第七章
代数结构基本知识

计算机系网络所：张小平

主要内容

- 7.1 集合与映射
- 7.2 等价关系
- 7.3 代数系统的概念
- 7.4 同构与同态

集合与映射

- 设S是任意一个集合，如果元素a属于S，记记为$a \in S$，否则记$a \notin S$。
- S中不同元素的个数称为该集合的基数，
  用$|S|$表示。
- 当集合S确定之后，能相应地得到另一个集合$\rho(S)$，$\rho(S)$是S的全部子集的集合。称为S的幂集
- $\rho(S)$的基数是 $2^{|S|}$

Tsinghua University

集合与映射

- $\rho(S)$中的元素A，是集合S的一个子集，可以刻划为

$$A=\{x\in S \mid P(x)\}$$

其中P代表某种性质

- 因此A可以解释为：具有性质P的S的元素的集合

集合与映射

- 集合运算：

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$$

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$$

分配律！

集合与映射

- 定义7.1.1 设S和T是给定的两个集合，如果有一个规则f，使对任意一个元素$x \in S$，在T中有唯一的元素y与之对应。则称f是S到T的一个映射

  记作$f: S \to T$和$y = f(x)$，S称为f的定义域，T为f的值域，y称为x的象，x称为y的原象。

集合与映射

- 根据定义：
  - S中每个元素在T中都有象
  - T中的每个元素在S中不一定都有原象
  - 习惯上我们将S中全部元素的象所构成的集合称为f的象，记作$f(S)$。显然$f(S)\subseteq T$。

集合与映射

- 定义7.1.2 两个映射f，g

$$f: \quad A_1 \to B_1$$

$$g: \quad A_2 \to B_2$$

当且仅当 $A_1 = A_2$，$B_1 = B_2$，且对任意 $x \in A$，都有 $f(x) = g(x)$，称f和g是**相等的映射**，记为f=g

集合与映射

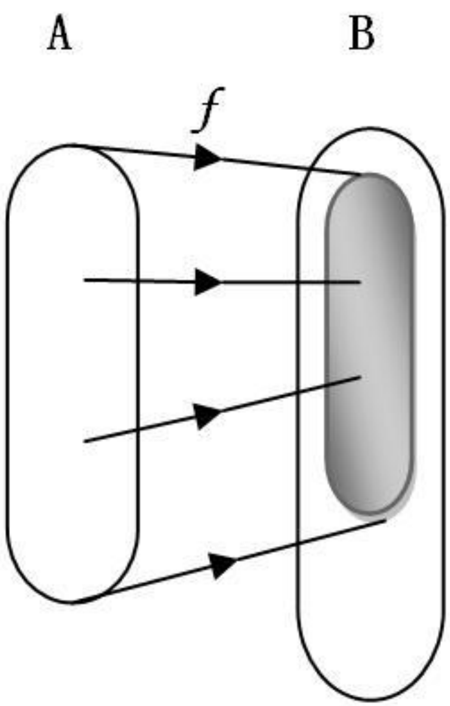
定义7.1.3 设 f 是 A 到 B 的一个映射。

1. 若对任意 $a_i \neq a_j,\ a_i, a_j \in A$，都有 $f(a_i) \neq f(a_j)$，称 f 是 A 到 B 的**单射**。

