离散数学

Discrete Mathematics

2020年新冠疫情网络教学版

蒋瀚

山东大学软件学院

Chapter 04

代数系统

CONTENT

运算

- 定义 1　设A是一个集合，$A\times A$到A的映射称为A上的二元运算．一般地，A^n到A的映射称为A上的n元运算．

- 设f是A上的n元运算，对任意的x_1 x_2，…，$x_n \in A$，$f(<x_1, x_2, \ldots, x_n>)$称作$x_1$，$x_2$，…，$x_n$在$f$下的运算结果，并简记为

$$f(x_1, x_2, \ldots, x_n).$$

运算

- 例 1　数的加法是实数集$\boldsymbol{R}$上的二元运算.

- 因为 对任意 $\langle a, b\rangle \in \mathbf{R}\times\mathbf{R}$，通过加法可唯一确定一个实数 $c=a+b$，故加法是$\boldsymbol{R}\times\boldsymbol{R}$到$\boldsymbol{R}$的映射；

  即是$\mathbf{R}$上的二元运算.

- 同样，数的乘法、减法都是实数集$\mathbf{R}$上的二元运算.

运算

- 例 2　数的除法不是实数集**R**上的二元运算.
- 因为0不能做除数，某些实数对〈a，b〉不能通过除法唯一确定一个与之相应的实数（比如，2 / 0无意义
- 但是，任何非0实数a，b，通过除法可唯一确定一个非0实数a/b，故除法是非0实数集R^*上的二元运算.

运算

- 例 3　设S是一个集合，集合的并、交是P（S）上的二元运算.

- 因为对任意$\langle A, B\rangle \in P(S)\times P(S)$，通过集合的并（交）可唯一确定$P$（$S$）的一个元素$A\cup B$（或$A\cap B$），故集合的并(交)是$P(S)$上的二元运算.

运算

□例 4　设$\boldsymbol{R}$是实数集，令

$$f:\ \langle a,\ b\rangle \mapsto a+b-ab \qquad a,\ b\in \mathbf{R}$$

则 f 是$\boldsymbol{R}$上的二元运算,

即　$f(a, b) = a+b-ab.$

运算

□例 5　设**R**是实数集，令

$$g: \langle a, b\rangle \mapsto \min\{a, b\}$$

$$h: \langle a, b\rangle \mapsto \max\{a, b\}, \forall a, b \in \mathbf{R}$$

则g，h均为**R**上的二元运算.

运算

- 今后主要讨论二元运算，简称“运算”

- 用一些称作运算符的特殊符号，表示二元运算，　比如：◊，
  *，·，∘，＋ × 等

- 将a，b在某运算“*”下的运算结果 $*(a, b)$ 记为$a*b$. 或简写成ab.

运算

- 实数加法: $a+b$
- 实数乘法: $a \cdot b$或ab
- 集合并、交运算：$A \cup B$，$A \cap B$
- 定义 * 运算：

$$a*b=a+b-ab$$

- 定义 ∘、⊕运算:

$$a \circ b=\min\{a, b\}$$

$$a \oplus b=\max\{a, b\}$$

运算

例 6 设n为正整数，$\mathbf{Z}_n$为 模n剩余类 的集合：

$$\mathbf{Z}_n = \{ [0], [1], \ldots, [n-1] \}$$

定义运算 $+_n$ 与 $\times_n$ 如下:

$\forall$ $[i]$，$[j] \in \mathbf{Z}_n$，规定

$$[i] +_n [j] = [i+j]$$

$$[i] \times_n [j] = [i \cdot j]$$

其中，$+$ 与 $\cdot$ 为通常整数的加法和乘法.

运算

- $+_n$，$\times_n$是不是二元运算？
- $[i]+_n[j]$ 与 $[i]\times_n[j]$ 由剩余类 $[i]$，$[j]$ 唯一确定，而与代表元i，j的选取无关
- 设 $[i']=[i]$，$[j']=[j]$

  则 $n \mid i'-i$，　$n \mid j'-j$.

