

0.1 么半群和群

定义 0.1 ((么) 半群)

设 S 是非空集合. 在 S 中定义了二元运算称为乘法, 满足结合律, 即

$$(ab)c = a(bc), \quad \forall a, b, c \in S,$$

则称 S 为**半群**.

如果在半群 M 中存在元素 1 , 使得

$$1a = a1 = a, \quad \forall a \in M, \quad (1)$$

则称 M 为**么半群**, 1 称为**么元素**或**么元**或**单位元**.

如果一个么半群 M (或半群 S) 的乘法还满足交换律, 即

$$ab = ba, \quad \forall a, b \in M \text{ (或 } S),$$

则称 M (或 S) 为**交换么半群** (或**交换半群**), 也简单地称 M (或 S) 为**可换的**.

对于交换么半群, 有时把二元运算记为加法, 此时么元素记为 0 , 改称**零元素**或**零**.

例题 0.1

- (1) \mathbb{N} 对乘法是么半群, 对加法是半群而不是么半群. 非负整数集对加法与乘法均为么半群.
- (2) 令 $M(X)$ 为非空集 X 的所有变换 (即 X 到 X 的映射) 的集合, 则对于变换的乘法, $M(X)$ 是一个么半群, id_X 是一个么元素. 当 $|X| \geq 2$ 时, $M(X)$ 不是可换的.
- (3) 设 $P(X)$ 为非空集合 X 的所有子集的集合. 空集 \emptyset 也是 X 的一个子集, 则 $P(X)$ 对集合的并的运算是一个么半群, \emptyset 为么元素. 同样, $P(X)$ 对集合的交的运算是一个么半群, X 为么元素, 这两种么半群都是可换的.

命题 0.1

么半群中的么元素是唯一的.

证明 如果 1 与 $1'$ 都是么半群 M 的么元素, 则由条件 (1) 可知 $1 = 1'$.

□

定义 0.2 (群)

在非空集合 G 中定义了二元运算, 称为乘法. 若满足下列条件:

- (1) 结合律成立, 即 $(ab)c = a(bc) (\forall a, b, c \in G)$, 也即 G 是半群;
- (2) 存在**左么元**, 即 $\exists e \in G$, 使 $ea = a (\forall a \in G)$;
- (3) 对 $\forall a \in G$ 有**左逆元**, 即有 $b \in G$, 使 $ba = e$,

则称 (G, \cdot) 或 G 是一个**群**. 若 G 的乘法还满足交换律, 则称 G 为**交换群**或**Abel 群**.

有时将 Abel 群的运算记作加法. 这时左么元改称**零元**, 以 0 表示; a 的左逆元改称 a 的**负元**, 记为 $-a$.

注 数域 \mathbb{P} 对加法构成一个群, 左么元为 0 , a 的左逆元为 $-a$. \mathbb{P} 对乘法是么半群, 不是群. 但是 \mathbb{P} 中非零元素的集合 \mathbb{P}^* 对乘法是群, 1 为左么元, $1/a$ 为 a 的左逆元.

例题 0.2 令 Ω 是任意一个集合, G 是一个群, G^Ω 是 Ω 到 G 的所有映射的集合. 对任意两个映射 $f, g \in G^\Omega$, 定义乘积 fg 是这样的映射: 对任意 $a \in \Omega$, $(fg)(a) = f(a)g(a)$. 则 G^Ω 是群, 并且这个群 G 为 Abel 群当且仅当 G 是 Abel 群.

证明 易知上述乘法有结合律, $1 \in G^\Omega$ 是其单位元, 其中 $1(a) = 1_G, \forall a \in \Omega$ (1_G 表示群 G 的单位元); 任一元 $f \in G^\Omega$ 有逆元 f^{-1} , 其中 $f^{-1}(a) := (f(a))^{-1}, \forall a \in \Omega$. 故 G^Ω 成为群.

显然群 G 为 Abel 群当且仅当 G 是 Abel 群.

□

例题 0.3 b 是含么半群 G 中的元 a 的逆元当且仅当成立 $aba = a, ab^2a = 1$.