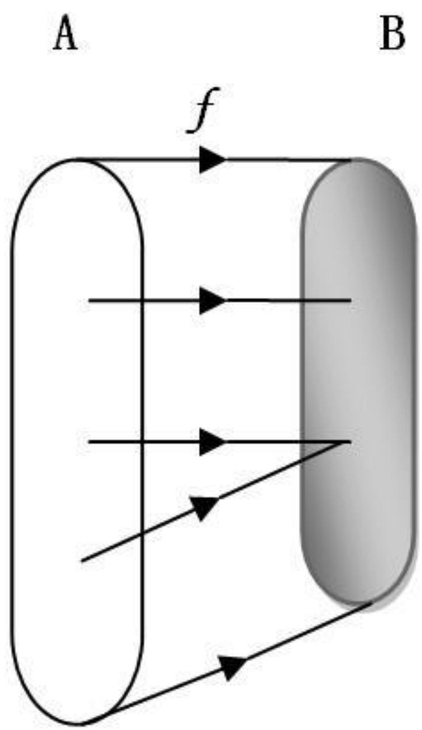
2. 若 $f(A) = B$，则称 f 是 A 到 B 的**满射**。

3. 若 f 既是单射又是满射，则称它是 A 到 B 的**双射**。

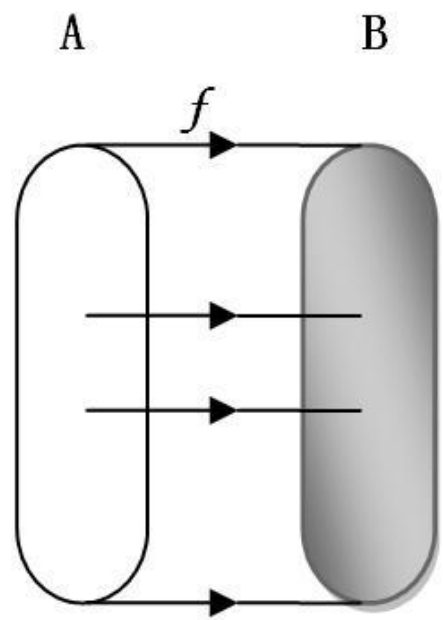
集合与映射



单射



满射



双射

集合与映射

定义7.1.4 设A、B、C是三个集合，有两个映射：

$$f: \quad A \to B$$

$$g: \quad B \to C$$

则由 f 和 g 可确定一个 A 到 C 的映射 h,

$$h: \quad a \to g(f(a))$$

称 h 为 f 与 g 的合成，记作 $h = gf$，亦即

$$h(a) = (gf)(a) = g(f(a))$$

$$gf(a) = g(f(a))$$

清華大学 Tsinghua University

集合与映射

- 映射的合成一般不满足交换律，

  但是满足结合律。

例如： $\alpha:\quad A\rightarrow B$， $\beta:\quad B\rightarrow C$， $\gamma:\quad C\rightarrow D$

$$\gamma(\beta(\alpha(a)))=(\gamma\beta)(\alpha(a))=((\gamma\beta)\alpha)(a)$$

$$\gamma(\beta(\alpha(a)))=\gamma((\beta\alpha)(a))=(\gamma(\beta\alpha))(a)$$

$$\gamma(\beta\alpha)=(\gamma\beta)\alpha$$

集合与映射

- 定理7.1.1 设f是A到B的映射，I_A和I_B分别是A与B中的恒等映射，则

$$I_B f = f \quad , \quad f I_A = f$$

证明：

- $I_B f$和f具有相同的定义域A和相同的值域B，且对于任意的$a \in A$，都有

$$I_B f(a) = I_B(f(a)) = f(a)$$

- 因此 $I_B f = f$
- 同理可证：$f I_A = f$

集合与映射

- 定义7.1.5 设两个映射：

$$f: \quad A \to B \qquad g: \quad B \to A$$

若 $gf = I_A$ 成立，则称 f 是左可逆映射，g 是右可逆映射，并称 g 是 f 的左逆映射，f 是 g 的右逆映射。

又若 $fg = I_B$ 也成立，则称 f 和g 都是可逆映射。

思考：可逆映射是否一定是双射？

集合与映射

- 定理7.1.2 A 到 B 的映射f：

  f是左可逆的充要条件是f为单射

  f是右可逆的充要条件是f为满射

集合与映射

- 证明：
  - 必要性：f左可逆 $\Longrightarrow$ f为单射
  - 如何证明f是单射？

$$\forall a_1, a_2 \in A \quad f(a_1) = f(a_2) \ \Rightarrow \ a_1 = a_2$$

  - 由f左可逆，可知必存在 g： $B \to A$，使得 $gf = I_A$

$$a_1 = I_A(a_1) = gf(a_1) = g(f(a_1)) = g(f(a_2)) = gf(a_2) = I_A(a_2) = a_2$$

必要性得证！

集合与映射

- 证明：
  - 充分性：f为单射 $\Longrightarrow$ f左可逆
  - 如何证明f左可逆？构造g！ $gf = I_A$
  - 定义g： $B \to A$ 如下：

