离散数学

第五章：代数系统的一般概念

卢杨
厦门大学信息学院计算机科学系
luyang@xmu.edu.cn

代数系统

- 从具体到抽象是数学发展的一条重要大道.
- 数学结构是对研究对象 (数字, 多项式, 矩阵, 文字, 命题, 集合, 图, 代数系统和更一般元素) 定义种种运算 (加, 减, 乘; 与, 或, 非; 交, 并, 补), 然后讨论这些对象及运算的有关性质.
- 我们发现它们中存在许多共通之处.

例 实数对于加, 乘, 负运算; 命题对于且, 或, 非运算; 集合对于并, 交, 补运算甚至可以作统一的描述.

- 这就使人们自然地想到, 可以作进一步抽象的研究.
- 不管对象集合的具体特性, 也不管对象集合上运算的具体意义, 主要讨论这些数学结构的一般特性, 并按运算所遵循的一般定律, 特性, 对这些数学结构进行分类研究. 这就是抽象代数学的基本内容.

代数系统

- 抽象代数有三个显著特点:
  1. 采用集合论的符号.
  2. 重视运算及其运算规律.
  3. 使用抽象化和公理化的方法.
- 抽象化表现在运算对象是抽象的，代数运算也是抽象的，而且是用公理规定的. 代数系统的集合和运算仅仅是一些符号, 都是些抽象的东西, 故称抽象代数.
- 采用抽象化和公理化方法的结果使所得到的理论具有普遍性, 并使论证确切和严格, 从而结果是精确的, 这样的理性认识更深刻地反映了客观世界.
- 抽象代数已成为计算机科学理论基础之一, 在计算数学模型, 计算复杂性, 刻画抽象数据结构和密码学等中有着直接的应用. 它不仅在知识方面，而且在思想方法上, 都是研究计算机科学不可缺少的工具.

代数系统

- 在定义一种新的数学对象, 例如集合, 矩阵, 图, 或命题之后:
  - 首先需要引进符号, 以表示这类新的对象.
  - 其次就是把新的对象分类, 例如, 有限集合或无限集合; 布尔矩阵或对称矩阵.
  - 然后对这些对象定义运算, 并对运算的性质进行验证.
- 代数系统是带有若干运算的集合 (或系统), 运算是代数系统的决定性因素.

5.1 二元运算及其性质

二元运算

- 把二元运算定义为具有某种性质的一个函数.

定义 5.1

设S为集合, 函数$f: S\times S \to S$称为S上的二元运算. 对$\forall x, y, c \in S$, 如果$f(\langle x, y\rangle) = c$, 则称$x$和$y$是运算数, c是x和y的运算结果.

例 $f: \mathbf{N}\times\mathbf{N} \to \mathbf{N}$, $f(\langle x, y\rangle) = x + y$是自然数集合上的一个二元运算, 即普通加法运算.

但普通的减法不是自然数集合上的二元运算, 因为两个自然数相减可能得负数, 而负数不是自然数, 不满足f的定义$f: \mathbf{N}\times\mathbf{N} \to \mathbf{N}$.

- 通常用$\circ, *, \cdot, \cdots$等符号表示二元运算, 称为算符. 设$f: S\times S \to S$是S上的二元运算, 对任意$x, y \in S$, 如果x与y的运算结果是z, 即$f(\langle x, y\rangle) = z$, 可利用算符$\circ$简记为$x \circ y = z$.

二元运算

- 集合S上的二元运算是一个处处有定义的函数, 且必须具有**确定性**和**封闭性**的特征, 即需满足函数$f: S\times S \rightarrow S$.

  (1) **确定性**: f把$S\times S$中每个有序对$\langle a,b\rangle$, 仅对应于S中的惟一确定的元素$f(\langle a,b\rangle)$.

  (2) **封闭性**: 如果运算总是产生对象集合内(S上) 的另一成员, 那么称这个结构关于这种运算是**封闭的**.

- S上定义的二元运算的重要特性就是运算的封闭性, 这是与通常所说的运算的**重要区别**.

二元运算

例 5.1 (1) 普通的加法和乘法是自然数集**N**上的二元运算，但减法和除法不是，因为$2-3 \notin \mathbf{N}$; $2/3 \notin \mathbf{N}$, 0不可以做除数.

(2) 普通的加法，减法和乘法是整数集**Z**，有理数集**Q**，实数集**R**，复数集**C**上的二元运算. 除法不是**Z**, **Q**, **R**, **C**上的二元运算, 0不可以做除数.

(3) 普通的乘法和除法是非零实数集$\mathbf{R}^*$上的二元运算，但加法和减法不是$\mathbf{R}^*$上的二元运算, $\forall x \in \mathbf{R}^*$, $x+(-x)=0$, $x-x=0$, 而$0 \notin \mathbf{R}^*$.

(4) 令$M_n(\mathbf{R})=\{[a_{ij}]_{n\times n} \mid a_{ij} \in R\}(n \geq 2)$是$n$阶实矩阵的集合，则矩阵加法和乘法是$M_n(\mathbf{R})$上的二元运算.

(5) $P(S)=\{x \mid x \subseteq S\}$是集合$S$的幂集，则集合的并，交，相对补和对称差运算都是$P(S)$上的二元运算.

(6) S为集合, S^S为S上的所有函数的集合, 即$\{f \mid S \to S\}$, 则函数的复合运算是S^S上二元运算.

一元运算

定义 5.2

设S为集合, 函数$f: S \to S$称为S上的一个一元代数运算, 简称为一元运算.

例 5.3 (1) 求一个数的相反数是整数集合$\mathbf{Z}$, 有理数集合$\mathbf{Q}$, 实数集合$\mathbf{R}$上的一元运算, 但不是自然数集$\mathbf{N}$上的一元运算.

(2) 求一个n阶$(n \geq 2)$实矩阵的转置矩阵是$M_n(\mathbf{R})$上的一元运算, 而求逆矩阵不是$M_n(\mathbf{R})$上的一元运算.

一元运算

例5.3 (3) 如果令S为全集，则集合绝对补运算~是$P(S)$上的一元运算.

(4) 令$R(S)$为集合S上的所有二元关系的集合，则关系的逆运算是$R(S)$上的一元运算.

(5) 设A为集合，S是所有从A到A的双射函数构成的集合，则求反函数的运算是S上的一元运算.

(6) 阶乘$n!$是自然数集合$\mathbf{N}$上的一元运算.

