离散数学讲义

陈建文

May 13, 2020

课程学习目标：

1. 训练自己的逻辑思维能力和抽象思维能力
2. 训练自己利用数学语言准确描述计算机科学问题和电子信息科学问题的能力

学习方法：

1. MOOC自学
2. 阅读该讲义
3. 做习题
4. 学习过程中有不懂的问题，在课程QQ群中与老师交流

授课教师QQ：2129002650

第 二 章　映射

定义2.1. **设**X和Y为两个非空集合。一个从X到Y的**映射**f为一个法则，根据f，对X中的每个元素x都有Y中唯一确定的元素y与之对应。从X到Y的映射f常记为$f: X \to Y$。

例. 设集合$X = \{-1, 0, 1\}$，集合$Y = \{0, 1, 2\}$，$\forall x \in X, f(x) = x^2$，即$f(-1) = 1, f(0) = 0, f(1) = 1$，则$f$为从集合$X$到集合$Y$的映射。

定义2.2. 设X和Y为两个非空集合。一个从X到Y的**映射**为一个满足以下两个条件的$X \times Y$的子集f：

1. 对X的每一个元素x，存在一个$y \in Y$，使得$(x, y) \in f$；
2. 若$(x, y) \in f$，$(x, y') \in f$，则$y = y'$。

$(x, y) \in f$记为$y = f(x)$。

例. 设集合$X = \{-1, 0, 1\}$，集合$Y = \{0, 1, 2\}$，$f = \{(-1, 1), (0, 0), (1, 1)\}$，则$f$为从集合$X$到集合$Y$的映射。

定义2.1和定义2.2是等价的。

定义2.3. 设f为从集合X到集合Y的映射，$f: X \to Y$，　如果$y = f(x)$，则称y为x在f下的**象**，称x为y的**原象**。X称为f的**定义域**；集合$\{f(x) | x \in X\}$称为f的**值域**，记为$Im(f)$。

定义2.4. 设$f: X \to Y$，$A \subseteq X$，当把f的定义域限制在A上时，就得到了一个$\phi: A \to Y$，$\forall x \in A$，$\phi(x) = f(x)$。ϕ称为f在A上的限制，并且常用$f|A$来表示ϕ。反过来，我们也称f为ϕ在X上的扩张。

定义2.5. 设$f: A \to Y$，$A \subseteq X$，则称f为X上的一个部分映射。

定义2.6. 两个映射f与g称为是相等的当且仅当f和g都为从X到Y的映射，并且$\forall x \in X$总有$f(x) = g(x)$。

定义2.7. 设$f: X \to X$，如果$\forall x \in X, f(x) = x$，则称$f$为$X$上的恒等映射。$X$上的恒等映射常记为$I_X$。

定义2.8. 设$f: X \to Y$，如果$\forall x_1, x_2 \in X$，只要$x_1 \neq x_2$，就有$f(x_1) \neq f(x_2)$，则称f为从X到Y的**单射**。

定义2.9. 设$f : X \to Y$，如果$\forall y \in Y$，$\exists x \in X$使得$f(x) = y$，则称f为从X到Y的**满射**。

定义2.10. 设$f : X \to Y$，如果f既是单射又是满射，则称f为从X到Y的**双射**，或者称f为从X到Y的一一对应。

定义2.11. 设$f : X \to Y$，$A \subseteq X$，A在f下的**象**定义为

$$f(A) = \{f(x)|x \in A\}$$

例. 设$f : \{-1, 0, 1\} \to \{-1, 0, 1\}$，$f(x) = x^2$，则$f(\{-1, 0\}) = \{0, 1\}$

定义2.12. 设$f : X \to Y$，$B \subseteq Y$，B在f下的**原象**定义为

$$f^{-1}(B) = \{x \in X|f(x) \in B\}$$

例. 设$f : \{-1, 0, 1\} \to \{-1, 0, 1\}$，$f(x) = x^2$，则$f^{-1}(\{-1, 0\}) = \{0\}$

定理2.1. 设$f : X \to Y$，$A \subseteq Y$，$B \subseteq Y$，则

1. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$
2. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
3. $f^{-1}(A^c) = (f^{-1}(A))^c$
4. $f^{-1}(A \triangle B) = f^{-1}(A) \triangle f^{-1}(B)$