  知 $n \mid (i'+j')-(i+j)$

  故 $[i'+j']=[i+j]$.

运算

- 定义 2　设 f 是 A 上的 n元运算，$S \subseteq A$，如果对x_1，x_2，…，$x_n \in S$，恒有 f（x_1，x_2，…，x_n）$\in S$，则称S对运算f是封闭的．运算 f 在 S 上是封闭的。
- 自然数集对实数集上的加法、乘法封闭
- 自然数集对实数集上的减法不是封闭的
- 设$A \subseteq S$，则P（A）对P（S）上的并、交封闭

运算表

□当A是有限集时，A上的运算可用一个表来表示：

$$
\begin{array}{c|cccccc}
\circ & a_1 & a_2 & \cdots & a_j & \cdots & a_n \\
\hline
a_1 & a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\
a_2 & a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\
\vdots & & & & & & \\
a_j & a_{j1} & a_{j2} & \cdots & a_{ij} & \cdots & a_{in} \\
\vdots & & & & & & \\
a_n & a_{n1} & a_{n2} & \cdots & a_{nj} & \cdots & a_{nn}
\end{array}
$$

运算表

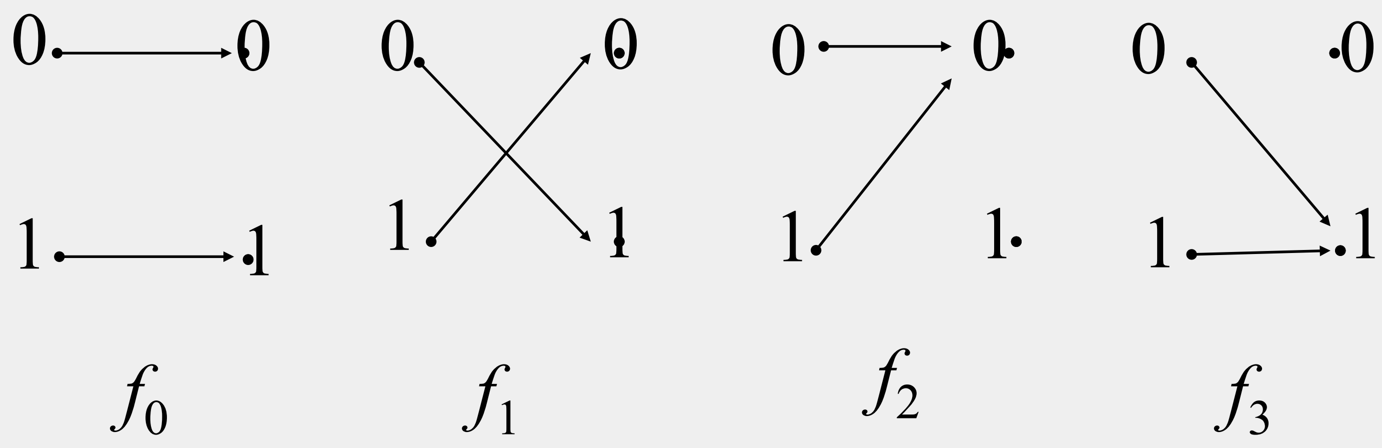
□例 7　$Z_3=\{[0],[1],[2]\}$，$+_3$、$\times_3$的运算表分别为：

$+_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\times_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

