代数结构

Algebra Structures

3、群与子群

概念：

半群, 子半群, 元素的幂，独异点，群，群的阶数，子群，平凡子群，陪集，拉格朗日（Lagrange）定理

半群（Semigroup）

设$V=<S, \circ>$是代数系统，$\circ$为二元运算，如果$\circ$运算是可结合的，则称V为半群。

独异点(Monoid).

设$V=<S,\circ>$是半群，若$e \in S$是关于$\circ$运算的单位元，则称V是含幺半群，也叫做独异点。 有时也将独异点V记作$V=<S,\circ,e>$.

实例

(1) $\langle \mathbf{Z}^+,+\rangle,\langle \mathbf{N},+\rangle,\langle \mathbf{Z},+\rangle,\langle \mathbf{R},+\rangle$**都是半群，+是普通加 法. 这些半群中除**$\langle \mathbf{Z}^+,+\rangle$**外都是独异点**

(2) $\langle P(B),\oplus\rangle$**为半群，也是独异点，其中**$\oplus$**为集合对称差运算**

(3) $\langle R^*,\circ\rangle$**为半群，但不是独异点，其中**R^***为非零实数集合，**$\circ$**运算定义如下：**$\forall x, y\in R^*, x\circ y=y$

群(Group)

设V=<G,∘>是独异点，e∈ G关于∘运算的单位元，若 ∀a∈G，a^{-1}∈G，则称V是群(Group). 通常将群记作G.

群的另一种定义（基本形式）

设<G, ∘ >是代数系统，∘为二元运算。

(1) ∘ 对G是封闭的；

(2) ∘ 是可结合的；

(3) 存在幺元 e；

(4) 对于每一个元素 x∈ G，都存在它的逆元x^{-1}∈ G

则称<G, ∘ >是一个群.

实例

设$G=\{e, a, b, c\}$，G上的运算由下表给出，称为**Klein四元群**。

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

特征：

1. 满足交换律
2. 每个元素都是自己的逆元
3. a, b, c中任何两个元素运算结果都等于剩下的第三个元素

群的阶数

设<G,*>是一个群,如果G是有限集，那么称<G,*>为有限群，并且|G| 为该有限群的阶数；如果G是无限集，则称<G,*>为无限群。

注：阶数为1（即只含单位元）的群称为平凡群.

例：<Z,+>和<R,+>是无限群；

<Z_n,⊕>是有限群，也是 n 阶群；

Klein四元群是4阶群；

<{0},+>是平凡群。

n阶($n\geq 2$)实可逆矩阵集合关于矩阵乘法构成的群是非交换群.

群的性质

设<G,*>是一个群。

（1）非平凡群中不可能有零元.

（2）对于∀a,b∈ G, 必存在唯一的x∈ G,使得a* x =b.

（3）对于∀{a,b,c}∈ G若:

$$a*b = a*c$$或

$$b*a = c*a$$

则必有b=c (消去律)。

（4）运算表中的每一行或每一列都是一个置换。

（5）除幺元e外,不可能有任何别的幂等元。

元素的幂

设G是群，$a \in G$，$n \in Z$，则a 的 n次幂.

$$a^n = \begin{cases} e & n = 0 \\ a^{n-1}\mathrm{a} & n > 0 \\ (a^{-1})^m & n < 0, n = -m \end{cases}$$

注：群中元素可以定义负整数次幂.

在<Z_3,⊕ >中有

$$2^{-3} = (2^{-1})^3 = 1^3 = 1 \oplus 1 \oplus 1 = 0$$

在<Z,+>中有

$$(-2)^{-3} = 2^3 = 2+2+2 = 6$$

幂运算性质

设G 为群，则G中的幂运算满足：

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

(2) $\forall a,b \in G$，$(ab)^{-1}=b^{-1}a^{-1}$

(3) $\forall a \in G$，$a^n a^m = a^{n+m}$，$n, m \in Z$

(4) $\forall a \in G$，$(a^n)^m = a^{nm}$，$n, m \in Z$

(5) 若G为交换群，则 $(ab)^n = a^n b^n$.