定理2.2. 设$f : X \to Y$，$A \subseteq X$，$B \subseteq X$，则

1. $f(A \cup B) = f(A) \cup f(B)$
2. $f(A \cap B) \subseteq f(A) \cap f(B)$
3. $f(A \triangle B) \supseteq f(A) \triangle f(B)$

定义2.13. 设$f : X \to Y$，$g : Y \to Z$为映射，映射f与g的**合成**$g \circ f : X \to Z$定义为

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

定理2.3. 设$f : X \to Y$，$g : Y \to Z$，$h : Z \to W$ 为映射，则

$$(h \circ g) \circ f = h \circ (g \circ f)$$

定义2.14. 设$f : X \to Y$为双射，f的**逆映射**$f^{-1} : Y \to X$定义为：对任意的$y \in Y$，存在唯一的x使得$f(x) = y$,则$f^{-1}(y) = x$。

定义2.15. 设$f : X \to Y$为一个双射, 则$g : Y \to X, g = \{(y, x)|(x, y) \in f\}$称为$f$的**逆映射**，记为$g = f^{-1}$。

例. 设集合$X = \{1, 2, 3\}$，$Y = \{4, 5, 6\}$，$f = \{(1, 4), (2, 5), (3, 6)\}$为从$X$到$Y$的双射，则$f^{-1} = \{(4, 1), (5, 2), (6, 3)\}$。

定义2.16. 设$f: X \to Y$为一个映射。如果存在一个映射$g: Y \to X$使得

$$f \circ g = I_Y \text{且} g \circ f = I_X,$$

则称映射f为**可逆**的，而g称为f的**逆映射**。

例. 设集合$X = \{1, 2, 3\}$，$Y = \{4, 5, 6\}$，$f = \{(1, 4), (2, 5), (3, 6)\}$为从$X$到$Y$的双射，$g = \{(4, 1), (5, 2), (6, 3)\}$,由于$f \circ g = I_Y$且$g \circ f = I_X$，$f^{-1} = g$。

定理2.4. *定义2.15和定义2.16是等价的。*

证明. 设f为从集合X到集合Y的映射，g为从集合Y到集合X的映射。

以下先假设g满足定义2.15，往证g满足定义2.16。

假设f为从集合X到集合Y的满射，g为从集合Y到集合X的映射，$g = \{(y, x) | (x, y) \in f\}$，易验证$f \circ g = I_Y$且$g \circ f = I_X$。

接下来，假设g满足定义2.16，往证g满足定义2.15。

假设f为从集合X到集合Y的映射，存在一个映射$g : Y \to X$使得$f \circ g = I_Y$且$g \circ f = I_X$,往证f为双射，且$g = \{(y, x) | (x, y) \in f\}$。

对任意的$x_1 \in X$，$x_2 \in X$，如果$f(x_1) = f(x_2)$，则$g(f(x_1) = g(f(x_2))$，再由$g \circ f = I_X$知$x_1 = x_2$，从而f为单射。对任意的$y \in Y$，由$f \circ g = I_Y$知$f(g(y)) = y$，从而f为满射。这证明了f为双射。

以下证明$g = \{(y, x) | (x, y) \in f\}$，这就是要证明左边的集合等于右边的集合。

对任意的$(y, x) \in g$，则$x = g(y)$，从而$f(x) = f(g(y))$，由$f \circ g = I_Y$知$f(x) = y$，从而$(x, y) \in f$。

对任意的$(x, y) \in f$，则$y = f(x)$，从而$g(y) = g(f(x))$，由$g \circ f = I_X$知$g(y) = x$，从而$(y, x) \in g$。 □

定理2.5. *设$f : X \to Y$为可逆映射，则$(f^{-1})^{-1} = f$。*

定理2.6. *设$f : X \to Y$，$g : Y \to Z$都为可逆映射，则$g \circ f$也为可逆映射并且$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$。*

定义2.17. 设$f : X \to Y$为一个映射，如果存在一个映射$g : Y \to X$ 使得$g \circ f = I_X$，则称f为左可逆的，g称为f的左逆映射；如果存在一个映射$h : Y \to X$ 使得$f \circ h = I_Y$，则称f为右可逆的，h称为f的右逆映射。

定理2.7. *设$f : X \to Y$为一个映射，则*

1. *f左可逆当且仅当f为单射；*
2. *f右可逆当且仅当f为满射。*

证明. 先证(1)。

设f为左可逆的，则存在一个映射$g : Y \to X$ 使得$g \circ f = I_X$。对任意的$x_1 \in X$，$x_2 \in X$，如果$f(x_1) = f(x_2)$，则$g(f(x_1) = g(f(x_2))$，再由$g \circ f = I_X$知$x_1 = x_2$，从而f为单射。

