

第三讲群的简单性质

陈建文

February 14, 2023

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. $\forall a \in G \exists b \in G b \circ a = e$, 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 $\forall a, b \in G$, 如果 $ba = e$, 则 $ab = e$ 。

证明. 在

$$ba = e$$

的两边同时右乘以 b 得

$$(ba)b = eb$$

从而

$$b(ab) = b$$

在 G 中存在 c 使得 $cb = e$, 于是

$$c(b(ab)) = cb$$

所以

$$ab = e$$

□

定理2. 设 G 为一个群, 则 G 的左单位元 e 也是右单位元。

证明. $\forall a \in G$, 设 $b \in G$, $ba = e$, 则 $ae = a(ba) = (ab)a = ea = a$, 所以 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 $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$ 。

证明. 由

$$aa^{-1} = e$$

得

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

由

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = e$$

得

$$(ab)^{-1} = b^{-1}a^{-1}$$

□

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 $f : G \rightarrow aG = \{ag | g \in G\}$, $\forall x \in G, f(x) = ax$ 。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 $f : G \rightarrow aG = G$ 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 $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ 。

证明. 1. $a^m a^n = a^{m+n}$

$$a^2 a^3 = a^5 : (aa)(aaa) = a^5$$

$$a^2 a^{-2} = e : (aa)(a^{-1}a^{-1}) = e$$

$$a^{-2} a^2 = e : (a^{-1}a^{-1})(aa) = e$$

$$a^2 a^{-3} = aa(a^{-1}a^{-1}a^{-1}) = a^{-1}$$

$$a^{-2} a^3 = (a^{-1}a^{-1})aaa = a$$

$$a^{-2} a^{-3} = (a^{-1}a^{-1})(a^{-1}a^{-1}a^{-1}) = a^{-5}$$

$$m \geq 0, n \geq 0 :$$

对 n 归纳:

$$(1) \text{ 当 } n = 0 \text{ 时, } a^m a^0 = a^{m+0}$$

$$(2) \text{ 当 } n = k + 1 \text{ 时, } a^m a^{k+1} = a^m (a^k a) = (a^m a^k) a = a^{m+k} a = a^{m+k+1}$$

$$m \geq 0, n \leq 0 :$$

$$m = s, n = -t, s \geq 0, t \geq 0 :$$

当 $s = t$ 时, 要证 $a^s a^{-s} = a^{s+(-s)} = a^0 = e$, 对 s 归纳:

$$(1) \text{ 当 } s = 0 \text{ 时, } a^0 a^{-0} = a^{0+(-0)} = e$$

$$(2) \text{ 当 } s = k + 1 \text{ 时, } a^{k+1} a^{-(k+1)} = (a^k a)(a^{-1})^{k+1} = (a^k a) a^{-1} (a^{-1})^k = a^k a^{-k} = e$$

$$\text{当 } s > t \text{ 时, } a^s a^{-t} = a^{s-t} a^t a^{-t} = a^{s-t}$$

$$\text{当 } s < t \text{ 时, } a^s a^{-t} = a^s (a^{-1})^t = a^s (a^{-1})^s (a^{-1})^{t-s} = a^s a^{-s} a^{-(t-s)} = a^{s-t}$$

$$m \leq 0, n \geq 0 :$$

$$m = -s, n = t, s \geq 0, t \geq 0 :$$

$$a^{-s} a^t = (a^{-1})^s ((a^{-1})^{-1})^t = (a^{-1})^s (a^{-1})^{-t} = (a^{-1})^{s-t} = a^{-(s-t)} = a^{t-s}$$

$$m < 0, n < 0 :$$

$$m = -s, n = -t, s > 0, t > 0$$

$$a^{-s} a^{-t} = (a^{-1})^s (a^{-1})^t = (a^{-1})^{s+t} = a^{-(s+t)} \quad \square$$

设 $(G, +)$ 为一个阿贝尔群, G 的单位元记为 0 。 $\forall a \in G$, a 的逆元记为 $-a$ 。 $\forall a \in G$, 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 $a^0, a^1, a^2, \dots, a^N$ 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 。 \square

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： $ab = ba$ 。

证明. 由已知条件知 $abab = aabb$ ，两边同时左乘 a^{-1} ，右乘 b^{-1} ，得 $ab = ba$ 。□

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

证明. $\forall a, b \in G$ ，由已知条件知 $a^2 = e, b^2 = e$ ，同时 $(ab)^2 = e$ ，即 $abab = e$ ，两边同时左乘 a ，右乘 b ，得 $ba = ab$ ，这证明了 G 为交换群。□