运算表

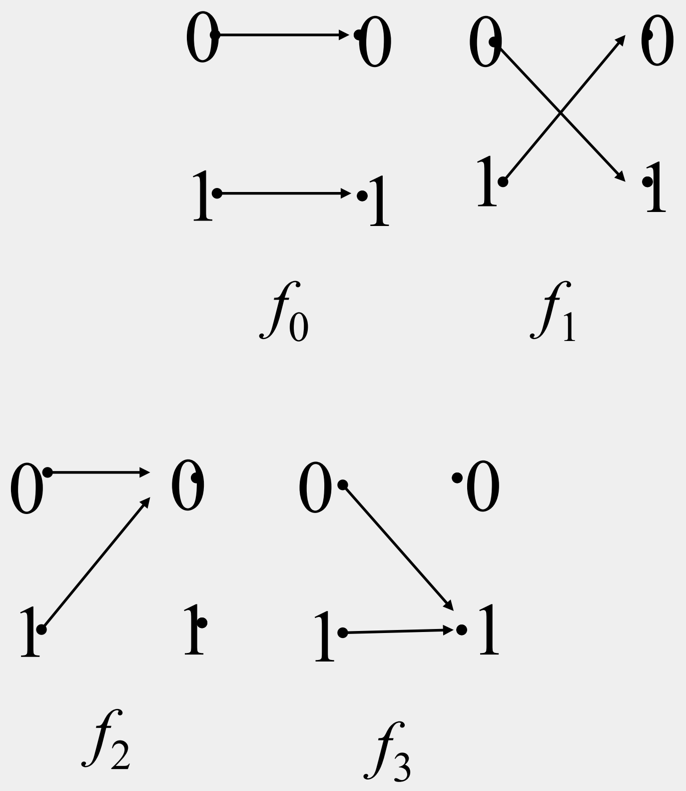
□例 8　设A＝｛0，1｝，则A到A的映射构成的集合A^A中有四个元素f_0，f_1，f_2，f_3，如下：



运算表

□A^A中的函数复合的运算表

$\circ$	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	f_3
f_1	f_1	f_0	f_3	f_2
f_2	f_2	f_2	f_2	f_2
f_3	f_3	f_3	f_3	f_3



运算律

- 定义 3 设X为集合，$*$，$\circ$ 为X上的运算.
- 如果对任意x，y，$z\in X$，有 $(x*y)*z=x*(y*z)$
  则称 $*$ 满足结合律（可结合的）；
- 如果对任意x，$y\in X$，有 $x*y=y*x$
  则称 $*$ 满足交换律（可交换的）；
- 如果对任意x，y，$z\in X$，有 $x*(y\circ z)=(x*y)\circ(x*z)$
  则称 $*$ 对 $\circ$ 满足左分配律（左可分配）；
- 如果对任意x，y，$z\in X$，有 $(y\circ z)*x=(y*x)\circ(z*x)$
  则称 $*$ 对 $\circ$ 满足右分配律（右可分配）；
- 若 $*$ 对 $\circ$ 既满足左分配律，又满足右分配律，称 $*$ 对 $\circ$ 满足分配律（可分配）.

运算律

- 如果对任意x，y，$z \in X$，
  当$x * y = x * z$时，必有$y = x$，
  则称 * 满足左消去律；
- 如果对任意x，y，$z \in X$，
  当$y * x = z * x$时，必有$y = z$，
  则称 * 满足右消去律；
- 若 * 既满足左消去律，又满足右消去律，称其满足消去律.

运算律

- 整数集上的加法、乘法 满足哪些运算律
- 设A是一集合，P（A）上的并、交运算均满足结合律、交换律、分配律,不满足消去律.
- 运算表怎么表现运算律？

作业

- 习题一 1，3

CONTENT

代数系统

- 定义 1　设A是一个非空集合，f_1，f_2，…，f_n是A上的运算（其元数可以不同），我们说A在运算f_1，f_2，…，f_n下构成一个代数系统，记为$<A, f_1, f_2, \ldots, f_n>$. 在不引起混乱的情况下，也可将其简记为$A$.
- $\langle \mathbf{N}, + \rangle$，$\langle \mathbf{N}, \cdot \rangle$，$\langle \mathbf{N}, +, \cdot \rangle$.
- $\langle \mathbf{Z}, + \rangle$，$\langle \mathbf{Z}, \cdot \rangle$，$\langle \mathbf{Z}, +, \cdot \rangle$，
- $\langle \mathbf{Q}, + \rangle$，$\langle \mathbf{Q}, \cdot \rangle$，$\langle \mathbf{Q}, +, \cdot \rangle$，$\langle \mathbf{R}, + \rangle$，$\langle \mathbf{R}, \cdot \rangle$，$\langle \mathbf{R}, +, \cdot \rangle$.