运算表

- 如果$S=\{a_1,a_2,\dots,a_n\}$是一个有穷集合, 可通过运算表来定义S上的一个一元或二元运算.
- 以下是一元运算表和二元运算表的一般形式.

a_i	$\circ(a_i)$
a_1	$\circ(a_1)$
a_2	$\circ(a_2)$
$\vdots$	$\vdots$
a_n	$\circ(a_n)$

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1\circ a_1$	$a_1\circ a_2$	$\cdots$	$a_1\circ a_n$
a_2	$a_2\circ a_1$	$a_2\circ a_2$	$\cdots$	$a_2\circ a_n$
$\vdots$	$\cdots\circ\cdots$	$\cdots\circ\cdots$	$\cdots$	$\cdots\circ\cdots$
a_n	$a_n\circ a_1$	$a_n\circ a_2$	$\cdots$	$a_n\circ a_n$

运算表

例5.4 设$S=\{1,2\}$, 给出$P(S)=\{\emptyset,\{1\},\{2\},\{1,2\}\}$上的二元运算$\oplus$和一元运算~的运算表, 其中全集为S.

a_i	$\sim(a_i)$
$\emptyset$	$\{1,2\}$
$\{1\}$	$\{2\}$
$\{2\}$	$\{1\}$
$\{1,2\}$	$\emptyset$

$\oplus$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\emptyset$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1,2\}$	$\{2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\emptyset$	$\{1\}$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	$\emptyset$

运算表

- 在同一个集合上可以定义多少个二元运算?
- 设$S = \{a, b\}$，现在确定能够定义在S上的二元运算的个数. S的每个二元运算$\circ$可以用该表描述.
- 由于**封闭性**，每个空格只可以用元素a或b填充，共有$2 \times 2 = 4$个空格，所以存在$2^{2\times 2} = 16$ 种方法来完成这张表.
- 所以对于任意集合S，存在$|S|^{|S\times S|}$种不同的二元运算.

$\circ$	a	b
a	□	□
b	□	□

交换律与结合律

- 对代数系统的考察最根本的就是对运算性质的讨论，只有当其运算满足一定的条件时，该代数系统才有研究的价值和意义.

定义 5.3

设$\circ$为集合S上的二元运算，如果$\forall x, y \in S$都有$x \circ y = y \circ x$，则称$\circ$运算在S上是可交换的，也称$\circ$运算在S上满足交换律.

定义 5.4

设$\circ$为集合S上的二元运算，如果$\forall x, y \in S$都有$(x \circ y) \circ z = x \circ (y \circ z)$，则称$\circ$运算在$S$上是可结合的，也称$\circ$运算在$S$上满足结合律.

交换律与结合律

例 (1) 实数集**R** (有理数集**Q**, 整数集**Z**, 自然数集**N**) 上的加法和乘法是可交换的, 可结合的, 而减法和除法不满足交换律和结合律.

(2) $M_n(\mathbf{R})$ $(n \geq 2)$上的矩阵加法是可交换的, 可结合的; 而矩阵乘法是可结合的, 但不是可交换的.

(3) 幂集$P(S)$上的并, 交, 对称差运算是可交换, 可结合的.

(4) S^S上的函数复合运算是可结合的, 一般不是可交换的.

二元运算的性质

- 如果每一次参加运算的元素都是相同的，且在表达式中有n个元素参加运算，则可以将这个表达式写成该元素的n次幂. 例如

$$x \circ x \circ \cdots \circ x = x^n.$$

- 关于x的幂运算，使用数学归纳法不难证明以下公式:

$$x^m \circ x^n = x^{m+n}, (x^m)^n = x^{mn},$$

其中m, n为正整数.

- 普通的乘法幂，关系复合的幂以及矩阵乘法的幂的公式就是以上公式的特例.

幂等律

定义 5.5

设$\circ$为集合S上的二元运算,

(1) 若$\forall x \in S$都有$x \circ x = x$, 则称$\circ$运算在S上是幂等的, 也称$\circ$运算在S上满足幂等律.

(2) 若S中的某些x满足$x \circ x = x$, 则称x为运算$\circ$的幂等元.

- 如果S上的二元运算$\circ$适合幂等律, 则S中的所有元素都是运算$\circ$的幂等元.

例 上例中的所有运算中只有集合的并和交运算满足幂等律，即$S \cup S = S$，$S \cap S = S$, 其他的运算一般说来都不是幂等的.

$\oplus$运算只有当$A = \emptyset$时满足$A \oplus A = A$，所以$\oplus$运算不适合幂等律，但是$\emptyset$是$\oplus$运算的幂等元.

普通的加法和乘法不适合幂等律, 但是0是加法的幂等元, 1是乘法的幂等元.

分配律和吸收律

- 以上讨论的运算性质只涉及一个二元运算．下面考虑与两个二元运算相关的性质，即分配律和吸收律.

定义 5.6

设$\circ$和$*$是集合S上的二元运算. 若$\forall x, y, z \in S$有

$$x * (y \circ z) = (x * y) \circ (x * z), \qquad (y \circ z) * x = (y * x) \circ (z * x),$$

则称$*$运算对$\circ$运算是可分配的, 也称$*$运算对$\circ$运算满足分配律.

- 在讲到分配律时一定要指明哪个运算对哪个运算可分配，因为往往一个运算对另一个运算可分配时反之不然.
  - 例如, 普通乘法对普通加法可分配, 但是普通加法对普通乘法不是可分配的.
- 分配律的意义在于将两个运算联系起来, 通过这种联系, 能在运算过程中改变两个运算的次序.

分配律和吸收律

定义 5.7

若$\circ$和$*$是S上两个**满足交换律**的二元运算, 且$\forall x, y \in S$有

$$x \circ (x * y) = x, \qquad x * (x \circ y) = x,$$

则称$\circ$和$*$运算是**可吸收的**, 或称$\circ$和$*$运算满足**吸收律**.

- 和分配律不同, 满足吸收律的两个二元运算地位是一样的.

分配律和吸收律

例 (1) 实数集**R**上的乘法对加法是可分配的, 但加法对乘法不满足分配律.

(2) $n(\geq 2)$阶实矩阵集合$M_n(\mathbf{R})$上的矩阵乘法对矩阵加法是可分配的.

(3) 幂集$P(S)$上的并和交是互相可分配的，并且满足吸收律. $A \cup (A \cap B) = A; A \cap (A \cup B) = A.$

(4) $\forall a, b \in R$有$a * b = \max\{a, b\}$，$a \circ b = \min\{a, b\}$，则$*$和$\circ$满足吸收律.

证明 $\forall a, b \in R$，$a * (a \circ b) = \max\{a, \min\{a, b\}\} = a$，$a \circ (a * b) = \min\{a, \max\{a, b\}\} = a$, 因为$*$和$\circ$是可交换的, 所以$\circ$和$*$满足吸收律.

单位元与零元

除了算律以外, 还有一些和二元运算有关的的特异元素: 单位元, 零元, 逆元和幂等元.

定义 5.8

设$\circ$为集合S上的二元运算. 若存在e_l (或e_r) $\in S$使得$\forall x \in S$都有

$$e_l \circ x = x \text{ (或} x \circ e_r = x\text{)},$$

则称e_l (或e_r) 是S中关于$\circ$运算的左 (或右) 单位元. 若$e \in S$关于$\circ$运算既为左单位元又为右单位元, 则称e为S中关于$\circ$运算的单位元 (又称幺元).

定义 5.9

若存在$\theta_l \in S$ (或$\theta_r \in S$) 使得$\forall x \in S$都有

$$\theta_l \circ x = \theta_l \text{(或} x \circ \theta_r = \theta_r\text{)},$$

则称θ_l (或θ_r) 是S中关于$\circ$运算的左 (或右) 零元. 若$\theta \in S$关于$\circ$运算既为左零元又为右零元, 则称θ为S中关于$\circ$运算的零元.

单位元与零元

例 (1) $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$上, 关于加法的单位元是0, 没有零元; 关于乘法的单位元是1, 零元是0; 减法运算的右单位元是0, 无左单位元, 故无单位元.

(2) $n(\geq 2)$阶实矩阵集合$M_n(\mathbf{R})$中关于矩阵加法的单位元是n阶全0矩阵, 没有零元; 而关于矩阵乘法的单位元是n阶单位矩阵, 零元是n阶全0矩阵.