元素的阶

设G是群，$a \in G$，使得等式 $a^k=e$ 成立的最小正整数k 称为元素a 的阶，记作$|a|=k$，称 a 为 k 阶元。若不存在这样的正整数 k，则称 a 为无限阶元。

例：(1) 在$<Z_6,\oplus>$中，2和4是3阶元， 3是2阶元， 1和5是6阶元，0是1阶元 。

(2) 在$<Z,+>$中，0是1阶元，其它整数的阶均为无限。

元素的阶的性质

G为群，$a \in G$且 $|a| = r$. 设k是整数，则

(1) $a^k = e$当且仅当$r \mid k$

(2)$|a^{-1}| = |a|$

子群（Subgroup）

设G 是群，H 是G 的非空子集， 如果H关于G中的运算构成群，则称H是G 的子群，记作$H \leqslant G$。

① 若H是G 的子群，且$H \subset G$，则称H是G的真子群，记作$H < G$.

② 对任何群G都存在子群. G和$\{e\}$都是G 的子群，称为G 的平凡子群.

例： $n\mathbf{Z}$ (n是自然数) 是整数加群<Z,+> 的子群. 当$n \neq 1$时，$n\mathbf{Z}$是Z的真子群.

子群判定定理1

设G为群，H是G的非空子集，则H是G的子群当且仅当

(1) $\forall a,b\in H$有$ab\in H$；

(2) $\forall a\in H$有$a^{-1}\in H$。

证 必要性是显然的. 为证明充分性，只需证明$e\in H$.
因为H非空，存在$a\in H$. 由条件(2) 知$a^{-1}\in H$，根据条件(1) $aa^{-1}\in H$，即$e\in H$.

子群判定定理2

设G为群，H是G的非空子集. H是G的子群当且仅当$\forall a,b\in H$有$ab^{-1}\in H$.

证　必要性显然. 只证充分性.

因为H非空，必存在$a\in H$.

根据给定条件得$aa^{-1}\in H$，即$e\in H$.

任取$a\in H$, 由$e,a\in H$ 得 $ea^{-1}\in H$，即$a^{-1}\in H$.

任取$a,b\in H$，知$b^{-1}\in H$. 再利用给定条件得$a(b^{-1})^{-1}\in H$，即$ab\in H$.

综合上述，可知H是G的子群.

子群判定定理3

设G为群，H是G的非空有穷子集，则H是G的子群当且仅当

$\forall a,b\in H$有$ab\in H$.

证 必要性显然. 为证充分性，只需证明 $a\in H$有$a^{-1}\in H$.

任取$a\in H$, 若$a = e$, 则$a^{-1} = e\in H$.

若$a\neq e$，令$S=\{a,a^2,\ldots\}$，则$S\subseteq H$.

由于H是有穷集，必有$a^i = a^j$（$i<j$）.

根据G中的消去律得 $a^{j-i} = e$，由$a \neq e$可知 $j-i>1$，由此得

$$a\,a^{j-i-1} = e \text{ 和 } a^{j-i-1}a = e$$

从而证明了$a^{-1} = a^{j-i-1}\in H$.

生成子群

设G为群，$a \in G$，令$H=\{a^k \mid k \in \mathbf{Z}\}$，则$H$是$G$的子群，称为由$a$ 生成的子群，记作$<a>$.

例：

（1）整数加群，由2生成的子群是 $<2>=\{2^k \mid k \in \mathbf{Z}\}=2\mathbf{Z}$

（2）$<\mathbf{Z}_6, \oplus>$中，由2生成的子群$<2>=\{0,2,4\}$

（3）Klein四元群 $G=\{e,a,b,c\}$的所有生成子群是：

$<e>=\{e\}$, $<a>=\{e,a\}$, $<b>=\{e,b\}$, $<c>=\{e,c\}$.