$$g(b)=\begin{cases} a, & 若存在a\in A,使f(a)=b \\ a_0, & 若b\notin f(A) \quad 且a_0\in A \end{cases}$$

  - 此时， $\forall a \in A \quad gf(a)=g(f(a))=g(b)=a$
  - 因此 $gf = I_A$

充分性也得证！

Tsinghua University

集合与映射

- 定理7.1.2 A 到 B 的映射f:

  f是左可逆的充要条件是f为单射

  f是右可逆的充要条件是f为满射

集合与映射

- 推论：$f: A \to B$ 是可逆映射，当且仅当 f 是双射

集合与映射

- 定理7.1.3 设 f 是 A 到 B 的映射。

  且 $gf = I_A$， $fh = I_B$， 则 $g = h$

  证明：

$$g = gI_B = g(fh) = (gf)h = I_A h = h$$

可逆映射的逆映射是唯一的！

主要内容

- 7.1 集合与映射
- **7.2 等价关系**
- 7.3 代数系统的概念
- 7.4 同构与同态

等价关系

- 定义7.2.0 设A，B是集合，称集合

$$\{\langle a,b\rangle \mid a\in A, b\in B\}$$

是A和B的笛卡儿积，记为A×B

等价关系

- 对于集合A到集合B的任何一个映射 f，都可以写出很多二元组 (a,b)，其中 $a \in A$，$b \in B$。显然，这是A×B的子集。

- 我们将映射的概念加以推广，即定义域不一定是A本身，定义域元素对应值域元素也不一定是唯一的，就引出二元关系。

等价关系

- 定义7.2.1 集合 A 和 B 的笛卡儿积 A×B 的任一子集 R 称为A 与 B 之间的一个**二元关系**，它的元素是有序对 (a,b)，记为 aRb，其中 $a\in A, b\in B$。当 $(a,b)\notin R$ 时，说 a 与 b 没有 R 关系，记作 $a\not R b$。
- 当A=B时，称 R 为集合 A 上的二元关系

等价关系

- 定义7.2.2 设R是集合A上的二元关系，如果
  1.对所有的$a \in A$，都有aRa，即R具有**自反性**
  2.对所有的$a,b \in A$，若aRb，则bRa，即R具有**对称性**
  3.对所有的$a,b,c \in A$，若aRb，bRc，则aRc，即R具有**传递性**

则称R是A上的**等价关系**。用符号**~**表示。

等价关系

- 设R是集合A上的一个等价关系，对任一元素 $a \in A$，可以把所有与a有R关系的元素构成一个集合，称之为A的一个等价类，记做 $\overline{a}$，即 $\overline{a} = \{x \in A \mid x \sim a\}$

  其中，a为该等价类的代表元

Tsinghua University

等价关系

- 等价类 $\overline{a}$ 的性质：

1. $a \in \overline{a}$

2. 若 $b, c \in \overline{a}$，则 $b \sim c$

   等价类中任两个元素都有等价关系！

3. 若 $b \in \overline{a}$ 且 $b \sim x$，则 $x \in \overline{a}$

   任两个有等价关系的元素都在同一等价类中！

等价关系

- 定理7.2.1 设～是A上的一个等价关系，对任意元素 $a,b \in A$

若非 $\overline{b} = \overline{a}$

则有 $\overline{b} \cap \overline{a} = \phi$

等价关系

- 定理7.2.2　设$\overline{a_1},\overline{a_2},\cdots,\overline{a_n}$是A上由等价关系～确定的全部等价类，那么

$$\bigcup_{i=1}^{n}\overline{a_1}=A \qquad \overline{a_i}\bigcap_{i\neq j}\overline{a_j}=\phi$$

