代数系统

赵建华

南京大学计算机系

内容

- 二元运算
  - 交换律、结合律、幂等、分配律、吸收律
  - 单位元、左单位元、右单位元
  - 零元、左零元、右零元
  - 逆元、左逆元、右逆元
- 代数系统
- 代数系统的同态与同构

二元运算

- 设S为集合，函数$f: S \times S \rightarrow S$称为S上的二元运算。
  - 如果S已经明了，不需指明，简称二元运算
- 要求：
  - 任何两个元素都可以进行运算
  - 运算结果唯一、且属于S。
- 例子
  - 自然数上的加法运算
  - 非0实数上的除法运算
  - 实数上不能定义二元运算
  - n阶实数矩阵上的矩阵加法运算和乘法运算
  - S->S的所有函数的集合，以及函数复合运算
  - 其它自定义的运算

一元运算

- 给定S，函数$f: S \to S$称为S上的一元运算

- 运算的表示
  - 函数定义
  - 运算表

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

S={1，2，3，4}
x*y = (xy) mod 5

结合律

- 设$\circ$为S上的二元运算，如果对于S中任意的三个元素x,y,z，都有
$$(x \circ y) \circ z = x \circ (y \circ z)$$
则称$\circ$在S上是可结合的，或称$\circ$适合结合律。
- 例子
  - 自然数集N、整数集Z、有理数集Q、实数集上的加法和乘法
  - 函数集合上复合运算
- 对于满足结合律的二元运算，可以去掉括号
  - $(x + y) + (z + u) = x + y + z + u$

幂等律

- 设∘为S上的二元运算，如果对于S中任意元素x，都有

$$x \circ x = x$$

  则称∘适合幂等律。

- 如果S中的某些元素x满足$x \circ x = x$，则称x为幂等元

- 例子
  - 集合的交、并运算
  - 整数集合上，求GCD，LCM的运算
  - 对于对称差，∅是幂等元

分配律

- 设$\circ$和$*$为S上的两个二元运算，如果对于S中任意的三个元素x, y, z，都有

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

则称$*$对$\circ$是可分配的，也称$*$对$\circ$满足分配律

- 例子
  - n阶矩阵的乘法对矩阵加法是可分配的
  - 实数集上的乘法对加法是可分配的
  - 集合的交、并运算相互可分配

吸收律

- 设∘和∗为S上的两个可交换的二元运算，如果对于S中任意的两个元素x,y，都有

$$x * (x \circ z) = x$$

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

则称∘和∗满足吸收律

- 例子
  - 幂集P(S)上的并和交运算满足吸收律

左单位元/右单位元/单位元

- 设$\circ$为S上的二元运算，如果存在S中元素e_l（或e_r），使得对于S中的任何元素x都有

  $$e_l \circ x = x \quad （或\ x \circ e_r = x）$$

  则称e_l（或e_r）为$\circ$的左单位元（或右单位元）；

- 如果e既是左单位元又是右单位元，则称e是单位元（也称幺元）。

- 例子
  - N上的加法的单位元是0，乘法的单位元是1。
  - N阶矩阵加法的单位元是全0矩阵，矩阵乘法的单位元是n阶单位矩阵。
  - 集合交的单位元：全集；集合并：空集

单位元的相关定理

- 定理：设$\circ$为S上的二元运算，且e是单位元，则e是唯一的单位元
  - 证明：设有e’是单位元，则$e' = e' \circ e = e$

- 定理：设$\circ$为S上的二元运算，e_l和e_r分别为$\circ$运算的左单位元和右单位元，则
$$e_l = e_r = e$$
其中e是单位元
- 证明：
  - $e_l = e_l \circ e_r = e_r$，
  - 设$e_l = e_r = e$，根据定义，e是单位元

