近世代数 半群和幺半群

任 世 军

Email: ren_shijun@163.com

哈尔滨工业大学 计算机学院

January 3, 2019

目录

近世代数的特点

它有如下几个显著特点：

- 采用集合论的记号；
- 重视运算以及运算规律；
- 使用抽象化和公理化方法。

学好近世代数应该做到

- 必须清楚的掌握每个概念;
- 掌握基本的推理方法,学会运用概念和公理进行正确的逻辑推理；
- 学会把抽象的理论和方法与具体的对象相联系；
- 在课堂多做练习。

数学归纳法

最小数原理,良序原理,Well-Ordering Principle

正整数集合 Z^+ 的每一个非空子集都有一个最小元素。

$Z^+ = N$ 自然数集合

最小数原理,良序原理,Well-Ordering Principle

正整数集合 Z^+ 的每一个非空子集都有一个最小元素。

$Z^+ = N$ 自然数集合

第一数学归纳法

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。
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。

数学归纳法

从数理逻辑的角度,是要证明:
$\{P(1), (\forall k)(P(k) \to P(k+1))\} \vdash (\forall n)P(n)$

下面的序列,说明
$\{P(1), (\forall k)(P(k) \to P(k+1))\} \vdash P(n)$
再使用全称推广定理就得到结论。

1). $(\forall k)(P(k) \to P(k+1))$
2). $P(1)$
3). $(\forall k)(P(k) \to P(k+1)) \to (P(1) \to P(2))$
4). $P(1) \to P(2)$
5). $P(2)$
6). $(\forall k)(P(k) \to P(k+1)) \to (P(2) \to P(3))$
7). $P(2) \to P(3)$
8). $P(3)$
$\vdots$
$2n-2$). $(\forall k)(P(k) \to P(k+1)) \to (P(n-1) \to P(n))$

数学归纳法（续）

第二数学归纳法

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。

归纳法的练习

the Fibonacci sequence $f_1, f_2, f_3, \cdots$ is defined as follows:

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

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

瞒天过海——使用归纳法应注意的问题

证明所有的马都有同样的颜色

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。

证明所有的马都有同样的颜色

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。

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,$S=\{h_1,h_2,\cdots,h_{m+1}\}$,因为 $h_1,h_2,\cdots,h_m$ 是 m 匹马,所有由于 P(m) 成立,所以 $h_1,h_2,\cdots,h_m$ 具有同样的颜色,同理 $h_2,h_3,\cdots,h_{m+1}$ 是 m 匹马,所以 $h_2,h_3,\cdots,h_{m+1}$ 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)。

基本概念

回顾:映射,函数,变换,泛函数......

基本概念

回顾:映射,函数,变换,泛函数......

定义 1.1 —— 二元代数运算的定义

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

回顾:映射,函数,变换,泛函数......

定义 1.1 —— 二元代数运算的定义

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

二元代数运算的表示, 前缀表示与中缀表示

回顾:映射,函数,变换,泛函数......

定义 1.1 —— 二元代数运算的定义

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

二元代数运算的表示,前缀表示与中缀表示

定义 1.2 —— 一元代数运算的定义

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。

基本概念

回顾:映射,函数,变换,泛函数......

定义 1.1 —— 二元代数运算的定义

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

二元代数运算的表示, 前缀表示与中缀表示

定义 1.2 —— 一元代数运算的定义

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。

定义 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

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

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

$$a \circ b = b \circ a$$

则称二元代数运算“$\circ$”满足交换律。

代数系

定义 1.4——代数系的定义

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。

定义 1.4——代数系的定义

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。

定义 1.4——代数系的定义

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 1.1

设 $(S, \circ)$ 为一个代数系。如果二元代数运算“$\circ$”满足结合律，则 $\forall a_i \in S, i = 1, 2, \cdots, n$, $a_1, a_2, \cdots, a_n$ 的乘积仅与这 n 个元素及其次序有关而唯一确定。乘法方案数目为 $\frac{1}{n}C_{2n-2}^{n-1}$.

