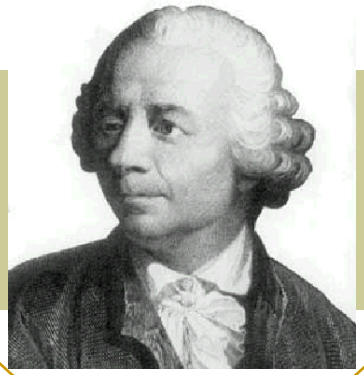
南京大学
NANJING UNIVERSITY



离 散 数 学
Discrete Mathematics

第十一讲：代数系统引论

吴 楠
南京大学计算机科学与技术系

2020 年 11 月 16 日

前 情 提 要

- 数学归纳法
- 强数学归纳法
- 递归的定义
- 函数的递归结构与结构归纳法

本讲主要内容

- 运算及其封闭性
- 运算的性质
- 运算表
- 代数系统
- 代数系统的性质
  - 结合性、交换性、分配性
  - 单位元、零元、逆元
- 代数系统的同构与同态

Abū ʿAbdallāh Muḥammad ibn Mūsā al-Khwārizmī (B.C. 780 – 850 ?)

Arab mathematician, born in Khwarizm(now in Uzbekstan). His works on algebra, arithmetic, and astronomical tables greatly advanced mathematical thought, and he was the first to use for mathematical purposes the expression *al jabr*, from which the English word *algebra* is derived. The Latin version of his treatise on algebra was responsible for much of the mathematical knowledge of medieval Europe. His work on algorithm, a term derived from his name, introduced the method of calculating by use of Arabic numerals and decimal notation.

— — **from Funk & Wagnalls:** ***New Encyclopedia***

实际上，*al jabr* 一词出自他的著名的书“Kitab al jabr w'al-muqabala”(《复原和化简的规则》)的标题,这个词在阿拉伯语中意思相当于“reunite”。

而中文“代数”一词作为学科名，首先出现于在华的英国人维列利于1853年为介绍西方数学而写的《数学启蒙》(1853)，此时距离Al-Khwarizmi那本书的出版已经超过一千年了。几年后，维列利与中国学者李善兰合作，先后将欧几里德《几何原本》后9卷以及德·摩根的代数学翻译成中文。

引 子（续）

- 代数系统一般称为“抽象代数（abstract algebra）”或者“近世代数（modern algebra）”，20世纪初被命名，但其研究的主要内容却肇始于19世纪早期
- 代数系统研究的主要内容：代数结构、群、环、域、模、向量空间、格、布尔代数、李代数、张量代数 等

运算的函数定义

- 函数$f: A^n \to B$称为(从A到B的) n元运算以下主要讨论二元运算
  - 例如：利用普通四则运算定义实数集上的一个新运算 “$*$” ：

$$x * y = x + y - xy$$

则：$2 * 3 = -1$；$0.5 * 0.7 = 0.85$

- 有限集合上的m元运算的个数是确定的

运 算 表

- 通常用于定义有限集合(一般元素很少)上的一元或二元运算 (如在集合$\{a, b, c, d\}$上定义如下的运算$*$)

*	a	b	c	d
a	1	®	✱	M
b	&	6	K	M
c	7	6	Q	0
d	G	#	~	◘

运算的封闭性

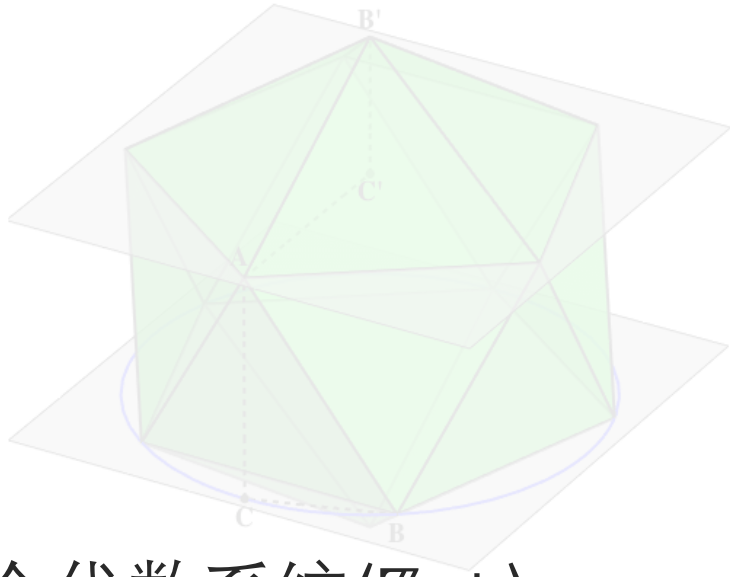
- 对于运算$f: A^n \to B$，若$B \subseteq A$，则称该运算在集合A上封闭（closeness）
- 例：
  - 加法在自然数集上封闭，但减法在自然数集上不封闭
  - 减法在整数集上封闭，但除法在整数集上不封闭
  - 对集合$A = \{1,2,3,\cdots,10\}$，gcd运算封闭，lcm则否

