西北工業大學 NORTHWESTERN POLYTECHNICAL UNIVERSITY

循环群

循环群

定义6.14 设G是群，$a\in G$，$n\in Z$，则a 的 n次幂.

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

a的逆元

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

元素的阶

定义6.15 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a 的阶(或周期)，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.

例如，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.

在$<Z,+>$中，0是1阶元，其它整数的阶都不存在.

幂运算规则

定理6.15 设G 为群，则G中的幂运算满足：

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

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

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

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

(5) 若G为交换群，则 $(a \circ b)^n = a^n \circ b^n$.

证 (1) $(a^{-1})^{-1}$是a^{-1}的逆元，a也是a^{-1}的逆元. 根据逆元唯一性，等式得证.

(2) $(b^{-1}\circ a^{-1})\circ(a\circ b)= b^{-1}\circ(a^{-1}\circ a)\circ b = b^{-1}\circ b = e$,

同理 $(a\circ b)\circ(b^{-1}\circ a^{-1}) =e$，

故$b^{-1} \circ a^{-1}$是$a \circ b$的逆元. 根据逆元的唯一性等式得证.

元素的阶

定理6.16 $<G,\circ>$为群，$a\in G$且 $|a| = r$. 设k是整数，则

(1) $a^k = e$当且仅当$r \mid k$ （ r 整除 k ）

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

因此r 又称为a的周期

证 (1) 充分性. 由于$r|k$，必存在整数m使得$k = mr$，所以有

$$a^k = a^{mr} = (a^r)^m = e^m = e.$$

必要性. 根据除法，存在整数 m 和 i 使得

$$k = mr+i,\ 0\le i\le r-1$$

从而有 $e = a^k = a^{mr+i} = (a^r)^m\circ a^i = e\circ a^i = a^i$

因为$|a| = r$，必有$i = 0$. 这就证明了$r \mid k$.

a的逆元的阶是a的阶的因子

(2) 由 $(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$

可知 a^{-1} 的阶存在. 令$|a^{-1}| = t$，根据上面的证明有$t \mid r$.

a又是a^{-1}的逆元，所以 $r \mid t$. 从而证明了$r = t$，即$|a^{-1}| = |a|$

循环群

定义6.16 设G是群，若存在$a \in G$使得

$$G=\{a^k \mid k \in Z\}$$

则称G是循环群，记作$G=<a>$，称 a 为G 的生成元.

循环群的分类：n 阶循环群和无限循环群.

设$G=<a>$是循环群，若a是n 阶元，则 $G = \{ a^0=e, a^1, a^2, \ldots , a^{n-1} \}$

那么$|G| = n$，称 G 为 n 阶循环群.

若a 是无限阶元，则 $G = \{ a^0=e, a^{\pm 1}, a^{\pm 2}, \ldots \}$

称 G 为无限循环群.

例如$<Z,+>$是无限循环群，生成元是1和-1； $<Z_6,\oplus>$是6阶循环群，生成元是1和5. 以上生成元互逆。

循环群的性质

定理6.17 设$G=\langle a\rangle$是循环群.

(1) 若G是无限循环群，则G与$<Z,+>$同构;

(2) 若G是 n 阶循环群，则G与$<Z_n,\oplus>$同构.

证明 略.

Note:

(1) 无限循环群同构于整数加法群;

(2) 周期为n的循环群同构于模n加法群.

(3) 我们对整数加法群和模n加法群的研究很充分.

THE END