设f为单射，则f为从集合X到$Im(f)$的双射。于是，有$g : Im(f) \to X$使得$g \circ f = I_X$。扩充g到Y上：对任意的$y \in Y$，若$y \in Y \setminus Im(f)$，则$g(y)$不变，

而当$y \in Im(f)$时，规定$g(y)$为X中任意一个固定的元素x_0，则g为从集合Y到集合X的映射，且$g \circ f = I_X$。所以，f为左可逆的。

再证(2)。

设f为右可逆的，则存在一个映射$g: Y \to X$ 使得$f \circ g = I_Y$。对任意的$y \in Y$，由$f \circ g = I_Y$知$f(g(y)) = y$，从而f为满射。

设f为满射，则对任意的$y \in Y$，$f^{-1}(\{y\}) \neq \phi$。令$g: Y \to X$，其定义为，对任意的$y \in Y$，$g(y) = x$，其中x为$f^{-1}(\{y\})$中一个特定元素。于是，对任意的$y \in Y$，设$g(y) = x$，则$f(x) = y$，从而$(fg)(y) = f(g(y)) = f(x) = y = I_y(y)$。所以$fg = I_y$，即$f$为右可逆的。 □

定义2.18. 有穷集合S到自身的一一对应称为S上的一个置换。如果$|S| = n$，则S上的置换就说成是n次置换。

设$S = \{1, 2, \ldots, n\}$，$\sigma : S \to S$为S上的一个置换，$\sigma(1) = k_1$，$\sigma(2) = k_2$，…，$\sigma(n) = k_n$，我们用如下的一个表来表示置换σ:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}$$

例. 设$S = \{1, 2, 3, 4\}$，$\sigma(1) = 3$，　$\sigma(2) = 2$，　$\sigma(3) = 4$，　$\sigma(4) = 1$，则σ可以表示为

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

这里，列的次序无关紧要，例如，σ还可以表示为

$$\sigma = \begin{pmatrix} 2 & 1 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

定义2.19. 设α与β为集合$S = \{1, 2, 3, 4\}$上的两个置换，则α与β为两个从S到S的双射，讨论置换时，我们用$\alpha\beta$表示α与β的合成$\beta \circ \alpha$。注意这里α与β的次序，从运算的角度看有一定的便利性，但也有的教材中采用相反的顺序。按照我们的写法，讨论置换时，如果$i \in S$，则用$(i)\alpha$表示i在α下的像，简记为$i\alpha$。

例. 设$S = \{1, 2, 3\}$，α和β为S上的两个置换，

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

，则

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

，

若α与β为两个n次置换，当把β的表示式中的上一行按α的下一行的顺序写出时，则$\alpha\beta$的下一行就是β的新表示式中的下一行。

例. 设$S=\{1,2,3\}$，α和β为S上的两个置换，

$$\alpha=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\beta=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

，则

$$\alpha\beta=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&3&2\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

，

定义2.20. 设σ为S上的一个n次置换，若$i_1\sigma=i_2$，$i_2\sigma=i_3$，$\cdots$，$i_{k-1}\sigma=i_k$，$i_k\sigma=i_1$，而$\forall i\in S\setminus\{i_1,i_2,\ldots,i_k\}$，$i\sigma=i$，则称$\sigma$为一个$k$循环置换，记为$(i_1i_2\cdots i_k)$。$2-$循环置换称为对换。

例. 设$S=\{1,2,3,4,5\}$，则

$$(1,2,3)=\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix},(2,3)=\begin{pmatrix}1&2&3&4&5\\1&3&2&4&5\end{pmatrix}$$

定理2.8. 每个置换都能被分解成若干个没有共同数字的循环置换的乘积。如果不计这些循环置换的顺序以及略去的$1-$循环置换，这个分解是唯一的。

定理2.9. 当$n\geq 2$时，每个n次置换都能被分解成若干个对换的乘积。

定理2.10. 如果把置换分解成若干个对换的乘积，则对换个数的奇偶性是不变的。

证明. 设σ为一个n次置换。σ的符号$sign(\sigma)$定义为$(-1)^{|\{(x,y)|x<y\wedge(x)\sigma>(y)\sigma\}|}$。

