0.1 幺半群和群

定义 0.1 ((幺) 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

$$1a = a1 = a, \quad \forall a \in M, \tag{1}$$

则称 M 为幺半群, 1 称为**幺元素**或**幺元**或**单位元**.

如果一个幺半群 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**交换幺半群** (或**交换半群**), 也简单地称 M(或 S) 为**可换的**.

对于交换幺半群, 有时把二元运算记为加法, 此时幺元素记为 0, 改称**零元素**或**零**.

♣

例题 0.1

(1) $\mathbb{N}$ 对乘法是幺半群, 对加法是半群而不是幺半群. 非负整数集对加法与乘法均为幺半群.

(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, $M(X)$ 是一个幺半群, id_X 是一个幺元素. 当 $|X| \geqslant 2$ 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 $\varnothing$ 也是 X 的一个子集, 则 $P(X)$ 对集合的并的运算是一个幺半群, $\varnothing$ 为幺元素. 同样, $P(X)$ 对集合的交的运算是一个幺半群, X 为幺元素, 这两种幺半群都是可换的.

命题 0.1

幺半群中的幺元素是唯一的.

♠

证明 如果 1 与 $1'$ 都是幺半群 M 的幺元素, 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 $(ab)c = a(bc)(\forall a, b, c \in G)$;

(2) 存在**左幺元**, 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. 这时左幺元改称**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, 左幺元为 0, a 的左逆元为 $-a$. $\mathbb{P}$ 对乘法是幺半群, 不是群. 但是 $\mathbb{P}$ 中非零元素的集合 $\mathbb{P}^*$ 对乘法是群, 1 为左幺元, $1/a$ 为 a 的左逆元.

定理 0.1

设 m 是大于 1 的正整数, 记

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

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

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

♡

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

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

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

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

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

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

所以结合律成立.

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

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

所以 $\overline{1}$ 为 $U(m)$ 的单位元.

对任意的 $\overline{a} \in U(m)$, 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 $\overline{u} \in U(m)$, 且

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

所以 $\overline{u}$ 为 $\overline{a}$ 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 $a_1, a_2, \cdots, a_r \in G$, 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

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

(6) 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

(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 $(a_1a_2\cdots a_r)(a_r^{-1}a_{r-1}^{-1}\cdots a_1^{-1}) = 1$ 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.

(6) 事实上, $x = a^{-1}b$ 和 $x = ba^{-1}$ 分别为两个方程的解, 由性质 (5)知解唯一.

□

定理 0.3

设 G 是一个具有乘法运算 (对乘法封闭) 且满足结合律的非空集合, 则 G 构成群的充分必要条件是对任意的 $a, b \in G$, 方程

$$ax = b \quad 与 \quad ya = b$$

在 G 中都有解. 并且当 G 为群时, 上述方程的解存在且唯一. ♡

证明 **必要性**: 由定理 0.2(6)立得.

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.

□

命题 0.2

设 G 是群.

(1) 如果对任意的 $x \in G$, 都有 $x^2 = e$, 则 G 是一个交换群.

(2) G 是交换群的充分必要条件是对任意的 $a, b \in G$, $(ab)^2 = a^2b^2$. ♠

证明

(1) 对任意的 $x, y \in G$, 有

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

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

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

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

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

所以 G 为交换群.

□

例题 0.2 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.

□

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 $G = \{1, a_1, a_2, \cdots, a_{n-1}\}$ 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_1a_2		a_1a_{n-1}
a_2	a_2	a_2a_1	a_2^2		a_2a_{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, 可定义半群与幺半群的阶, 对于有限半群与幺半群, 其运算也可列表给出.

♣

命题 0.3

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

♠

命题 0.4

(1) 设 G 是一个具有乘法运算 (对乘法封闭) 的非空有限集合. 如果 G 满足结合律, 有左单位元, 且右消去律成立, 则 G 是一个群.

(2) 一个具有乘法运算 (对乘法封闭) 的非空集合 G, 如果满足结合律, 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 $aa' = e$), 则 G 构成群.

♠

证明

(1) 只需证 G 中每个元素有左逆即可. 设 $G = \{a_1, a_2, \cdots, a_n\}$, 则对任意的 $a \in G$,

$$Ga = \{a_1a, a_2a, \cdots, a_na\} \subseteq G.$$

当 $i \neq j$ 时, 有 $a_ia \neq a_ja$. 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 $a_ia = e$. 于是 a 有左逆元 a_i. 故由群的定义知 G 为群.

(2) 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

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

且

$$ea = (aa')a = a(a'a) = ae = a.$$

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.

□

定义 0.5

设 a 是群 G 的元素. 若 $\forall k \in \mathbb{N}, a^k \neq 1$, 则称 a 的**阶为无穷**, 记作 $\operatorname{ord} a = \infty$. 若 $\exists k \in \mathbb{N}$, 使得 $a^k = 1$, 则 $r = \min\{k | k \in \mathbb{N}, a^k = 1\}$ 称为 a 的**阶**, 记作 $\operatorname{ord} a = r$.

♣

定理 0.5 (群的阶的基本性质)

设 $(G, \cdot)$ 是一个群,$a \in G$, 则

(1) a 的阶为无穷当且仅当 $\forall m, n \in \mathbb{Z}$ 且 $m \neq n$ 时, $a^m \neq a^n$.

(2) 设 a 的阶为 d, 则

$$a^m = a^n \iff m \equiv n \pmod{d}. \tag{2}$$

特别地, 如果有 $m \in \mathbb{Z}$, 使 $a^m = 1$, 则 $d \mid m$.

(3) a 与 a^{-1} 阶相同.

♡

证明

(1) 事实上, 若 a 的阶为无穷, 而有 $m \neq n$, 使 $a^m = a^n$. 设 $m > n$, 于是 $a^m(a^n)^{-1} = 1$, 而 $a^m(a^n)^{-1} = a^{m-n} = 1$, 自然 $m - n \in \mathbb{N}$. 矛盾.

反之, $\forall m, n \in \mathbb{Z}$ 且 $m \neq n$, 有 $a^m \neq a^n$, 则 $a^{m-n} = a^m(a^n)^{-1} = 1$, 即 $\forall k \in \mathbb{N}$ 有 $a^k \neq 1$, 故 a 的阶为无穷.

(2) 设 a 的阶为 d, $m, n \in \mathbb{N}$, 由带余除法知, 一定能找到整数 t_1, t_2, r_1, r_2, 使 $m = dt_1 + r_1 (0 \leqslant r_1 < d)$, $n = dt_2 + r_2 (0 \leqslant r_2 < d)$. 于是 $a^m = (a^d)^{t_1}a^{r_1} = a^{r_1}$, $a^n = (a^d)^{t_2}a^{r_2} = a^{r_2}$, 因而

$$a^m = a^n \iff a^{r_1} = a^{r_2} \iff a^{r_1 - r_2} = a^{r_2 - r_1} = 1.$$

又 $|r_1 - r_2| < d$, 故上式也等价于 $r_1 - r_2 = 0$, 即式 (2) 成立.

(3) 由 $(a^n)^{-1} = (a^{-1})^n$ 知 $a^k = 1$ 当且仅当 $(a^{-1})^k = 1$, 故 a^{-1} 与 a 同阶.

□