第六章 代数系统

大连理工大学软件学院

陈志奎 教授

办公室: 综合楼405, Tel:

62274392

实验室:综合楼

Mobile: 13478461921

Email: zkchen@dlut.edu.cn zkchen00@hotmail.com

回顾

- 数理逻辑
 - 命题逻辑
 - 谓词逻辑
- 关系理论
 - 集合理论
 - 关系理论
 - 函数理论

什么是代数?

爱因斯坦小时候曾好奇的问他的叔叔: "代数是什么"? (那时候他只学过算术) 他的叔叔回答的很妙: "代数是一种懒惰人的算术,当你不知道某些数时,你就暂时假设它为x、y,然后再想办法去寻找它们。" 道理一经点破,就好象"哥伦布立蛋"的故事一样,人人都会做了。

代数是什么?以符号代替数的解题方法就是代数。 代数是从算术精炼出来的结晶,虽平凡但妙用无穷。 因此它又叫做广义算术(generalized arithmetic) 或进阶算术(advanced arithmetic)或普遍算术 (universal arithmetic)。

代数的由来

Algebra一名来自阿拉伯文al-jabr, al为冠词, jabr之意为恢复或还原,解方程式时将负项移至另一边变成正项,也可说是还原,也有接骨术的意思。

中国在1859年正式使用代数这个名词(李善商在代微积拾级一书中的序中指出"中法之四元,即西法之代数也"),在不同的时期有人用算术作为代数的名称,中国古书九章算术其实是一本数学百科全书,代数问题分见于各章,特别是第八章方程,主要是论述线性(一次)联立方程组的解法,秦九韶(1249)的数书九章中有"立天元一"的术语,天元就是代表未知数,用现在的术语来说就是"设未知数为x"。

代数(Algebra)是数学的其中一门分支,可大致分为初等代数学和抽象代数学两部分。

初等代数学是指19世纪中期以前发展的方程理论, 主要研究某一方程〔组〕是否可解,如何求出方 程所有的根〔包括近似根〕,以及方程的根有何 性质等问题。 抽象代数是在初等代数学的基础上产生和发展起 来的。它起始于十九世纪初,形成于20世纪30年 代。在这期间,挪威数学家阿贝尔(N.H. Abel)、 法国数学家伽罗瓦(E'. Galois)、英国数学家德·摩 根(A. De Morgan)和布尔(G. Boole)等人都做出了 杰出贡献,荷兰数学家范德瓦尔登(B.L. Van Der Waerden)根据德国数学家诺特(A.E. Noether)和奥 地利数学家阿廷(E. Artin)的讲稿,于1930年和 1931年分别出版了《近世代数学》一卷和二卷, 标志着抽象代数的成熟。

代数系统是以研究数字、文字和更一般元素的运算的规律和由这些运算适合的公理而定义的各种数学结构的性质为中心问题。它对现代数学如扑拓学、泛函分析等以及一些其他科学领域,如计算机科学、编码理论等,都有重要影响和广泛地应用。

- 第六章 代数系统基本概念及性质
- 6.1 代数系统的定义
- 定义6.1.1 设S是个非空集合且函数 $f: S^n \rightarrow S$,则称f为S上的一个n元运算。其中n是自然数,称为运算的元数或阶。
- 当n = 1时,称f为一元运算,当n = 2时,称f为二元运算,等等。
- 注意到,n元运算是个闭运算,因为经运算后产生的象仍在同一个集合中。封闭性表明了n元运算与一般函数的区别之处。此外,有些运算存在幺元或零元,它在运算中起着特殊的作用,称它为S中的特异元或常数。

运算的例子很多。例如,在数理逻辑中,否定是谓词集合上的一元运算,合取和析取是谓词集合上的二元运算;在集合论中,并与交是集合上的二元运算;在整数算术中,加、减、乘运算是二元运算,而除运算便不是二元运算,因为它不满足封闭性。