定义 1.4 —— 代数系的定义

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 1.1

设 $(S,\circ)$ 为一个代数系。如果二元代数运算“$\circ$”满足结合律，则 $\forall a_i \in S, i=1,2,\cdots,n$, $a_1,a_2,\cdots,a_n$ 的乘积仅与这 n 个元素及其次序有关而唯一确定。乘法方案数目为 $\frac{1}{n}C_{2n-2}^{n-1}$.

定理 1.2

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。

分配律

定义 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 1.3

$(S, \circ, +)$ 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 $\forall a, a_i \in S, i = 1, 2, \cdots, n$，我们有

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

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

定义 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）。

单位元 (续)

定理 1.4

$(S,\circ)$ 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 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。

同样可以定义左零元素和右零元素。

一些记号

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

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

把 $A\circ B$ 简单的写成 AB,把 $a\circ b$ 写成 ab。

当 $A=\{a\}$ 时,$AB=\{a\}B$,简记为 aB。于是

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

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

定义 11.3.1

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。集合 S 上的元素可以是任何类型。

定义 11.3.1

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。集合 S 上的元素可以是任何类型。

小集合作为集合的元素

令 $S = \{\{1,2\},\{3,4\}\}$,定义 S 上的乘法 $\circ$ 如下:

$\circ$	$\{1,2\}$	$\{3,4\}$
$\{1,2\}$	$\{1,2\}$	$\{3,4\}$
$\{3,4\}$	$\{3,4\}$	$\{1,2\}$

$(S, \circ)$ 是一个半群。

半群的例子

小集合作为集合的元素

令 $S=\{\{1,3\},\{2,4\}\}$,定义 S 上的乘法 $\circ$ 如下:

$\circ$	$\{1,3\}$	$\{2,4\}$
$\{1,3\}$	$\{1,3\}$	$\{2,4\}$
$\{2,4\}$	$\{2,4\}$	$\{2,4\}$

$(S,\circ)$ 是一个半群。

半群的例子

小集合作为集合的元素

令 $S = \{\{1,3\},\{2,4\}\}$,定义 S 上的乘法 $\circ$ 如下:

$\circ$	$\{1,3\}$	$\{2,4\}$
$\{1,3\}$	$\{1,3\}$	$\{2,4\}$
$\{2,4\}$	$\{2,4\}$	$\{2,4\}$

$(S,\circ)$ 是一个半群。

小集合作为集合的元素

令 $S = \{\{1,3,\cdots\},\{2,4,\cdots\}\}$,定义 S 上的乘法 $\circ$ 如下:

$\circ$	$\{1,3,\cdots\}$	$\{2,4,\cdots\}$
$\{1,3,\cdots\}$	$\{1,3,\cdots\}$	$\{2,4,\cdots\}$
$\{2,4,\cdots\}$	$\{2,4,\cdots\}$	$\{2,4,\cdots\}$

半群的例子

对于 $Z_3 = \{\{0,3,6,\cdots\},\{1,4,7,\cdots\},\{2,5,8,\cdots\}\}$ 定义的加法为:

$+_1$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$
$\{0,3,6,\cdots\}$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$
$\{1,4,7,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$	$\{0,3,6,\cdots\}$
$\{2,5,8,\cdots\}$	$\{2,5,8,\cdots\}$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$

$+_2$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$
$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$	$\{0,3,6,\cdots\}$
$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$
$\{2,5,8,\cdots\}$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$

半群的例子——模 n 剩余类

设 $Z_n = \{[0],[1],\cdots,[n-1]\}$ 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

$$[i] = \{m|m \in Z, m \equiv i(mod\ n)\} \quad [i] = [n+i]?$$

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

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

证明加法“+”是 Z_n 上的一个二元代数运算。$(Z_n,+)$ 是一个半群。

在 Z_n 中定义加法 $[i]+[j] = [i+1+j]$ 是否可行?