代数系统

- 设A是一个集合，P（A）与集合的并和交运算构成代数系统

  $<P(A), \cup>$，$<P(A), \cap>$，$<P(A), \cup, \cap>$

- 模n剩余类集$\mathbf{Z}_n$在运算$+_n$和$\times_n$下可构成代数系统

  $<\mathbf{Z}_n, +_n>$，$<\mathbf{Z}_n, \times_n>$，$<\mathbf{Z}_n, +_n, \times_n>$

- 设A是一个集合，在A上规定运算$*$如下：

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

  则得到一个代数系统 $<A, *>$

代数系统

- 定义 2　设$<A, *>$是代数系统，$S \subseteq A$，如果S对 $*$ 封闭，则称$<S, *>$为$<A, *>$的子代数.

- 任一代数系统均为自身的子代数

- $\langle \mathbf{N}, + \rangle$, $\langle \mathbf{Z}, + \rangle$, $\langle \mathbf{Q}, + \rangle$, $\langle \mathbf{R}, + \rangle$, $\langle \mathbf{Z}, \cdot \rangle$

代数系统

- **定义 3** 设$<A, \circ>$是一个代数系统，$e_l \in A$，如果 $\forall x \in A$，有$e_l x = x$，则称e_l为A的左单位元（左恒等元）；设$e_r \in A$，如果 $\forall x \in A$，有$x e_r = x$，称e_r为A的右单位元（右恒等元）；A中的一个元素如果既是左单位元，又是右单位元，则称之为单位元（恒等元）.
- $\langle \mathbf{N}, + \rangle$，$\langle \mathbf{N}, \cdot \rangle$ $\langle \mathbf{Z}, + \rangle$，$\langle \mathbf{Q}, + \rangle$，
- $\langle \mathbf{R}, + \rangle$，$\langle \mathbf{Z}, \cdot \rangle$，$\langle \mathbf{Q}, \cdot \rangle$，$\langle \mathbf{R}, \cdot \rangle$，
- $<P(A), \cup>$，$<P(A), \cap>$，$<\mathbf{Z}_n, +_n>$，$<\mathbf{Z}_n, \times_n>$
- $\forall\ x, y \in A$，$x * y = x$，任何元素均为右单位元

代数系统

- 定理 1　设代数系统〈A，$\circ$〉中既有左单位元e_l，又有右单位元e_r，则 $e_l = e_r$.

- 证明　因e_l为左单位元，故$e_l\,e_r = e_r$，又因e_r为右单位元，故$e_l\,e_r = e_l$，所以$e_l = e_r$.

- 推论　代数系统〈A，$\circ$〉中的单位元如果存在，则必定唯一.

代数系统

□定义 4　代数系统 $\langle A, *\rangle$，e是单位元.

对于$a \in A$，

如果存在$b \in A$，使得$ba = e$，则称a为左可逆的，且称b为a的左逆元；

如果存在$c \in A$，使得$ac = e$，则称a是右可逆的，且称c为a的右逆元；

如果存在$a' \in A$，使得$a'a = aa' = e$，则称a是可逆的，且称a'为a的逆元.

代数系统

- $\langle \mathbf{N}, +\rangle$, $\langle \mathbf{Z}, +\rangle$, $\langle \mathbf{Q}, +\rangle$, $\langle \mathbf{R}, +\rangle$
- $\langle \mathbf{N}, \cdot\rangle$, $\langle \mathbf{Z}, \cdot\rangle$,
- $\langle \mathbf{Q}, \cdot\rangle$, $\langle \mathbf{R}, \cdot\rangle$
- $<P(A), \cup>$, $<P(A), \cap>$
- $<\mathbf{Z}_n, +_n>$, $<\mathbf{Z}_n, \times_n>$

$\times_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

代数系统

- 定理 2　设e是代数系统$\langle A, *\rangle$的单位元，$*$满足结合律，如果$a\in A$的左逆元b及右逆元c均存在，则$b = c$.