运算表:表示有穷集上的一元和二元运算

0	a_1 a_2	a_n
a_1	$a_1 \circ a_1 \ a_1 \circ a_2 \ \dots$	$a_1 \circ a_n$
a_2	$a_2 \circ a_1 \ a_2 \circ a_2 \ \dots$	$a_2 \circ a_n$
•	•••	
•		
•		
a_n	$a_n \circ a_1 \ a_n \circ a_2 \dots$	$a_n o a_n$

	oa_i		
a_1	o a_1		
$\begin{vmatrix} a_1 \\ a_2 \end{vmatrix}$	$\circ a_2$		
•	•		
•	•		
•	•		
a_n	$\circ a_n$		

二元运算的运算表

一元运算的运算表

- 在本章讨论的代数结构中,主要限于一元和二元运算。将用 ′、¬或 等符号表示一元运算符;用⊕、⊗、⊙、*、∨、∧、□、□等表示二元运算符。一元运算符常常习惯于前置、顶置或肩置,如¬x、、x′;而二元运算符习惯于前置、中置或后置,如:+xy,x + y,xy +。
- 有了集合上运算的概念后,便可定义代数系统了。

定义6.1.2 设S是个非空集合且 f_i 是S上的 n_i 元运算,其中i=1, 2, ..., m。由S及 f_1 , f_2 , ..., f_m 组成的结构,称为代数系统,记作

< S, f_1 , f_2 , ..., $f_m > 0$

- 此外,集合S的基数即/S/定义代数系统的基数。如果S是有限集合,则说代数结构是有限代数系统; 否则便说是无穷代数系统。
- 有时,要考察两个或多个代数系统,这里就有个是否同类型之说,请看下面定义:

定义6.1.3 设两个代数系统

<S, f_1 , f_2 , ..., $f_m>$ 和

<T, g_1 , g_2 , ..., $g_m>$, 如果 f_i 和 g_i ($1 \le i \le m$)具有相同的元数,则称这两个代数系统是同类型的。

可见,判定两个代数系统是否同类型,主要是对其运算进行考察。

此外,有时还需要在代数系统中集合的某个子集上讨论其性质,这就引出子代数结构的概念。

• 定义6.1.4 设<S, f_1 , f_2 , ..., f_m >是一代数系统,且非空集T $\subseteq S$ 在运算 f_1 , f_2 , ..., f_m 作用下是封闭的,则称<T, f_1 , f_2 , ..., f_m >为代数系统

<S, f_1 , f_2 , ..., f_m >的子代数,记为<T, f_1 , f_2 , ..., f_m >。

- 下面举例说明上述各个概念。
- 例6.1.1 设R是实数集合,且+和×是R上的普通加法和乘法运算,则<R,+,×>是一代数系统。因为运算+和×在R中是封闭的。
- 例6.1.2 设S是非空集合,P(S)是它的幂集。对任意集合A,B∈P(S)上的运算⊕和⊗如下:
- $A \oplus B = (A B) \cup (B A)$
- $A \otimes B = A \cap B$
- ・则<P(S),⊕,⊗>是一代数系统。因为,显然⊕和⊗是闭运算。

• 例6.1.3 设Σ是由有限个字母组成的集合, 称为 字母表。由 Σ 中的字母组成的有序集合,称为 Σ 上的串。串中的字母个数m称为该串的长度。m = 0时,叫做空串,用 λ 表示之。用 Σ^* 表示 Σ 上的 串集合。在 Σ^* 上定义一个并置或者连接运算, 用 // 表示之。如 α 、 $\beta \in \Sigma^*$,则 α // $\beta = \alpha\beta$ 。那么, $<\Sigma^*$,//>是一代数系统。如果 \diamondsuit $\Sigma^{+=}\Sigma^*-\{\lambda\}$,则 $<\Sigma^+$, //>也是一个代数系统。

