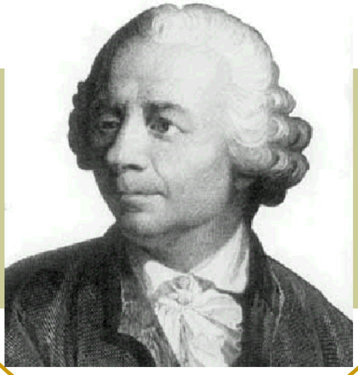

离散数学·习题课

Discrete Mathematics

第五次：代数系统、幺半群与群（1）

南京大学计算机科学与技术系

2010年4月7日

Al-Khwarizmi (c.780 – c.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。

前 情 提 要

- 二元运算和一元运算的概念：
  - 设S为集合，函数$f: S \times S \rightarrow S$称为集合$S$上的二元运算。
  - 设S为集合，函数$f: S \rightarrow S$称为集合S上的一元运算。
- 二元运算与一元运算的算符及表示法：
  - 算符：$\circ$, $*$, $\cdot$, Δ, $\diamond$ 等。
  - 表示法：表达式或者运算表。

前 情 提 要（续）

- 二元运算的性质与特异元素：
  - ✧ 交换律：$\forall x,y \in S, x \circ y = y \circ x$
  - ✧ 结合律：$\forall x,y,z \in S, (x \circ y) \circ z = x \circ (y \circ z)$
  - ✧ 幂等律：$\forall x \in S, x \circ x = x$
  - ✧ 消去律：$\forall x,y \in S, x \circ y = x \circ z \wedge x \neq \Phi \Rightarrow y = z, y \circ x = z \circ x$
  - ✧ 分配律：$\forall x,y,z \in S, x \circ (y \circ z) = (x \circ y) * (x \circ z), (y * z) \circ x = (y \circ x) * (z \circ x)$
  - ✧ 吸收律：$\circ$与$*$可交换，$\forall x,y \in S, x \circ (x * y) = x, x * (x \circ y) = x$
  - ✧ 单位元e：$\forall x \in S, x \circ e = e \circ x = x$
  - ✧ 零元θ：$\forall x \in S, x \circ \theta = \theta \circ x = \theta$
  - ✧ 幂等元x：$\forall x \in S, x \circ x = x$
  - ✧ 可逆元x及其逆元素x^{-1}：$x \circ x^{-1} = x^{-1} \circ x = e$

前 情 提 要（续）

- **二元运算中的重要定理：**
  - 单位元如果存在，则其唯一。
  - 零元如果存在，则其唯一。
  - 如果$|S| > 1$，则单位元不等于零元。
  - 对于可结合的二元运算，可逆元素x只有唯一 的逆元x^{-1}。

前 情 提 要（续）

- **代数系统的相关概念：**
  - 非空集合S与S上的k个一元或二元运算$f_1, f_2, \cdots, f_k$组成的系统称为代数系统，记为$\langle S, f_1, f_2, \cdots, f_k \rangle$。
  - 设$V = \langle S, f_1, f_2, \cdots, f_k \rangle$是代数系统，$B \subseteq S$，若$B$对运算$f_1, f_2, \cdots, f_k$均封闭，且$B$和$S$含有相同的代数常数，则称$\langle S, f_1, f_2, \cdots, f_k \rangle$为代数$V$的子代数。

前 情 提 要（续）

- **代数系统的同构与同态：**
  - 设$V_1 = \langle A,\circ\rangle$，$V_2 = \langle B,*\rangle$是同类型的代数系统，若存在**双射函数**$f: V_1 \to V_2$使得$\forall x, y \in A, f(x \circ y) = f(x) * f(y)$，则称$f$是$V_1$到$V_2$的同构映射，简称$V_1$与$V_2$同构（isomorphism）。
  - 设$V_1 = \langle A,\circ\rangle$，$V_2 = \langle B,*\rangle$是同类型的代数系统，若存在函数$f: V_1 \to V_2$使得$\forall x, y \in A, f(x \circ y) = f(x) * f(y)$，则称$f$是$V_1$到$V_2$的同态映射，简称$V_1$与$V_2$同态（homomorphism）；特别地，若上述映射f是满射，则称V_1与V_2满同态（epimorphism）。

前 情 提 要（续）

- **半群与幺半群：**
  - 设$V = \langle S,\circ\rangle$是代数系统，$\circ$是二元运算，如果$\circ$可结合，则称$V$为半群。
  - 设$V = \langle S,\circ\rangle$是半群，若$e \in S$是关于$\circ$的单位元，则称$V$为幺半群（Monoid），或可记为$\langle S,\circ, e\rangle$。
  - 半群的子代数称为子半群，幺半群的子代数称为子幺半群，子幺半群还要求幺元（单位元）在S的子集中。

前 情 提 要（续）

群的定义与概念：

- 群是特殊的半群和幺半群。
- 设$\langle G,\circ\rangle$是代数系统，$\circ$为二元运算。若$\circ$是可结合的，存在幺元$e\in G$，且对G中任意元素x都存在逆元$x^{-1}\in G$，则称G为群，或记作$\langle G,\circ,e,^{-1}\rangle$。
- 若群G为有穷集，则称为有限群，否则成无限群，群G的基数称为群的阶。只含幺元（阶为1）的群称为平凡群。
- 若群G中的二元运算可交换，称G为交换群（阿贝尔群）。