证明 设 b 是 a 的逆元, 显然有 $aba = a$ 和 $ab^2a = 1$. 反之, 若 $aba = a, ab^2a = 1$, 则

$$ab = ab(ab^2a) = ab^2a = 1, \quad ba = (ab^2a)ba = ab^2a = 1.$$

即 b 是 a 的逆元.

□

例题 0.4

(1) 令 G 是所有秩不大于 r 的 $n \times n$ 复方阵的集合, 则 G 在矩阵乘法下构成一个半群, 并且当 $r < n$ 时, 它不是一个含么半群; 当 $r = n$ 时, 它是一个含么半群, 但不是群.

(2) 整数集 \mathbb{Z} 对于乘法成为一个含么半群, 但不是群.

定理 0.1

设 m 是大于 1 的正整数, 记

$$U(m) = \{\bar{a} \in \mathbb{Z}_m \mid (a, m) = 1\},$$

则 $U(m)$ 关于剩余类的乘法构成群. 群 $(U(m), \cdot)$ 称为 \mathbb{Z} 的模 m 单位群, 显然这是一个交换群. 当 p 为素数时, $U(p)$ 常记作 \mathbb{Z}_p^* . 易知

$$\mathbb{Z}_p^* = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}.$$

♡

注 由初等数论可知, $U(m)$ 的阶等于 $\phi(m)$, 这里 $\phi(m)$ 是欧拉函数, 如果

$$m = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s},$$

其中 p_1, p_2, \dots, p_s 为 m 的不同素因子, 那么

$$\phi(m) = (p_1^{r_1} - p_1^{r_1-1})(p_2^{r_2} - p_2^{r_2-1}) \cdots (p_s^{r_s} - p_s^{r_s-1}) = m \prod_{i=1}^s \left(1 - \frac{1}{p_i}\right).$$

证明 对任意的 $\bar{a}, \bar{b} \in U(m)$, 有 $(a, m) = 1, (b, m) = 1$, 于是 $(ab, m) = 1$, 从而 $\overline{ab} \in U(m)$. 所以剩余类的乘法 “ \cdot ” 是 $U(m)$ 的代数运算.

对任意的 $\bar{a}, \bar{b}, \bar{c} \in U(m)$,

$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{ab} \cdot \bar{c} = \overline{(ab)c} = \overline{a(bc)} = \bar{a} \cdot \overline{bc} = \bar{a} \cdot (\bar{b} \cdot \bar{c}).$$

所以结合律成立.

因为 $(1, m) = 1$, 从而 $\bar{1} \in \mathbb{Z}_m$, 且对任意的 $\bar{a} \in U(m)$,

$$\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a},$$

$$\bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a},$$

所以 $\bar{1}$ 为 $U(m)$ 的单位元.

对任意的 $\bar{a} \in U(m)$, 有 $(a, m) = 1$. 由整数的性质可知, 存在 $u, v \in \mathbb{Z}$, 使

$$au + mv = 1.$$

显然 $(u, m) = 1$, 所以 $\bar{u} \in U(m)$, 且

$$\bar{a} \cdot \bar{u} = \overline{au} = \overline{au + mv} = \bar{1},$$

$$\bar{u} \cdot \bar{a} = \overline{ua} = \overline{au} = \bar{1}.$$

所以 \bar{u} 为 \bar{a} 的逆元. 从而知, $U(m)$ 的每个元素在 $U(m)$ 中都可逆.

这就证明了, $U(m)$ 关于剩余类的乘法构成群.

□

定理 0.2 (群的基本性质)

设 (G, \cdot) 是一个群, $a \in G, 1$ 是 G 的左么元, 则

- (1) 若 b 为 a 的左逆元, 则 b 也是 a 的右逆元, 即有 $ab = 1$, 故称 b 为 a 的逆元.
- (2) 任一元素 a 的逆元唯一, 记为 a^{-1} , 并且 $1^{-1} = 1, (a^{-1})^{-1} = a, (ab)^{-1} = b^{-1}a^{-1}, (a^n)^{-1} = (a^{-1})^n$.
- (3) 若 $a_1, a_2, \dots, a_r \in G$, 则

