离散数学

Discrete Mathematics

吴梅红

厦门大学计算机科学系

E-mail: wmh@xmu.edu.cn

第三部分　代 数 结 构

- 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。
- 我们发现它们中不无雷同之处。

例 数与多项式对于代数运算有相当的一致性;

命题对于与、或、非运算和集合对于并、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。

- 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。
- 不同的代数系统具有一些共同的性质, 这说明研究抽象的代数系统的必要性。
- 把数学结构自身看成对象并且按照它们的运算性质分类 (半群、独异点、群、环、域、格)是十分有用的。
- 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。

第五章　代数系统的一般概念

- **Mathematics ≈ Definitions + Symbols**
- 定义一种新的数学对象, 例如集合, 矩阵, 图, 或命题等

  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

- 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为非空集合, 函数 $f: S \times S \to S$ 称为S上的一个二元代数运算, 简称二元运算(binary operation)。 ∎

- 对$\forall x, y, c \in S$, 如果$f(\langle x, y\rangle) = c$, 则称x和y是运算数(operand), c是x和y的运算结果。

(1) 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 (closed)。

- 集合S上的二元运算是一个处处有定义的函数, 必须具有 确定性 和 封闭性 的特征。

(2) Dom(f) = S × S, 所以f 把S × S中每个有序对(a, b)

仅对应于 S中的惟一确定的元素 f(a, b),

可以说二元运算是把S中元素的每个有序对对应于S的惟一确定元素的 一个函数 (或法则)。

- 是否构成代数系统关键是考查运算是否封闭。

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 $\notin$N; 2/3 $\notin$N, 0不做除数。

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

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

(6) 令R(B)表示集合B上的所有二元关系的集合，则关系的合成运算是R(B)上二元运算。

(7) $S^S = \{f \mid S \to S\}$，则函数的合成运算是S^S上二元运算。

- 二元运算的概念可推广到 n元运算。

定义 5.2 设S为集合, n为正整数, $S^n = \underbrace{S \times S \times \ldots \times S}_{n个}$表示S的n阶笛卡尔积。 函数f: $S^n \to S$称为S上的一个n元代数运算, 简称 n元(n-ary)运算, n称为此运算的阶。

若f 是S上的运算, 也可以称S在运算f 下是封闭。

- 若f: $S \to S$, 则f 是S上的一元运算。 /*特例 ▌
- 从本质上讲, 集合S上的一个 n元运算 就是从 S^n 到 S 的一个 特定函数。
- S上定义的n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。
- 只要f 是集合S上的n元运算, 则f 关于S是封闭的 ⇔ 只要f 是关于S封闭的函数, 则f 是S上定义的n元运算。

例 5.2 一元 (unary) 运算 (one operand)

(1) 求一个数的相反数是整数集Z、有理数集Q、实数集R上的一元运算。 但不是自然数集N上的一元运算。

通常的减法可以看作是取相反数与加的合成。

(2) 求一个n阶(n≥2)实矩阵的转置矩阵是$M_n(R)$上的一元运算, 而求逆矩阵不是$M_n(R)$上的一元运算。 **Why?**

(3) 如果令B为全集, 则集合绝对补运算~是P(B)上的一元运算。

(4) 令R(B)为集合B上的所有二元关系的集合,

则关系的逆运算是R(B)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) R为实数集, 令$f : R^n \to R$, $\forall <x_1, x_2, \ldots, x_n> \in R^n$有 $f(<x_1, x_2, x_3, \ldots, x_n>) = x_3$, 则f 是R上的一元运算。

它是求一个n维向量的第三个分量的运算 (投影运算)。

(7) 阶乘n! 是一元运算。

- 为了书写的方便, 习惯上用算符operator如*, ◦, •, ▫ 等而不是f 来表示n元运算, 例5.2(6) ◦$(x_1, x_2, \ldots, x_n) = x_3$,
- 二元运算用中缀a ◦ b (而不是前缀◦(a, b))
  表示对应于(a, b)的元素。
- 一元运算将运算数x的括号省略简记为 ▫x。

