第八章　群和环

第七节 群的阶与群中元素的阶

三. 群的阶与群中元素的阶

1. 群的阶：

定义：设<G,★>是群，如果 |G|=n，则称 <G,★>是 n 阶群。

当 G 所包含的元素个数为有限时，群 <G,★>的阶为 G 所包含的元素个数。

当 G 所包含的元素个数为无限时，群 <G,★>为无限群。

群<{a},★>，<{a,b},★>，<{a,b,c},★> 分别是 1、2、3 阶群，假定 a 是幺元，根据有限群运算表的特征，它们的运算表分别是：

★	a
a	a

★	a	b
a	a	b
b	b	a

★	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

从运算表可以看出：所有的一阶群都同构；
所有的二阶群都同构；
所有的三阶群都同构。

2. 群中元素的阶

定义：设<G,★>是群，a∈G，使得 $a^k = e$ 成立的最小正整数 k 称为 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 的阶是无限的。

例如：群 <I,+>是一个无限群，只有幺元 0 的阶是 1，其余元素的阶都是无限的。

例： <X, ∘>的运算表如下图所示：<X, ∘>是否是群？若是群求各元素的阶。

∘	S	R	A	L
S	S	R	A	L
R	R	A	L	S
A	A	L	S	R
L	L	S	R	A

解：显然<X, ∘>是封闭的；可以验证 <X, ∘>是可结合的；S是幺元； S的逆元为S，A的逆元为A，R与 L 互为逆元。所以<X, ∘>是群。

因为 $S^1=S$， $A\circ A=A^2=S$，

$R^4=R^2\circ R^2=A\circ A=S$， $L^4=L^2\circ L^2=A\circ A=S$ ，

所以 $|S|=1$， $|A|=2$， $|R|=4$， $|L|=4$。

定理

设<G,★>是群，$a \in G$ 且 $|a| = k$。 设 n 是整数，则

(1) $a^n = e$ 当且仅当 k/n。

(2) $|a^{-1}| = |a|$。

证明 (1) 充分性：由于 k/n，必存在整数 m 使得 $n=mk$，因 $|a| = k$，所以 $a^k = e$，因此有

$a^n = a^{mk} = (a^k)^m = e^m = e$。

必要性：已知 $a^n=e$，(反证法)假设 n 不是 k 的整数倍，

根据除法规则，一定存在整数 m 和 r 使得 $n=mk+r$ ($m,r \in I$, $0 \le r < k$)，于是有 $e= a^n= a^{mk+r} = (a^k)^m ★ a^r = e★a^r = a^r$

由 $a^r=e$，而 $r<k$，与 $|a| = k$ 矛盾。

所以 n 一定是 k 的整数倍。 这就证明了 k/n。

(2) 证明 $|a^{-1}| = |a|$

证明：(I) 当 $|a|$ 为有限数，

由 $(a^{-1})^k = (a^k)^{-1} = e^{-1} = e$ 可知 a^{-1} 的阶存在。

令 $|a^{-1}| = t$，根据 (1) 有 $t|k$

推论：$<G,\star>$是个群，对任何 $a \in G$，有

$(a^n)^{-1} = (a^{-1})^n$

(II) 当 $|a|$ 为无限，

若 $|a^{-1}|$ 为有限数， 设 $|a^{-1}|=n$，

$a^n = ((a^{-1})^{-1})^n = ((a^{-1})^n)^{-1} = e^{-1} = e$

这与 $|a|$为无限矛盾。所以 $|a^{-1}|$也为无限的。

综上 $|a^{-1}| = |a|$ 。

第七节 结束