证明运算封闭的例子

- 普通加法在正整数集的子集 $A=\{n|9|21n\}$ 上封闭
- 证明：
  - 设x,y是A中任意2个元素，存在$p,q\in\mathbb{Z}^+$，满足：$21x=9p$，$21y=9q$，则$21(x+y)=9(p+q)$，由于$p+q\in\mathbb{Z}^+$，故$9|21(x+y)$，即$x+y\in A$. □

代 数 系 统

- 定义（代数系统）：
  - 给定1个非空集合（其元素可以是任何对象）；
  - 给定1个或者若干个运算（以下主要讨论存在1个二元运算的情况）；
  - 运算对上述集合封闭.
- 记法：$\langle S, \circ \rangle$
- 例子：
  - 整数集与普通加法构成一个代数系统$\langle \mathbb{Z}, + \rangle$



一个较复杂的代数系统的例子

- 设集合$S = \mathbb{R} - \{0,1\}$，定义S上的6个函数如下：
  - $f_1(x) = x$, $f_2(x) = (1-x)^{-1}$
  - $f_3(x) = x^{-1}(x-1)$, $f_4(x) = x^{-1}$
  - $f_5(x) = x(x-1)^{-1}$, $f_6(x) = 1-x$
- 则$\langle\{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ\rangle$是代数系统，其中$\circ$是函数的复合运算

只需考虑运算的封闭性。例如：$f_2 \circ f_3 = f_1$, $f_4 \circ f_5 = f_2$, $f_3 \circ f_6 = f_4$等

（注：此处采用复合左先制，即$f \circ g(x) = g(f(x))$，易验证右先制依然满足封闭性）

函数本身作为运算对象

- 在集合 $S = \mathbb{R} - \{0,1\}$上定义函数如下：
  - $f_1(x) = x,$ $f_2(x) = (1-x)^{-1}$
  - $f_3(x) = x^{-1}(x-1),$ $f_4(x) = x^{-1}$
  - $f_5(x) = x(x-1)^{-1},$ $f_6(x) = 1-x$
- 要证明$f_4 \circ f_5 = f_2$，需证：$\forall x \in S, f_5(f_4(x)) = f_2(x)$

$$f_5(f_4(x)) = f_5\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)\left(\frac{1}{x}-1\right)^{-1} = \left(\frac{1}{x}\right)\left(\frac{x}{1-x}\right) = \left(\frac{1}{1-x}\right)$$

结合性（associativity）

- 集合A上的运算$\circ$具有结合性定义为：

$$\forall x, y, z \in A, (x \circ y) \circ z = x \circ (y \circ z)$$

- 如果$\circ$满足结合性，表达式$x_1 \circ x_2 \circ \cdots \circ x_n$可以在保持诸$x_i$先后次序不变的前提下按照任何顺序进行计算

