第十章 群与环

本章将讨论特殊的代数系统--群与环。 群是一个具有二元运算的抽象代数，而环是具有两个二元运算的代数系统。

10.1 群的定义及性质

① 半群

定义 1: 设 V=<S, ∘>是一个代数，∘为二元运算。如果∘是可结合的，即

$$\forall a,b,c \in S,(a \circ b) \circ c = a \circ (b \circ c),$$

则称 V 为半群。

另外，如果半群<S, ∘>中的∘运算满足交换律，则称<S, ∘>为可交换的半群。

- 例如， $<\mathbb{N},+>$， $<\mathbb{Z},+>$，$<\mathbb{R},+>$ 都是可交换的半群。

定义 2: 假设 V=<S, ∘> 是一个半群，如果 V 中有单位元 e，则称 V 是独异点，或幺半群。

- 例如， $<\mathbb{N},+>$，$<\mathbb{N}, \times>$ 都是半群。因 0 是$<\mathbb{N},+>$的单位元，1 是$<\mathbb{N}, \times>$的单位元，故它们都是独异点。

$<\mathbb{N}-\{0\},+>$是半群，但它没有单位元，故它不是独异点。

例 1： 设$<S,*>$ 是一个半群。如果 S 是一个有限集，则必有 $a\in S$，使得 $a*a=a$。

② 群

定义 3： 设 $<G,*>$ 是一代数系统，如果满足以下几点：

(1) 运算是可结合的；

(2) 存在单位元 e；

(3) 对任意 $a\in G$，都存在逆元a^{-1}；

则称 $<G,*>$ 是一个群。

- 例如， $<\mathbb{Z},+>$，$<\mathbb{Q}-\{0\}$，$\times>$ 都是群。但$<\mathbb{Q}$，$\times>$不是群。

例 2： 设 $G=\{e,a,b,c\}$，$\circ$为 G 上的二元运算，它由以下运算表给出。不难证明 G 是一个群，称该群为 Klein 四元群。简称四元群。

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

注 1： 在半群，群这些概念中，只含有一个二元运算，所以在不发生混淆的情况下，经常将算符省去。例如将 $x*y$ 写成 xy。

定义 4： 一个群如果运算满足交换律，则称该群为交换群，或阿贝尔(Abel)群。

例如：$<\mathbb{Z},+>$，$<\mathbb{Q},+>$，$<\mathbb{R},+>$中每个元素都有逆元即它的相反数，且运算满足交换律，所以它们是交换群。

注 2： 接定义，群是一个集合对其中某个代数运算而言的。仅说某个集合是一个群是不完整的。同一个集合，对其中的两个不同的运算有时都构成群，但这是两个不同的群。然而为了说话方便，当已知集合 G 对某种运算构成群时，就可简单地说 G 是一个群。

定义 5： (1) 当群 G 是有限集时，则称 G 是有限群，否则称为无限群。

(2) 有限群 G 中元素的个数称为该群的阶，记为$|G|$。

(3) 阶数为 1 的群称为平凡群，它只含一个单位元。

例如：$<\mathbb{Z},+>$，$<\mathbb{Q},+>$，$<\mathbb{R},+>$都是无限群。四元群是有限群，它的阶是 4。$<\{0\},+>$是平凡群。

例 3： 群中不可能有零元。

例 4: 设 G 是一个群，且$|G|>1$。对于$\forall a, b\in G$, 必存在唯一的 $x\in G$, 使得 $ax = b$。

定义 6: 设 G 是一个群，$a\in G, n\in \mathbb{Z}$, 则 a 的 n 次幂为

$$a^n = \begin{cases} e & n = 0; \\ a^{n-1}a & n > 0; \\ \left(a^{-1}\right)^{-n} & n < 0。 \end{cases}$$

例 5: 设 G 是一个群，则 G 是阿贝尔群$\Leftrightarrow\forall a, b\in G$, 有

$$(ab)^2 = a^2b^2。$$

定义 7: 设 G 是一个群，$a\in G$, 使得等式

$$a^k = e$$

成立的最小正整数 k 称为 a 的阶，记作$|a|$，并称 a 是 k 阶元。若不存在这样的正整数 k，则称 a 为无限阶元。

例如： 在$<\mathbb{Z}, +>$中，0 是 1 阶元，其它的都是为无限阶元。在四元群中，e 是 1 阶元，其它的都是 2 阶元。

定理 1: 设 G 是一个群，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) $\forall a \in \mathrm{G}$，$a^n a^m = a^{n+m}$，$n, m \in \mathbb{Z}$。

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

(5) 若 G 是一个阿贝尔群, 则$(ab)^n = a^n b^n$，$n \in \mathbb{Z}$。

例 6： 设 G 是一个群。若$\forall x \in \mathrm{G}$ 有 $x^2 = \mathrm{e}$，则 G 是阿贝尔群。

定理 2： 设 G 是一个群，则 G 中运算满足消去律，即对$\forall a, b, c \in \mathrm{G}$，有

(1) 若$ab = ac$，则$b = c$。

(2) 若$ba = ca$，则$b = c$。

例 7： 设 G 是一个群, $n \in \mathbb{N} - \{0\}$。如果$\forall a, b \in \mathrm{G}$，有

$$(ab)^{n+i} = a^{n+i} b^{n+i},\quad i = 0,1,2,$$

则 G 是阿贝尔群。

例 8： 设 G 是一个群。如果$\forall a, b \in \mathrm{G}$，有

$$(ab)^5 = a^5 b^5,\quad 及\quad (ab)^3 = a^3 b^3,$$

则 G 是阿贝尔群。

定理 3： 设 G 是一个群，$a \in \mathrm{G}$，且$|a| = r$。设 k 为整数，则

(1) $a^k = \mathrm{e} \Leftrightarrow r | k$。

(2) $|a^{-1}| = |a|$。

例 9：设 G 是一个群。$a, b \in$ G 是有限阶元。证明

(1) $|b^{-1}ab| = |a|$。

(2) $|ab| = |ba|$。