集合A上的等价关系～可确定它的一个划分！

等价关系

- 把由等价关系～确定的等价类的集合称为等价类族，用 $\overline{A}$ 表示：

$$\overline{A}=\{\ \overline{a}\mid a\in A\ \}$$

为表示等价类族是由等价关系～确定的，常使用记号A/~表示 $\overline{A}$，并称之为集合A关于～的商集

商集就是由A上等价关系~确定的等价类的集合

等价关系

- 商集A/~确定后，对每一个 $a \in A$，它必定属于唯一的等价类，即对应商集中某个确定元 $\bar{a}$。

- 令映射 γ： $a \to \bar{a}$ 为集合A到A/~的一个映射，称之为A到A/~的自然映射

- 显然，自然映射为满射

Tsinghua University

等价关系

- 思考
  - 集合A上的等价关系~可以确定A的一个划分
  - 那么，如果给定集合A的一个划分，能否确定一个集合A上的等价关系呢?

等价关系

- 定理7.2.3 集合A的一个划分可以确定A的一个等价关系！

证明：

- 假定 $A=\bigcup A_i$ ，$(i=1,2,\cdots,n)$
- 构造关系R：

$$R=\{(x,y)\mid \exists A_i, x\in A_i 且 y\in A_i\}$$

- 如果能够证明A上的关系R满足自反性、对称性、传递性，即可说明该关系为等价。

等价关系-小结

- 基本概念：
  - 二元关系、等价关系
  - 等价类、代表元
- 等价类的性质
  - 等价类的基本性质
  - 商集的概念
  - 等价类与集合划分的关系

主要内容

- 7.1 集合与映射
- 7.2 等价关系
- **7.3 代数系统的概念**
- 7.4 同构与同态

Tsinghua University

代数系统的概念

- 定义7.3.1 设A是非空集合，A^2到A的一个映射 f： $A^2 \to A$ 称为A的一个二元代数运算，简称二元运算

- 定义7.3.2 设A是非空集合，A^n到A的一个映射 f： $A^n \to A$ 称为A的一个 n 元代数运算，简称n元运算

代数系统的概念

- 定义7.3.3 设A是一个非空集合，$f_1, f_2, \cdots, f_s$ 分别是A的 $k_1, k_2, \cdots, k_s$ 元运算，$k_i(i=1,2,\cdots,s)$ 是正整数。称集合A和运算 $f_1, f_2, \cdots, f_s$ 所组成的系统为一个**代数系统**(或一个**代数结构**)，简称为一个**代数**，用记号 $(A, f_1, f_2, \cdots, f_s)$ 表示。当A是有限集合时，也称该系统是**有限代数系统**。

代数系统的概念

- 例： $(R, +, \times)$ 是一个代数系统，其中R为实数集，运算为普通的加法和乘法。

- 例： $(M_n(R), \times)$是一个代数系统，其中$M_n(R)$是全体 $n\times n$ 实矩阵的集合，运算为通常的矩阵乘法。

清華大學 Tsinghua University

代数系统的概念

- 思考：
  - 如何判定一个给定的系统是代数系统？

$(R, \ +, \ \times)$　　**1. 定义的运算应该满足映射成立条件**

$(R, \ \div)$　　**2. 所有运算的封闭性**

$(R, \ -)$

$(N, \ -)$

代数系统的概念

- 例：给定一个系统，集合 $X=\{a,b,c,d\}$，定义二元运算 • 如下表：

•	a	b	c	d
a	a	b	c	d
b	b	c	b	d
c	c	a	b	c
d	c	a	c	c

代数系统的概念

- 例：设 $Z_m=\{\overline{0},\overline{1},\cdots,\overline{m-1}\}$ 是整数模 m 同余所确定的等价类集合，Z_m 上的运算 + 定义如下：