设$\alpha=\beta(i,j)$，$i<j$，此时如果$(i)\beta>(j)\beta$,则$(i)\alpha<(j)\alpha$；反之，如果$(i)\beta<(j)\beta$,则$(i)\alpha>(j)\alpha$。

易知，$sign(\alpha)=-sign(\beta)$。

于是，如果置换σ可以分解为m个对换的乘积$\sigma=I(i_1,k_1)(i_2,k_2)\cdots(i_m,k_m)$，其中$I$为恒等置换，由$sign(I)=1$知$sign(\sigma)=(-1)^m$。而$sign(\sigma)$只能为1和$-1$两者之一，因此如果$\sigma$能分解成偶数个对换的乘积，则只能分解成偶数个对换的乘积；如果σ能分解成奇数个对换的乘积，则只能分解成奇数个对换的乘积。 □

定义2.21. 能被分解为偶数个对换的乘积的置换称为偶置换；能被分解为奇数个对换的乘积的置换称为奇置换。

定理2.11. 当$n\geq 2$时，n次奇置换的个数与n次偶置换的个数相等，都等于$\frac{n!}{2}$。

定义2.22. 一个集合及其在该集合上定义的若干个代数运算合称为一个代数系。

我们熟知的实数集R，与其上的加法运算”+”和乘法运算”$*$”一起构成了一个代数系，满足如下性质：

定理2.12. 设$x,y,z\in\mathbb{R}$，则

1. $x + y = y + x$
2. $(x + y) + z = x + (y + z)$
3. $0 + x = x + 0 = x$
4. $(-x) + x = x + (-x) = 0$
5. $x * y = y * x$
6. $(x * y) * z = x * (y * z)$
7. $1 * x = x * 1 = x$
8. $x^{-1} * x = x * x^{-1} = 1$
9. $x * (y + z) = x * y + x * z$
10. $(y + z) * x = y * x + z * x$

定义2.23. 设X，Y，Z为任意三个非空集合。一个从$X \times Y$到Z的映射ϕ 称为X与Y到Z的一个二元（代数）运算。当$X = Y = Z$时，则称ϕ为X上的二元(代数)运算。

定义2.24. 从集合X到Y的任一映射称为从X到Y的一元(代数)运算。如果$X = Y$，则从X到X的映射称为X上的一元(代数)运算。

定义2.25. 设$A_1, A_2, \cdots, A_n, D$为非空集合。一个从$A_1 \times A_2 \times \cdots \times A_n$到$D$的映射$\phi$称为$A_1, A_2, \cdots, A_n$到$D$的一个$n$元（代数）运算。如果$A_1 = A_2 = \cdots = A_n = D = A$，则称$\phi$为$A$上的$n$元代数运算。

定义2.26. 设"$\circ$"为集合X上的一个二元代数运算。如果$\forall a, b \in X$，恒有
$a \circ b = b \circ a$，则称二元代数运算"$\circ$"满足交换律。

定义2.27. 设"$\circ$"为集合X上的一个二元代数运算。如果$\forall a, b, c \in X$，恒有$(a \circ b) \circ c = a \circ (b \circ c)$，则称二元代数运算"$\circ$"满足结合律。

定义2.28. 设"$+$"与"$\circ$"为集合X上的两个二元代数运算。
如果$\forall a, b, c \in X$，恒有

$$a \circ (b + c) = a \circ b + a \circ c,$$

则称二元代数运算"$\circ$"对"$+$"满足左分配律。如果$\forall a, b, c \in X$，恒有

$$(b + c) \circ a = b \circ a + c \circ a,$$

则称二元代数运算"$\circ$"对"$+$"满足右分配律。

定义2.29. 设$(X, \circ)$为一个代数系。如果存在一个元素$e \in X$使得对任意的$x \in X$恒有$e \circ x = x \circ e = x$，则称$e$为"$\circ$"的单位元素。

定义2.30. 设$(X, \circ)$为一个代数系，“$\circ$”有单位元素e，$a \in X$，如果$\exists b \in X$使得

$$a \circ b = b \circ a = e,$$

则称b为a的逆元素。

定义2.31. 设$(S, +)$与$(T, \oplus)$为两个代数系。如果存在一个一一对应$\phi : S \to T$，使得$\forall x, y \in S$，有

$$\phi(x + y) = \phi(x) \oplus \phi(y),$$

则称代数系$(S, +)$与$(T, \oplus)$同构，并记为$S \cong T$，ϕ称为这两个代数系之间的一个同构。

定义2.32. 设$(S, +, \circ)$与$(T, \oplus, *)$为两个代数系。如果存在一个一一对应$\phi : S \to T$，使得$\forall x, y \in S$，有

$$\phi(x + y) = \phi(x) \oplus \phi(y),$$
$$\phi(x \circ y) = \phi(x) * \phi(y),$$