运算表 Operation Table

- 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。

表 5.2 左表在S上定义一个二元运算$\circ$，在(i, j)位置上的值表示元素$a_i * a_j$。 表 5.1右表在S上定义一元运算~ 。

$\circ$	a_1	a_2	…	a_j	…	a_n
a_1						
a_2						
…						
a_i				$a_i \circ a_j$		
…						
a_n						

a_i	$\sim a_i$
a_1	$\sim a_1$
a_2	$\sim a_2$
…	…
a_i	$\sim a_i$
…	…
a_n	$\sim a_n$

例 5.3 B = {1, 2}, P(B) = {∅, {1}, {2}, {1, 2}}的二元运算⊕和一元运算~ 的定义如表5.2所示。

⊕	∅	{1}	{2}	{1, 2}
∅	∅	{1}	{2}	{1, 2}
{1}	{1}	∅	{1, 2}	{2}
{2}	{2}	{1, 2}	∅	{1}
{1, 2}	{1, 2}	{2}	{1}	∅

~	
∅	{1, 2}
{1}	{2}
{2}	{1}
{1, 2}	∅

- 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 (函数)的个数。S的每个二元运算$\circ$可以用下表描述。

$\circ$	a	b
a	□	□
b	□	□

- 因为每个空格可以用元素a或b填充, 所以推出存在 $2\cdot2\cdot2\cdot2 = 2^{2\times2} = 16$ 种方法来完成这张表。
- S上不同的二元运算对应着$S \times S \to S$的不同的函数, 因$S \times S \to S$的不同函数共有$|S|^{|S\times S|}$个, 所以 why?
- S上存在$|S|^{|S\times S|}$种不同的二元运算。 S上存在有$|S|^{|S|}$种不同的一元运算, 存在$|S|^{|S\times S\times S|}$种不同的三元运算。

二元运算的性质

- 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。
- 设◦为集合S上的二元运算。

定义 5.3 若∀ x, y ∈ S 有 x◦y = y◦x, 则称◦运算在S上是 可交换的,
也称◦运算在S上满足交换律。

定义 5.4 若∀ x, y, z ∈ S有(x ◦ y) ◦ z = x ◦ (y ◦ z), 则称◦ 运算在S上是可结合的, 也称◦运算在S上满足结合律。

定义 5.5 若∀x ∈ S有x ◦ x = x, 则称◦运算在S上是幂等的,
也称◦运算在S上满足幂等律。

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) $M_n(R)$ ($n \geqslant 2$)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$P(B) = \{x \mid x \subseteq B\}$上的并、交、对称差运算是可交换、可结合的。集合的并和交运算满足幂等律。

(4) S^S上的函数合成运算是可结合的, 一般不是可交换的.

- 以上所有的运算中只有集合的并和交运算满足幂等律, $S \cup S=S$, $S \cap S=S$其他的运算一般说来都不是幂等的.

定义 5.4.2 设◦为S上的二元运算, 如果对于S中任取的n个元素$a_1, a_2, \ldots, a_n$, $n \geqslant 3$, 在$a_1, a_2, \ldots, a_n$中任意加括号所得的运算结果都相等, 则称◦运算在S上是广义可结合的, 或称◦运算在S上适合广义结合律。

- 对于适合广义结合律的二元运算, 通常用$a_1 \circ a_2 \circ \ldots \circ a_n$来表示$a_1, a_2, \ldots, a_n$的运算结果。
- 如果二元运算◦满足交换律与结合律, 则在计算$a_1 \circ a_2 \circ \ldots \circ a_n$时可按照元素的任意次序进行运算。

- 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。和 * 是集合S上的二元运算。

若 $\forall x, y, z \in S$ 有 $x \circ (y * z) = (x \circ y) * (x \circ z)$ 和 $(y * z) \circ x = (y \circ x) * (z \circ x)$成立, 则称。运算对*运算是可分配的, 或称。和 * 运算满足分配律。

定义5.7 若。和*满足交换律且$\forall x, y \in S$有$x \circ (x * y) = x$和 $x * (x \circ y) = x$成立, 则称。和 * 运算是可吸收的, 或称。和 * 运算满足吸收律。 /*2 : 1, $(x * y) \circ x = x$