(3) 幂集$P(S)$中关于$\cup$运算的单位元是$\emptyset$, 零元是S; 而关于$\cap$运算的单位元是S, 零元是$\emptyset$. $\oplus$运算的单位元是$\emptyset$, 没有零元.

单位元与零元

例 (4) S^S中关于函数复合运算的单位元是S上的恒等函数I_S，$I_S(x) = x$. 没有零元.

(5) $S = \{a_1, a_2, \ldots, a_n\}$, $n \geq 2$. 定义S上的二元运算$\circ$, $\forall a_i, a_j \in S$ 有$a_i \circ a_j = a_i$，则S中的每个元素都是$\circ$运算的右单位元，但没有左单位元，所以S中没有单位元. 同样地，S中的每个元素都是$\circ$运算的左零元, 但无零元.

厦门大学信息学院 SCHOOL OF INFORMATICS XIAMEN UNIVERSITY 厦门大学计算机科学系 Computer Science Department of Xiamen University

单位元与零元

- 零元和单位元是代数系统中两个比较特殊的全局元素，占有**重要的地位**. 在任一代数系统中, 可能存在零元和单位元, 但也可能不存在零元, 或不存在单位元.
- 直观地说，单位元e是集合S上的“弱势”元素 ，它与别的元素进行代数运算所产生的作用为“**自我消亡, 成全别人**”.
- 零元θ是集合S上的“强势”元素 , 它与别的元素进行代数运算所产生的作用为“**见谁灭谁, 唯我独尊**”.

单位元与零元

关于单位元和零元存在以下定理.

定理 5.1

设$\circ$为集合S上的二元运算, 存在e_l和e_r分别为运算$\circ$的左单位元和右单位元, 则$e_l = e_r = e$, 且e就是S中关于$\circ$运算的惟一的单位元.

证明 首先证明相等. 因为e_r是右单位元, 所以有$e_l \circ e_r = e_l$;

又由于e_l是左单位元, 因此有$e_l \circ e_r = e_r$;

由这两个等式可得$e_l = e_r$, 把这个单位元记作e.

再证明唯一性. 假设关于$\circ$运算存在另一个单位元e', 则有$e' = e' \circ e = e$, 所以e是关于$\circ$运算的惟一的单位元.

- 该定理说明: S中关于$\circ$运算的左单位元和右单位元若存在, 则它们相等且是惟一的.

单位元与零元

定理 5.2

设$\circ$为集合S上的二元运算，若存在θ_l和θ_r分别为运算$\circ$的左零元和右零元, 则$\theta_l = \theta_r = \theta$, 且$\theta$是$S$中关于$\circ$运算的惟一的零元.

证明 首先证明相等, 因为θ_l和θ_r分别是$\circ$的左零元和右零元, 则

$$\theta_l = \theta_l \circ \theta_r = \theta_r.$$

再证明唯一性, 令$\theta_l = \theta_r = \theta$, 则$\theta$是$\circ$的一个零元.

设θ'是$\circ$的另一个零元, 则$\theta' = \theta' \circ \theta = \theta$, 即$\theta$是$\circ$的惟一零元.

- 该定理与上一定理类似，说明了S中关于$\circ$运算的左零元和右零元若存在, 则它们相等且是惟一的.

单位元与零元

定理 5.3

设集合S至少有两个元素，e和θ分别为S中关于$\circ$运算的单位元和零元, 则$e \neq \theta$.

证明 反证法. 假设$e = \theta$, 则$\forall x \in S$有

$$x = x \circ e = x \circ \theta = \theta,$$

即S中所有元素都等于θ, 这与S中至少有两个元素矛盾.

- 若$|S| = 1$，$\circ$为S上的二元运算，则S中的唯一元素既是运算$\circ$的单位元又是零元.

逆元

定义 5.10

设$\circ$是集合S上的二元运算，$e \in S$是关于$\circ$运算的单位元．对于$x \in S$, 若存在$y_l \in S$ (或$y_r \in S$) 使得

$$y_l \circ x = e\ (\text{或} x \circ y_r = e),$$

则称y_l（或y_r）是x关于$\circ$的左（或右）逆元．若$y \in S$既是x关于$\circ$的左逆元, 又是x关于$\circ$的右逆元, 则称y是x关于$\circ$的逆元. 如果x的逆元存在, 则称x是可逆的.

逆元

例 (1) 自然数集合$\mathbf{N}$关于加法运算只有$0 \in \mathbf{N}$有逆元0，其他的自然数都没有加法逆元.

(2) 整数集$\mathbf{Z}$中，任何整数n关于加法的逆元是$-n$．关于乘法只有1和-1存在逆元, 就是它们自己, 其他整数没有乘法逆元.

(3) $n(\geq 2)$阶实矩阵集合$M_n(\mathbf{R})$中任何矩阵M的加法逆元为$-M$, 而对于矩阵乘法只有实可逆矩阵M存在乘法逆元M^{-1}.

(4) 幂集$P(S)$中关于$\cup$运算只有空集$\emptyset$有逆元，就是$\emptyset$本身，S的其他子集没有逆元. $\cap$运算只有S有逆元, 就是S本身.

逆元

- 对于集合S上的二元运算$\circ$，单位元e和零元θ是全局的概念，是常元，是对S上的所有元素而言的，不针对某个元素x.
- 逆元是局部的概念，不是常元，它不仅依赖运算，而且还依赖个别的元素，只针对S中的某元素x而言的.
- 对于任何二元运算，单位元总是可逆的，其逆元就是单位元自身，$e \circ e = e$.
- 而一般地 (除了$|S| = 1$)，零元是不可逆的.
- 对于有单位元的代数系统而言，任一元素可能不存在逆元，也可能存在逆元，甚至存在多个逆元 (不满足结合律).

逆元

定理 5.4

设$\circ$为集合S上**可结合的**二元运算且单位元为e, 对于$x \in S$若存在y_l和$y_r \in S$, 使得$y_l \circ x = e$和$x \circ y_r = e$, 则$y_l = y_r = y$, 且y是x关于$\circ$运算的惟一逆元.

证明 $$y_l = y_l \circ e = y_l \circ (x \circ y_r) = (y_l \circ x) \circ y_r = e \circ y_r = y_r.$$

令$y_l = y_r = y$, 则y是x关于$\circ$运算的逆元.

假设y'也是x关于$\circ$运算的逆元,则有

$$y' = y' \circ e = y' \circ (x \circ y) = (y' \circ x) \circ y = e \circ y = y.$$

所以y是x关于$\circ$运算的惟一的逆元.

- 满足结合律的二元运算, $\forall x \in S$存在关于二元运算的逆元, 则是惟一的. 可将这个惟一的逆元记作x^{-1}.
- **若不满足结合律, 则本定理不一定成立.**

逆元

例　设$\circ$为实数集**R**上的二元运算, $\forall x \in \mathbf{R}$有$x \circ y = x + y - 2xy$, 说明$\circ$运算是否可交换的, 可结合的, 幂等的, 然后确定关于$\circ$运算的单位元, 零元和所有可逆元素的逆元.

解 $\circ$运算是可交换的和可结合的, 但不是幂等的.