- 例6.1.4 设有一台字长为8位的计算机,它以定点加、减、乘、除以及逻辑加和逻辑乘为运算指令,并分别用 O_1 , O_2 ,…, O_6 表示之。则在计算机中由 2^8 个不同数字所组成集合S同该机中运算指令构成一代数结构< S, O_1 , O_2 ,…, O_6 >。
- 在结束本节时,声明记号
- <*S*, f_1 , f_2 , ..., $f_m >$ 即为一代数系统,除特别指明外,运算符 f_1 , f_2 , ..., f_m 均为二元运算。根据需要对S及 f_1 , f_2 , ..., f_m 可置不同的集合符和运算符。

• 6.2 代数系统的基本性质

对于代数系统的性质的考察方法不是一个一个研究各个结构,而是列举一组性质,并且对于具有这些性质的任何代数结构推导可能的结论。把那些被选出的性质看成是公理并且由这些公理推导出的任何有效结论,对于满足这些公理的任何代数结构也都必定成立。

• 因此,为了作出这样的讨论,将不考虑任何 特定的集合,也不给所涉及到的运算赋予任 何特定的含义。这种系统的集合及集合上的 诸运算仅仅看成是一些符号,或更确切地说, 它们都是些抽象对象。因此,与此相应的代 数系统,通常称为抽象代数。对于那些特定 的代数系统只能是具有基本性质中的某些性 质。

- 6.2.1结合律
- 给定<S, \odot >,运算" \odot "满足结合律或" \odot " 是可结合的, $(\forall x)(\forall y)(\forall z)(x,y,z \in S \rightarrow (x \odot y) \odot z = x \odot (y \odot z))$ 。
- ・ 例6.2.1 给定<A,⊙>且对任意a,b ∈ A有 a ⊙ b = b ⊙ 证明运算"⊙"是可结合的。
- 6.2.2交换律
- 给定<S, $\bigcirc>$,运算" \bigcirc "满足交换律或" \bigcirc " 是可交换的: $(\forall x)(\forall y)(x,y) \in S \rightarrow x \bigcirc y = y \bigcirc x$)。

- 例6.2.2 给定< Q, *>, 其中Q为有理数集合,并且对任意a, $b \in Q$ 有a*b = a + b a b, 问运算* 是否可交换?
- 可见,如果一代数结构中的运算②是可结合和可交换的,那么,在计算 a_1 ② a_2 ②…③ a_m 时可按任意次序计算其值。特别当 $a_1 = a_2 = ... = a_m = a$ 时,则 a_1 ③ a_2 ②…② $a_m = a^m$ 。称 a^m 为a的m次幂, a_n 0的指数。下面给出 a^m 的归纳定义:
- 设有<*S*, \bigcirc >且a∈S。对于m∈N⁺,其中N⁺表示正整数集合,可有
- (1) $a^1 = a$
- (2) $a^{m+1} = a^m \odot a$

- 由此利用归纳法不难证明指数定律:
- (1) $a^m \odot a^n = a^{m+n}$
- (2) $(a^m)^n = a^{mn}$
- 这里, $m, n \in \mathbb{N}^+$ 。
- 似地定义某代数结构中的负幂和给出负指数定律。

- 6.2.3分配律
- 一个代数结构若具有两个运算时,则分配律可建立这两个运算之间的某种联系。
- 给定<S, \bigcirc ,*>,运算 \bigcirc 对于*满足左分配律,或者 \bigcirc 对于*是可左分配的,即 $(\forall x)(\forall y)(\forall z)(x,y)$, $z \in S \rightarrow x \bigcirc (y*z) = (x \bigcirc y)*(x \bigcirc z))。$
- 运算 \odot 对于*满足右分配律,或者 \odot 对于*是可右分配的,即 $(\forall x)(\forall y)(\forall z)(x, y, z \in S \rightarrow (y*z) \odot x$ = $(y \odot x)*(z \odot x))$ 。

