代数结构

Algebra Structures

内容提要

1. 运算及其性质
2. 代数系统
3. 群与子群
4. 阿贝尔群和循环群
5. 环与域
6. 格与布尔代数

内容提要

1. 运算及其性质
2. 代数系统
3. 群与子群
4. 阿贝尔群和循环群
5. 环与域
6. 格与布尔代数

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

群的定义

半群（Semigroup）

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

独异点(Monoid).

设V=<S,∘>是半群，若$e \in S$是关于∘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,∘,e>。

实例

(1) $<Z^+,+>$,$<N,+>$,$<Z,+>$,$<R,+>$都是半群，+是普通加 法. 这些半群中除$<Z^+,+>$外都是独异点。

(2) $<P(B),\oplus>$为半群，也是独异点，其中$\oplus$为集合对称差运算。

(3) $<R^*,\circ>$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 $\forall a\in G$，$a^{-1}\in G$，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；

$<Z_n,\oplus>$是有限群，也是 n 阶群；

Klein四元群是4阶群；

<{0},+>是平凡群。

群的性质与元素的阶

群的性质

设$\langle G,*\rangle$是一个群。

（1）非平凡群中不可能有零元。

（2）对于$\forall a,b \in G$, 必存在唯一的$x \in G$,使得$a * x = b$。

（3）对于$\forall \{a,b,c\} \in G$，若:

$$a*b = a*c \text{或}$$

$$b*a = c*a$$

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。

例：

在$<Z_3, \oplus>$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 $(ab)^n = a^n b^n$.

幂运算性质

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

证明：当m,n均大于0时，容易证明。

不妨设 $m < 0$，令 $t = a^n a^m$ ，则 $t = a^n a^{-|m|} = a^n (a^{-1})^{|m|}$

- 若 $n \geq |m|$， $t = a^{n-|m|} = a^{n+m}$

- 若 $n < |m|$， $t = (a^{-1})^{|m|-n} = (a^{-1})^{-m-n} = a^{n+m}$

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,⊕>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) $|a^{-1}| = |a|$ 。

证明：

(1) $\Leftarrow$易。

"$\Rightarrow$"

设$k = nr + m$, $0 \le m < r$

则$a^k = a^{nr+m} = a^{nr} a^m = a^m = e$

$\therefore r \mid k$

(2) 反证。