假设e和θ分别为$\circ$运算的单位元和零元, 则$\forall x \in R$有

$$x + e - 2xe = x \circ e = x \text{和} x + \theta - 2x\theta = x \circ \theta = \theta,$$

即$(1-2x)e = 0$和$x(1-2\theta) = 0$.

要使这些等式对一切实数x都成立, 只有$e = 0$和$\theta = 1/2$.

$\forall x \in R$, 设y为x关于$\circ$运算的逆元, 则有$x \circ y = e$,

$x + y - 2xy = 0$. 从而解得$x^{-1} = y = \frac{-x}{1-2x}(x \neq \frac{1}{2})$.

二元运算的性质与运算表

- 关于二元运算∘的有些性质可以直接从运算表中看出:

1. 运算∘具有封闭性⇔运算表中每个元素都属于S.
2. 运算∘具有可交换性⇔运算表关于主对角线对称.
3. θ是关于∘的零元⇔θ所对应的行和列中的元素都和该零元相同.
4. e是关于∘的单位元⇔e所对应的行和列依次和运算表头的行和列相一致.

二元运算的性质与运算表

5. 运算$\circ$具有幂等性$\Leftrightarrow$运算表的主对角线上的每个元素与它所在行或列的表头元素相同.

6. 关于$\circ$的幂等元$\Leftrightarrow$运算表的主对角线上的第i个元素与它所在行或列的表头第i个元素相同.

7. $e \in S$, a和b互逆$\Leftrightarrow$位于a所在行, b所在列的元素以及b所在行, a所在列的元素都是单位元（即这两个单位元关于对角线成对称, 则a与b互为逆元). 如果a所在的行和列具有共同的单位元, 则单位元一定在主对角线上, 则a的逆元是a自己. 否则a无逆元.

二元运算的性质与运算表

例 设S上二元运算$\circ$由下表所确定. 求S中关于$\circ$运算的单位元, 零元和所有可逆元素的逆元.

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

解 由表不难看出:

a是$\circ$运算的单位元, d是$\circ$运算的零元.

a, b, c为可逆元素, 且$a^{-1}=a$, $b^{-1}=b$, $c^{-1}=c$.

二元运算的性质与运算表

例 表-1中, e是单位元, a和b都是a的逆元, 但运算不满足结合律, 如

$$(a * b) * b = e * b = b \neq a * (b * b) = a * a = e,$$

表-2中, e是单位元, 运算也不满足结合律, 如

$$(a \circ b) \circ b = e \circ b = b \neq a \circ (b \circ b) = a \circ e = a,$$

但是每个元素的逆元都是惟一的. 这说明结合律成立是逆元惟一的充分但不必要的条件.

$*$	a	b	e
a	e	e	a
b	e	a	b
e	a	b	e

表-1

$\circ$	a	b	e
a	e	e	a
b	b	e	b
e	a	b	e

表-2

消去律

定义 5.11

设$\circ$是集合S上的二元运算, 若对于任意的$x, y, z \in S$, 且x不是$\circ$运算的零元时, 都有

$$x \circ y = x \circ z \Rightarrow y = z, (\text{左消去律})$$

$$y \circ x = z \circ x \Rightarrow y = z, (\text{右消去律})$$

则称$\circ$运算在S中满足消去律.

例 (1) 普通加法和乘法在整数集**Z**, 有理数集**Q**, 实数集**R**上适合消去律.

(2) 幂集$P(S)$上的并和交运算一般不适合消去律, 但对称差运算适合消去律.

语言

例 5.7 设Σ是字母的有穷集，称为字母表，Σ中的有限个字母构成的序列w称作为Σ上的串．串中字母的个数叫做串的长度，记作$|w|$．长度为0的串叫做空串，记作λ. 对任意的$k \in \mathbf{N}$，令

$$\Sigma^k = \{v_{i_1} v_{i_2} \dots v_{i_k} \mid v_{i_j} \in \Sigma, j = 1,2, \dots, k\}$$

为Σ上所有长度为k的串构成的集合，特别地有

$$\Sigma^0 = \{\lambda\},$$
$$\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \cdots,$$
$$\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \cdots,$$

定义Σ^+是Σ上长度至少是1的串的集合，而Σ^*是Σ上所有串的集合.

语言

- 在Σ^*上定义二元运算∘, $\forall w_1, w_2 \in \Sigma^*$, $w_1 = a_1a_2 \dots a_m$, $w_2 = b_1b_2 \dots b_n$有

$$w_1 \circ w_2 = a_1a_2 \dots a_m b_1b_2 \dots b_n,$$

称∘为Σ^*上的连接运算. 它是Σ^*上的二元运算. 对于$w_1, w_2, w_3 \in \Sigma^*$有

$$(w_1 \circ w_2) \circ w_3 = w_1(w_2 \circ w_3),$$

即连接运算满足结合律, 但不满足交换律, 幂等律. 它的单位元是空串λ, 没有零元.

语言

- Σ^* 上还可以定义一个一元运算，即求一个串的反串. $\forall w \in \Sigma^*$，$w = a_1a_2 \dots a_m$, 有$w' = a_m a_{m-1} \dots a_1$, 则 $'$ 运算为$\forall w \in \Sigma^*$上的一元运算.
- 如果$w' = w$, 则称串w是一个回文.

例 0, 11, 101, 0110, 01010都是$\{0,1\}^*$上的回文.

- Σ^*上的任何子集都称为Σ上的一个语言L, $L \subseteq \Sigma^*$.

例

$$L_1 = \{(01)^n | n \in \mathbf{N}\} = \{\lambda, 01, 0101, 010101, \dots\};$$

$$L_2 = \{0^n 1^n | n \in \mathbf{N}\} = \{\lambda, 01, 0011, 000111, \dots\};$$

$$L_3 = \{0^n 1 0^n | n \in \mathbf{N}\} = \{1, 010, 00100, 0001000, \dots\};$$

都是$\Sigma = \{0,1\}$上的语言. 其中L_3是回文语言，即该语言中的所有串都是回文.

语言

- 幂集$P(\Sigma^*)$是Σ^*的所有子集的集合, 它就是Σ上所有语言的集合.
- 在$P(\Sigma^*)$上定义二元运算$\cup$, $\cap$和 $\cdot$, 其中 $\cdot$ 运算是语言的连接运算. 定义为: $\forall L_1, L_2 \in P(\Sigma^*)$有

$$L_1 \cdot L_2 = \{w_1 \circ w_2 | w_1 \in L_1 \text{且} w_2 \in L_2\}$$

- 不难证明并和交是可交换, 可结合, 幂等的,
- 语言连接运算 $\cdot$在$P(\Sigma^*)$上是可结合的, 但交换律不成立, 且 $\cdot$ 运算有单位元$\Sigma^0 = \{\lambda\}$.

语言

- 在$P(\Sigma^*)$上还可以定义一元运算$'$，$\forall L \in P(\Sigma^*)$有

$$L' = \{w' | w \in L\}.$$

例 $L = \{0^n 1^n | n \in N\}$, 则有$L' = \{1^n 0^n | n \in N\}$.

- 如果对于某个$L \in P(\Sigma^*)$有$L' = L$, 则称L为Σ上的镜像语言.
- 易见回文语言一定是镜像语言，但镜像语言可不一定是回文语言.

例 语言$\{01, 10\}$是$\Sigma = \{0, 1\}$上的镜像语言. 但不是回文语言.