则称代数系$(S, +, \circ)$与$(T, \oplus, *)$同构，并记为$S \cong T$，ϕ称为这两个代数系之间的一个同构。

p	q	p ∧ q
T	T	T
T	F	F
F	T	F
F	F	F

p	q	p ∨ q
T	T	T
T	F	T
F	T	T
F	F	F

p	¬ p
T	F
F	T

x	y	x ∧ y
1	1	1
1	0	0
0	1	0
0	0	0

x	y	x ∨ y
1	1	1
1	0	1
0	1	1
0	0	0

x	$\bar{x}$
1	0
0	1

代数系$(\{T, F\}, \wedge, \vee, \neg)$与$(\{1, 0\}, \wedge, \vee, \bar{\ })$是同构的。

定义2.33. 设X为一个集合，$E \subseteq X$。E的特征函数$\chi_E : X \to \{0, 1\}$定义为

$$\chi_E(x) = \begin{cases} 1 & \text{如果} x \in E, \\ 0 & \text{如果} x \notin E. \end{cases}$$

定义2.34. 令$Ch(X) = \{\chi | \chi : X \to \{0, 1\}\}$。$\forall \chi, \chi' \in Ch(X)$及$x \in X$，

$$\begin{aligned} (\chi \vee \chi')(x) &= \chi(x) \vee \chi'(x) \\ (\chi \wedge \chi')(x) &= \chi(x) \wedge \chi'(x) \\ \bar{\chi}(x) &= \overline{\chi(x)} \end{aligned} \tag{2.1}$$

定理2.13. 设X为一个集合，则代数系$(2^X, \cup, \cap, ^c)$与$(Ch(X), \vee, \wedge, ^-)$同构。

定理2.14 (鸽笼原理)**.** 如果把$n+1$个物体放到n个盒子里，则必有一个盒子里至少放了两个物体。

练习2.1. 设$X = \{a, b, c\}, Y = \{0, 1\}, Z = \{2, 3\}$。$f : X \to Y, f(a) = f(b) = 0, f(c) = 1$；$g : Y \to Z, g(0) = 2, g(1) = 3$。试求$g \circ f$。

练习2.2. 设$f : X \to Y$，$C \subseteq Y$，$D \subseteq Y$，证明
$f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$

练习2.3. 设$f : X \to Y$，$A \subseteq X$，$B \subseteq X$，证明
$f(A \setminus B) \supseteq f(A) \setminus f(B)$

练习2.4. 设$f : X \to Y$，$A \subseteq X$，则$(f(A))^c \subseteq f(A^c)$成立吗？$f(A^c) \subseteq (f(A))^c$成立吗?

练习2.5. 设$f : X \to Y$， 证明：f为满射当且仅当$\forall E \in 2^Y, f(f^{-1}(E)) = E$。

练习2.6. 设$f : X \to Y$， 证明：f为单射当且仅当$\forall F \in 2^X, f^{-1}(f(F)) = F$。

练习2.7. 设$f : X \to Y$，$g : Y \to Z$，$A \subseteq Z$，证明：$(gf)^{-1}(A) = f^{-1}(g^{-1}(A))$。

练习2.8. 设$N = \{1, 2, \ldots\}$，试构造两个映射$f : N \to N$与$g : N \to N$，使得$fg = I_N$，但$gf \neq I_N$。

练习2.9. 设$f : X \to Y$，
（1）如果存在唯一的一个映射$g : Y \to X$，使得$gf = I_X$，那么f是否可逆呢?
（2）如果存在唯一的一个映射$g : Y \to X$，使得$fg = I_Y$，那么f是否可逆呢?

练习2.10. 是否存在一个从集合X到X的一一对应，使得$f = f^{-1}$，但$f \neq I_X$?

练习2.11. 已知m个整数$a_1, a_2, \ldots, a_m$，试证：存在两个整数k，l，
$0 \leq k < l \leq m$，使得$a_{k+1} + a_{k+2} + \ldots + a_l$能被$m$整除。

第 三 章