

# 近世代数教程

root

March 17, 2015



# 目录

## 0.1 半群和幺半群

### 0.1.1 预备知识

在近世代数中,集合论与图论中的术语被广泛的使用。所以我们先来回顾一下集合论中的一些基本概念,那就是集合与映射。

#### 数学归纳法

数学归纳法在近世代数中被广泛的使用。我们在这里给出数学归纳法的证明。在前面的课程中,我们只是利用数学归纳法给出证明。但是数学归纳法的正确性并没有被谈及。在这里我们给出数学归纳法的正确性证明。首先给出良序原理,又称为最小数原理。英文是 well ordering principle

最小数原理:

**定理 0.1.1** 对于自然数集合  $Z^+$  的每一个非空子集都有一个最小元素。

第一数学归纳法:

**定理 0.1.2** 设  $P(n)$  是关于正整数  $n$  的一个命题,如果下面的两个事实成立:

- (1)  $P(1)$  是真的;
  - (2) 对于每一个正整数  $k$ ,如果  $P(k)$  是真的,那么  $P(k+1)$  也是真的。
- 那么在上述条件下,就能得出结论:对于所有的正整数  $n$ ,  $P(n)$  都是真的。

**证明:** 1 令集合  $Z_1 = \{n | n \in \mathbb{Z}^+, P(n) \text{不真}\}$ , 如果  $Z_1 = \phi$ , 那么结论成立。因为此时不存在正整数  $n_0$ , 使得  $P(n_0)$  不真。

如果  $Z_1 \neq \phi$ , 那么由于  $Z_1 \subseteq \mathbb{Z}^+$ , 由最小数原理知  $Z_1$  中必有一个最小数, 设这个最小数是  $m$ 。由于  $P(1)$  为真, 所以  $m \neq 1$ , 这样有  $m > 1$ 。由于它是  $Z_1$  中最小的元素, 所以有  $P(m)$  不真, 但  $P(m-1)$  为真。由  $m > 1$ , 所以  $m-1 > 0$ ,  $m-1$  是自然数集合  $\mathbb{Z}^+$  中的一元。由归纳法的第二个条件知  $P(m)$  为真。所以  $m$  应该不在  $Z_1$  中。这与  $m$  是在  $Z_1$  中的最小元素相矛盾。

第二数学归纳法:

**定理 0.1.3** 设  $P(n)$  是关于正整数  $n$  的一个命题, 如果下面的两个事实成立:

(1)  $P(1)$  是真的;

(2) 对于每一个正整数  $m$ , 如果对于所有正整数  $k < m$ ,  $P(k)$  是真的, 那么  $P(m)$  也是真的。

在这种情况下, 我们就能够得出结论: 对于所有的正整数  $n$ ,  $P(n)$  都是真的。

### 例子

the Fibonacci sequence  $(f_1, f_2, f_3, \dots)$  is defined as follows:

$[f_1 = f_2 = 1, f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 3]$

Prove that  $(f_{5k})$  is divisible by 5 for every  $(k \geq 1)$ , that is, 5 divides every 5th member of

**证明:** 2 这个数列的前几项为 1, 1, 2, 3, 5, 8, 13, 21,  $\dots$ , 可以看出  $f_5 = 5$ , 所以  $5 | f_5$ . 这说明当  $k = 1$  时结论成立。

假定当  $k = m$  时结论成立, 也就是说  $5 | f_{5m}$ , 于是

$$\begin{aligned} f_{5(m+1)} &= f_{5m+5} = f_{5m+4} + f_{5m+3} \\ &= 2f_{5m+3} + f_{5m+2} \\ &= 3f_{5m+2} + 2f_{5m+1} \\ &= 5f_{5m+1} + 3f_{5m} \end{aligned} \tag{1}$$

从而 5 整除上式的右端, 得到  $5 | f_{5(m+1)}$ , 也就是当  $k = m+1$  时结论也成立。由数学归纳法知对任意的正整数  $k$ , 都有  $5 | f_{5k}$ 。

归纳法在使用的时候应该注意各个步骤的衔接,不能大意,否则就会出问题。下面的例子称为是瞒天过海。让你证明所有的马都具有相同的颜色。

设 $(P(n))$ 是如下的命题:“对于每个由 $(n)$ 匹马组成的集合来说,集合中所有的马都具有同样的颜色”。我们用归纳法证明对所有的 $(n)$ , $(P(n))$ 成立。