半群的例子

$+_3$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$
$\{0,3,6,\cdots\}$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$
$\{1,4,7,\cdots\}$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$
$\{2,5,8,\cdots\}$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$

$+_4$	$\{0,3,6,\cdots\}$	$\{1,4,7,\cdots\}$	$\{2,5,8,\cdots\}$
$\{0,3,6,\cdots\}$	$\{0,3,6,\cdots\}$	$\{0,3,6,\cdots\}$	$\{0,3,6,\cdots\}$
$\{1,4,7,\cdots\}$	$\{0,3,6,\cdots\}$	$\{0,3,6,\cdots\}$	$\{0,3,6,\cdots\}$
$\{2,5,8,\cdots\}$	$\{0,3,6,\cdots\}$	$\{0,3,6,\cdots\}$	$\{0,3,6,\cdots\}$

集合上的二元关系

集合 A 上的一个二元关系 ρ 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。

半群的例子

例 11.3.5

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。

半群的例子

例 11.3.5

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。

例 11.3.6

设 S 是一切形如

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, a, b \in N$$

的 2×2 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, 并且对于 $\forall d \in N$,

$$\begin{pmatrix} 1 & d \\ 0 & 0 \end{pmatrix}$$

是左单位元素。从而 $(S, \circ)$ 有无限多个左单位元素。

半群中的单位元

定理 11.3.1

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 11.3.2

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。

幺半群

定义 11.3.2

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。

例 11.3.7

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

幺半群

定义 11.3.2

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。

例 11.3.7

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

例 11.3.9

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

有限半群满足什么条件可以成为幺半群呢?

定理 11.3.2

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

$$sS = S, St = S$$

有限半群满足什么条件可以成为幺半群呢?

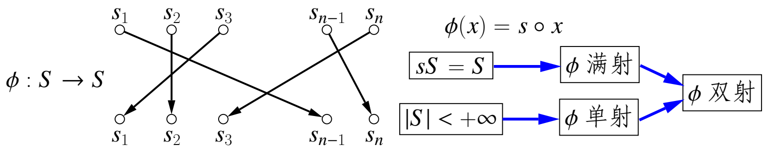
定理 11.3.2

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: $\Rightarrow$ 显然。

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

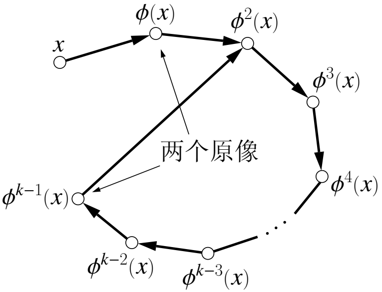


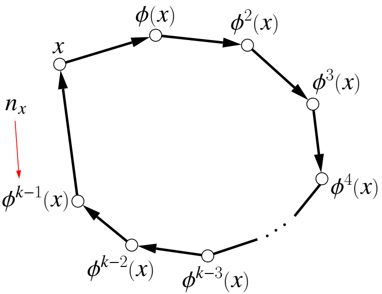
任取 $x \in S$, 序列 $x, \phi(x), \phi^2(x), \cdots, \phi^n(x)$ 中必有两项相同,设 $\phi^p(x) = \phi^q(x)$,其中 $p < q$,ϕ 有逆映射 ϕ^{-1},故 $\phi^{q-p}(x) = x$。从而对任取的 x,有非负整数 n_x,使得 $\phi^{n_x}(x) = x$。令 $k = lcm\{n_x | x \in S\}$, 于是

$$\phi^k(x) = \phi^{m_x n_x}(x) = (\underbrace{\phi^{n_x}\phi^{n_x}\cdots\phi^{n_x}}_{m_x})(x) = (\underbrace{\phi^{n_x}\phi^{n_x}\cdots\phi^{n_x}}_{m_x-1})(x) = \cdots =$$

$\phi^{n_x}(x) = x$,从而对 $\forall x \in S$,有 $s^k \circ x = \phi^k(x) = x$,$s^k$ 为一个左幺元。

有限半群满足什么条件可以成为幺半群?