- 证明　$b = b\,e = b\,(ac) = (ba)\,c = ec = c$.

- 推论　设$\langle A, *\rangle$是有单位元的代数系统，$*$满足结合律．如果$a\in A$的逆元存在，则必定唯一.

代数系统

- 定义 5　设 $\langle A, *\rangle$ 是一个代数系统，如果 $a \in A$ 满足 $a * a = a$，称 a 为 A 的幂等元.

- 代数系统的单位元如果存在则必为幂等元.

- $\langle P(A), \cup\rangle$，$\langle P(A), \cap\rangle$

$\langle Z_n, +_n, \times_n \rangle$ 的性质

- 关于$+n$的性质：
- 结合律 $([i]+_n[j])+_n[k]=[i]+_n([j]+_n[k])$
- 交换律 $[i]+_n[j]=[j]+_n[i]$
- 单位元 $[i]+_n[0]=[0]+_n[i]=[i]$
- 逆元 $[i]+_n[n-i]=[n-i]+_n[i]=[0]$

〈Z_n，$+_n$，$\times_n$〉的性质

□关于$\times n$的性质.

□结合律

$$([i]\times_n[j])\times_n[k]=[i]\times_n([j]\times_n[k])$$

□交换律 $[i]\times_n[j]=[j]\times_n[i]$

□单位元 $[i]\times_n[1]=[1]\times_n[i]=[i]$

$\langle Z_n, +_n, \times_n \rangle$ 的性质

- $\times_n$对$+_n$的分配律
- $[i] \times_n ([j] +_n [k])$
  $= ([i] \times_n [j]) +_n ([i] \times_n [k])$
- $([j] +_n [k]) \times_n [i]$
  $= ([j] \times_n [i]) +_n [k] \times_n [i])$

作业

习题二 1，3，4

CONTENT

同态与同构

- **定义 1** 对 $<A, *>$，$<B, \circ>$，$f: A \to B$，如果 f 保持运算，即：

$$\forall x, y \in A \text{ 有 } f(x * y) = f(x) \circ f(y)$$

称 f 为 $<A, *>$ 到 $<B, \circ>$ 的同态映射(同态)

- **例 1** 设 $\langle A, * \rangle$，$\langle B, \circ \rangle$ 是两个代数系统，$e \in B$ 是 B 的单位元．令

$$f(a) = e \quad , \quad \forall a \in A$$

则 f 是 A 到 B 的同态（？），称 f 为零同态．

同态与同构

□例 2　令 f：$\mathbf{Z}\to\mathbf{Z}$　定义如下

$$f(a)=8a\ ,\quad \forall a\in\mathbf{Z}$$

则 f 是〈$\mathbf{Z}$，$+$〉到〈$\mathbf{Z}$，$+$〉的同态，但不是〈$\mathbf{Z}$，$\cdot$〉到〈$\mathbf{Z}$，$\cdot$〉的同态.

□证：

$\forall a$，$b\in\mathbf{Z}$，$f(a+b)=8(a+b)=8a+8b=f(a)+f(b)$;

$f(ab)=8(ab)\neq 8a\cdot 8b=f(a)\cdot f(b)$;

同态与同构

□定义 2　设 $\langle A, *\rangle$，$\langle B, \circ\rangle$ 为两个代数系统，$f: A\to B$ 为 A 到 B 的同态.

