0.1 幺半群　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**.

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. **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 $|X| \geq 2$ 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 $\varnothing$ 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**.

♣

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

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 $-a$.

定义 0.3 (全变换群/置换群)

设 X 是非空集合. 以 S_X 表示 X 的所有可逆变换 (即 X 到 X 的一一对应) 的集合, 则 S_X 对变换的乘法构成一个群, id_X 为左幺元, f^{-1} 为 f 的左逆元. S_X 称 X 的**全变换群**.

如果集合 X 所含元素的个数 $|X| = n < +\infty$. 此时 S_X 记为 S_n, 称为 n 个文字的**对称群**或 n 个文字的**置换群**, 其元素称为**置换**.

♣

注 S_X 的子群称为 X 上的**变换群**.

例题 0.2 假定集合 $X = \{1, 2, \cdots, n\}$, 记 S_n 为 X 的对称群, 设 $\sigma \in S_n$, 则 $\sigma(1), \sigma(2), \cdots, \sigma(n)$ 是 $1, 2, \cdots, n$ 的一个

排列. 常用下面记法:

$$\sigma = \begin{pmatrix} 1 & 2 & & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

更一般地, 若 $i_1, i_2, \cdots, i_n$ 是 $1, 2, \cdots, n$ 的一个排列, 则可记

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$$

易知 S_n 中有 $n!$ 个元素, S_n 中一个元素可以有 $n!$ 种表示法.

例如, $\sigma \in S_3$, 满足 $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$, 则可记

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \cdots$$

定理 0.1 (群的基本性质)

设 $(G, \cdot)$ 是一个群,$a \in G$,1 是 G 的左幺元, 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. 1 也是 G 的**右幺元**, 即 $a \cdot 1 = a\ (\forall a \in G)$, 故 1 为 G 的**幺元**. 故 G 为幺半群, 幺元唯一.
3. 任一元素 a 的逆元唯一, 记为 a^{-1}, 并且 $1^{-1} = 1, (a^{-1})^{-1} = a, (ab)^{-1} = b^{-1}a^{-1}, (a^n)^{-1} = (a^{-1})^n$.
4. 群运算满足**消去律**, 即
$$ax = bx\ (\text{或} xa = xb),\ \text{则} a = b,\ \forall a, b, x \in G.$$
5. 若 $a, b \in G$, 则群中方程 $ax = b$(或 $xa = b$) 的解存在且唯一.

♡

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 为 a 的逆元, 则有
$$a \cdot 1 = a(ba) = (ab)a = 1 \cdot a = a.$$
3. 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.
4. 两边同乘 x^{-1} 即得.
5. 事实上, $x = a^{-1}b$(或 $x = ba^{-1}$) 为解, 由性质 4 知解唯一.

□

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**.

♣

注 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.

定义 0.5

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

♣

定义 0.6

设 a 是群 G 的元素, 可定义 a 的**非正整数次乘幂**如下:

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

♣

定理 0.2

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

□

定理 0.3 (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

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

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 $m - n \in \mathbf{N}$. 矛盾.

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

□