第三讲群的简单性质

陈建文

October 13, 2022

定义1. 设G为一个非空集合，"$\circ$"为G上的一个二元代数运算。如果下列各个条件成立，则称G对"$\circ$"运算构成一个群（*group*）：

I. "$\circ$"运算满足结合律，即$\forall a,b,c \in G\ (a \circ b) \circ c = a \circ (b \circ c)$;

II. 对"$\circ$"运算，G中有一个左单位元e，即$\forall a \in G\ e \circ a = a$;

III. 对G中的每个元素，关于$\circ$运算有一个左逆元，即$\forall a \in G \exists b \in G b \circ a = e$，其中$e$为$II$中的同一个左单位元素。

在群$(G, \circ)$中，$\forall a, b \in G, a \circ b$简写为$ab$。

定理1. 设G为一个群，则$\forall a \in G$，a的左逆元也是a的右逆元。

定理2. 设G为一个群，则G的左单位元e也是右单位元。

定理3. 设a与b为群G的任意两个元素，则$(a^{-1})^{-1} = a$，$(ab)^{-1} = b^{-1}a^{-1}$。

定理4. 在群G中，$\forall a, b \in G$，方程

$$ax = b$$
$$ya = b$$

关于未知量x与y都有唯一解。

定理5. 非空集合G对其二元代数运算$\circ$构成一个群的充分必要条件是下列两个条件同时成立：

1. "$\circ$"运算满足结合律，即$\forall a,b,c \in G (a \circ b) \circ c = a \circ (b \circ c)$。

2. $\forall a, b \in G$，方程

$$ax = b$$
$$ya = b$$

关于未知量x与y有解。

证明. $\Leftarrow$

由G非空知$\exists b, b \in G$。方程$yb = b$有解，设e为一个解，则$eb = b$。$\forall a \in G$,方程$bx = a$有解，设c为一个解，则$bc = a$。于是

$$ea = e(bc) = (eb)c = bc = a$$

从而e为左单位元。

$\forall a \in G$，方程$ya = e$有解，其解为a的左逆元。 □

定理6. 设$(G,\circ)$为一个群，则"$\circ$"运算满足消去律，即$\forall x,y,a\in G$，
如果$ax=ay$，则$x=y$（左消去律）
如果$xa=ya$，则$x=y$（右消去律）

定理7. 非空有限集合G对在其上定义的二元代数运算$\circ$构成一个群的充分必要条件是下列两个条件同时成立：
1. "$\circ$"运算满足结合律。
2. "$\circ$"运算满足左、右消去律。

证明. $\Leftarrow$
先证$\forall a,b\in G$，方程$ax=b$有解。
令$f:G\to aG=\{ag|g\in G\}$，$\forall x\in G, f(x)=ax$。则f为单射,这是因为$\forall x_1,x_2\in G$，如果$f(x_1)=f(x_2)$，则$ax_1=ax_2$，由左消去律得$x_1=x_2$；同时，f为满射，这是因为$\forall y\in aG$，$\exists x\in G$，$y=ax$，于是$f(x)=ax=y$。此时必有$aG=G$，否则$aG\subseteq G$且$aG\neq G$，从而aG为G的真子集，于是f为有限集G与其真子集之间的一个双射，矛盾。由$f:G\to aG=G$为双射知，$\forall b\in G$，$\exists c\in G$，$ac=b$。所以，方程$ax=b$在G中有解。
同理可证，$\forall a,b\in G$，方程$ya=b$有解。 □

例. *3*阶群是交换群。

定义2. 设G为一个群，$\forall a\in G$，定义$a^0=e$，$a^{n+1}=a^n\circ a(n\geq 0)$，$a^{-n}=(a^{-1})^n(n\geq 1)$。

定理8. 设G为一个群，$a\in G$，m，n为任意整数，则$a^ma^n=a^{m+n}$，$(a^m)^n=a^{mn}$。

设$(G,+)$为一个阿贝尔群，G的单位元记为0。$\forall a\in G$，定义$0a=0$，$(n+1)a=na+a(n\geq 0)$，$(-n)a=n(-a)(n\geq 1)$。对任意整数m，n，$ma+na=(m+n)a$，$(mn)a=m(na)$，$n(a+b)=na+nb$。

定义3. 设$(G,\circ)$为一个群，$a\in G$，使$a^n=e$的最小正整数n称为a的阶。如果不存在这样的正整数n，则称a的阶为无穷大。

定理9. 有限群的每个元素的阶不超过该有限群的阶。

证明. 设群G的阶为N，则$a^0,a^1,a^2,\cdots,a^N$为G的$N+1$个元素，所以必有两个是相同的，设$a^k=a^l$，$0\leq k<l\leq N$。于是，$a^{l-k}=e$，$0<l-k\leq N$，从而a的阶不超过N。 □

课后作业题：

练习1. 设a和b为群G的两个元素。如果$(ab)^2=a^2b^2$，试证：$ab=ba$。

练习2. 设G为群。如果$\forall a\in G$，$a^2=e$，试证：G为交换群。

练习3. 证明：四阶群是交换群。

练习4. 证明：在任一阶大于*2*的非交换群里必有两个非单位元a和b，使得$ab=ba$。

练习5. 有限阶群里阶大于2的元素的个数必为偶数。

练习6. 证明：偶数阶群里，阶为2的元素的个数必为奇数。

练习7. 设a为群G的一个元素，a的阶为n且$a^m = e$，试证n能整除m。

练习8. 设$a_1, a_2, \cdots, a_n$为n阶群中的n个元素（它们不一定各不相同）。证明：存在整数p和q（$1 \leq p \leq q \leq n$），使得

$$a_p a_{p+1} \cdots a_q = e$$