一解x_1,满足$a*x_1=b$,则

$a^{-1}*(a*x_1)= a^{-1}*b$

即 $x_1= a^{-1}*b$

定理5-4.3设<G,*>是一个群，对于任意的 $a,b,c \in G$,如果有 $a*b=a*c$ 或者 $b*a=c*a$,则必有 $b=c$(消去律，可约性)。

证明　设 $a*b=a*c$,且a的逆元是 a^{-1},则有

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

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

$$e*b=e*c$$

$$b=c$$

当 $b*a=c*a$ 时，可同样证得 $b=c$。

由定理**5-3.3**可知：

群的运算表中没有两行（或两列）是相同的。为了进一步考察群的运算表所具有的性质，现在引进置换的概念。

定义5-4.3 设S是一个非空集合，从集合S到S的一个双射称为S的一个**置换**。

例如，对于集合S={a, b, c, d}，将a映射到b, b映射到d，c映射到a，d映射到c，是一个从S到S上的一个一对一映射，这个置换可以表示为

$$\begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$$

即上一行中按任何次序写出集合中的全部元素，而在下一行中写每个对应元素的像。

定理5-4.4群<G,*>的运算表中的每一行或每一列都是G的元素的一个置换。

证明：首先，证明运算表中的任一行或任一列所含G中的一个元素不可能多于一次。用反证法，如果对应于元素$a \in G$的那一行中有两个元素都是c,即有b_1，$b_2 \in G$

$$a*b_1=a*b_2=c \text{ 且 } b_1 \neq b_2$$

由可约性可得$b_1=b_2$,这与$b_1 \neq b_2$矛盾。

其次，要证明G中的每一个元素都在运算表的每一行和每一列中出现。

考察对应于元素$a \in G$的那一行，设b是G中的任一元素，由于$b=a*(a^{-1}*b)$,所以b必定出现在对应于a的那一行中。

再由运算表中没有两行（或两列）相同的事实，便可得出：<G,*>的运算表中每一行都是G的元素的一个置换，且每一行都是不相同的。同样的结论对于列也是成立的。

定义5-4.4

代数系统<G,*>中，如果存在$a \in G$，有$a*a=a$，则称a为**等幂元**。

定理5-4.5 群<G,*>中，除幺元e外，不可能有任何别的等幂元。

证明： 因为$e*e=e$,所以e是等幂元。

现设 $a \in A, a \neq e$且$a*a=a$

则有 $a=e*a=(a^{-1}*a)*a= a^{-1}*(a*a)$

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

与假设$a \neq e$相矛盾。

定义5-4.5[子群]

设<G,*>是一个群，S是G的非空子集，如果<S,*>也构成群，则称<S,*>是<G,*>的一个子群。

定理5-4.6设<G,*>是一个群，<S,*>是<G,*>的一个子群，那么，<G,*>中的幺元e必定也是<S,*>中的幺元。

证明：设<S,*>中的幺元为e_1, 对于任一$x\in S\subseteq G$, 必有$e_1*x=x=e*x$, 故$e_1=e$。

定义5-4.6[平凡子群]

设<G,*>是一个群，<S,*>是<G,*>的子群，如果 S={e}，或者S=G，则称<S,*>为<G,*>的平凡子群

例题3： $<I,+>$是一个群，设$I_E=\{x|x=2n,n\in I\}$,证明$<I_E,+>$是$<I,+>$的一个子群。

证明：（1） 对于任意的$x,y\in I_E$,不妨设 $x=2n_1,y=2n_2$, n_1，$n_2\in I$,则

$x+y=2n_1+2n_2=2(n_1+n_2)$，而 $n_1+n_2\in I$

所以 $x+y\in I_E$，即+在I_E上封闭。

（2） 运算+在I_E上保持可结合性。

（3） $<I,+>$中的幺元0也在I_E中。

（4） 对于任意的$x\in I$,必有n使得$x=2n$,而

$-x=-2n=2(-n)$, $-n\in I$

所以$-x\in I_E$,而$x+(-x)=0$, 因此，$<I_E,+>$是$<I,+>$的一个子群。

定理5-4.7设<G,*>是一个群，B是G的非空子集，如果B是一个有限集，那么，只要运算*在B上封闭，<B,*>必定是<G,*>的子群。

证明：设b是B的任一个元素。若*在B上封闭，则元素$b^2=b*b, b^3=b^2*b, \ldots$都在B中。由于B是有限集，所以必存在正整数i和j,不妨假设i<j,使得

$$b^i = b^j \quad 即\ b^i = b^i * b^{j-i}.$$

这就说明b^{j-i}是<G,*>中的幺元，且这个幺元也在子集B中。

如果j-i>1,那么由$b^{j-i} = b * b^{j-i-1}$可知b^{j-i-1}是b的逆元，且$b^{j-i-1} \in B$;如果j-i=1,那么由$b^i = b^i * b$可知b就是幺元，而幺元是以自身为逆元的。因此，<B,*>是<A,*>的一个子群。

定理5-4.8设$<G,\Delta>$是群，S是G的非空子集，如果对于S中的任意元素a和b有$a\Delta b^{-1}\in S$,则$<S,\Delta>$是$<G,\Delta>$的子群。

证明：首先证明，G中的幺元e也是S中的幺元。

任取S中的元素a,$a\in S\subseteq G$,所以$e=a\Delta a^{-1}\in S$且$a\Delta e=e\Delta a=a$,即e也是S中的幺元。

其次证明，S中的每一元素都有逆元。

对任一$a\in S$, 因为$e\in S$, 所以$e\Delta a^{-1}\in S$即$a^{-1}\in S$。

最后证明，Δ在S上是封闭的。

对任意的$a,b\in S$，由上可知$b^{-1}\in S$

而 $b=(b^{-1})^{-1}$

所以 $a\Delta b=a\Delta (b^{-1})^{-1}\in S$

至于运算Δ在S上的可结合性是保持的。

因此，$<S,\Delta>$是$<G,\Delta>$的子群。

例题4：设<H,*>和<K,*>都是群<G,*>的子群，试证明<H∩K，*>也是<G,*>的子群。

证明：设任意的a,b∈H∩K,

因为<H,*>和<K,*>都是子群，

所以b^{-1}∈H∩K,

由于*在H和K中的封闭性，

所以a*b^{-1}∈H∩K,

由定理5-4.8即得<H∩K,*>是<G,*>的子群。

作业5-4

P197 (1)

(3)

(5)

(4)选作