课堂练习

设$\mathbf{N}_k = \{0,1,\ldots,k-1\}$. $k \in \mathbf{Z}^+$, $\forall x, y \in \mathbf{N}_k$, 有

$$x \circ y = (xy) \bmod k$$

(1) 构造当$k = 5$时的运算表.

(2) 说明$\circ$是否有交换律, 结合律, 单位元和零元.

(3) 如果$\circ$有单位元, 求$\mathbf{N}_5$中所有的可逆元和逆元.

课堂练习

设$\mathbf{N}_k = \{0,1,\dots,k-1\}$. $k \in \mathbf{Z}^+$, $\forall x,y \in \mathbf{N}_k$, 有

$$x \circ y = (xy) \bmod k$$

(1) 构造当$k = 5$时的运算表.

(2) 说明$\circ$是否有交换律, 结合律, 单位元和零元.

(3) 如果$\circ$有单位元, 求$\mathbf{N}_5$中所有的可逆元和逆元.

$\circ$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

解 $\circ$运算是可交换的, 可结合的, 单位元是1, 零元是0.

1和4的逆元是自己, 2和3互为逆元, 0没有逆元.

5.2 代数系统及其子代数和积代数

代数系统

定义 5.12

非空集合S和S上k个一元或二元运算$\circ_1, \circ_2, \dots, \circ_k$组成的系统成为一个代数系统，简称代数，记作$\langle S, \circ_1, \circ_2, \dots, \circ_k \rangle$.

例 (1) $\langle \mathbf{N}, + \rangle$, $\langle \mathbf{Z}, +, \cdot \rangle$, $\langle \mathbf{R}, +, \cdot \rangle$都是代数系统，其中+和·分别表示普通加法和乘法．但N和普通减法不能构成代数系统，因为两个自然数相减可能会得到一个负数，所以不能写成$\langle \mathbf{N}, - \rangle$.

(2) $\langle M_n(\mathbf{R}), +, \cdot \rangle$也是代数系统，其中+和·分别表示$n$阶实矩阵的加法和乘法.

(3) $\langle \mathbf{Z}_n, \oplus, \otimes \rangle$也是代数系统，其中$\mathbf{Z}_n = \{0,1, \dots, n-1\}$；$\oplus$和$\otimes$表示模$n$的加法和乘法，即$\forall x, y \in \mathbf{Z}_n$,

$$x \oplus y = (x + y) \bmod n, \qquad x \otimes y = (x \cdot y) \bmod n,$$

易见$\oplus$和$\otimes$都是$\mathbf{Z}_n$上的二元运算.

(4) $\langle P(S), \cup, \cap, \sim \rangle$也是代数系统，其中含有两个二元运算$\cup$和$\cap$以及一个一元运算$\sim$.

代数系统

- 在某些代数系统中存在着一些特定的元素，它对该系统的一元或二元运算起着重要的作用，如二元运算的单位元和零元等，称这些元素为该代数系统的特异元素或代数常数.
- 有时为了强调这些特异元素的存在，也把它们列到有关的代数系统的表达式中.

例 (1) $\langle \mathbf{Z}, + \rangle$中的$+$运算存在单位元0，为了强调0的存在，也可将$\langle \mathbf{Z}, +, 0 \rangle$记为.

(2) $\langle P(S), \cup, \cap, \sim \rangle$中的$\cup$和$\cap$存在单位元$\emptyset$和$S$，也可将该代数系统记为$\langle P(S), \cup, \cap, \sim, \emptyset, S \rangle$.

- 具体采用哪一种记法要看当前研究的问题是否与这些代数常数有关.

代数系统

定义 5.13

如果两个代数系统中运算的个数相同，对应运算的元数也相同，且代数常数的个数也相同，则称这两个代数系统具有相同的构成成分，也称它们是同类型的代数系统.

例 (1) $V_1 = \langle \mathbf{R}, +, \cdot, -, 0, 1 \rangle$, $\mathbf{R}$为实数集, $+$和$\cdot$为普通的加法和乘法, $-$是求相反数运算.

(2) $V_2 = \langle P(S), \cup, \cap, \sim, \emptyset, S \rangle$, $P(S)$为幂集 ,$\cup$和$\cap$为集合的并和交, $\sim$为绝对补运算, S为全集.

显然V_1, V_2都是同类型的代数系统, 它们都有着共同的构成成分, 但在运算性质方面却不一定相同:

- $+$和 $\cdot$ 没有幂等律和吸收律, 但是有消去律.
- $\cup$和$\cap$有幂等律和吸收律, 但是没有消去律.

同类型就是长得像而已，不看细节

代数系统

- 代数结构并不是要研究每一个具体的代数系统，而是通过规定集合及集合上的二元和一元运算，以及运算所具有的性质来规范每一种代数系统.
- 这个代数系统是许多具有共同构成成分和运算性质的实际代数系统的模型或者抽象.
- 针对这个模型来研究它的结构和内在特征，然后应用到每个具体的代数系统, 这种研究方法就是抽象代数的基本方法.
- 后面涉及到的半群, 独异点和群, 环和域, 格和布尔代数就是具有广泛应用背景的抽象的代数系统.

子代数

定义

设$V=\langle S,\circ_1,\circ_2,\dots,\circ_k\rangle$是代数系统，$B$是$S$的非空子集，若$B$对$V$中所有的运算封闭，且$B$和$S$含有相同的代数常数．则称$V'=\langle B,\circ_1,\circ_2,\dots,\circ_k\rangle$是$V$的子代数系统, 简称子代数. 当$B$是$S$的真子集时, 称$V'$是$V$的真子代数.

- 子代数和原代数不仅是同类型的代数系统，而且对应的二元运算都具有相同的性质.
  - 因为代数系统中的二元运算都一样, 只是对应的集合变成了子集.
- 对于任何代数系统V, 其子代数一定存在, 最大的子代数就是V本身.
- 如果令V中所有代数常数构成的集合是B，且B对V中所有的运算都是封闭的, 则B就构成了V的最小的子代数.
- 这种最大和最小的子代数称为V的平凡的子代数.

子代数

例 5.8

令$n\mathbf{Z}=\{nk|k\in\mathbf{Z}\},n\in\mathbf{N}$，$\langle n\mathbf{Z},+,0\rangle$是$\langle\mathbf{Z},+,0\rangle$的子代数．因为$\forall nk_1$, $nk_2\in n\mathbf{Z}$有

$$nk_1+nk_2=n(k_1+k_2)\in n\mathbf{Z},$$

且$0\in n\mathbf{Z}$, 所以$n\mathbf{Z}$对$\langle\mathbf{Z},+,0\rangle$的运算都是封闭的.

- 当$n=0$时，$n\mathbf{Z}=\{0\}$，$\langle\{0\},+,0\rangle$是$\langle\mathbf{Z},+,0\rangle$的最小子代数，平凡的真子代数.
- 当$n=1$时, $n\mathbf{Z}=\mathbf{Z}$, $\langle\mathbf{Z},+,0\rangle$是最大 (和平凡) 的子代数.
- 当$n\neq 0,1$时, $\langle n\mathbf{Z},+,0\rangle$是$\langle\mathbf{Z},+,0\rangle$非平凡的真子代数.

积代数

- 由两个代数系统V_1和V_2可以产生一个新的代数系统$V_1 \times V_2$，就是V_1和V_2的积代数. 它是笛卡尔积概念的推广.