- 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。

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(≥2)阶实矩阵集合$M_n(R)$上的矩阵乘法对矩阵加法是可分配的;

(3) 幂集P(B)上的并和交是互相可分配的, 并且满足吸收律。$A \cup (A \cap B) = A$;　　$A \cap (A \cup B) = A$　　/* 2 : 1

(4) $\forall a, b \in R$ 有 $a * b = \max\{a, b\}$, $a \circ b = \min\{a, b\}$,

则 * 对 ◦ , ◦ 对 * 分别满足吸收律。

证 $\forall a, b \in R$, $a * (a \circ b) = \max\{a, \min\{a, b\}\} = a$,

$a \circ (a * b) = \min\{a, \max\{a, b\}\} = a$,

因为* 和◦ 是可交换的, * 对◦ , ◦ 对* 分别满足吸收律。

- 除了算律以外, 还有一些和二元运算有关的的特异元素, 如单位 (或幺) 元、零元、逆元和幂等元。

定义 5.8 设 ◦为集合S上的二元运算。若存在e_l (或e_r)∈ S 使得∀x ∈ S都有 e_l ◦ x = x (或x◦e_r = x), 则称e_l (或e_r)是S中关于◦运算的左(或右)单位元。

若 e ∈ S关于◦运算既为左单位元又为右单位元, e◦x = x◦e = x, 则称e为S中关于◦运算的单位元。 ∎

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,

$\theta \circ x = x \circ \theta = \theta$, 则称e为S中关于 $\circ$ 运算的零元。

例 (1) N、Z、Q、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(≥2)阶实矩阵集合$M_n(R)$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(B)中关于并运算的单位元是∅, 零元是B;

而关于交运算的单位元是B, 零元是∅。

(4) S^S中关于函数合成运算的单位元是S上的恒等函数I_S, $I_S(x) = x$。没有零元。

(5) $S = \{a_1, a_2, \ldots, a_n\}$, $n \geqslant 2$。定义S上的二元运算 ◦,

$\forall a_i, a_j \in S$有$a_i \circ a_j = a_i$, 则S中的每个元素都是 ◦ 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◦运算的左零元, 但无零元.

- 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。
- 关于单位元(identity)和零元(zero)存在以下定理。

定理5.1 设◦为集合S上的二元运算, 若存在$e_l \in S$和$e_r \in S$满足$\forall x \in S$有$e_l \circ x = x$和$x \circ e_r = x$, 则 $e_l = e_r = e$, 且e就是S中关于◦运算的惟一的单位元。

(即: S中关于 ◦ 运算的单位元若存在, 则是惟一的!)

证 因为e_r是右单位元, 所以有 $e_l = e_l \circ e_r$;

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。

- 假设关于 ◦ 运算存在另一个单位元 e',

则有 e' = e' ◦ e = e,

所以e是关于 ◦ 运算的惟一的单位元。 ∎

定理 5.2 设$\circ$为集合S上的二元运算, 若存在$\theta_l \in S$和$\theta_r \in S$,

使得$\forall x \in S$有 $\theta_l \circ x = \theta_l$ 和 $x \circ \theta_r = \theta_r$, 则 $\theta_l = \theta_r = \theta$,

且θ是S中关于$\circ$运算的惟一的零元。

证 因为θ_l和θ_r分别是$\circ$的左零元和右零元,

则 $\theta_l = \theta_l \circ \theta_r = \theta_r$。

令 $\theta_l = \theta_r = \theta$, 则 θ是$\circ$的一个零元。

- 设θ'是$\circ$的另一个零元, 则 $\theta' = \theta' \circ \theta = \theta$,

即θ是$\circ$的惟一零元。 ∎

例 二元运算$\circ$有两个左零元, 则$\circ$一定_____。

A. 不满足交换律　　B. 满足交换律

C. 不满足结合律　　D. 满足结合律

解 设θ_1和θ_2是$\circ$两个左零元,

$\theta_1 \circ \theta_2 = \theta_1$,　　$\theta_2 \circ \theta_1 = \theta_2$。

若满足交换律, 则有$\theta_1 = \theta_2$矛盾。

- 故运算$\circ$不满足交换律。应选 A 。 ■

- 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。
- 零元e 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 消灭别人, 见谁灭谁。

例 设S为彩色光的集合, a ◦ b表示两色光a与b混合所得的彩色光。很显然, 白光就是该光谱系统的单位元。

例 一组学生用扳手腕比赛来测定谁的臂力大, 问谁是单位元? 谁是零元?