**证明:** 3 显然  $P(1)$  是真的。假设  $P(m)$  是真的,我们来证明  $P(m+1)$  也是真的。设  $S$  是  $m+1$  匹马组成的集合,  $S = \{h_1, h_2, \dots, h_{m+1}\}$ , 因为  $h_1, h_2, \dots, h_m$  是  $m$  匹马,由于  $P(m)$  成立,所以  $h_1, h_2, \dots, h_m$  具有同样的颜色,同理  $h_2, h_3, \dots, h_{m+1}$  是  $m$  匹马,所以  $h_2, h_3, \dots, h_{m+1}$  也具有同样的颜色。将这两个论断结合在一起,就有所有的  $m+1$  匹马都具有同样的颜色(比如,它们都有  $h_2$  的颜色)。

在上述的证明过程中,对于任意的  $k > 1$ ,如果  $P(k)$  为真,可以推得  $P(k+1)$  也为真。如果能够正确使用第一数学归纳法,当  $k = 1$ ,也可以做同样地推理才可以。但此时不能从  $P(1)$  为真,推出  $P(2)$  也为真。这说明第一数学归纳法的第二个条件是不成立的。

### 0.1.2 若干基本概念

#### 代数运算

下面给出二元代数运算的定义:

**定义 0.1.1** 设  $X$  是一个集合,一个从  $X \times X$  到  $X$  的一个映射  $\varphi$  称为  $X$  上的一个二元代数运算。

设 $(X = \{a, b\})$ , $(\phi)$ 是 $(X)$ 上的一个二元代数运算,于是它是一个从 $(X^2)$ 到 $(X)$ 的映射。不妨设 $(\phi(a, a) = a, \phi(a, b) = b, \phi(b, a) = b, \phi(b, b) = a)$ 。

可以用下面的表来表示这样一个映射:

$(\phi)$	a	b
a	a	b
b	b	a

$|b \quad |b|a|$

该表被称之为Cayley乘法表。

二元函数  $\phi(x, y)$  有三种表示方法,  $\phi(x, y), x\phi y, (x, y)\phi$ 。

$\phi(x, y)$  称为前缀表示,  $x\phi y$  称为中缀表示,  $(x, y)\phi$  称为后缀表示。

二元代数运算往往用中缀表示  $x\phi y$ , 并且  $\phi$  往往用符号“ $\circ$ ”或“ $*$ ”表示, 读作乘法。

**定义 0.1.2** 一个从集合  $X$  到集合  $Y$  的映射称为  $X$  到  $Y$  的一个一元代数运算。当  $X = Y$  时, 称此一元代数运算为  $X$  上的一元代数运算。

$X$  上的一元二元代数运算对于运算是封闭的。

### 运算律

**定义 0.1.3** 设“ $\circ$ ”是  $X$  上的二元代数运算, 如果对于  $\forall a, b, c \in X$ , 恒有

$$(a \circ b) \circ c = a \circ (b \circ c) \quad (2)$$

则称二元代数运算“ $\circ$ ”满足结合律。如果对于  $\forall a, b \in X$ , 恒有

$$a \circ b = b \circ a \quad (3)$$

则称二元代数运算“ $\circ$ ”满足交换律。

**定义 0.1.4** 设“ $\circ$ ”是非空集合  $S$  上的一个二元代数运算, 则称二元组  $(S, \circ)$  为一个(有一个代数运算的)代数系。

类似的可以定义具有多个代数运算的代数系, 代数系也称为代数结构。

**定理 0.1.4** 设  $(S, \circ)$  为一个代数系。如果二元代数运算“ $\circ$ ”满足结合律, 则  $\forall a_i \in S, i = 1, 2, \dots, n, a_1, a_2, \dots, a_n$  的乘积仅与这  $n$  个元素及其次序有关而唯一确定。

**证明:** 4 用第二数学归纳法进行证明。当  $n = 3$  时结论成立。因为对  $\forall a_1, a_2, a_3 \in S$ , 按照结合律的定义有  $(a_1 \circ a_2) \circ a_3 = a_1 \circ (a_2 \circ a_3)$ 。

假设  $k < m$  时, 结论成立。当  $n = m$  时, 我们可以证明  $m$  个元素的任何一种相乘的方式都和  $(\cdots((a_1 \circ a_2) \circ a_3) \circ \cdots \circ a_{m-1}) \circ a_m$  相等。

任意给定一种相乘的方式, 由于  $a_1, a_2, a_3, \cdots, a_m$  的顺序已经排定, 而代数运算“ $\circ$ ”是一个二元代数运算, 所以这  $m$  个元素的乘积最终一定化归为  $S$  中的两个元素相乘而得到最终结果。从而一定有一个正整数  $k$ , 使得这两个元素分别是前面的  $k$  个元素相乘的结果和后面  $n - k$  个元素相乘的结果。由于这两部分中的元素个数  $< m$ , 所以由归纳假设, 这两部分乘积只与这些元素及其顺序有关。这个乘积可以写成  $(a_1 \circ a_2 \circ \cdots \circ a_k) \circ (a_{k+1} \circ a_{k+2} \circ \cdots \circ a_m)$ 。