左零元/右零元/零元

- 设∘为S上的二元运算，如果存在S中元素θ_l（或θ_r），使得对于S中的任何元素x都有

$$\theta_l \circ x = \theta_l \quad (或\ x \circ \theta_r = \theta_r)$$

则称θ_l（或θ_r）为∘的左零元（或右零元）；

- 如果θ既是左零元又是右零元，则称θ是零元。

关于零元的定理

- 设$\circ$为S上的二元运算，θ_l和θ_r分别是左零元和右零元，则

$$\theta_l = \theta_r = \theta$$

且θ是S上关于$\circ$的唯一零元。

- 证明
  - $\theta_l = \theta_l \circ \theta_r = \theta_r$
  - 设θ'是零元，则$\theta = \theta \circ \theta' = \theta'$

单位元和零元

- 设$\circ$为S上的二元运算，e和θ分别是单位元和零元。如果S至少有两个元素，则$e \neq \theta$
- 证明
  - 设x是不等于θ的元素，则$x = x \circ e$且$\theta = x \circ \theta$，因为$\theta \neq x$，因此$x \circ e \neq x \circ \theta$，因此$e \neq \theta$

逆元

- 设∘为S上的二元运算，e是单位元，对于$x \in S$，如果存在元素$y_l \in S$（或$y_r \in S$）使得

  $$y_l \circ x = e \qquad （或者x \circ y_r = e）$$

  那么，y_l（或y_r）称为x的左逆元（或右逆元）。

- 如果y既是x的左逆元，又是右逆元，则称y是x的逆元。如果x存在逆元，则称x是可逆的。

- 例子
  - 自然数加法，只有0有逆元；
  - 整数加法，x的逆元是-x；

关于逆元的定理

- 设∘为S上的可结合二元运算，e为该运算的单位元，如果S中的x存在左逆元y_l和右逆元y_r，则有$y_l = y_r = y$，且y是x的唯一逆元。
- 证明
  - $y_l = y_l \circ e = y_l \circ x \circ y_r = e \circ y_r = y_r = y$
  - 设y'是x的逆元，则$y = y_l = y_l \circ e = y_l \circ x \circ y' = y'$

消去律

- 设∘为S上的二元运算，如果对于S中任意的x,y,z，满足以下条件：
  - 若$x \circ y = x \circ z$且$x \neq \theta$，则$y = z$
  - 若$y \circ x = z \circ x$且$x \neq \theta$，则$y = z$

  则称∘满足消去律。
- 例子
  - 整数集合上的加法/乘法满足消去律
  - 集合交、并运算不满足消去律，集合对称差满足消去律

例子

- 在正整数集合上的运算$x * y = \mathrm{lcm}(x, y)$，即x和y的最小公倍数
  - 满足交换律，结合律，具有幂等性，不满足消去律。
  - 单位元：1，无零元；
  - 逆元：仅元素1有逆元

代数系统

- 定义：非空集合S和S上的k个一元或者二元运算$f_1, f_2, \ldots, f_k$组成的系统称为一个代数系统，简称代数，记作$< S, f_1, f_2, \ldots, f_k >$
- 例子
  - <N,+>，<Z,+,*>，…
  - $< P(S), \cup, \cap, \sim >$
- 包含有特殊元素（如零元，单位元）的代数系统的记法
  - <Z,+,0>，0是单位元
  - $< P(S), \cup, \cap, \sim, \emptyset, S >$
  - 这些特殊元素称为特异元素或者代数常数

同类型的代数系统

- 如果两个代数系统中运算个数相同，对应运算的元数相同，且代数常量个数也相同，则称两个代数系统具有相同的构成部分，或称是同类型的代数系统。
  - 同类型的代数系统仅仅是构成成分相同，不一定具有相同的性质。
- 例子
  - $< R, +, *, -, 0,1 >$，其中-是求负运算
  - $< P(B), \cup, \cap, \sim, \emptyset, B >$