如果f是单射，称f为单同态；

如果f为满射，称f为满同态，称 B 是A在f下的同态象，记为f: $A\sim B$ 或A $\sim$ B；

如果f是双射，称f为同构映射（同构），这时称A与B在f映射下同构. 记为

$$f: A\cong B \quad \text{或} \quad A \overset{f}{\cong} B.$$

同态与同构

- 存在同态映射f，使 f：$A \sim B$，称代数系统〈B，∘〉是〈A，$*$〉的同态象，并记为$A \sim B$；
- 存在同构映射f，使 f：$A \cong B$，称两个代数系统〈A，$*$〉，〈B，∘〉是同构的，并记为$A \cong B$.

同态与同构

- 例 3　对 $\langle \mathbf{Z}, +\rangle$ 与 $\langle \mathbf{Z}_n, +_n\rangle$，令

$$f(i) = [i],$$

则 f 是满射，且 $\forall i, j \in \mathbf{Z}$

$$f(i+j) = [i+j] = [i] +_n [j]$$

$$= f(i) +_n f(j)$$

故　f: $\langle \mathbf{Z}, +\rangle \sim \langle \mathbf{Z}_n, +_n\rangle$

- 同样讨论可知 $\langle \mathbf{Z}, \cdot\rangle \sim \langle \mathbf{Z}_n, \times_n\rangle$.

同态与同构

□例 4　用$\boldsymbol{R}^{+}$表示正实数集，考虑〈$\boldsymbol{R}$，＋〉与〈$\mathbf{R}^{+}$，·〉，令

$$f(x)=e^{x}\quad,\quad \forall x\in \boldsymbol{R},$$

则f是双射，

并且 $\forall x$，$y\in \mathbf{R}$

$$f(x+y)=e^{x+y}=e^{x}\cdot e^{y}=f(x)\cdot f(y)$$

故　f: 〈$\mathbf{R}$，＋〉$\cong$〈$\mathbf{R}^{+}$，·〉

同态与同构

□定理 1

f是 $<A, *>$到$<B, \cdot>$ 的同态，

g是 $<B, \cdot>$到$<C, \triangle>$的同态，则

$g\circ f$是$<A, *>$到$<C, \triangle>$的同态.

且当f，g均为单同态、满同态、同构时，$g\circ f$也必是单同态、满同态、同构.

同态与同构

证明

1） $g\circ f$: $A\to C$.

2） $g\circ f$ 保持运算.

$\forall x, y\in A$

$(g\circ f)(x*y)=g(f(x*y))$

$=g(f(x)\cdot f(y))$

$=g(f(x))\triangle g(f(y))$

$=(g\circ f)(x)\triangle(g\circ f)(y)$

因而, $g\circ f$ 是 A 到 C 的同态. ……

$<A, *>$,

$<B, \cdot>$,

$<C, \triangle>$

同态与同构

- 定理 2　φ：$\langle A, *\rangle \cong \langle B, \circ\rangle$，则

$$\varphi^{-1}: \langle B, \circ\rangle \cong \langle A, *\rangle$$

- 证明　由函数的性质可知，φ^{-1}是B到A的双射; 又，$\forall x, y \in B$

  记 $\varphi^{-1}(x) = x_1$，$\varphi^{-1}(y) = y_1$，则

$$x = \varphi(x_1), \ y = \varphi(y_1), \text{故}$$

  $\varphi^{-1}(x \circ y)$

  $= \varphi^{-1}(\varphi(x_1) \circ \varphi(y_1)) = \varphi^{-1}(\varphi(x_1 * y_1))$

  $= x_1 * y_1$

  $= \varphi^{-1}(x) * \varphi^{-1}(y)$，……

同态与同构

- **定理 3** （满同态保持结合律）
  设 φ：$<A, *> \sim <B, \circ>$，$*$ 满足结合律，则 $\circ$ 也必满足结合律.