如果  $k = m - 1$ , 那么上式的第一项中的元素个数  $< m$ , 由归纳假设知  $a_1 \circ a_2 \circ \cdots \circ a_{m-1} = (\cdots((a_1 \circ a_2) \circ a_3) \circ \cdots \circ a_{m-2}) \circ a_{m-1}$ 。从而

$$\begin{aligned} (a_1 \circ a_2 \circ \cdots \circ a_k) \circ (a_{k+1} \circ a_{k+2} \circ \cdots \circ a_m) &= (a_1 \circ a_2 \circ \cdots \circ a_{m-1}) \circ a_m \\ &= ((\cdots((a_1 \circ a_2) \circ a_3) \circ \cdots \circ a_{m-2}) \circ a_{m-1}) \circ a_m \end{aligned} \quad (4)$$

如果  $k < m - 1$ , 那么

$$\begin{aligned} (a_1 \circ a_2 \circ \cdots \circ a_k) \circ (a_{k+1} \circ a_{k+2} \circ \cdots \circ a_m) &= (a_1 \circ a_2 \circ \cdots \circ a_k) \circ ((a_{k+1} \circ a_{k+2} \circ \cdots \circ a_{m-1}) \circ a_m) \\ &= ((a_1 \circ a_2 \circ \cdots \circ a_k) \circ (a_{k+1} \circ a_{k+2} \circ \cdots \circ a_{m-1})) \circ a_m \end{aligned} \quad (5)$$

上式右端的前一项中有  $m - 1$  个元素, 再由归纳假设知上式的最后乘积的结果为  $(a_1 \circ a_2 \circ \cdots \circ a_k) \circ (a_{k+1} \circ a_{k+2} \circ \cdots \circ a_m) = (a_1 \circ a_2 \circ \cdots \circ a_{m-1}) \circ a_m = (\cdots((a_1 \circ a_2) \circ a_3) \circ \cdots \circ a_{m-1}) \circ a_m$ 。

**定理 0.1.5** 设  $(S, \circ)$  为一个代数系。如果二元代数运算“ $\circ$ ”满足结合律和交换律, 则  $\forall a_i \in S, i = 1, 2, \cdots, n, a_1, a_2, \cdots, a_n$  的乘积仅与这  $n$  个元素有关而与它们的次序无关。

**定义 0.1.5** 设  $(S, \circ, +)$  是具有两个代数运算“ $\circ$ ”和“ $+$ ”的代数系。如果对于  $\forall a, b, c \in S$ , 恒有

$$a \circ (b + c) = a \circ b + a \circ c$$

则称“ $\circ$ ”对“ $+$ ”满足左分配律。如果对于  $\forall a, b, c \in S$ , 总有

$$(b + c) \circ a = b \circ a + c \circ a$$

则称“ $\circ$ ”对“ $+$ ”满足右分配律。

**定理 0.1.6**  $(S, \circ, +)$  是具有两个代数运算“ $\circ$ ”和“ $+$ ”的代数系。如果“ $+$ ”满足结合律, “ $\circ$ ”对“ $+$ ”满足左(右)分配律, 则  $\forall a, a_i \in S, i = 1, 2, \dots, n$ , 我们有

$$a \circ (a_1 + a_2 + \dots + a_n) = (a \circ a_1) + (a \circ a_2) + \dots + (a \circ a_n)$$

$$((a_1 + a_2 + \dots + a_n) \circ a = (a_1 \circ a) + (a_2 \circ a) + \dots + (a_n \circ a))$$

### 幺元和零元

**定义 0.1.6** 设  $(S, \circ)$  是一个代数系, 如果存在一个元素  $a_l \in S$ , 使得  $\forall a \in S$  都有

$$a_l \circ a = a$$

则称  $a_l$  为乘法“ $\circ$ ”的左单位元素(左幺元)。如果存在一个元素  $a_r \in S$ , 使得  $\forall a \in S$  都有

$$a \circ a_r = a$$

则称  $a_r$  为乘法“ $\circ$ ”的右单位元素(右幺元)。如果存在一个元素  $e \in S$ , 使得  $\forall a \in S$  都有