$$(a_1 a_2 \cdots a_r)^{-1} = a_r^{-1} a_{r-1}^{-1} \cdots a_1^{-1}.$$

- (4) 1 也是 G 的右么元, 即 $a \cdot 1 = a (\forall a \in G)$, 故 1 为 G 的么元. 故 G 为么半群, 么元唯一.
- (5) 群运算满足消去律, 即

$$ax = bx \text{ 或 } xa = xb, \text{ 则 } a = b, \forall a, b, x \in G.$$

**证明**

- (1) 事实上, 设 c 是 b 的左逆元, 则有

$$ab = 1 \cdot (ab) = (cb)(ab) = c(ba)b = c(1 \cdot b) = 1.$$

- (2) 设 b_1, b_2 均为 a 的逆元, 则有

$$b_1 = b_1 \cdot 1 = b_1(ab_2) = (b_1a)b_2 = 1 \cdot b_2 = b_2.$$

其余各式显然.

- (3) 只需注意到 $(a_1 a_2 \cdots a_r)(a_r^{-1} a_{r-1}^{-1} \cdots a_1^{-1}) = 1$ 即可.
- (4) 设 b 为 a 的逆元, 则有

$$a \cdot 1 = a(ba) = (ab)a = 1 \cdot a = a.$$

- (5) 两边同乘 x^{-1} 即得.

**定理 0.3**

设 (G, \cdot) 是半群, 则 G 构成群的充分必要条件是对任意的 $a, b \in G$, 方程

$$ax = b \quad \text{与} \quad ya = b$$

在 G 中都有解. 并且当 G 为群时, 上述方程的解存在且唯一, 即对 $\forall a, b \in G$, 群中方程 $ax = b$ 与 $xa = b$ 的解都存在且唯一.



证明 必要性: 事实上, $x = a^{-1}b$ 和 $x = ba^{-1}$ 分别为两个方程的解, 由定理 0.2(5) 知解唯一.

充分性: 任取 $b \in G$, 由条件知, $yb = b$ 有解, 设为 e , 则 $eb = b$. 又对任意的 $a \in G, bx = a$ 有解, 设为 c . 于是

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

从而知 e 是 G 的左单位元.

其次, 对每个 $a \in G, ya = e$ 有解, 设为 a' . 于是

$$a'a = e,$$

从而知 a 有左逆元. 故 G 构成群.

**定义 0.3**

设 a 是群 G 的元素, 可定义 a 的非正整数次乘幂如下:

$$a^0 = 1, \quad a^{-n} = (a^{-1})^n, \quad \forall n \in \mathbb{N}.$$



定理 0.4

设 G 是一个群, 则对 $\forall m, n \in \mathbb{Z}, a, b \in G$ 有

$$a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad 1^m = 1.$$

又若 $ab = ba$, 则有 $(ab)^m = a^m b^m$.



证明

**定义 0.4**

群 G 中所含元素个数 $|G|$ 称为 G 的阶. 若 $|G|$ 有限, 则称 G 为有限群; 若 $|G|$ 无限, 则称 G 为无限群.

有限群 G 的乘法可列表给出, 此表称为 G 的群表. 设 $G = \{1, a_1, a_2, \dots, a_{n-1}\}$ 为 n 阶群, 则 G 的群表为

	1	a_1	a_2	\cdots	a_{n-1}
1	1	a_1	a_2	\cdots	a_{n-1}
a_1	a_1	a_1^2	$a_1 a_2$		$a_1 a_{n-1}$
a_2	a_2	$a_2 a_1$	a_2^2		$a_2 a_{n-1}$
\vdots	\vdots	\vdots	\vdots	\ddots	\vdots
a_{n-1}	a_{n-1}	$a_{n-1} a_1$	$a_{n-1} a_2$	\cdots	a_{n-1}^2

同样, 可定义半群与么半群的阶, 对于有限半群与么半群, 其运算也可列表给出.

**命题 0.2**

设 G 是一个群且 $|G| = n$, 若 $A \subseteq G$ 且 $|A| = n$, 则 $A = G$.



证明 证明是显然的.