• 类似地可定义*对于①是满足左或右分配律。

若⊙对于*即满足左分配律又满足右分配律, 则称⊙对于*满足分配律或是可分配的。同 样可定义*对于⊙满足分配律。

- 由定义不难证明下面定理:
- 定理6.2.1 给定<*S*,⊙,*>且⊙是可交换的。如果⊙对于*满足左或右分配律,则⊙对于*满足分配律。
- 例6.2.3 给定<*B*, \bigcirc ,*>,其中 $B=\{0, 1\}$ 。表 6.2.1分别定义了运算 \bigcirc 和*,问运算 \bigcirc 对于*是可分配的吗?*对于 \bigcirc 呢?

表6.2.1

0	0	1	
0	0	0	
1	0	1	

*	0	1	
0	0	1	
1	1	1	

• 形如表6.2.1的表常常称为运算表或复合表,它由运算符、行表头元素、列表头元素及复合元素四部分组成。对于集合S的基数很小,特别是2或3时,代数结构中运算常常用这种表给出。优点是简明直观,一目了然。

- 6.2.4吸收律
- · 给定<S, ⊙, *>, 则
- \bigcirc 对于*满足左吸收律: $(\forall x)(\forall y)(x, y) \in S \rightarrow x \bigcirc (x^*y) = x)$
- \bigcirc 对于*满足右吸收律: $(\forall x)(\forall y)(x, y) \in S \rightarrow (x*y) \bigcirc x = x)$
- 若⊙对于*既满足左吸收律又满足右吸收律,则称⊙对于*满足吸收律或者可吸收的。
- •*对于①满足左、右吸收律和吸收律类似地定义。
- 若⊙对于*是可吸收的且*对于⊙也是可吸收的, 则⊙和*是互为吸收的或⊙和*同时满足吸收律。

- 例6.2.4 给定<N, ⊙, *>, 其中N是自然数集合,
 ⊙和*定义如下:
- 对任意a, $b \in N$ 有 $a \odot b = max\{a, b\}$, $a*b = min\{a, b\}$, 试证, \odot 和*互为吸收的。
- 6.2.5等幂律与等幂元
- · 给定<S, ⊙>, 则
- "①"是等幂的或"①"满足等幂律: $(\forall x)(x \in S \rightarrow x \odot x = x)$
- 给定<S, \odot >且 $x \in$ S,则
- x是关于"⊙"的等幂元: x⊙x = x

- 于是,不难证明下面定理:
- 定理6.2.2 若x是<S, \odot >中关于 \odot 的等幂元, 对于任意正整数n, 则 $x^n = x$ 。
- 例6.2.5 给定<P(S), ∪ , \cap >,其中P(S)是集合S 的幂集, \cup 和 \cap 分别为集合的并和交运算。
- · 验证: U和∩是等幂的。

- 6.2.6幺元或单位元
- 给定<S, $\bigcirc>$ 且 e_1 , e_r , $e \in S$, 则
- e_l 为关于①的左幺元:($\forall x$)($x \in S \rightarrow e_l$ ①x = x)
- e_r 为关于①的右幺元:($\forall x$)($x \in S \rightarrow x \odot e_r = x$)
- 若e既为⊙的左幺元又为⊙的右幺元,称e为关于⊙的幺元。亦可定义如下:
- e为关于①的幺元: $(\forall x)(x \in S \rightarrow e \bigcirc x = x \bigcirc e = x)$ 。

