§10.1 群的定义及性质

定义

（1）设$V=<S,\circ>$是一个代数系统，$\circ$为二元运算。若$\circ$满足结合律，则称V为**半群**；

（2）设$V=<S,\circ>$是一个半群，若S有单位元e，则称V为**幺半群**或**独异点**，记为$<S, \circ, e>$；

（3）设$V=<S, \circ, e>$是幺半群，若$\forall x\in S$，有$x^{-1}\in S$，则称V是**群**，简记为G。

例 $<\mathbb{Z}, +>$，$<\mathbb{Q}, +>$，$<\mathbb{R}, +>$，$<\mathbb{R}^*, \times>$，$<\mathbb{R}^{n\times n}, +>$，$<Z_n, \oplus_n>$，$<P(B), \oplus>$都是群。

注 ① 群中的运算常称为“乘法”，运算符可省略不写，只记为G；

② 设G是群，若G为有穷集，则称G为**有限群**，否则，称为**无限群**；有限群G的基数称为**群G的阶**，记为 $|G|$；

③ 只含单位元的群称为**平凡群**；

④ 若群G中的二元运算满足交换律，则称G为**交换群**或**Abel群**。

例 klein四元群$G=\{e,a,b,c\}$，运算表如下

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

klein四元群是交换群，e是单位元，每个元素的逆元是其自身，a,b,c中任意两元的运算结果都等于第三个元素。

例 某二进制码的码字$\alpha = x_1x_2\cdots x_7$由7位构成，其中 x_1,x_2,x_3,x_4为数据位，x_5,x_6,x_7为校验位，并且

$$x_5 = x_1 \oplus_2 x_2 \oplus_2 x_3\text{，}\quad x_6 = x_1 \oplus_2 x_2 \oplus_2 x_4$$

$$x_7 = x_1 \oplus_2 x_3 \oplus_2 x_4$$

这里，表示模2加法。设G为所有码字构成的集合，在G上定义二元运算“$\circ$”：

$$\text{对}\forall \alpha = x_1x_2\cdots x_7,\ \beta = y_1y_2\cdots y_7 \in G,$$

$$\forall \alpha \circ \beta = z_1z_2\cdots z_7\text{，}\ z_i = x_i \oplus_2 y_i\text{，}\ i=1,2,\cdots,7$$

则 $\langle G,\circ\rangle$ 构成群。

定义 设G是群，$a\in G$，$n\in\mathbb{Z}$，则a的n次幂为

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

例如，在群 $<\mathbb{R}^{n\times n},+>$ 中，

$$I^3=I+I+I=3I$$

在群 $<\mathbb{Z},+>$ 中，

$$3^{-2}=(3^{-1})^2=(-3)^2=(-3)+(-3)=-6$$

性质 设G是一个群，则

（1）$\forall a\in G, (a^{-1})^{-1}=a$;

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

（3）$\forall a\in G, a^n a^m=a^{n+m}$;

（4）$\forall a\in G, (a^n)^m=a^{nm}$;

（5）若G为交换群，则$\forall a,b\in G, (ab)^n=a^n b^n$。

例 群的运算满足消去律。

例 设G是有限群。任取$a\in G$，有$G=aG$。这里

$$aG=\{ ag \mid g\in G \}$$

定义 设G是一个群，$a\in G$，称使得 $a^k=e$ 成立的最小正整数k为a的**阶**，记为 $|a|$。若不存在这样的k，则称a为**无限阶**的。

单位元e是1阶元素。

例 群 $<\mathbb{Z}, +>$ 中，除了单位元0，其它元素都是无限阶的。

例 群 $<Z_6, \oplus_6>$中，除了单位元0以外，1与5的阶为6，2与4的阶为3，3的阶为2，

定理 设G是一个群，$a\in G$，且$|a|=r$。设k是整数，则

（1） $a^k=e$ 当且仅当 $r|k$;

（2） $|a^{-1}|=|a|$。

例 设G是一个群，$a,b\in G$是有限阶，

（1） $|b^{-1}ab|=|a|$

（2） $|ab|=|ba|$

例 有限群中阶数大于2的元素个数为偶数。