**定理 0.5**

- (1) 设 G 是一个有限半群, 则 G 是群的充要条件是在 G 内左右消去律均成立, 即由 $ax = ay$ 或 $xa = ya$ 可推出 $x = y$.
- (2) 设 G 是一个具有乘法运算 (对乘法封闭) 的非空有限集合, 则 G 是一个群的充要条件是 G 满足结合律, 有左单位元, 且右消去律成立.
- (3) 一个具有乘法运算 (对乘法封闭) 的非空集合 G , 则 G 是一个群的充要条件是 G 满足结合律, 有右单位元 (即有 $e \in G$, 使对任意的 $a \in G$, 有 $ae = a$), 且 G 中每个元素有右逆元 (即对每个 $a \in G$, 有 $a' \in G$, 使 $aa' = e$).



证明

- (1) 必要性由定理 0.2(5) 立得, 下证充分性. 设 $G = \{a_1, \dots, a_n\}$, 由消去律知

$$\{a_1 a_i, \dots, a_n a_i\} = G = \{a_i a_1, \dots, a_i a_n\},$$

$\forall a_i \in G$. 故存在 $e \in G$, 使得 $a_i = ea_i$.

于是对于任一 $a_j \in G$, 有 $a_k \in G$ 使得 $a_j = a_i a_k$. 从而

$$ea_j = ea_i a_k = a_i a_k = a_j.$$

这表明 e 是左单位元, 又因为 $e \in G = Ga_j$, 故 a_j 有左逆元. 由此即知 G 是群.

- (2) 必要性由定理 0.2 立得, 下证充分性. 只需证 G 中每个元素有左逆即可. 设 $G = \{a_1, a_2, \dots, a_n\}$, 则对任意的 $a \in G$,

$$Ga = \{a_1 a, a_2 a, \dots, a_n a\} \subseteq G.$$

当 $i \neq j$ 时, 有 $a_i a \neq a_j a$. 否则, 由右消去律得 $a_i = a_j$ 矛盾! 从而 $|Ga| = |G|$, 所以 $Ga = G$. 于是, 对 G 中任一元素 a 及 G 的左单位元 e , 因 $e \in G = Ga$, 所以必存在 $a_i \in G$, 使 $a_i a = e$. 于是 a 有左逆元 a_i . 故由群的定义知 G 为群.

- (3) 必要性由定理 0.2 立得, 下证充分性. 只需证 e 是 G 的单位元, $a \in G$ 的右逆元 a' 是 a 的逆元即可. 由已知, $a' \in G$, 因此 a' 也有右逆元, 设为 a'' , 则

$$a' a'' = e.$$

于是

$$a' a = (a' a) e = (a' a)(a' a'') = a' (a a') a'' = (a' e) a'' = a' a'' = e,$$

且

$$e a = (a a') a = a (a' a) = a e = a.$$

于是 e 是 G 的单位元, a' 是 a 的逆元. 从而, 由群的定义知 G 为群. □

命题 0.3

设 G 是群.

- (1) 如果对任意的 $x \in G$, 都有 $x^2 = e$, 则 G 是一个 Abel 群.
- (2) G 是 Abel 群的充分必要条件是对任意的 $a, b \in G$, $(ab)^2 = a^2 b^2$.

证明

- (1) 对任意的 $x, y \in G$, 有

$$yx = eyx = (xy)^2 yx = xyxyyx = xyexx = xyxx = xy.$$

所以 G 是一个交换群.

- (2) 必要性: 如果 G 为交换群, 则对任意的 $a, b \in G$, 有

$$(ab)^2 = abab = aabb = a^2 b^2.$$

充分性: 如果对任意的 $a, b \in G$, 有 $(ab)^2 = a^2 b^2$, 则

$$ba = (a^{-1} a) ba (bb^{-1}) = a^{-1} (abab) b^{-1} = a^{-1} (ab)^2 b^{-1} = a^{-1} a^2 b^2 b^{-1} = ab.$$

所以 G 为交换群. □

例题 0.5 设 G 是有限群. 证明: G 中使 $x^3 = e$ 的元素 x 的个数是奇数.