$$e \circ a = a \circ e = a$$

则称  $e$  为乘法“ $\circ$ ”的单位元素(幺元)。

**定理 0.1.7**  $(S, \circ)$  是一个代数系。如果二元代数运算“ $\circ$ ”既有左单位元素  $a_l$ , 又有右单位元素  $a_r$ , 则  $a_l = a_r$ , 从而有单位元素。

**定义 0.1.7** 设  $(S, \circ)$  是一个代数系, 如果存在一个元素  $z \in S$ , 使得  $\forall a \in S$  都有



$$z \circ a = a \circ z = z$$

则称  $z$  为乘法“ $\circ$ ”的零元素。

设  $(S, \circ)$  是一个具有二元代数运算“ $\circ$ ”的代数系。  $A, B \subseteq S$ , 则定义

$$A \circ B = \{a \circ b | a \in A, b \in B\}$$

我们也常把  $A \circ B$  写成  $AB$ , 把  $a \circ b$  写成  $ab$ 。

当  $A = \{a\}$  时,  $AB = \{a\}B$ , 简记为  $aB$ 。于是

$$aB = \{a \circ b | b \in B\}$$

$$Ba = \{b \circ a | b \in B\}$$

### 0.1.3 半群与么半群的概念

#### 半群

**定义 0.1.8** 设  $(S, \circ)$  是一个代数系, 如果“ $\circ$ ”满足结合律, 那么就称  $S$  对于乘法“ $\circ$ ”构成一个半群 (Semigroup), 记为  $(S, \circ)$ 。

交换半群或者可换半群, 有限半群, 无限半群。

半群的例子 \pozhehao 模  $n$  剩余类

设  $(Z_n = \{[0], [1], \dots, [n-1]\})$  是整数集合  $(Z)$  上在模  $(n)$  的同余关系之下的等价类之集合。其中

$$[i] = \{m | m \in Z, m \equiv i \pmod{n}\}$$

在  $(Z_n)$  上定义加法“ $(+)$ ”如下:  $(\forall [i], [j] \in Z_n)$ ,

[

$$[i] + [j] = [i + j]$$

$\setminus$

证明加法“ $(+)$ ”是 $(\mathbb{Z}_n, +)$ 上的一个二元代数运算。 $(\mathbb{Z}_n, +)$ 是一个半群。

集合上的二元关系关系的合成

**定义 0.1.9** 集合  $A$  上的一个二元关系  $\rho$  是笛卡尔乘积  $A \times A$  的一个子集。

令  $\mathcal{R}(A)$  表示  $A$  上的所有二元关系构成的集合。在集合  $\mathcal{R}(A)$  上定义二元代数运算“ $\circ$ ”如下：

$$\rho \circ \sigma = \{(x, y) | (x, y) \in A \times A, \text{ 存在 } z \in A, \text{ 使得 } (x, z) \in \rho \text{ 并且 } (z, y) \in \sigma\}$$

那么代数系  $(\mathcal{R}(A), \circ)$  形成一个半群。

全体偶数的集合 $(E)$ 对于通常的乘法构成一个可换半群 $(E, \cdot)$ ,它没有单位元。

设 $S$ 是一切形如

$$\begin{array}{cc} \left( \begin{array}{cc} a & b \\ 0 & 0 \end{array} \right), \\ a, b \in \mathbb{N} \end{array}$$

的 $(2 \times 2)$ 矩阵的集合。容易验证 $(S)$ 对矩阵的乘法 $(\circ)$ 构成一个不可交换半群,并且

$$\begin{array}{cc} \left( \begin{array}{cc} 1 & d \\ 0 & 0 \end{array} \right) \\ d \in \mathbb{N} \end{array}$$

是左单位元素。从而 $(S, \circ)$ 有无限多个左单位元素。

### 幺半群

**定理 0.1.8** 如果半群  $(S, \circ)$  中既有左单位元素又有右单位元素, 则左单位元素和右单位元素相等, 从而有单位元素且单位元素唯一

**定义 0.1.10** 有单位元素  $e$  的半群  $(S, \circ)$  称为独异点或者称为幺半群。记为  $(S, \circ, e)$ 。如果  $S$  是一个有限集合, 则称  $(S, \circ, e)$  为有限幺半群,  $S$  的基数称为幺半群  $(S, \circ, e)$  的阶。

设  $(S, \circ)$  是一个非空集合, 则  $(2^S, \cup, \cap)$  和  $(2^S, \cap, \cup)$  都是幺半群。

设  $(S, \circ)$  是一个非空集合,  $M(S) = \{f: S \rightarrow S\}$ , 则  $(M(S), \circ)$  对映射的合成构成了一个以  $(I_S, \circ)$  为单位的幺半群。它是不可交换的幺半群。

### 有限半群成为幺半群的条件

**定理 0.1.9** 有限半群  $(S, \circ)$  是一个幺半群当且仅当  $\exists s, t \in S$  使得

$$sS = S, St = S$$

**证明:**  $\Rightarrow$  显然。

$\Leftarrow$  设  $(S, \circ)$  是一个半群且  $\exists s, t \in S$  使得  $sS = S, St = S$ 。令  $\varphi: S \rightarrow sS, \forall x \in S, \varphi(x) = s \circ x$ 。于是  $\varphi$  是满射。而由  $sS = S$  并且  $|S| < +\infty$ , 从而  $\varphi$  又是单射。从而  $\varphi$  是双射。由数学归纳法可以证明  $\forall x \in S, \varphi^n(x) = s^n x$ 。