- **证明** $\forall x, y, z \in B$，
  由于 φ 是A到B的满同态，故必存在$x_1, y_1, z_1 \in A$，使

$$\varphi(x_1) = x,\ \varphi(y_1) = y,\ \varphi(z_1) = z，\text{于是}$$

$$
\begin{aligned}
&(x \circ y) \circ z \\
&= (\varphi(x_1) \circ \varphi(y_1)) \circ \varphi(z_1) \\
&= \varphi(x_1 * y_1) \circ \varphi(z_1) \\
&= \varphi((x_1 * y_1) * z_1) \\
&= \varphi(x_1 * (y_1 * z_1)) \\
&= \varphi(x_1) \circ \varphi(y_1 * z_1) \\
&= \varphi(x_1) \circ (\varphi(y_1) \circ \varphi(z_1)) \\
&= x \circ (y \circ z)
\end{aligned}
$$

同态与同构

定理 4（满同态保持交换律）

设 $\langle A, *\rangle \sim \langle B, \circ\rangle$，$*$满足交换律，则 $\circ$ 必满足交换律.

同态与同构

- 定理 5　（满同态保持单位元）φ：$<A, *> \sim <B, \circ>$，$e \in A$是A的单位元，则 $\varphi(e)$是B的单位元.

- 证明　$\forall b \in B$，

  由于 φ 是满同态，必存在$a \in A$使 $\varphi(a) = b$，因此，

  $b \circ \varphi(e)$

  $= \varphi(a) \circ \varphi(e)$

  $= \varphi(a * e)$

  $= \varphi(a)$

  $= b$

  同理　$\varphi(e) \circ b = b$，……

同态与同构

定理 6（满同态保持逆元）

设 φ：$\langle A, *\rangle \sim \langle B, \circ\rangle$，$e_A$，$e_B$分别为$A$，$B$的单位元，$a$，$a' \in A$ 且 a' 是a的逆元，则 $\varphi(a')$ 是$\varphi(a)$ 的逆元.

证明 $\varphi(a') \circ \varphi(a)$

$= \varphi(a' * a) = \varphi(e_A)$

$= e_B$

同理 $\varphi(a) \circ \varphi(a') = e_B$.

故 $\varphi(a')$ 是 $\varphi(a)$ 的逆元.

同态与同构

□定理 7（同态保持幂等元）

设 φ 是 $\langle A, *\rangle$ 到 $\langle B, \circ\rangle$ 的同态，若$a\in A$是幂等元，则$\varphi(a)\in B$也是幂等元.

证： $\varphi(a)\circ\varphi(a)=\varphi(a)$

同态与同构

□定义 3　设〈A，$*$〉为一个代数系统，<A，$*$>到自身的同态称为A的自同态，<A，$*$>到自身的同构称为 A 的自同构.

□例 5　设〈A，$*$〉是一个代数系统，A上的恒等映射I_A是A的自同构.

若 A 中存在单位元e，令$f(a)=e$，$\forall a\in A$，则f是A的自同态.

作业

- 习题三　2,3,4,6

CONTENT

同余关系与商代数

□定义 1　设 $\langle A, *\rangle$ 是一个代数系统，E是A上的等价关系，如果 $\forall x_1, x_2, y_1, y_2 \in A$，

当$x_1\ E\ y_1$，$x_2\ E\ y_2$ 时，必有 $x_1 * x_2\ E\ y_1 * y_2$，

则称E为A上的同余关系.

例 2　整数集**Z**上的模m同余关系是 $\langle \mathbf{Z}, +\rangle$ 及 $\langle \mathbf{Z}, \cdot\rangle$ 上的同余关系.

同余关系与商代数

- 设E为〈A，$*$〉上的同余关系，在商集

$$A/E = \{[x]_E \mid x \in A\}$$

上合理地引入一个运算：

令 ∘ 是A/E上的运算，由下式定义：

$$[x] \circ [y] = [x * y],\quad \forall [x], [y] \in A/E$$

- 代数系统〈A/E，∘〉，称为A对E的商代数

同余关系与商代数

- $\langle \mathbf{Z}, +\rangle$ 对R_m的商代数为$\langle \mathbf{Z}/R_m, \circ\rangle$

  其中，$\mathbf{Z}/R_m = \mathbf{Z}_m = \{[0], [1], \ldots, [m-1]\}$,

  运算$\circ$由下式定义：

  $$[i] \circ [j] = [i+j] = [i] +_m [j]$$

  即$<\mathbf{Z}, +>$对R_m的商代数为$\langle \mathbf{Z}_m, +_m\rangle$.