有限半群满足什么条件可以成为幺半群?

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

有限半群满足什么条件可以成为幺半群呢?

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

$$c(a,b,c) = (b,c,a)$$

有限半群满足什么条件可以成为幺半群?

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

$$c(a,b,c) = (b,c,a)$$

$$c^2(a,b,c) = c(b,c,a) = (c,a,b) \text{ 注意 } c \circ c = a$$

有限半群满足什么条件可以成为幺半群呢?

$$
\begin{array}{c|ccc}
\circ & a & b & c \\
\hline
a & & & \\
b & & & \\
c & b & c & a
\end{array}
\quad \Rightarrow \quad
\begin{array}{c|ccc}
\circ & a & b & c \\
\hline
a & c & a & b \\
b & & & \\
c & b & c & a
\end{array}
$$

$c(a, b, c) = (b, c, a)$

$c^2(a, b, c) = c(b, c, a) = (c, a, b)$ 注意 $c \circ c = a$

有限半群满足什么条件可以成为幺半群呢?

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

$\Rightarrow$

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

$c(a, b, c) = (b, c, a)$

$c^2(a, b, c) = c(b, c, a) = (c, a, b)$ 注意 $c \circ c = a$

$c^3(a, b, c) = c(c, a, b) = (a, b, c)$ 此时 $c^3 = c \circ c^2 = c \circ a = b$

有限半群满足什么条件可以成为幺半群?

$$\begin{array}{c|ccc} \circ & a & b & c \\ \hline a & & & \\ b & & & \\ c & b & c & a \end{array} \quad \Rightarrow \quad \begin{array}{c|ccc} \circ & a & b & c \\ \hline a & c & a & b \\ b & a & b & c \\ c & b & c & a \end{array}$$

$c(a,b,c) = (b,c,a)$

$c^2(a,b,c) = c(b,c,a) = (c,a,b)$ 注意 $c \circ c = a$

$c^3(a,b,c) = c(c,a,b) = (a,b,c)$ 此时 $c^3 = c \circ c^2 = c \circ a = b$

元素的幂

在半群中 $(S,\circ)$ 可以定义元素的正整数次幂,对 $\forall a\in S$

$$a^1=a,\quad a^{n+1}=a^n\circ a\ (n\geq 1)$$

在幺半群 $(S,\circ,e)$ 中可以定义元素的非负整数次幂,对于 $\forall a\in S$,

$$a^0=e,\quad a^{n+1}=a^n\circ a\ (n\geq 0)$$

定理 11.3.3

设 $(S,\circ,e)$ 是一个幺半群,m,n 是任意的非负整数,则对 $\forall a\in S$,

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

定义 11.3.3

设 $(S, \circ, e)$ 是一个幺半群,$a \in S$。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 11.3.3

设 $(S, \circ, e)$ 是一个幺半群，$a \in S$。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 11.3.4

每个元素都有逆元素的幺半群称为群。

定理 11.3.4

如果幺半群 $(S, \circ, e)$ 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 11.3.5

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 $St = S$。

习题

P343.5

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

P343.5

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

以下解法成立否?

任取 $b \in S$,于是有序列 $b^{2^0}, b^{2^1}, b^{2^2}, \cdots, b^{2^n}, \cdots$,因 S 有限,故有 $m < n$,使得 $b^{2^m} = b^{2^n}$,所以 $b^{2^n-2^m} \circ b^{2^n-2^m} = b^{2^n} \circ b^{2^n-2^m-2^m} = b^{2^m} \circ b^{2^n-2^m-2^m} = b^{2^n-2^m}$。令 $a = b^{2^n-2^m}$ 即为所求。

习题（续）

P343.1

找一个半群，它有有限多个左单位元。

习题（续）

P343.1

找一个半群，它有有限多个左单位元。

给出乘法表如下：

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

乘法表又称为 cayley 表。

习题（续）

P343.1

找一个半群,它有有限多个左单位元。

给出乘法表如下：

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

将上面表中的元素转置,就得到有 4 个右单位元素的半群。

乘法表又称为 cayley 表。

P343.1

找一个半群,它有有限多个左单位元。

给出乘法表如下:

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

将上面表中的元素转置,就得到有 4 个右单位元素的半群。
将上面表中的元素个数增加,就得到有限多个右单位元素的半群。

乘法表又称为 cayley 表。

定义 11.4.1

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。

定义 11.4.1

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 11.4.1

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 11.4.2

设 $(S, \circ, e)$ 是一个幺半群,$P \subseteq S$。如果 $e \in P$,并且 P 是 S 的子半群,则称 P 是 S 的子幺半群。

例 11.4.1

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

例子

例 11.4.1

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

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

例子

例 11.4.1

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

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

例 11.4.2

设 $(S, \circ)$ 是半群,$a \in S$,$B = \{a^n | n \geq 1\}$ 是 $(S, \circ)$ 的子半群。设 $(M, \circ, e)$ 是幺半群,$a \in M$,$P = \{a^n | n \geq 0\}$ 是 $(M, \circ, e)$ 的子幺半群。设 Q 是 $(M, \circ, e)$ 的可逆元素的集合,则 $(Q, \circ, e)$ 也是 $(M, \circ, e)$ 的子幺半群。

有 A 生成的子半群和子幺半群

定理 11.4.1

一个幺半群的任意多个子幺半群的交集仍是子幺半群。

有 A 生成的子半群和子幺半群

定理 11.4.1

一个幺半群的任意多个子幺半群的交集仍是子幺半群。

定理 11.4.2

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。

有 A 生成的子半群和子幺半群

定理 11.4.1

一个幺半群的任意多个子幺半群的交集仍是子幺半群。

定理 11.4.2

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 11.4.3

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 (A)。设 $(M, \circ, e)$ 是幺半群,A 是 M 的一个非空子集,则 M 的一切包含 A 的子幺半群的交集称为由 A 生成的子幺半群,记为 (A)。

理想

定义 11.4.4

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。

理想

定义 11.4.4

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。

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。

定义 11.4.4

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。

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 11.4.3

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 $A \cup SA \cup AS \cup SAS$.

理想（续）

定理 11.4.4

设 A 是幺半群 $(M, \circ, e)$ 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 11.4.5

一个半群（幺半群）称为循环半群（循环幺半群），如果这个半群（幺半群）是由其中的某个元素生成的半群（幺半群）。由元素 a 生成的循环半群记为 (a)。

定义 11.4.5

一个半群（幺半群）称为循环半群（循环幺半群），如果这个半群（幺半群）是由其中的某个元素生成的半群（幺半群）。由元素 a 生成的循环半群记为 (a)。

例 11.4.3

自然数集合 N 对通常加法的半群 $(N,+)$ 是由 1 生成的循环半群。所有非负整数之集 $N_0 = N \cup \{0\}$ 对通常加法构成的幺半群 $(N_0,+)$ 是由 1 生成的循环幺半群。

循环半群

定义 11.4.5

一个半群（幺半群）称为循环半群（循环幺半群），如果这个半群（幺半群）是由其中的某个元素生成的半群（幺半群）。由元素 a 生成的循环半群记为 (a)。

例 11.4.3

自然数集合 N 对通常加法的半群 $(N, +)$ 是由 1 生成的循环半群。所有非负整数之集 $N_0 = N \cup \{0\}$ 对通常加法构成的幺半群 $(N_0, +)$ 是由 1 生成的循环幺半群。

定理 11.4.5

循环半群（幺半群）必是可交换半群（幺半群）。

同构

定义 11.5.1

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 φ，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 $S\cong T$。φ 称为从 S 到 T 的一个同构（映射）。

同构

定义 11.5.1

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 φ,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 $S\cong T$。φ 称为从 S 到 T 的一个同构(映射)。