任取  $x \in S$ , 序列  $x, \phi(x), \phi^2(x), \dots, \phi^n(x)$  中必有两项相同, 设  $\phi^p(x) = \phi^q(x)$ , 其中  $p < q$ ,  $\phi$  有逆映射  $\phi^{-1}$ , 故  $\phi^{q-p}(x) = x$ 。从而对任取的  $x$ , 有非负整数  $n_x$ , 使得  $\phi^{n_x}(x) = x$ 。令  $k = \text{lcm}\{n_x | x \in S\}$ , 于是  $\phi^k(x) = \phi^{m_x n_x}(x) = \underbrace{(\phi^{n_x} \phi^{n_x} \dots \phi^{n_x})}_{m_x}(x) = \underbrace{(\phi^{n_x} \phi^{n_x} \dots \phi^{n_x})}_{m_x-1}(\phi^{n_x}(x)) = \dots = \phi^{n_x}(x) = x$ , 从而对  $\forall x \in S$ , 有  $s^k \circ x = \phi^k(x) = x, s^k$  为一个左幺元。

proof of semigroups with unity

proof of semigroups with unity111

### 另外一个证明方法

先看下面的例子, 设集合  $S = \{a, b, c\}$ , 为一个有限半群, 乘法由如下给定的

部分 Cayley 乘法表确定:

	$\circ$	$a$	$b$	$c$
$a$				
$b$				
$c$		$b$	$c$	$a$

由此乘法表可知  $c \circ (a, b, c) = (b, c, a)$ 。所以有  $c^2 \circ (a, b, c) = c \circ [c \circ (a, b, c)] = c \circ (b, c, a) = (c, a, b)$ 。这里面  $c \circ c = a$ , 由此可以得到  $a \circ (a, b, c) = (c, a, b)$ , 这就确定了上面乘法表中对应元素  $a$  的行。

继续下去, 我们有  $c^3 \circ (a, b, c) = c \circ [c^2 \circ (a, b, c)] = c \circ (c, a, b) = (a, b, c)$ 。而  $c^3 = c^2 \circ c = a \circ c = b$ , 上式变成  $b \circ (a, b, c) = (a, b, c)$ , 这就确定了上面乘法表中对应元素  $b$  的行。cayley 乘法表变成了

	$\circ$	$a$	$b$	$c$
$a$		$c$	$a$	$b$
$b$		$a$	$b$	$c$
$c$		$b$	$c$	$a$

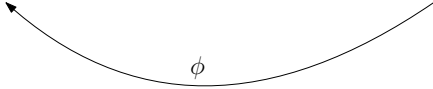
由此可以得到半群  $S$  的一个左么元  $b$ 。

仿照这个例子, 给出上面定理的一个证明。

设  $(s_1, s_2, \dots, s_n)$  是  $S$  中所有不同元素构成的一个向量。由于  $sS = S$ , 所以  $(ss_1, ss_2, \dots, ss_n)$  也是  $S$  中所有不同元素构成的一个向量。设  $K$  是  $S$  中所有不同元素构成向量的集合, 即  $K = \{(s_1, s_2, \dots, s_n) | s_i \in S, s_k \neq s_j (if \ k \neq j)\}$ 。做映射  $\phi: K \rightarrow K$ , 使得  $\phi(s_1, s_2, \dots, s_n) = (ss_1, ss_2, \dots, ss_n)$ 。可以证明  $\phi$  为单射。即如果  $(s_1, s_2, \dots, s_n) \neq (t_1, t_2, \dots, t_n)$ , 那么必有  $(ss_1, ss_2, \dots, ss_n) \neq (st_1, st_2, \dots, st_n)$ 。否则  $ss_i = st_i (i = 1, 2, \dots, n)$ 。不妨设  $s_1 \neq t_1$ , 但  $ss_1 = st_1$ 。于是  $sS = s(\{s_1, t_1\} \cup S \setminus \{s_1, t_1\}) = s\{s_1, t_1\} \cup s(S \setminus \{s_1, t_1\})$ , 从而  $|sS| = |s\{s_1, t_1\} \cup s(S \setminus \{s_1, t_1\})| \leq |s\{s_1, t_1\}| + |s(S \setminus \{s_1, t_1\})| \leq 1 + n - 2 = n - 1$ , 与  $sS = S$  相矛盾。做序列  $(s_1, s_2, \dots, s_n), \phi(s_1, s_2, \dots, s_n), \phi^2(s_1, s_2, \dots, s_n), \dots$ , 这些序列都在  $K$  中。但  $K$  中只有有限个元素, 所以必有一个  $k$ , 使得  $(s_1, s_2, \dots, s_n), \phi(s_1, s_2, \dots, s_n), \phi^2(s_1, s_2, \dots, s_n), \dots, \phi^k(s_1, s_2, \dots, s_n)$  互不相同, 但  $\phi^{k+1}(s_1, s_2, \dots, s_n)$  与前面的某一项相同。可以证明