- 单位元: 臂力最小者, 遇谁输谁。 /*男足
- 零元: 臂力最大者, 见谁灭谁。 /*跳水

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 $y_l \circ x = e$ (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inverse。 ∎

- 对于集合S上的二元运算$\circ$, 单位元e和零元θ 是 global 全局的概念, 是常元, 是对S上的所有元素而言的。
- 逆元是local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** ∘ **e** = **e**。
- 而一般地 (除了|S| = 1), 零元是不可逆的。
- 在任意的代数系统中, 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。
- 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)。

例(1) 整数集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。

(2) n(≥2)阶实矩阵集合$M_n(R)$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}。

(3) 幂集P(B)中关于并运算只有空集∅有逆元,

就是∅本身, B的其他子集没有逆元。

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∘运算的单位元和零元, 则 $e \neq \theta$; 且θ 无左(或右)逆元。

证 假设$e = \theta$, 则 $\forall x \in S$有

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

与S中至少有两个元素矛盾。

假设 若θ有左(或右)逆元x, 那么 $\theta = \theta \circ x$ (或$x \circ \theta$) $= e$,

与$e \neq \theta$矛盾, 故θ无左(或右)逆元。 ■

- 若$|S| = 1$, 其惟一元素既是单位元又是零元。
- 单位元e和零元θ是代数系统中两个比较特殊的元素, 它们在代数系统中占有很重要的地位。

- 如果集合中的所有元素都是关于$\circ$运算的幂等元，则$\circ$运算满足幂等(或等幂idempotent)律。
- 对满足幂等律的运算$\circ$，有$\forall a \in S, a^n = a$, n为正整数。
- 某些二元运算$\circ$尽管不满足幂等律，但仍存在着某些元素x满足$x \circ x = x$，称这样的x是关于$\circ$运算的幂等元。
- 单位元和零元都是幂等元。

例 N、Z、Q、R关于 + 有幂等元0。

- N、Z、Q、R关于 * 有幂等元1, 0。

例 每个集合都是幂集上并运算和交运算的幂等元。

定理 5.4 设◦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◦运算的惟一逆元。

证 $y_l = y_l \circ e = y_l \circ (x \circ y_r) = (y_l \circ x) \circ y_r = e \circ y_r = y_r$。

令 $y_l = y_r = y$, 则y是x关于◦运算的逆元。

- 假设y' 也是x关于◦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◦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。/*充分不必要

例 设$\circ$为实数集R上的二元运算, $\forall x \in R$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

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

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 $x^{-1} = y = \frac{-x}{1-2x} (x \neq \frac{1}{2})$。

- 零元未必是数0, 单位元未必是数1。
- 代数系统(S; •)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。

5. 运算•具有等幂性 ⇔ 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•的等幂元⇔ 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 ⇔ 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。)

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$a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$。

- 零元未必是数0, 单位元未必是数1。

表-1

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

表-2

∘	a	b	e
a	e	e	a
b	b	e	b
e	a	b	e

- 运算表-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

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

- 运算表-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。

例 构造一个代数系统, 使其中只有一个元素具有逆元。

解1 设 $p, q \in I, S = \{x \mid p \le x \le q\}$,

则代数系统(S; min)中有一个单位元是q,

且只有q有逆元, $q^{-1} = q$, 因为min(q, q) = q。

解2 令S = {e, a}, 在S上定义运算*如下表所示, 则 <S, *> 符合要求。

*	e	a
e	e	a
a	a	a

- 与逆元概念密切相关的是可约的(cancelable)概念。
- 下面给出关于二元运算的最后一条算律 – 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 $x, y, z \in S$ (x不是$\circ$运算的零元) 都有