交换性（commutativity）

- 集合A上的运算$\circ$具有交换性定义为：

$$\forall x, y \in A, x \circ y = y \circ x$$

- 如果$\circ$同时满足交换律和结合律，表达式

$x_1 \circ x_2 \circ \cdots \circ x_n$可以按照任何顺序进行计算，

包括可以随便重新排列诸x_i的先后次序

分配性（distributivity）

- 分配性涉及两个不同的运算
- 集合A上的运算$\circ$对$*$满足分配性定义为：

$$\forall x, y, z \in A, x \circ (y * z) = (x \circ y) * (x \circ z)$$

单位元（identity element）

- 对于实数集$\mathbb{R}$上的普通乘法$(\cdot)$，实数1满足

  对任意实数$x \in \mathbb{R}$，有$1 \cdot x = x \cdot 1$

- 元素e是代数系统$\langle S, \circ \rangle$的单位元当且仅当

$$\forall x \in S, e \circ x = x \circ e = x$$

- 单位元可记为$\mathbf{1}_S$，或简记为$\mathbf{1}$（读作么）
- 代数系统不一定有单位元

左单位元和右单位元

- e_L称为系统的左单位元(或左幺)当且仅当

$$\forall x \in S, e_L \circ x = x$$

- 可以相应地定义系统的右单位元(右幺) e_R

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

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

关于单位元的进一步讨论

- 左、右单位元不一定存在
- 左、右单位元不一定唯一
- 假设一个代数系统同时有左、右单位元，则左、右单位元必相等且唯一；即系统的单位元（幺元）
  - $e_L = e_L \circ e_R = e_R$
- 系统若有单位元，必是唯一的
  - $e_1 = e_1 \circ e_2 = e_2$

逆 元（inverse element）

- 只对存在单位元的代数系统讨论逆元
- 给定系统S中的元素x，若存在S中的元素x'，满足$x' \circ x = \mathbf{1}_S$，则称$x'$是$x$的左逆元；若存在$x''$，满足$x \circ x'' = \mathbf{1}_S$，则称$x''$是$x$的右逆元
- 给定系统S中的元素x，如果存在S中的元素x^*，满足$x \circ x^* = x^* \circ x = \mathbf{1}_S$，则称$x^*$是$x$的逆元，一般记为$\boldsymbol{x^{-1}}$
  - 逆元既是左逆元，又是右逆元
  - 如果y是x的逆元，则x也是y的逆元

一个关于逆元的例子

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

- 注意：

(1) b的左、右逆不同；

(2) c有2个右逆，无左逆；

(3) d有左逆，无右逆

关于逆元的进一步讨论

- 如果代数系统$\langle S,\circ\rangle$具有结合性：
  - 若给定的元素既有左逆，又有右逆，二者必相等且唯一
    - 假设x的左逆是x'，右逆是x''：

$$x' = x' \circ \mathbf{1}_S = x' \circ (x \circ x'') = (x' \circ x) \circ x'' = \mathbf{1}_S \circ x'' = x''$$

  - 若每个元素均有左逆，则左逆即右逆，且逆元唯一
    - 任给S中元素a，设a的左逆是b，b的左逆是c，则

$$a \circ b = (\mathbf{1}_S \circ a) \circ b = \big((c \circ b) \circ a\big) \circ b$$

$$= \big(c \circ (b \circ a)\big) \circ b = (c \circ \mathbf{1}_S) \circ b = c \circ b = \mathbf{1}_S$$

零 元

- 对于实数集上的普通乘法$(\cdot)$，实数0满足

  对任意实数x，$0 \cdot x = x \cdot 0 = 0$

- 元素t是代数系统$\langle S, \circ \rangle$的零元当且仅当

$$\forall x \in S, t \circ x = x \circ t = t$$

- 零元可记为$\mathbf{0}_S$，或简记为$\mathbf{0}$
- 一个代数系统不一定存在零元

一个例子

- 利用普通加减法和乘法定义实数集上的二元运算“$\circ$”如下：

$$\forall x, y \in \mathbb{R}, x \circ y = x + y - xy$$

  - 交换性：显然
  - 结合性：$(x \circ y) \circ z = x \circ (y \circ z) = x + y + z - xy - xz - yz + xyz$
  - 单位元：0；零元：1
  - $x\ (x \neq 1)$ 的逆元为：$\frac{x}{x-1}$，1无逆元

一个与编码有关的代数系统

- 设字母表$A=\{0,1\}$，A^*是A上的长度为n的字符串的集合
- 定义A^*上的运算$\oplus$如下：

  $\forall x,y\in A^*$，$x\oplus y$是长度为n的二进数字串，第i位$(i=0,1,\cdots,n-1)$为1当且仅当x,y的相应位互异
- $\langle A^*,\oplus\rangle$是代数系统
- 该系统满足：结合性、交换性、有单位元、每个元素均有逆元