前 情 提 要（续）

- 群的基本性质：
  - 幂运算规则：设G为群，则
    - $\forall a \in G, (a^{-1})^{-1} = a \quad\quad \forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$
    - $\forall a \in G, a^n a^m = a^{n+m}, n, m \in \mathbb{Z}$
    - $\forall a \in G, (a^n)^m = a^{nm}, n, m \in \mathbb{Z}$
    - $(a_1 a_2 \cdots a_r)^{-1} = a_r^{-1} a_{r-1}^{-1} \cdots a_2^{-1} a_1^{-1}$
  - 设G为群，则G适合消去律：$\forall a, b, c \in G$有$ab = ac \Rightarrow b = c$（左）和$ba = ca \Rightarrow b = c$（右）。
  - 设G为群，$a \in G$且$|a| = r$；设k为整数，则$a^k = e \Leftrightarrow r|k$且$|a^{-1}| = |a|$。

代数系统课堂练习题（续）

- 1、课本228页第1题。（5分钟）

解：

$A^A = \{f \mid f:\{0,1\} \to \{0,1\}\} = \{f_1, f_2, f_3, f_4\}$。其中，

$f_1 = \{\langle 0,0\rangle, \langle 1,0\rangle\}$，$f_2 = \{\langle 0,0\rangle, \langle 1,1\rangle\}$，$f_3 = \{\langle 0,1\rangle, \langle 1,0\rangle\}$，$f_4 = \{\langle 0,1\rangle, \langle 1,1\rangle\}$

易见，其运算表为：

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_1	f_4	f_4
f_2	f_1	f_2	f_3	f_4
f_3	f_1	f_3	f_2	f_4
f_4	f_1	f_4	f_1	f_4

代数系统课堂练习题（续）

- 2、课本228页第2题。（4分钟）

解：

(1)是半群、幺半群和群　(2)是半群、幺半群和群

(3)是半群，不是幺半群也不是群

(4)是半群、幺半群和群　(5)是半群、幺半群，不是群

(6)是半群、幺半群和群

- 3、课本228页第3题。（5分钟）

证明：

（1） 封闭性：显然对于$\forall a, b \in \mathbb{R}, a * b \in \mathbb{R}$。

（2） 结合律：$\forall a, b, c \in \mathbb{R}, (a * b) * c = (a + b + ab) + c + (a + b + ab)c$

$$= a + b + c + ab + ac + bc + abc$$

$$a * (b * c) = a * (b + c + bc) = a + b + c + bc + a(b + c + bc)$$

$$= a + b + c + ab + ac + bc + abc$$

故$(a * b) * c = a * (b * c)$

（3） 单位元：0

因此$\mathbb{R}$关于$*$构成幺半群。 $\square$

代数系统课堂练习题（续）

- 4、课本229页第13题(2)(5)。（6分钟）

证明：

(2) $\forall a,b\in G$，$(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aa^{-1}=e$

$$(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)b=b^{-1}b=e$$

因此，$b^{-1}a^{-1}$是ab的逆元，根据逆元的唯一性，命题得证。 □

(5) 设G为交换群，当n为自然数时对n归纳如下：

Basis：$n=0$，$(ab)^0=e=ee=a^0b^0$ 成立；

I.H.：$(ab)^k=a^kb^k$；

I.S.：$(ab)^{k+1}=(ab)^k(ab)=(a^kb^k)ab=a^k(b^ka)b$

$$=a^k(ab^k)b=(a^ka)(b^kb)=a^{k+1}b^{k+1}$$

根据数学归纳法，命题得证。

若$n<0$，则令$n=-m$ $(\mathrm{m}>0)$，有：

$$(ab)^n=(ba)^n=(ba)^{-m}=((ba)^{-1})^m=(a^{-1}b^{-1})^m$$

$$=(a^{-1})^m(b^{-1})^m=a^{-m}b^{-m}=a^nb^n$$

综上，命题得证。 □

代数系统课堂练习题（续）

- 5、设 $\boldsymbol{Z}_n$ 为模 n 整数加群，$f:\boldsymbol{Z}_{12}\to\boldsymbol{Z}_3$，$f(x)=x \bmod 3$。证明：$f$ 为满同态。（5分钟）

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。 □

代数系统课堂练习题（续）

- 6、课本229页第12题。（8分钟）

证明：

先证明封闭性：$1 \in T$，$\forall x, y \in T$，$(x,n)=1$，$(y,n)=1$，故存在整数a,b,c,d，使得：

$$xa+nb=1,\quad yc+nd=1$$

从而有：$xa=1-nb,\ yc=1-nd$

$$(xa)(yc)=1-nb-nd+n^2bd \Rightarrow (xy)(ac)+n(b+d-nbd)=1$$

设$xy=tn+i, t, i \in Z^+, 0 \le i < n$，则$x \otimes y = i$。故根据上式可得：

$$(tn+i)(ac)+n(b+d-nbd)=1 \Rightarrow i(ac)+n(tac+b+d-nbd)=1$$

由于$ac, tac+b+d-nbd$皆为整数，故$(i,n)=1$，即$x \otimes y \in T$。

故而 1 为T中单位元，$\forall x \in T$，由于$(x,n)=1$, 故存在$xa+nb=1$；若$0<a<n$, 则$x \otimes a=1$，即a就是x的逆元。下证存在a满足$0<a<n$：

根据除法定则，存在整数k和a'使得$a=nk+a'$，其中$0<a'<n$；于是有$x(kn+a')+nb=1$，即$xa'+n(b+xk)=1$中a'满足要求。

显然，$\otimes$满足结合律和交换律，综上，T关于模n乘法构成 Abelian 群。 $\square$

本周课后作业

- pp. 229
  - 4，5，7，8
  - 9，15

- 本次作业大概需要20分钟，下周二交。