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

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

则称$\circ$运算在S中满足消去律 (称x是可约的)。

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) n(≥2)阶实矩阵集合$M_n(R)$上的矩阵加法适合消去律, 但矩阵乘法不适合消去律。 /*可逆矩阵才可约

(3) 幂集P(B)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。 /*⊕不存在零元

弱定理 若<S, ◦>中 ◦ 运算满足结合律, 且元素a有逆元, 那么a必定是可约的。

证 设a的逆元为a^{-1}, 由$a \circ b = a \circ c$ 及 $b \circ a = c \circ a$ 可得

$a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$ 及 $(b \circ a) \circ a^{-1} = (c \circ a) \circ a^{-1}$

即$(a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$及 $b \circ (a \circ a^{-1}) = c \circ (a \circ a^{-1})$

$\Rightarrow b = c$。因此, a是可约的。 ■

- 本定理之逆并不成立。

反例 <N, +>中, 任一非零元素a均满足

$a + b = a + c \Rightarrow b = c$, (a是左可约的)

$b + a = c + a \Rightarrow b = c$, (a是右可约的),

但a无逆元。

例 5.7 设Σ是有穷字母表, Σ上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|。λ表示空串, |λ| = 0。对任意的k ∈ N, 令

$$\Sigma_k = \{a_{i1}a_{i2}\ldots a_{ik} \mid a_{ij} \in \Sigma\}$$

为Σ上所有长为k的串构成的集合, 那么 $\Sigma_0 = \{\lambda\}$。 ■

- 定义Σ*为Σ上所有串的集合, 则

$$\Sigma^* = \bigcup_{i=0}^{\infty} \Sigma_i, \quad \Sigma^+ = \Sigma^* - \{\lambda\} = \bigcup_{i=1}^{\infty} \Sigma_i 。$$ ■

不难证明Σ_k为有穷集, Σ^* 和 Σ^+ 为可数集。

- 在Σ*上定义二元运算◦, ∀ $w_1, w_2 \in \Sigma^*$, $w_1 = a_1a_2\ldots a_m$, $w_2 = b_1b_2\ldots b_n$ 有 $w_1 \circ w_2 = a_1a_2\ldots a_m\, b_1b_2\ldots b_n$, 称◦为Σ*上的串连接(concatenation)运算。 ■

$\forall w \in \Sigma^*$, $w = a_1a_2\ldots a_m$,

令 $w' = a_ma_{m-1}\ldots a_1$,

则 ’ 运算为Σ^*上的一元运算, 称为求反串(逆)运算。 ■

- 可以证明Σ^*上的串连接运算满足结合律和消去律, 但交换律不成立, 单位元是空串λ。
- $\forall w \in \Sigma^*$, 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 $L_1 = \{(01)^n \mid n \in N\} = \{\lambda, 01, 0101, 010101, \ldots\}$;

$L_2 = \{0^n1^n \mid n \in N\} = \{\lambda, 01, 0011, 000111, \ldots\}$;

$L_3 = \{0^n10^n \mid n \in N\} = \{1, 010, 00100, 0001000, \ldots\}$;

- 都是$\Sigma = \{0, 1\}$上的语言。其中

  L_3是回文语言, 即该语言中的所有字都是回文。
- 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 $\bullet$,

  其中$\bullet$运算是语言的连接运算。

定义 为: $\forall L_1, L_2 \in P(\Sigma^*)$ 有

$$L_1 \bullet L_2 = \{w_1 \circ w_2 \mid w_1 \in L_1 \text{且} w_2 \in L_2\}$$

- 不难证明并和交是可交换、可结合、幂等的,

  而且它们也是互相可分配的、可吸收的。

- 语言连接运算 •在P(Σ*)上是可结合的,

  但交换律不成立, 且 • 运算有单位元 $\Sigma^0 = \{\lambda\}$。

- 在P(Σ*)上还可以定义一元运算’ : C_i

  $\forall L \in P(\Sigma^*)$ 有 $L' = \{w' \mid w \in L\}$。

例 $L = \{0^n1^n \mid n \in N\}$, 则有 $L' = \{1^n0^n \mid n \in N\}$。

- 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Σ = {0, 1}上的镜像语言。

但不是回文语言。