$\phi^{k+1}(s_1, s_2, \dots, s_n) = (s_1, s_2, \dots, s_n)$ 。否则如下图所示,  $\phi^{k+1}(s_1, s_2, \dots, s_n) = \phi(s_1, s_2, \dots, s_n)$ , 那么  $\phi(s_1, s_2, \dots, s_n)$  就会有两个不同的原像  $(s_1, s_2, \dots, s_n)$  和  $\phi^k(s_1, s_2, \dots, s_n)$ 。

$$(s_1, s_2, \dots, s_n) \xrightarrow{\phi} (ss_1, ss_2, \dots, ss_n) \xrightarrow{\phi} (s^2s_1, s^2s_2, \dots, s^2s_n) \xrightarrow{\phi} \dots \xrightarrow{\phi} (s_1^k, s_2^k, \dots, s_n^k)$$



这与  $\phi$  是单射相矛盾。从而  $\phi^{k+1}(s_1, s_2, \dots, s_n) = (s_1, s_2, \dots, s_n)$ 。也就是  $s^{k+1}s_i = s_i (i = 1, 2, \dots, n)$ , 所以  $s^{k+1}$  为  $S$  的一个左么元。

### 元素的幂

在么半群  $(S, \circ, e)$  中可以定义元素的非负整数次幂。对于  $\forall a \in S, a^0 = e, a^{n+1} = a^n \circ a (n \geq 0)$ 。

在半群  $(S, \circ)$  中可以定义元素的正整数次幂。对于  $\forall a \in S, a^1 = a, a^{n+1} = a^n \circ a (n \geq 1)$ 。

**定理 0.1.10** 设  $(S, \circ, e)$  是一个么半群,  $m, n$  是任意的非负整数, 则对  $\forall a \in S,$

$$\begin{cases} a^m \circ a^n = a^{m+n} \\ (a^m)^n = a^{mn} \end{cases}$$

**证明:** 6 对  $n$  用数学归纳法。对第一个式子, 当  $n = 1$  时, 由定义知, 由定义知  $a^{m+1} = a^m \circ a$ 。假设当  $n = k$  时成立, 即  $a^{m+k} = a^m \circ a^k$ 。那么当  $n = k+1$  时有  $a^{m+(k+1)} = a^{(m+k)+1} = a^{m+k} \circ a = (a^m \circ a^k) \circ a = a^m \circ (a^k \circ a) = a^m \circ a^{k+1}$ 。

对第二个式子, 当  $n = 1$  时显然成立。假设当  $n = k$  时成立, 即  $(a^m)^k = a^{mk}$ , 当  $n = k+1$  时有  $(a^m)^{k+1} = (a^m)^k \circ a^m = a^{mk} \circ a^m = a^{mk+m} = a^{m(k+1)}$ 。

### 么半群中的逆元素和群

**定义 0.1.11** 设  $(S, \circ, e)$  是一个么半群,  $a \in S$ 。称  $a$  有左逆元素, 如果存在  $a_l \in S$  使得  $a_l \circ a = e$ , 这时  $a_l$  称为  $a$  的左逆元素。称  $a$  有右逆元素, 如果存在  $a_r \in S$  使得  $a \circ a_r = e$ , 这时  $a_r$  称为  $a$  的右逆元素。如果存在  $b \in S$  使得  $a \circ b = b \circ a = e$ , 则称  $a$  有逆元素,  $b$  称为  $a$  的逆元素。

**定义 0.1.12** 每个元素都有逆元素的么半群称为群。

**定理 0.1.11** 如果么半群  $(S, \circ, e)$  中的元素  $a$  有左逆元素  $a_l$ , 又有右逆元素  $a_r$ , 则  $a_l = a_r$ 。于是  $a$  有逆元素并且逆元素唯一。记为  $a^{-1}$

**定理 0.1.12** 有限半群  $(S, \circ)$  是一个群当且仅当对于  $\forall s \in S$  有  $sS = S$  并且  $\exists t \in S$  使得  $St = S$ 。

证明:有限半群  $((S, \circ))$  中一定有一个元素  $(a \in S)$ , 使得  $(a \circ a = a)$ 。

#### 0.1.4 子半群、子么半群和理想

**定义 0.1.13** 设  $(S, \circ)$  是一个半群,  $B$  是  $S$  的一个非空子集。如果对于  $\forall a, b \in B$ , 都有  $a \circ b \in B$ , 则称代数系  $(B, \circ)$  是  $(S, \circ)$  的一个子半群。简称  $B$  是  $S$  的一个子半群。

