

第三讲群

陈建文

September 21, 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, 即对 G 的每个元素 a 有一个相应元素 b , 使得 $b \circ a = e$, 其中 e 为II中的同一个左单位元素。即 $\forall a \in G \exists b \in G b \circ a = e$ 。

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。

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。

2. “ \circ ”运算满足左、右消去律。

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 $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ 。

设 $(G, +)$ 为一个阿贝尔群, $\forall a \in G$, 定义 $0a = 0$, $(n+1)a = na + a (n \geq 0)$, $-na = n(-a) (n \geq 1)$ 。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。

课后作业题:

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

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