• 例6.2.6 给定<{α, β}, *>, 表6.2.2, 表6.2.3和表6.2.4分别给出*的不同定义的运算表, 试指出左 幺元、右幺元及幺元。

•	表6	.2.2	表6.2.	3	表6.2.4	
•	*	αβ	*	α β	*	α β
•	α	αβ	α	α α	α	ββ
•	β	ββ	β	ββ	β	αβ

- 定理6.2.3 给定<S, \odot >且 e_l 和 e_r 分别关于 \odot 的左、右幺元,则 e_l = e_r =e且幺元e惟一。
- 6.2.7零元
- 给定 $\langle S, * \rangle$ 及 $\theta_I, \theta_r, \theta \in S, 则$
- θ_l 为关于*的左零元: $(\forall x)(x \in S \rightarrow \theta_l^* x = \theta_l)$
- θ_r 为关于*的右零元: $(\forall x)(x \in S \rightarrow x^*\theta_r = \theta_r)$
- θ 为关于*的零元: $(\forall x)(x \in S \rightarrow \theta^*x = x^*\theta = \theta)$

- 例6.2.7 在例6.2.6中,*如表6.2.2所定义,β是*的零元; *如表6.2.3所定义,α和β都是*的左零元; *如表6.2.4所定义,β是*的右零元。
- 定理6.2.4 给定<S, \odot >且 θ_l 和 θ_r 分别为关于 \odot 的 左零元和右零元,则 θ_l = θ_r = θ 且零元 θ 是惟一的。
- 定理6.2.5 给定<S, $\bigcirc>$ 且|S|>1。如果 θ , $e \in S$,其中 θ 和e分别为关于 \bigcirc 的零元和幺元,则 $\theta \neq e$ 。

- 6.2.8逆元
- 给定<S, $\bigcirc>$ 且幺元e, $x \in S$,则
- x为关于 \odot 的左逆元: $(\exists y)(y \in S \land x \bigcirc y = e)$
- x为关于 \odot 的右逆元: $(\exists y)(y \in S \land y \bigcirc x = e)$
- x为关于①可逆的: $(\exists y)(y \in S \land y \bigcirc x = x \bigcirc y = e)$
- 给定<S, $\bigcirc>$ 及幺元e; x, $y \in S$, 则
- y为x的左逆元: $y \odot x = e$
- y为x的右逆元: $x \odot y = e$
- y为x的逆元: $y \odot x = x \odot y = e$

- ·显然,若y是x的逆元,则x也是y的逆元,因此称 x与y互为逆元。通常x的逆元表为x-1。
- 一般地说来,一个元素的左逆元不一定等于该元素的右逆元。而且,一个元素可以有左逆元而没有右逆元,反之亦然。甚至一个元素的左或右逆元还可以不是惟一的。
- 例6.2.8 给定<S,*>,其中 $S=\{\alpha, \beta, \gamma, \delta, \zeta\}$ 且 *的定义如表6.2.5所示。试指出该代数结构中各元素的左、右逆元情况。

表6.2.5 βγδζ βγδζ α α δ α γ α β α β δ δ α γ δ γ

δ α γ ζ

- 定理**6.2.6** 给定<S,O>及幺元 $e \in S$ 。如果O是可结合的并且一个元素x的左逆元 x_i -1和右逆元 x_r -1存在,则 x_i -1= x_r -1。
- 定理6.2.7 给定<S, \bigcirc >及幺元e \in S。如果 \bigcirc 是 可结合的并且x的逆元x-1存在,则x-1是惟一的。
- 例如在例6.1.1中,显然< R,+, $\times >$ 中运算+和 \times 都是可结合的,而1和0分别为 \times 和+的幺元,故可验证,对于 \times 来说,除0外每个元素 $r \in R$ 都有逆元1/r;对于+而言,对每个元素 $r \in R$ 都有逆元(-r)。

- 6.2.9可约律与可约元
- 给定<S, \odot >且零元 $\theta \in S$,则
- \bigcirc 满足左可约律或是左可约的: $(\forall x)(\forall y)(\forall z)((x), y)$, $z \in S \land x \neq \theta \land x \bigcirc y = x \bigcirc z) \rightarrow y = z)$, 并称x是关于 \bigcirc 的左可约元。
- \bigcirc 满足右可约律或是右可约的: $(\forall x)(\forall y)(\forall z)((x), y)$, $z \in S \land x \neq \theta \land y \odot x = z \odot x) \rightarrow y = z)$, 并称x是关于 \bigcirc 的右可约元。
- 若○既满足左可约律又满足右可约律或○既是左可约又是右可约的,则称⊙满足可约律或⊙是可约的。