$(B, \circ)$  的乘法与  $(S, \circ)$  的乘法是一样的, 否则即使  $B$  是  $S$  的子集,  $(B, \star)$  也不是  $(S, \circ)$  的一个子半群。

**定义 0.1.14** 设  $(S, \circ, e)$  是一个么半群,  $P \subseteq S$ 。如果  $e \in P$ , 并且  $P$  是  $S$  的子半群, 则称  $P$  是  $S$  的子么半群。

设  $((Z, \cdot))$  是整数的乘法半群, 则  $((\{0, 1\}, \cdot))$  是子半群和子么半群。

$(E, \cdot)$  也是  $(Z, \cdot)$  的一个子半群, 但是不是子么半群。

设  $((S, \circ))$  是半群,  $(a \in S)$ ,  $(B = \{a^n | n \geq 1\})$  是  $((S, \circ))$  的子半群。设  $(M)$  是子么半群。设  $(Q)$  是  $((M, \circ, e))$  的可逆元素的集合, 则  $((Q, \circ, e))$  也是  $((M, \circ, e))$  的

#### 有 $A$ 生成的子半群和子么半群

**定理 0.1.13** 一个么半群的任意多个子么半群的交集仍是子么半群。

**定理 0.1.14** 设  $(S, \circ)$  是半群,  $A$  是  $S$  的一个非空子集, 则  $S$  的一切包含  $A$  的子半群的交集  $Q$  也是子半群。

**定义 0.1.15** 设  $(S, \circ)$  是半群,  $A$  是  $S$  的一个非空子集, 则  $S$  的一切包含  $A$  的子半群的交集称为由  $A$  生成的子半群, 记为  $\langle A \rangle$ 。设  $(M, \circ, e)$  是么半群,  $A$  是  $M$  的一个非空子集, 则  $M$  的一切包含  $A$  的子么半群的交集称为由  $A$  生成的子么半群, 记为  $\langle A \rangle$ 。

**定义 0.1.16** 半群  $(S, \circ)$  的一个非空子集  $A$  称为  $S$  的一个左(右)理想。如果  $SA \subseteq A$  ( $AS \subseteq A$ )。如果  $A$  既是  $S$  的左理想又是  $S$  的右理想, 则称  $A$  是  $S$  的理想。

**定义 0.1.17** 设  $A$  是  $(S, \circ)$  的一个非空子集, 由  $A$  生成的左(右)理想为所有包含  $A$  的左(右)理想的交。 $S$  的一切包含  $A$  的理想的交称为由  $A$  生成的理想。

**定理 0.1.15** 设  $A$  是半群  $(S, \circ)$  的一个非空子集, 则

1. 由  $A$  生成的左理想是  $A \cup SA$ 。
2. 由  $A$  生成的右理想是  $A \cup AS$ 。
3. 由  $A$  生成的理想是  $A \cup SA \cup AS \cup SAS$ 。

**定理 0.1.16** 设  $A$  是么半群  $(M, \circ, e)$  的一个非空子集, 则

1. 由  $A$  生成的  $M$  的左理想是  $MA$ 。
2. 由  $A$  生成的  $M$  的右理想是  $AM$ 。
3. 由  $A$  生成的  $M$  的理想是  $MAM$ 。

### 循环半群

**定义 0.1.18** 一个半群(么半群)称为循环半群(循环么半群), 如果这个半群(么半群)是由其中的某个元素生成的半群(么半群)。由元素  $a$  生成的循环半群记为  $\langle a \rangle$ 。

自然数集  $(\mathbb{N}, +)$  对通常加法的半群  $(\mathbb{N}, +)$  是由  $(1)$  生成的循环半群。所有非负整数之集  $(\mathbb{N}_0, +)$  是由  $(1)$  生成的循环幺半群。

**定理 0.1.17** 循环半群 (幺半群) 必是可交换半群 (幺半群)。

### 0.1.5 同构、同态

#### 同构

**定义 0.1.19** 设  $(S, \circ)$  和  $(T, *)$  是两个半群。如果存在一个从  $S$  到  $T$  的一一对应  $\varphi$ , 使得  $\forall a, b \in S$  有

$$\varphi(a \circ b) = \varphi(a) * \varphi(b)$$

则称半群  $(S, \circ)$  与  $(T, *)$  同构。记为  $(S, \circ) \cong (T, *)$ , 简记为  $S \cong T$ 。 $\varphi$  称为从  $S$  到  $T$  的一个同构映射, 简称同构。