- $\langle \mathbf{Z}, \cdot\rangle$ 对R_m的商代数为$\langle \mathbf{Z}_m, \times_m\rangle$.

同余关系与商代数

- 定理 1　设E为$\langle A, *\rangle$上的同余关系，$\langle A/E, \circ\rangle$为$A$对$E$的商代数，令

  φ: $A \to A/E$，定义如下：

  $$\varphi(x) = [x], \quad \forall x \in A$$

  则　φ: $\langle A, *\rangle \sim \langle A/E, \circ\rangle$.

- φ称为<A，*>到<A/E，∘>的自然同态

同余关系与商代数

□定理 2 设f是〈A，$*$〉到〈B，$\circ$〉的同态，由f在A上按下式定义关系E_f

$$x\,E_f\,y \Leftrightarrow f(x)=f(y),\forall x, y\in A$$

则 E_f为〈A，$*$〉上的同余关系.

□定理 3 设 f:〈A，$*$〉$\sim$〈B，$\triangle$〉，E_f为由f确定的同余关系，$<A/E_f, \circ>$为A对 E_f的商代数，则$<A/E_f, \circ>\cong<B, \triangle>$.

CONTENT

直积

- **定义 1** 设 $\langle A, *\rangle$，$\langle B, \circ\rangle$ 为两个代数系统，$\langle A\times B, \triangle\rangle$ 称为A与B的直积，其中，$A\times B$是A，B的笛卡尔积，$\triangle$ 定义如下：

  $\langle x, y\rangle \triangle \langle u, v\rangle = \langle x * u, y \circ v\rangle \quad \forall \langle x, y\rangle, \langle u, v\rangle \in A\times B$

直积

- 直积 $A\times B$ 能够保持A，B的某些性质：

  如果 $*$，$\circ$均满足结合律（交换律），则 $\triangle$ 也必满足结合律（交换律）；

  如果A，B中分别有单位元e_A，e_B，则

  $\langle e_A, e_B\rangle$ 是$A\times B$的单位元；

  如果$x\in A$，$y\in B$分别有逆元x'，y'，则

  $\langle x', y'\rangle$ 是 $\langle x, y\rangle$ 的逆元.

直积

- 定理 1　设 $\langle A, *\rangle$，$\langle B, \circ\rangle$ 为两个代数系统，分别有单位元 e_A，e_B，则在 A，B 的直积 $\langle A\times B, \triangle\rangle$ 中存在子代数 S，T 使

$$S\cong A,\qquad T\cong B$$

- 证明　令 $S=A\times\{e_B\}=\{\langle x, e_B\rangle \mid x\in A\}$　则　$S\subseteq A\times B$，$\forall\langle x, e_B\rangle$，$\langle y, e_B\rangle\in S$，

$$\langle x, e_B\rangle\triangle\langle y, e_B\rangle=\langle x*y, e_B\circ e_B\rangle$$
$$=\langle x*y, e_B\rangle\in S$$

因此 $\langle S, \triangle\rangle$ 构成 $A\times B$ 的子代数，考虑映射 f：$A\to S$

$$f(a)=\langle a, e_B\rangle,\ \forall a\in A$$

显然，f 为双射，又 $\forall x$，$y\in A$

$$f(x*y)=\langle x*y, e_B\rangle=\langle x, e_B\rangle\triangle\langle y, e_B\rangle$$
$$=f(x)\triangle f(y)$$

则 f 保持运算，因此 f：$A\cong S$.

同理可证，若令 $T=\{e_A\}\times B$ 则 $B\cong T$.