定义 11.5.2

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 φ,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 $M\cong M'$。φ 称为从 M 到 M' 的一个同构(映射)。

定理 11.5.1

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

定理 11.5.1

(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: $L(M) = \{\rho_a | \rho_a : M \to M, a \in M, \rho_a(x) = a \circ x, \forall x \in M\}$。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。

定理 11.5.1

（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： $L(M)=\{\rho_a|\rho_a:M\to M,a\in M,\rho_a(x)=a\circ x,\forall x\in M\}$。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 $\psi:M\to L(M)$，使得对 $\forall a\in M,\psi(a)=\rho_a$。可以证明 ψ 是一个同构映射。

同态

定义 11.5.3

设 $(S,\circ)$ 和 $(T,*)$ 是两个半群。如果存在一个从 S 到 T 的映射 φ,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。φ 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 φ,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。φ 称为从 M 到 M' 的一个同态。

例子

例 11.5.1

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

例子

例 11.5.1

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

例 11.5.2

令 $(M, \circ, e)$ 和 $(M', *, e')$ 是两个幺半群。设
$\varphi : M \to M', \forall x \in M, \varphi(x) = e'$,则 φ 是一个同态,但是若 $|M'| > 1$,则 φ 不是满同态。

例子

例 11.5.1

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

例 11.5.2

令 $(M,\circ,e)$ 和 $(M',*,e')$ 是两个幺半群。设
$\varphi:M\to M',\forall x\in M,\varphi(x)=e'$,则 φ 是一个同态,但是若 $|M'|>1$,则 φ 不是满同态。

例 11.5.3

令 $(Z,\cdot,1)$ 是整数的乘法幺半群。设 $\varphi:Z\to Z,\forall z\in Z,\varphi(z)=0$,则 φ 不是同态,因为 $\varphi(1)=0\neq 1$。

几个定理

定理 11.5.2

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 $\varphi : S \to T$ 使得 $\forall x, y \in S$ 有

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

则 $(T, *)$ 是半群。

几个定理

定理 11.5.2

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 $\varphi : S \to T$ 使得 $\forall x, y \in S$ 有

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

则 $(T, *)$ 是半群。

定理 11.5.3

设 $(S, \circ, e)$ 是一个幺半群，$(T, *)$ 是半群。如果 φ 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。

几个定理（续）

定理 11.5.4

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

几个定理（续）

定理 11.5.4

设 $(M_1, \circ, e_1)$ 和 $(M_2, *, e_2)$ 是幺半群。如果 M_1 到 M_2 有一个同态 φ,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 11.5.5

设 φ 是半群 $(S_1, \circ)$ 到 $(S_2, *)$ 的同态,ψ 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

设 $(S,\circ)$ 和 $(T,*)$ 是两个半群。φ 是 S 到 T 的同态,则 φ 确定了 S 上的一个等价关系 $E_\varphi:\forall x,y\in S$,

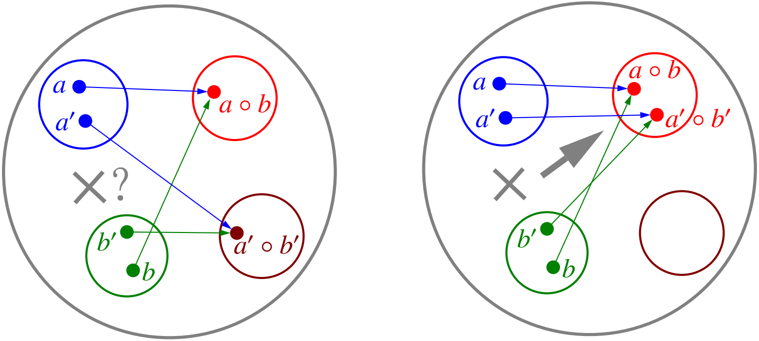
$$xE_\varphi y \text{当且仅当} \varphi(x)=\varphi(y)$$