**定义 0.1.20** 设  $(M, \circ, e)$  和  $(M', *, e')$  是两个幺半群。如果存在一个从  $M$  到  $M'$  的一一对应  $\varphi$ , 使得  $\forall x, y \in M$  有

$$\varphi(e) = e', \varphi(x \circ y) = \varphi(x) * \varphi(y)$$

则称幺半群  $(M, \circ, e)$  和  $(M', *, e')$  同构。记为  $(M, \circ, e) \cong (M', *, e')$ , 简记为  $M \cong M'$ 。 $\varphi$  称为从  $M$  到  $M'$  的一个同构 (映射)。

**定理 0.1.18** (幺半群的 Cayley 定理) 任何幺半群  $(M, \circ, e)$  同构于变换幺半群  $(L(M), \circ, I_M)$ 。

**证明:** 7  $L(M) = \{\rho_a | \rho_a : M \rightarrow M, a \in M, \rho_a(x) = a \circ x, \forall x \in M\}$ 。在  $L(M)$  上定义乘法 “ $\circ$ ” 如下:  $\rho_a \circ \rho_b = \rho_{a \circ b}, \forall \rho_a, \rho_b \in L(M)$ 。则  $(L(M), \circ)$  构成一个幺半群。}

做映射  $\psi : M \rightarrow L(M)$ , 使得对  $\forall a \in M, \psi(a) = \rho_a$ 。可以证明  $\psi$  是一个同构映射。



## 同态

**定义 0.1.21** 设  $(S, \circ)$  和  $(T, *)$  是两个半群。如果存在一个从  $S$  到  $T$  的映射  $\varphi$ , 使得  $\forall a, b \in S$  有

$$\varphi(a \circ b) = \varphi(a) * \varphi(b)$$

则称半群  $(S, \circ)$  与  $(T, *)$  是同态的。 $\varphi$  称为从  $S$  到  $T$  的一个同态。 $\varphi(S)$  称为同态象。

若  $(M, \circ, e)$  和  $(M', *, e')$  是两个幺半群。如果存在一个从  $M$  到  $M'$  的映射  $\varphi$ , 使得  $\forall x, y \in M$  有

$$\varphi(e) = e', \varphi(x \circ y) = \varphi(x) * \varphi(y)$$

则称幺半群  $(M, \circ, e)$  与  $(M', *, e')$  同态。 $\varphi$  称为从  $M$  到  $M'$  的一个同态。

设  $(S, \circ)$  是一个非空

集合,  $(S^* = \{f | f: S \rightarrow S\})$ , 则  $(S^*, \circ)$  对映射的合成形成一个半群  $(S^*, \circ)$ 。若  $(S, \circ)$  是一个半群, 则  $(S, \circ)$  与  $(S^*, \circ)$  同态。

令  $(M, \circ, e)$  和  $(M', *, e')$  是两个幺

半群。设  $(\varphi: M \rightarrow M', \forall x \in M, \varphi(x) = e')$ , 则  $(\varphi)$  是一个同态, 但是若  $(|M'| > 1)$ , 则  $(\varphi)$  不是满同态。

令  $(\mathbb{Z}, \cdot, 1)$  是整数的乘法幺半群。设

$(\varphi: \mathbb{Z} \rightarrow \mathbb{Z}, \forall z \in \mathbb{Z}, \varphi(z) = 0)$ , 则  $(\varphi)$  不是同态, 因为  $(\varphi(1) = 0 \neq 1)$ 。

**定理 0.1.19** 设  $(S, \circ)$  是一个半群,  $(T, *)$  是一个具有二元代数运算  $*$  的代数系。如果存在满映射  $\varphi: S \rightarrow T$  使得  $\forall x, y \in S$  有

$$\varphi(x \circ y) = \varphi(x) * \varphi(y)$$

则  $(T, *)$  是半群。

**定理 0.1.20** 设  $(S, \circ, e)$  是一个幺半群,  $(T, *)$  是半群。如果  $\varphi$  是  $S$  到  $T$  的满半群同态, 则  $\varphi(e)$  是  $T$  的单位元, 从而  $(T, *, \varphi(e))$  是幺半群。

**定理 0.1.21** 设  $(M_1, \circ, e_1)$  和  $(M_2, *, e_2)$  是么半群。如果  $M_1$  到  $M_2$  有一个同态  $\varphi$ , 则  $M_1$  的可逆元素  $a$  的象  $\varphi(a)$  也可逆并且  $(\varphi(a))^{-1} = \varphi(a^{-1})$ 。

**定理 0.1.22** 设  $\varphi$  是半群  $(S_1, \circ)$  到  $(S_2, *)$  的同态,  $\psi$  是半群  $(S_2, *)$  到  $(S_3, \cdot)$  的同态, 则  $\varphi \circ \psi$  是  $(S_1, \circ)$  到  $(S_3, \cdot)$  的同态。

**由映射诱导出的等价关系**