定义 5.15

设$V_1 = \langle S_1, \circ \rangle$, $V_2 = \langle S_2, * \rangle$是同类型的代数系统, 其中$\circ$和$*$是二元运算. V_1和V_2的积代数$V_1 \times V_2$是含有一个二元运算$\cdot$的代数系统，即$V_1 \times V_2 = \langle S, \cdot \rangle$，其中$S = S_1 \times S_2$，且对任意的$\langle x_1, y_1 \rangle, \langle x_2, y_2 \rangle \in S_1 \times S_2$有

$$\langle x_1, y_1 \rangle \cdot \langle x_2, y_2 \rangle = \langle x_1 \circ x_2, y_1 * y_2 \rangle$$

- 若V是V_1与V_2的积代数，这时也称V_1和V_2是V的因子代数.
- 显然积代数和它的因子代数是同类型的代数系统.

积代数

例 设$V_1 = \langle \mathbf{Z}, + \rangle$, $V_2 = \langle M_2(\mathbf{R}), \cdot \rangle$, 其中+和 · 表示整数加法和矩阵乘法, 则

$$V_1 \times V_2 = \langle Z \times M_2(\mathbf{R}), \circ \rangle.$$

对任意的$\langle z_1, M_1 \rangle, \langle z_2, M_2 \rangle \in Z \times M_2(\mathbf{R})$, 有

$$\langle z_1, M_1 \rangle \circ \langle z_2, M_2 \rangle = \langle z_1 + z_2, M_1 \cdot M_2 \rangle.$$

例如

$$\left\langle 5, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\rangle \circ \left\langle -2, \begin{bmatrix} 2 & -1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\langle 3, \begin{bmatrix} 2 & -1 \\ 2 & 0 \end{bmatrix} \right\rangle.$$

积代数

- 如果原来的代数系统分别含有代数常数，比如$V_1=\langle S_1,\circ,a_1\rangle$，$V_2=\langle S_2,*,a_2\rangle$，则$V_1$与$V_2$的积代数$V_1\times V_2=\langle S,\cdot,a\rangle$，其中$a=\langle a_1,a_2\rangle$.

例 设$V_1=\langle Z,+,0\rangle, V_2=\left\langle M_2(R),\cdot,\begin{bmatrix}1&0\\0&1\end{bmatrix}\right\rangle$, 则

$$V_1\times V_2=\left\langle Z\times M_2(R),\circ,\left\langle 0,\begin{bmatrix}1&0\\0&1\end{bmatrix}\right\rangle\right\rangle,$$

其中$\left\langle 0,\begin{bmatrix}1&0\\0&1\end{bmatrix}\right\rangle$就是积代数的代数常数$V_1\times V_2$.

积代数

定理

设$V_1 = \langle S_1,\circ\rangle$，$V_2 = \langle S_2,*\rangle$是代数系统，其中$\circ$，$*$为二元运算，它们的积代数$V_1{\times}V_2 = \langle S_1{\times}S_2, \cdot \rangle$，则有

(1) 如果$\circ$和$*$运算是可交换的，则 $\cdot$ 运算也是可交换的.

(2) 如果$\circ$和$*$运算是可结合的，则 $\cdot$ 运算也是可结合的.

(3) 如果$\circ$和$*$运算是幂等的，则 $\cdot$ 运算也是幂等的.

(4) 如果$\circ$和$*$运算分别具有单位元e_1和e_2，则$\langle e_1, e_2\rangle$是 $\cdot$ 运算的单位元.

(5) 如果$\circ$和$*$运算分别具有零元θ_1和θ_2，则$\langle \theta_1, \theta_2\rangle$是 $\cdot$ 运算的零元.

(6) 如果$x \in S$对于$\circ$运算的逆元x^{-1}，$y \in S_2$关于$*$运算的逆元为y^{-1}，则$\langle x, y\rangle$关于 $\cdot$ 运算的逆元为$\langle x^{-1}, y^{-1}\rangle$.

积代数

- 虽然积代数$V_1 \times V_2$与因子代数V_1和V_2在许多性质上是共同的，但并非因子代数的所有性质都在积代数中成立．例如消去律在积代数中就不一定成立.

例 5.9　$V_1 = \langle\{0,1\}, \otimes_2\rangle$, $V_2 = \langle\{0,1,2\}, \otimes_3\rangle$，其中$Z_2 = \{0, 1\}$，其中$\otimes_2$ 和$\otimes_3$分别为模2乘法和模3乘法:

$$x \otimes_2 y = (x \cdot y) \bmod 2, \qquad x \otimes_3 y = (x \cdot y) \bmod 3,$$

V_1和V_2的积代数为$\langle\{0,1\}\times\{0,1,2\},\otimes\rangle$, 且有

$$\langle 0,1\rangle \otimes \langle 1,0\rangle = \langle 0,0\rangle = \langle 0,1\rangle \otimes \langle 0,0\rangle.$$

$\langle 0,1\rangle$不是$\otimes$运算的零元，但不能在上式中消去$\langle 0,1\rangle$，因此$\otimes$运算不满足消去律，然而在因子代数V_1和V_2中容易验证消去律是成立的.

5.3 代数系统的同态与同构

同态

- 同态映射是研究代数系统之间相互关系的有力工具.
- 元素运算的像等于元素像的运算是函数与运算的重要联系.

定义 5.16

设$V_1 = \langle S_1, \circ \rangle$, $V_2 = \langle S_2, * \rangle$是同类型的代数系统, $\circ$和$*$是二元运算, 如果存在映射$\varphi: S_1 \to S_2$, 满足对任意的$x, y \in S_1$都有

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

则称φ是代数系统V_1到V_2的同态映射, 简称同态.

- 也就是说, 代数系统V_1中的元素先进行V_1中运算然后再通过φ取像, 与V_1中的元素先通过φ取像再进行V_2中相应的运算, 其运算结果是一样的.
- 同态是保持两个同类型代数系统之间运算的映射.
  - 同态是针对映射, 不是针对代数系统. 称某个映射φ是代数系统V_1到V_2的同态. 不能单独说V_1到V_2是同态的.

同态

例 5.10 设代数系统$V_1 = \langle \mathbf{Z}, + \rangle$, $V_2 = \langle \mathbf{Z}_n, \oplus \rangle$, 其中$\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$, $\oplus$为模n加法, 即$\forall x, y \in \mathbf{Z}_n$有

$$x \oplus y = (x + y) \bmod n,$$

令φ: $\mathbf{Z} \to \mathbf{Z}_n$,

$$\varphi(x) = (x) \bmod n,$$

则φ为V_1到V_2的同态. 因为$\forall x, y \in \mathbf{Z}$有

$$\begin{aligned}
&\varphi(x+y) \\
&= (x+y) \bmod n \\
&= \Big(\big((x) \bmod n\big) + \big((y) \bmod n\big)\Big) \bmod n \\
&= \big((x) \bmod n\big) \oplus \big((y) \bmod n\big) \\
&= \varphi(x) \oplus \varphi(y).
\end{aligned}$$

同态

定义 5.17

设φ是$V_1=\langle S_1,\circ\rangle$到$V_2=\langle S_2,*\rangle$的同态，则称$\langle\varphi(S_1),*\rangle$是$V_1$在$\varphi$下的同态像.