$$\overline{i}+\overline{j}=\overline{(i+j)(\bmod\ m)}$$

则 $(Z_m\ ,+)$ 是代数系统！

我们称该运算为模 m 加法运算。

清華大學 Tsinghua University

代数系统的概念

- 代数系统 $(X, \bullet)$ 中

  如果 $\forall x_i, x_j \in X$ ，

  都有 $x_i \cdot x_j = x_j \cdot x_i$ 成立，

  则称 $(X, \bullet)$ 对于二元运算•适合交换律。

$(M_n(R), +)$

$(M_n(R), \times)$

Tsinghua University

代数系统的概念

- 代数系统 $(X, \bullet)$ 中

  如果 $\forall x_i, x_j, x_k \in X$ ，

  都有 $(x_i \cdot x_j) \cdot x_k = x_i \cdot (x_j \cdot x_k)$ 成立，

  则称代数系统 $(X, \bullet)$ 对于 $\bullet$ 适合**结合律**。

$(R, +, \times)$

$(R, -)$

$(R^+, \div)$

代数系统的概念

- 定理7.3.1 若 $(X, \bullet)$ 对二元运算•适合结合律，则对于任何正整数 m 和 n，有

1. $x^m \cdot x^n = x^{m+n}$
2. $\left(x^m\right)^n = x^{m \times n}$

指数律！

Tsinghua University

代数系统的概念

- 定义7.3.4 给定一个代数系统 $V=(X,\ \bullet)$，如果 $\exists e_L \in X$，使得 $\forall x \in X$，都有 $e_L \times x = x$，则称 e_L 是X上关于运算•的一个左单位元。

代数系统的概念

- 定理7.3.2 若代数系统 $V=(X, \bullet)$ 既有左单位元 e_L，又有右单位元 e_R，则 $e=e_L=e_R$ 是X的唯一的单位元。

代数系统单位元唯一！

代数系统的概念

- 例：$(R, +)$ 单位元是 “0”

  $(R, \times)$ 单位元是 “1”

  $(R, -)$ 右单位元是 “0”

代数系统的概念

- 定义7.3.5 设 $V=(X,\ \bullet)$ 是有单位元 e 的代数系统，对于 $x\in X$，若 $\exists x'\in X$，使得 $x'\cdot x=e$，则称 x 是左可逆的，并称 x' 是 x 的一个左逆元；若 $\exists x''\in X$，使得 $x\cdot x''=e$，则称 x 是右可逆的，并称 x'' 是 x 的一个右逆元；若 x 既是左可逆的又是右可逆的，则说 x 是可逆元。

代数系统的概念

- 定理7.3.3 设代数系统 $V=(X, \bullet)$ 具有单位元e，且适合结合律，对于 $x \in X$ ，如果x 有左逆元x'，又有右逆元x''，则 x 有唯一逆元 $x^{-1}=x'=x''$ ，并且 $\left(x^{-1}\right)^{-1}=x$ 。

代数系统逆元素唯一！

代数系统的概念

- 如果代数系统 $V=(X,\ \bullet)$ 中每个元都有逆元，

  则 $\forall a,b,c \in X$

$$ab = ac \quad \Rightarrow \quad b = c$$

$$ba = ca \quad \Rightarrow \quad b = c$$

消去律！

代数系统的概念-小结

- 基本概念：
  - 二元运算、n元运算
  - 代数系统定义
  - 代数系统的判定
- 代数系统的运算
  - 结合律、交换律、指数律、消去律
- 代数系统的单位元
- 代数系统中的逆元素

清華大學 Tsinghua University

主要内容

- 7.1 集合与映射
- 7.2 等价关系
- 7.3 代数系统的概念
- **7.4 同构与同态**

同构与同态

- 有些代数系统，它们除了元素的名称和运算符号不同以外，在结构上是没有差别的

例：

$(\{a,b\}, \bullet)$　　　　$(\{0,1\}, \times)$

$\bullet$	a	b
a	a	b
b	b	a

$\times$	0	1
0	0	1
1	1	0

同构与同态

- 定义7.4.1 设$V_1=(X,o_1,o_2,\cdots,o_r)$和$V_2=(Y,\overline{o_1},\overline{o_2},\cdots,\overline{o_r})$是两个代数系统，若$o_i$和$\overline{o_i}$都是$k_i$元运算，且$k_i(i=1,2,\cdots,r)$是正整数