“相似”的系统

- 比较$\langle\{F,T\},\vee\rangle$（逻辑或）与$\langle\{0,1\},+\rangle$（布尔和）两代数系统：

$\vee$	F	T
F	F	T
T	T	T

$+$	0	1
0	0	1
1	1	1

- 若不考虑符号的形式及其含义，则两系统的“本质”没有差别

同构与同构映射

- 代数系统$\langle S_1,\circ\rangle$与$\langle S_2,*\rangle$同构（isomorphism）（记$S_1 \cong S_2$）当且仅当存在双射函数$f: S_1 \to S_2$，满足：$\forall x, y \in S_1, f(x \circ y) = f(x) * f(y)$。其中的双射函数$f$称作同构映射
- 同构关系是等价关系

同态与同态映射

- 只有两个代数系统的集合等大，它们才可能同构
- 代数系统$\langle S_1,\circ\rangle$与$\langle S_2,*\rangle$同态（homomorphism，记$S_1 \sim S_2$)当且仅当存在函数$f: S_1 \to S_2$，满足：

$$\forall x, y \in S_1, f(x \circ y) = f(x) * f(y)$$

- 特别地，若上述f是满射，则称两系统满同态(epimorphism)
- 例：整数加系统 $\langle \mathbb{Z}, + \rangle \sim \langle \mathbb{Z}_3, \oplus_3 \rangle$ （模3剩余加系统）
  - 同态映射：$f: \mathbb{Z} \to \mathbb{Z}_3, f(3k + r) = r$

课堂练习题

- 设代数系统$\boldsymbol{Z}_n = \langle \mathbb{Z}_n, \oplus_n \rangle$，$\oplus_n$为模$n$剩余加，$f: \boldsymbol{Z}_{12} \to \boldsymbol{Z}_3$，$f(x) = x \bmod 3$. 证明：$f$满同态

证明：

设$\oplus_{12}$和$\oplus_3$分别表示模 12 和模 3 加法，则有：

$$f(x \oplus_{12} y) = (x \oplus_{12} y) \bmod 3 = \big((x + y) \bmod 12\big) \bmod 3$$

$$= (x + y) \bmod 3 = (x \bmod 3) \oplus_3 (y \bmod 3) = f(x) \oplus_3 f(y)$$

显然，对于$\boldsymbol{Z}_{12}$的幺元$e_{12} = 0$，有$f(e_{12}) = e_3 = 0$，且$\operatorname{ran} f = \boldsymbol{Z}_3$

故f为从$\boldsymbol{Z}_{12}$到$\boldsymbol{Z}_3$的满同态映射。 □

代数系统部分参考教材

- 注：上述教材中有关格、布尔代数和群论部分的扫描文件（PDF格式）请在课程网站上最上面的“公共资源区”→“电子版教材”中下载

本次课后作业

- 教材内容：[屈婉玲] 9.1，9.2，9.3节
- 课后习题：
  - Problem Set 11
- 提交时间：11月23日

进程代数（Process Algebra）

进程代数是关于通信并发系统的代数理论的统称。20世纪70年代后期，英国学者提出了通信系统演算和通信顺序进程，开创了用代数方法研究通信并发系统的先河。 此后这一研究方向兴盛不衰，出现了众多类似而又相互区别的演算系统，如ACP，ATP，LOTC6等，统称为进程代数。这些代数理论都使用通信——而不是共享存储——作为进程之间相互作用的基本手段，表现出面向分布式系统的特征。 在语法上，进程代数用一组算子作为进程的构件。算子的语义通常用结构化操作语义方法定义， 这样进程就可看成是带标号的变迁系统。进程代数 的一个显著特征是把并发性归结为非确定性，将并发执行的进程的行为看成是各单个进程的行为的所 有可能的交错合成，即所谓交错语义。进程代数研究的核心问题是进程的等价性，即在什么意义下两个进程的行为相同?在进程代数领域使用的最为广泛的等价关系有互模拟、测试等价、失败等价(参见通信顺序进程)等。对这些语义等价 关系均建立了相应的公理系统。关于公理系统的研 究不仅加深了对语义理论的理解，而且使得有可能 对语义等价关系进行形式推理。为了将进程代数的理论成果应用于解决实际问题，20世纪80年代后期出现了许多计算机支持工具。用这些工具可对进程的行为进行推理或模拟。