证明 令 $S = \{x \in G \mid x^3 = e\}$. 由于 G 是有限群, 所以 S 为有限集. 又因为 $e^3 = e$, 所以 $e \in S$, 从而 S 不是空集. 如果另有 $x \neq e$, 使 $x^3 = e$, 则 $(x^{-1})^3 = e$. 因为 $x \neq e$, 所以 $x \neq x^{-1}$. 这说明 S 中的非单位元 (如果有的话) 总是成对出现, 又因为 $e^{-1} = e$, 所以 G 中使 $x^3 = e$ 的元素 x 的个数是奇数. □

例题 0.6 在偶数阶群 G 中, 方程 $x^2 = 1$ 总有偶数个解.

证明 注意到若 $g^2 \neq 1$, 则 $(g^{-1})^2 \neq 1$ 且 $g \neq g^{-1}$. 因此 G 中满足 $x^2 \neq 1$ 的元 x 是成对出现的. 从而 G 中满足 $x^2 \neq 1$ 的元 x 有偶数个. 因此在偶数阶群 G 中, 方程 $x^2 = 1$ 总有偶数个解. □


例题 0.7 令 G 是 n 阶有限群, a_1, a_2, \dots, a_n 是群 G 的任意 n 个元, 不一定两两不同. 试证存在整数 p 和 q , $1 \leq p \leq q \leq n$, 使得 $a_p a_{p+1} \cdots a_q = 1$.

证明 令 $S = \{a_1, a_1 a_2, \dots, a_1 a_2 \cdots a_n\}$. 若 $1 \in S$, 则结论已得证. 若 $1 \notin S$, 因 $|G| = n$, 故 S 中至少有两个元是相等的. 设 $a_1 \cdots a_i = a_1 \cdots a_i a_{i+1} \cdots a_j$, 则

$$a_{i+1} \cdots a_j = 1.$$

□

例题 0.8 设 a, b 是群 G 的两个元, 满足 $aba = ba^2b, a^3 = 1, b^{2n-1} = 1$. 试证 $b = 1$.

 **笔记** 注意到 $b = 1$ 等价于 a, b 可交换, 故只需证明 a, b 可交换. 再利用条件和数学归纳法证明即可.

证明 由题设条件得

$$ab^2a = aba^3ba = (aba)a^2ba = (ba^2b)a^2ba = ba^2(ba^2b)a = ba^2(aba)a = b^2a^2.$$

故 $ab^2 = b^2a$. 设 $ab^{2^r} = b^{2^r}a$, 则 $ab^{2^{r+1}} = ab^{2^r}b^2 = b^{2^r}ab^2 = b^{2^r}b^2a = b^{2^{r+1}}a$. 因此对任一正整数 k 有 $ab^{2^k} = b^{2^k}a$. 特别地, 取 $k = n$ 得到 $ab^{2^n} = b^{2^n}a$. 因为 $b^{2n-1} = 1$, 所以 $b^{2^n} = b$, 从而 $ab = ba$. 于是 $ba^2 = aba = ba^2b$. 故 $b = 1$.

□

例题 0.9 设群 G 的元 a_1, a_2, b_1, b_2 满足

$$a_1b_1 = a_2b_2 = b_1a_1 = b_2a_2, \quad a_1^m = a_2^m = b_1^n = b_2^n = 1,$$

其中 m 和 n 是互素的正整数. 则 $a_1 = a_2, b_1 = b_2$.

证明 设 k, l 是整数使得 $km + ln = 1$. 由 $a_1b_1 = a_2b_2$ 知

$$(a_1b_1)^{km} = (a_2b_2)^{km}.$$

因 $a_1b_1 = b_1a_1, a_2b_2 = b_2a_2, a_1^m = 1 = a_2^m$, 故

$$(a_1b_1)^{km} = a_1^{km}b_1^{km} = b_1^{km}, \quad (a_2b_2)^{km} = a_2^{km}b_2^{km} = b_2^{km}.$$

从而有 $b_1^{km} = b_2^{km}$. 而 $b_1^{ln} = b_2^{ln} = 1$, 故 $b_1 = b_1^{km+ln} = b_2^{km+ln} = b_2$. 同理可证 $a_1 = a_2$.

□