练习3. 证明：四阶群是交换群。

证明. 设在四阶群 (G, \circ) 中， $G = \{e, a, b, c\}$ ，

其乘法表为：

\circ	e	a	b	c
e	e	a	b	c
a	a	aa	ab	ac
b	b	ba	bb	bc
c	c	ca	cb	cc

$ab \neq a$ ，否则 $b = e$ ，矛盾； $ab \neq b$ ，否则 $a = e$ ，也矛盾。于是 $ab = e$ 或 c 。

当 $ab = e$ 时， a 为 b 的逆元，因此 $ba = e$ ，此时 $ab = ba$ 。

当 $ab = c$ 时，此时亦有 $ba \neq b$ 并且 $ba \neq a$ 。如果 $ba = e$ ，则 b 为 a 的逆元，于是 $ab = e$ ，与 $ab = c$ 矛盾。因此，必有 $ba = c$ ，于是， $ab = ba$ 。

同理可证 $ac = ca, bc = cb$ 。因此， (G, \circ) 一定为交换群。□

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 $ab = ba$ 。

证明. 设 G 为任一阶大于2的非交换群， $a \in G$ 且 a 不是 G 的单位元。令 $b = a^{-1}$ ， b 不是单位元， $ab = ba = e$ 。□

练习5. 有限阶群里阶大于2的元素的个数必为偶数。

证明. 设 G 为一个有限阶群，阶大于2的元素必成对出现，设 $a \in G$ ， a 的阶为 $n(n > 2)$ ，则 a^{-1} 的阶也为 n 。这里 $a \neq a^{-1}$ 。□

练习6. 证明：偶数阶群里，阶为2的元素的个数必为奇数。

证明. 在偶数阶群里，阶大于2的元素的个数为偶数，单位元的阶为1，其余元素的阶的2，显然阶为2的元素的个数为奇数。□

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 。

证明. 设 $m = nq + r(0 \leq r < n)$ ，则 $a^m = (a^n)^q a^r$ ，由 $a^n = e$ 且 $a^m = e$ 得 $a^r = e$ ，再由 n 为 a 的阶知 $r = 0$ （否则将存在比 n 更小的正整数 r ， $a^r = e$ ，与 a 的阶为 n 矛盾），这证明了 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

$$a_p a_{p+1} \cdots a_q = e。$$

证明. 考虑以下表达式:

$$\begin{aligned} & a_1 \\ & a_1 a_2 \\ & \dots \\ & a_1 a_2 \cdots a_i \\ & \dots \\ & a_1 a_2 \cdots a_n \end{aligned}$$

以上表达式中如果存在某个表达式计算结果为 e , 则结论成立。如果以上表达式中任意一个计算结果都不为 e , 则其中必有两个表达式计算结果相等, 不妨设 $a_1 a_2 \cdots a_{p-1} = a_1 a_2 \cdots a_{p-1} a_p a_{p+1} \cdots a_q$, 两边依次同时左乘 $a_1^{-1}, a_2^{-1}, \dots, a_{p-1}^{-1}$, 可得 $a_p a_{p+1} \cdots a_q = e$ 。

□

练习9. 设 a 和 b 为群 G 的两个元素, $ab = ba$, a 的阶为 m , b 的阶为 n 。试证: 乘积 ab 的阶为 m 与 n 的最小公倍数的约数。何时 ab 的阶为 mn ?

证明. 设 m 和 n 的最小公倍数为 k , 则 $m|k, n|k$ 。设 $k = xm, k = yn$, 则 $(ab)^k = a^k b^k = (a^m)^x (b^n)^y = e$, 于是 ab 的阶整除 k , 即 ab 的阶为 m 与 n 的最小公倍数的约数。

当 m 与 n 互素时, ab 的阶为 mn 。

设 ab 的阶为 t , 则 $e = (ab)^{mt} = (a^m)^t b^{mt} = b^{mt}$, 从而 $n|mt$, 由 n 与 m 互素知 $n|t$ 。同理, $e = (ab)^{nt} = a^{nt} (b^n)^t = a^{nt}$, 从而 $m|nt$, 由 m 与 n 互素知 $m|t$ 。由 $n|t$ 知 $\exists s \in \mathbb{Z}, t = ns$, 再由 $m|t$ 知 $m|ns$, 进一步, 由 m 与 n 互素知 $m|s$, 从而 $\exists p \in \mathbb{Z}, s = pm$, 于是 $t = ns = n(pm) = p(mn)$, 即 $mn|t$ 。

由 $(ab)^{mn} = a^{mn} b^{mn} = e$ 知 $t|mn$, 所以 $t = mn$ 。

当 ab 的阶为 mn 时, 必有 m 与 n 互素, 否则设 $d = (m, n), d > 1$, 则 m 与 n 的最小公倍数 $< mn$, 而 ab 的阶为 m 与 n 的最小公倍数的约数, 从而 ab 的阶 $< mn$, 矛盾。

□