例 5.11 设$V_1=\langle \mathbf{R},+\rangle$, $V_2=\langle \mathbf{R},\cdot\rangle$, 其中$\mathbf{R}$为实数集, $+$和 $\cdot$ 分别为普通加法和乘法. 令φ: $\mathbf{R}\to\mathbf{R}$, $\varphi(x)=e^x$, 则φ为V_1到V_2的同态, 因为$\forall x,y\in\mathbf{R}$有

$$\varphi(x+y)=e^{x+y}=e^x\cdot e^y=\varphi(x)\cdot\varphi(y),$$

在φ下的同态像为$\langle\mathbf{R}^+,\cdot\rangle$, 是$\langle\mathbf{R},\cdot\rangle$的子代数.

同构

定义 5.18

设φ是$V_1 = \langle S_1, \circ \rangle$到$V_2 = \langle S_2, * \rangle$的同态,

(1) 若φ是满射的, 则称φ是V_1到V_2的满同态, 记为$V_1 \overset{\varphi}{\sim} V_2$.

(2) 若φ是单射, 则称φ是V_1到V_2的单同态.

(3) 若φ双射, 则称φ是V_1到V_2的同构, 记为, 也称V_1同构于V_2, 记作$V_1 \overset{\varphi}{\cong} V_2$.

(4) 若$V_1 = V_2$, 则称φ是自同态. 若φ又是双射的则称φ是自同构.

- 如果代数系统V_1同构于V_2, 从抽象代数的观点看, 它们是没有区别的, 是同一个代数系统.
- 例 5.10的同态满同态, 而例 5.11的同态是单同态, 它们都不是同构.

同态

例 5.12 (1) 设$V = \langle \mathbf{Z}, + \rangle$, $a \in \mathbf{Z}$. 令φ_a: $\mathbf{Z} \to \mathbf{Z}$,

$$\varphi_a(x) = ax, \qquad \forall x \in \mathbf{Z}, ax \in \mathbf{Z}.$$

则φ_a是V上的自同态, 因为$\forall x, y \in \mathbf{Z}$有

$$\varphi_a(x+y) = a(x+y) = ax + ay = \varphi_a(x) + \varphi_a(y).$$

- 当$a = 0$时, $\forall x \in \mathbf{Z}$有$\varphi_0(x) = 0$, 它将$\mathbf{Z}$中所有元素映射到$\langle \mathbf{Z}, + \rangle$的单位元0, 称$\varphi_0$是零同态. 它不是单同态也不是满同态.
- 当$a = \pm 1$时, 有$\varphi_1(x) = x$, $\varphi_{-1}(x) = -x$, $\forall x \in \mathbf{Z}$. 显然φ_1和φ_{-1}都是双射的, 因此它们是V上的两个自同构.
- 当$a \neq \pm 1$且$a \neq 0$时, $\forall x \in \mathbf{Z}$有$\varphi_a(x) = ax$, φ_a是单射的, 称为V上的单自同态, 其同态像$\langle a\mathbf{Z}, + \rangle$是$\langle \mathbf{Z}, + \rangle$的真子代数.

同态

例 5.12 (2) 设Σ是有穷字母表, Σ^*为Σ上有限长度的串的集合. Σ^*和串的连接运算构成代数系统$\langle\Sigma^*,\circ\rangle$.

令$\varphi\colon \Sigma^* \to \mathbf{N}, \forall w \in \Sigma^*, \varphi(w) = |w|$, 则$\forall w_1, w_2 \in \Sigma^*$有

$$\varphi(w_1 \circ w_2) = |w_1 \circ w_2| = |w_1| + |w_2| = \varphi(w_1) + \varphi(w_2),$$

所以φ是$\langle\Sigma^*,\circ\rangle$到$\langle\mathbf{N},+\rangle$的同态, 且为满同态.

- 当Σ中只含一个字母时, φ是双射的, 此时φ为同构.

同态

- 定义 5.16中的同态概念可以推广到一般的代数系统中去.
- 下面我们考虑具有多个二元,一元运算和代数常数的代数系统.

定义 5.16.2

设 $V_1=\langle S_1,\circ_1,\circ_2,\dots,\circ_s,\blacktriangle_1,\blacktriangle_2,\dots,\blacktriangle_r,a_1,a_2,\dots a_t\rangle$, $V_2=\langle S_2,*_1,*_2,\dots,*_s,\vartriangle_1,\vartriangle_2,\dots,\vartriangle_r,b_1,b_2,\dots b_t\rangle$是同类型的代数系统, 对于$i=1,\dots,s$, $\circ_i$和$*_i$是二元运算, 对于$j=1,\dots,r$, $\blacktriangle_j$和$\vartriangle_j$是二元运算, 对于$k=1,\dots,t$, a_k和b_k是代数常数, 如果存在映射$\varphi: S_1\to S_2$, 满足对$\forall x,y\in S_1$, $\forall i,j,k$都有

$$\varphi(x\circ_i y)=\varphi(x)*_i\varphi(y),$$

$$\varphi\big(\blacktriangle_j(x)\big)=\vartriangle_j\varphi(x),$$

$$\varphi(a_k)=b_k,$$

则称φ是代数系统V_1到V_2的同态映射, 简称同态.

同态

例 $V_1=\langle \mathbf{Z},+,\cdot,0\rangle$, $V_2=\langle \mathbf{Z}_n,\oplus,\otimes,0\rangle$, 其中$\mathbf{Z}_n=\{0,1,\ldots,n-1\}$, $\oplus$为模n加法, $\otimes$为模n乘法, 即$\forall x,y\in\mathbf{Z}_n$有

$$x\oplus y=(x+y)\bmod n,$$

令$\varphi:\mathbf{Z}\to\mathbf{Z}_n$,

$$\varphi(x)=(x)\bmod n,$$

则有

$$\varphi(x+y)=(x+y)\bmod n=(x)\bmod n\oplus(y)\bmod n=\varphi(x)\oplus\varphi(y),$$
$$\varphi(x\cdot y)=(x\cdot y)\bmod n=(x)\bmod n\otimes(y)\bmod n=\varphi(x)\otimes\varphi(y),$$
$$\varphi(0)=(0)\bmod n=0,$$

所以φ是V_1到V_2的同态, 而且是满同态.

同态

例 $V_1=\langle \mathbf{R},+,-\rangle$, $V_2=\langle \mathbf{R}^+,\cdot,{}^{-1}\rangle$, 其中+和·分别表示普通加法和乘法, $-x$表示求x的相反数, x^{-1}表示求x的倒数.

令$\varphi:\mathbf{R}\to\mathbf{R}^+$, $\varphi(x)=e^x$, 则$\forall x,y\in\mathbf{R}$, 有

$$\varphi(x+y)=e^{x+y}=e^x\cdot e^y=\varphi(x)\cdot\varphi(y),$$

$$\varphi(-x)=e^{-x}=(e^x)^{-1}=\big(\varphi(x)\big)^{-1}.$$

所以φ是V_1到V_2的同态.

同态的性质

定理 5.5

设V_1, V_2是同类型的代数系统，$\circ$和$*$为V_1上的二元运算，$\circ'$和$*'$为V_2上的二元运算，φ是从V_1到V_2的**满同态**，则

(1) 若$\circ$是可交换的（或可结合的，幂等的），则$\circ'$也是可交换的（或可结合的，幂等的）.

(2) 若$\circ$对$*$是可分配的，$\circ'$对$*'$也是可分配的.