特殊的代数系统

- 对代数系统中运算所满足的算律加以限制，即构成特殊的代数系统
  - 由这些限制推导出的性质对于所有这类系统都成立。
- 常见的特殊系统
  - 半群：$< S, \circ >$，$\circ$是可结合的二元运算；
  - 群：$< S, \circ >$，$\circ$是可结合的二元运算，存在单位元，全部元素可逆；
  - 格：$< S, \circ, * >$，$\circ, *$满足交换律、结合律、幂等律和吸收律。
- 代数研究：从代数系统的构成成分和遵从的算律出发，将代数系统分类，然后研究每一类代数系统的共同性质，并将研究的结果运用到具体代数系统中去。

子代数系统

- 设V=$< S, f_1, f_2, \dots, f_k >$是代数系统，B是S的子集，且B对于$f_1, f_2, \dots, f_k$是封闭的，那么称$< B, f_1, f_2, \dots, f_k >$是V的子代数系统，简称子代数，有时简记为B。
  - 如果V中有特异元素，则B中也应该包含这些特异元素！

- 例子
  - $< N,+ >$是<Z,+>的子代数，
  - N也是<Z,+,0>的子代数，因为0也在N中，仍然是单位元
  - N-{0}不是<Z,+,0>的子代数，因为特异元素0不在N-{0}中！
- 平凡子代数
  - V的最大子代数是其自身，
  - 最小子代数是仅包含特异元素的子代数
- 真子代数：B是S的真子集

子代数系统的例子

- 设V=<Z,+,0>是一个代数系统，

$$nZ = \{nz | z \in Z\}$$

  则nZ是V的子代数

- 证明
  - nZ对于+封闭，
  - 0在nZ中

- 问题
  - 如果代数系统V具有零元/单位元，那么这些元素在其子系统中仍然是零元/单位元吗？Why？

积代数

- 设$V_1 =< A,\circ>$和$V_2 =< B,*>$是两个同类型的代数系统，$\circ$和$*$是二元运算，在集合$A \times B$上如下定义二元运算·

$$< a_1, b_1 > \cdot < a_2, b_2 > = < a_1 \circ a_2, b_1 * b_2 >$$

称$< A \times B,\cdot>$为V_1和V_2的积代数，记作$V_1 \times V_2$

- 性质
  - 如果$\circ$和$*$是可交换的，·也是可交换的
  - 如果e_1，e_2是$\circ$，$*$的单位元，$< e_1, e_2 >$是·的单位元。对于零元也有类似性质。
  - 如果x和y分别是$\circ$，$*$的可逆元素，<x,y>也是·的可逆元素，其逆元就是$<x^{-1},y^{-1}>$。

代数系统的同态和同构

- 同态：设$V_1=<A,\circ>$和$V_2=<B,*>$是同类型的代数系统，$f:A\to B$且
$$\forall x,y\in A(f(x\circ y)=f(x)*f(y))$$
则称f是V_1到V_2的同态映射，简称同态。
  - 单同态：f是单射
  - 满同态：f是满射，V_2称为V_1的同态像；
  - 同构：f是一一映射，记作：$V_1\cong V_2$
- 自同态：f是V到V的同态
  - 单自同态
  - 满自同态
  - 自同构

同态映射的性质

- 设f是$V_1 =< A,\circ >$ 到$V_2 =< B,* >$同构映射，那么
  - 如果$\circ$满足交换律、结合律、幂等律等，那么$*$也相应满足这些算律。
  - 消去律除外
- 特异元素
  - f把V_1中的单位元映射到V_2中的单位元
  - 零元映射为零元
  - 逆元映射为逆元

例子

- $< Z,+ >$到$< Z_n,\oplus >$的同态

$$f(x) = x \bmod n$$

- $< R,+ >$到$< R^*,\cdot >$的同态

$$f(x) = e^x$$

- $<Z,+>$到自身的自同态

$$f(x) = ax$$

例子

- 证明$< Z_n,\bigoplus >$有且仅有n个自同态
  - 存在n个自同态：$f_p(x) = px \bmod n$，其中p=0,1,…,n-1。
  - 没有其它的自同态：根据同态的定义和$\bigoplus$的性质，对于任意同态f，都有f(x) = f(x*1) = f(x)*f(1)，而f(1)的取值只能是0,1,2,…,n-1。

习题