  则说代数系统V_1和V_2是**同类型**的。

Tsinghua University

同构与同态

- 定义7.4.2 设 $(X, \bullet)$ 和 $(Y, *)$ 是两个同类型的代数系统，$f: \quad X \to Y$ 是一个双射。

  如果 $\forall a,b \in X$，恒有 $f(a \bullet b) = f(a) * f(b)$

  则称 f 是 $(X, \bullet)$ 到 $(Y, *)$ 的一个同构映射，

  并称 $(X, \bullet)$ 与 $(Y, *)$ 同构，用 $X \cong Y$ 表示。

同构与同态

- 定义7.4.3 设$(X, \bullet)$和$(Y, *)$是两个同类型的代数系统，$f: \quad X \to Y$是一个映射。

  如果$\forall a,b \in X$，恒有$f(a \bullet b) = f(a) * f(b)$

  则称f是$(X, \bullet)$到$(Y, *)$的一个同态映射，

  简称同态。

同构与同态

- 问题：
  - 如果给定一个映射 $f: \quad X \to Y$ 是从代数系统 $(X, \bullet)$ 到 $(Y, *)$ 的一个同态，则必定有 $f(X) \subseteq Y$
  - 那么，$f(X)$ 和运算 * 是否能够构成一个代数系统？

同构与同态

- 定义7.4.4 设$(X,\ \bullet)$是一个代数系统，R是X的一个非空子集，如果R在运算•下是封闭的，则称$(R,\ \bullet)$是$(X,\ \bullet)$的一个子代数系统或子代数。

同构与同态

- 定理7.4.1 设映射 $f: \quad X \to Y$ 是从代数系统 $(X, \bullet)$ 到 $(Y, *)$ 的一个同态，则 $(f(X), *)$ 是 $(Y, *)$ 的一个子代数，并称 $f(X)$ 是在 f 作用下 X 的**同态象**

同构与同态

- 定义7.4.5 设映射 $f: X \to Y$ 是从代数系统 $(X, \bullet)$ 到 $(Y, *)$ 的一个同态，如果：

1. f 是单射，则称 f 为单一同态
2. f 是满射，则称 f 是满同态，用 $X \sim Y$ 表示，并称 Y 是 X 的一个同态象。

同构与同态

- 定理7.4.2 给定代数系统 $(X, \bullet)$ 和 $(Y, *)$，其中 $\bullet$ 和 $*$ 都是二元运算。

设 f： $X \to Y$ 是 $(X, \bullet)$ 到 $(Y, *)$ 的满同态，则

1、如果 $\bullet$ 是可交换的或可结合的运算，则 $*$ 也是可交换的或可结合的运算。

2、若 $(X, \bullet)$ 中运算 $\bullet$ 具有单位元 e，则 $(Y, *)$ 中运算 $*$ 具有单位元 $f(e)$ 。

3、对运算 $\bullet$，如果每一个元素 $x \in X$ 都有逆元 x^{-1}，则对运算 $*$，每一个元素 $f(x) \in Y$ 都具有逆元 $f(x^{-1})$

Tsinghua University

同构与同态

- 定义7.4.6 代数系统 $(X, \bullet)$ 上的同态映射

$$f: \quad X \to X$$

称为**自同态**，若 f 是同构映射，则称之为**自同构**。

同构与同态-小结

- 基本概念：
  - 同类型代数系统
  - 同构、同态
  - 子代数系统
  - 单一同态、满同态
  - 自同态、自同构
- 同态基本性质

主要内容

- 7.1 集合与映射
- 7.2 等价关系
- 7.3 代数系统的概念
- **7.4 同构与同态**