(3) 若$\circ$对$*$是可吸收的，$\circ'$对$*'$也是可吸收的.

(4) 若e是V_1中关于$\circ$运算的单位元，则$\varphi(e)$是V_2中关于$\circ'$运算的单位元.

(5) 若θ是V_1中关于$\circ$运算的单位元，则$\varphi(\theta)$是V_2中关于$\circ'$运算的单位元.

(6) 若$\circ$是含有单位元的运算，$u^{-1} \in V_1$是u关于$\circ$运算的逆元，则$\varphi(u^{-1})$是$\varphi(u)$关于$\circ'$运算的逆元，即$\varphi(u)^{-1} = \varphi(u^{-1})$.

证明都是通过定义进行拆装，很简单，自己看书.

同态的性质

- 定理5.5中φ为满同态的条件很重要.
- 定理5.5说明与代数系统V_1相联系的一些重要公理，如交换律，结合律，分配律，同一律和可逆律，在V_1的任何同态像（特别同构像）中能够被保持下来.
- 但V_2具有的性质未必在V_1中成立. 即满同态对保持性质是单向的.
- 需要指出的是，若$\varphi: V_1 \to V_2$不是一个满同态，则定理5.5所列出的性质不一定成立. 因为这时在V_2中存在某些元素，它们不是V_1中任何元素的像.
- 当φ不是满同态时，定理的结论仅在V_1的同态像$\varphi(V_1)$中成立. 例5.13和例5.14作为反例说明了该问题.

同态的性质

例 5.13　设代数系统$V_1 = \langle A,* \rangle$, $V_2 = \langle B,\circ \rangle$, 其中$A = \{a, b, c, d\}$, $B = \{0, 1, 2, 3\}$. $*$和$\circ$运算由运算表所示, 是对称并且可交换的. 定义函数φ: $A \to B$,

$$\varphi(a) = 0, \qquad \varphi(b) = 1, \qquad \varphi(c) = 0, \qquad \varphi(d) = 1.$$

可以验证φ是V_1到V_2的同态. V_1在φ下的同态像是$\langle \{0, 1\},\circ \rangle$. 不难证明$V_1$的$*$运算满足结合律, 但$V_2$的$\circ$运算却不满足结合律, 因为有

$$(1 \circ 0) \circ 2 = 1 \circ 2 = 2, \qquad 1 \circ (0 \circ 2) = 1 \circ 1 = 1$$

但在同态像$\langle \{0, 1\},\circ \rangle$中的$\circ$满足结合律.

$*$	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

$\circ$	0	1	2	3
0	0	1	1	0
1	1	1	2	1
2	1	2	3	2
3	0	1	2	3

同态的性质

例 5.14 设$V=\langle A,\cdot\rangle$, 其中$A=\left\{\begin{bmatrix} a & 0\\ 0 & d\end{bmatrix} \middle| a,d\in\mathbf{R}\right\}$, 且 · 为矩阵乘法.

令$\varphi: A\to A, \varphi\left(\begin{bmatrix} a & 0\\ 0 & d\end{bmatrix}\right)=\begin{bmatrix} a & 0\\ 0 & 0\end{bmatrix}$, 则对于任意的$\begin{bmatrix} a_1 & 0\\ 0 & d_1\end{bmatrix}, \begin{bmatrix} a_2 & 0\\ 0 & d_2\end{bmatrix}\in A$有

$$\varphi\left(\begin{bmatrix} a_1 & 0\\ 0 & d_1\end{bmatrix}\cdot\begin{bmatrix} a_2 & 0\\ 0 & d_2\end{bmatrix}\right)=\varphi\left(\begin{bmatrix} a_1a_2 & 0\\ 0 & d_1d_2\end{bmatrix}\right)=\begin{bmatrix} a_1a_2 & 0\\ 0 & 0\end{bmatrix}$$
$$=\begin{bmatrix} a_1 & 0\\ 0 & 0\end{bmatrix}\cdot\begin{bmatrix} a_2 & 0\\ 0 & 0\end{bmatrix}=\varphi\left(\begin{bmatrix} a_1 & 0\\ 0 & d_1\end{bmatrix}\right)\cdot\varphi\left(\begin{bmatrix} a_2 & 0\\ 0 & d_2\end{bmatrix}\right)$$

φ是V上的自同态, 但不是满自同态, 其同态像为$\left\langle\left\{\begin{bmatrix} a & 0\\ 0 & 0\end{bmatrix} \middle| a\in\mathbf{R}\right\},\cdot\right\rangle$. 易见它是$V$的子代数. 但它的单位元是$\begin{bmatrix} 1 & 0\\ 0 & 0\end{bmatrix}$, 而不是$V$中的单位元$\begin{bmatrix} 1 & 0\\ 0 & 1\end{bmatrix}$.

同态加密

- 场景：用户拥有隐私数据，但是无算力．想要对数据进行计算需要将数据上传至服务器进行计算．然而这么做会造成隐私泄露．
- 在该应用中，映射就是一种加密算法，二元运算就是对数据进行计算．
- 如果一种加密算法是同态的，就可以将数据进行加密后发送至服务器进行计算．对加密的数据进行计算后再解密，将等价于对原始数据进行计算：

$$x \circ y = \varphi^{-1}\big(\varphi(x) \circ \varphi(y)\big)$$

- 通常来说，同态加密算法需要是同构的，因为需要双射函数φ的反函数来对加密计算的结果进行解密．

课堂练习

设$V=\langle \mathbf{R}^*, \cdot \rangle$, 下述映射$\varphi$是否为$V$的自同态? 如果是, 说明它是否为满同态, 单同态和同构, 并计算V的同态像$\varphi(V)$.

(1) $\varphi(x)=|x|$.

(2) $\varphi(x)=2x$.

(3) $\varphi(x)=x^2$.

(4) $\varphi(x)=\frac{1}{x}$.

(5) $\varphi(x)=-x$.

(6) $\varphi(x)=x+1$.

课堂练习

设$V = \langle \mathbf{R}^*, \cdot \rangle$，下述映射$\varphi$是否为$V$的自同态？如果是，说明它是否为满同态，单同态和同构，并计算V的同态像$\varphi(V)$.

(1) $\varphi(x) = |x|$.

(2) $\varphi(x) = 2x$.

(3) $\varphi(x) = x^2$.

(4) $\varphi(x) = \frac{1}{x}$.

(5) $\varphi(x) = -x$.

(6) $\varphi(x) = x + 1$.

解

(1)(3)是同态，但不是单同态，也不是满同态. $\varphi(V) = \langle \mathbf{R}^+, \cdot \rangle$.

(2)不是同态. 令$x = 2, y = 2$，则$2(x \cdot y) = 2 \times 4 = 8$，而$2x \cdot 2y = 16$.

(4)是同态，单同态，满同态，同构. $\varphi(V) = V$.

(5)不是同态. 令$x = 1, y = 2$，则$-(x \cdot y) = -2$，而$(-x) \cdot (-y) = 2$.

(6)不是同态. 令$x = 1, y = 2$，则$x \cdot y + 1 = 3$，而$(x + 1) \cdot (y + 1) = 6$.

作业

p118

2 (2)(4)(8)

3 (2)(4)(8)

4 (2)(4)(8)

8

11 (2)

12

14

谢谢

有问题欢迎随时跟我讨论