- 若x既是关于⊙的左可约元又是关于⊙的右可约元元,则称x是关于⊙的可约元。可约律与可约元也可形式地定义如下:
- \bigcirc 满足可约律: $(\forall x)(\forall y)(\forall z)(x, y, z \in S \land x \neq \theta \land ((x \bigcirc y = x \bigcirc z \lor y \bigcirc x = z \bigcirc x) \rightarrow y = z))$
- 给定<S, \odot >且零元 θ , $x \in S$ 。
- x是关于 \odot 的可约元: $(\forall y)(\forall z)(y, z \in S \land x \neq \theta \land ((x \odot y) = x \odot z \lor y \odot x = z \odot x) \rightarrow y = z))$ 。

- 例6.2.9 给定<Z, ×>, 其中Z 是整数集合, × 是一般乘法运算。显然,每个非零整数都是可约 元,而且运算×满足可约律。
- 定理6.2.8 给定<S,*>且*是可结合的,如果x是 关于*可逆的且 $x \neq \theta$,则x也是关于*的可约元。
- 最后,作一补充说明,用运算表定义一代数结构的运算,从表上能很好地反映出关于运算的各种性质。为确定起见,假定<S,*>及x,y, θ , $e \in S$ 。

- (1)运算*具有封闭性,当且仅当表中的每个元素都属于S。
- (2)运算*满足交换律,当且仅当表关于主对角线是对称的。
- (3)运算*是等幂的,当且仅当表的主对角线上的每个元素与所在行或列表头元素相同。

- (4)元素x是关于*的左零元,当且仅当x所对应的行中的每个元素都与x相同;元素y是关于*的右零元,当且仅当y所对应的列中的每个元素都与y相同;元素θ是关于*的零元,当且仅当θ所对应的行和列中的每个元素都与θ相同。
- (5)元素x为关于*的左幺元,当且仅当x所对应的行中元素依次与行表头元素相同;元素y为关于*的右幺元,当且仅当y所对应的列中元素依次与列表头元素相同;元素e是关于*的幺元,当且仅当e所对应的行和列中元素分别依次地与行表头元素和列表头元素相同。

• (6)x为关于*的左逆元,当且仅当位于x所在行的元素中至少存在一个幺元,y为关于*的右逆元,当且仅当位于y所在列的元素中至少存在一个幺元; x与y互为逆元,当且仅当位于x所在行和y所在列的元素以及y所在行和x所在列的元素都是幺元。

代数系统。	么走。	零元.	等幂元。	逆元。	可约元。
< R, +> .,	0.,	无.,	0.,	相反数。	任何元素。
< R,×>.,	1.,	0.1	1 . 0.,	除0外,为其	除 0 外的任
				倒数。	何元素。
$<\rho(S),\cap>$.	S.,	Ø.,	任何元素。	除S外,其余	S.,
				元素均不可	
				逆	
$< \rho(S), \cup >$	Ø. ₁	S.,	任何元素。	除②外,其余	Ø.,
				元素均不可	
				逆。	
< <i>P</i> , ∧>.,	T .1	F_{α}	任何元素。	除工外,其余	T .1
				元素均不可	
				逆。	
< <i>P</i> ,∨>	F_{α}	T	任何元素。	除下外,其余	F_{α}
				元素均不可	
				逆。	
< f, 0 >	$I_{x^{(i)}}$	无。	$I_{x^{\beta}}$	其反函数。	所有双射函
f是从n☆	恒等函数。				数.,
元素到自身					
的双射函数。					

作业

• 149页,2-8