代数系统引论

离散数学教学组

回顾

- 递归数列
- 函数“增长”

提要

- 运算及其封闭性
- 运算的性质
- 运算表
- 代数系统
- 代数系统的同构与同态

引子

- 代数系统一般称为“抽象代数（abstract algebra）”或“近世代数”，20世纪初被命名，但其研究的主要内容却于19世纪便已开展
- 代数系统研究的主要内容：有代数结构、群、环、域、模、向量空间、格、布尔代数、李代数等等

运算的函数定义

- 函数$f: A^n \to B$称为(从A到B的) $\boldsymbol{n}$**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$\boldsymbol{B \subseteq A}$，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之子集$A = \{n|9|21n\}$上封闭
- 证明：
  - 设x, y是A中任意元素，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：$\langle \mathbb{Z}, + \rangle$构成代数系统

例子

- 设集合$S = \mathbb{R} - \{0,1\}$，定义S上的6个函数如下：
  - $f_1(x) = x,$ $\quad f_2(x) = (1 - x)^{-1}$
  - $f_3(x) = x^{-1}(x - 1),$ $\quad f_4(x) = x^{-1}$
  - $f_5(x) = x(x - 1)^{-1},$ $\quad f_6(x) = 1 - x$
- 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

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：
  - $f_1(x)=x$, $\quad f_2(x)=(1-x)^{-1}$
  - $f_3(x)=x^{-1}(x-1)$, $\quad f_4(x)=x^{-1}$
  - $f_5(x)=x(x-1)^{-1}$, $\quad f_6(x)=1-x$
- 要证明$f_4\circ f_5=f_2$，需证：$\forall x\in S, f_5\big(f_4(x)\big)=f_2(x)$

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

结合性

- 集合A上的运算∘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∘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

- 集合A上的运算$\circ$具有交换性定义为：

$$\forall \boldsymbol{x}, \boldsymbol{y} \in \boldsymbol{A}, \boldsymbol{x} \circ \boldsymbol{y} = \boldsymbol{y} \circ \boldsymbol{x}$$

- 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

- 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

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

$$\forall \boldsymbol{x} \in \boldsymbol{S}, \boldsymbol{e} \circ \boldsymbol{x} = \boldsymbol{x} \circ \boldsymbol{e} = \boldsymbol{x}$$

- 单位元可记为$\mathbf{1}_S$，或简记为$\mathbf{1}$（读作幺）
- 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

- 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$\boldsymbol{x^{-1}}$
  - 逆元素既是左逆元，又是右逆元
  - 如果y是x的逆元，则x也是y的逆元

一个关于逆元素的例子

$*$	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$\langle S,\circ\rangle$满足结合律：
  - 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

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

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

$$\forall \boldsymbol{x} \in \boldsymbol{S}, \boldsymbol{t} \circ \boldsymbol{x} = \boldsymbol{x} \circ \boldsymbol{t} = \boldsymbol{t}$$

- 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“∘”如下：

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

  - 交换律：显然
  - 结合律：$(x \circ y) \circ z = x \circ (y \circ z) = x + y + z - xy - xz - yz + xyz$
  - 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：结合律、交换律、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$\boldsymbol{S_1 \sim S_2}$)当且仅当存在函数$f$: $S_1 \to S_2$，满足：

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

- 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 $\langle \mathbb{Z}, +\rangle \sim \langle \mathbb{Z}_3, +_3\rangle$（模3剩余加系统）

课堂练习题

- 设代数系统$\boldsymbol{Z}_n \equiv \langle \mathbb{Z}_n, \oplus_n \rangle$为（模$n$整数加），$f: \boldsymbol{Z}_{12} \to \boldsymbol{Z}_3$，$f(x) = x \bmod 3$。证明：$f$满同态

课堂练习题

证明：

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

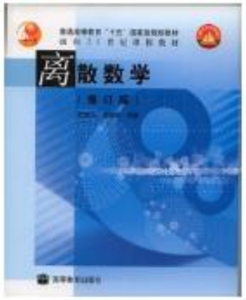
$$f(x \oplus_{12} y) = (x \oplus_{12} y) \bmod 3 = \big((x+y) \bmod 12\big) \bmod 3$$
$$= (x+y) \bmod 3 = (x \bmod 3) \oplus_3 (y \bmod 3) = f(x) \oplus_3 f(y)$$

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

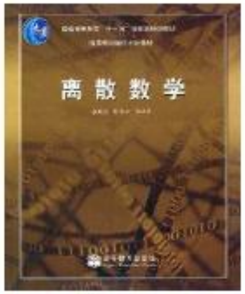
故f为从$\boldsymbol{Z}_{12}$到$\boldsymbol{Z}_3$的满同态映射。 □

教材和练习

- 课后习题：



- pp. 191－193
  - 2，4，9
  - 11－14



- pp. 178－180
  - 2，4，9
  - 11－14