利用 S 上的代数运算"$\circ$"可以定义 S/E_φ 上的一个代数运算"$\cdot$"如下:

$$\forall [a],[b]\in S/E_\varphi, [a]\cdot[b]=[a\circ b]$$

可以证明:"$\cdot$"满足结合律,$(S/E_\varphi,\cdot)$ 是一个半群。

由等价关系确定的等价类之间如何才能建立代数运算



如果能够证明:若 a' 在等价类 $[a]$ 中并且 b' 在等价类 $[b]$ 中,则 $a' \circ b'$ 必在等价类 $[a \circ b]$ 中,就可以依据半群中的乘法“$\circ$”建立等价类中的二元代数运算。

定义 11.5.5

设 $\cong$ 是代数系 $(X,\circ)$ 上的等价关系。$\forall a,a',b,b'\in X$,如果 $a'\cong a$ 并且 $b'\cong b$,则必有 $a'\circ b'\cong a\circ b$,那么就称 $\cong$ 是代数系 X 上的同余关系。

同态基本定理

定义 11.5.5

设 $\cong$ 是代数系 $(X, \circ)$ 上的等价关系。$\forall a, a', b, b' \in X$,如果 $a' \cong a$ 并且 $b' \cong b$,则必有 $a' \circ b' \cong a \circ b$,那么就称 $\cong$ 是代数系 X 上的同余关系。

定理 11.5.7

设 $\cong$ 是代数系 $(X, \circ)$ 上的一个关系,$\forall [a], [b] \in X/\cong$,定义

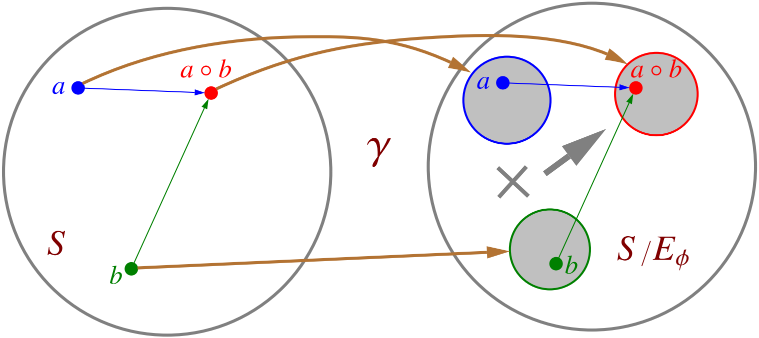
$$[a] \cdot [b] = [a \circ b]$$

则"$\cdot$"是 $X/\cong$ 上的二元代数运算当且仅当 $\cong$ 是同余关系。

同态基本定理（续）

定义 11.5.4

设 $(S,\circ)$ 和 $(T,*)$ 是两个半群。φ 是 S 到 T 的同态。半群 $(S/E_\varphi,\cdot)$ 称为商半群。令 $\gamma: S\to S/E_\varphi, \forall a\in S, \gamma(a)=[a]$ 则称 γ 为 S 到商半群 S/E_φ 的自然同态。



同态基本定理（续）

定理 11.5.6

（幺半群的同态基本定理）设 φ 是幺半群 $(M, \circ, e)$ 到 $(M', *, e')$ 的同态,则

1. 同态象 $\varphi(M)$ 是 M' 的一个子幺半群。
2. 由 φ 确定的等价关系是同余关系,即如果 $a'E_\varphi a, b'E_\varphi b$,那么 $a' \circ b' E_\varphi a \circ b$。于是 $\forall [a], [b] \in M/E_\varphi, [a] \cdot [b] = [a \circ b]$ 是 M/E_φ 上的二元代数运算,$(M/E_\varphi, \cdot, [e])$ 是幺半群。
3. 存在唯一的 M/E_φ 到 M' 的单同态 $\bar{\varphi}$ 使得
$$\varphi = \bar{\varphi} \circ \gamma$$
其中 γ 是 M 到 M/E_φ 的自然同态。
4. 如果 φ 是满同态,则 M/E_φ 与 M' 同构。

同态基本定理（续）