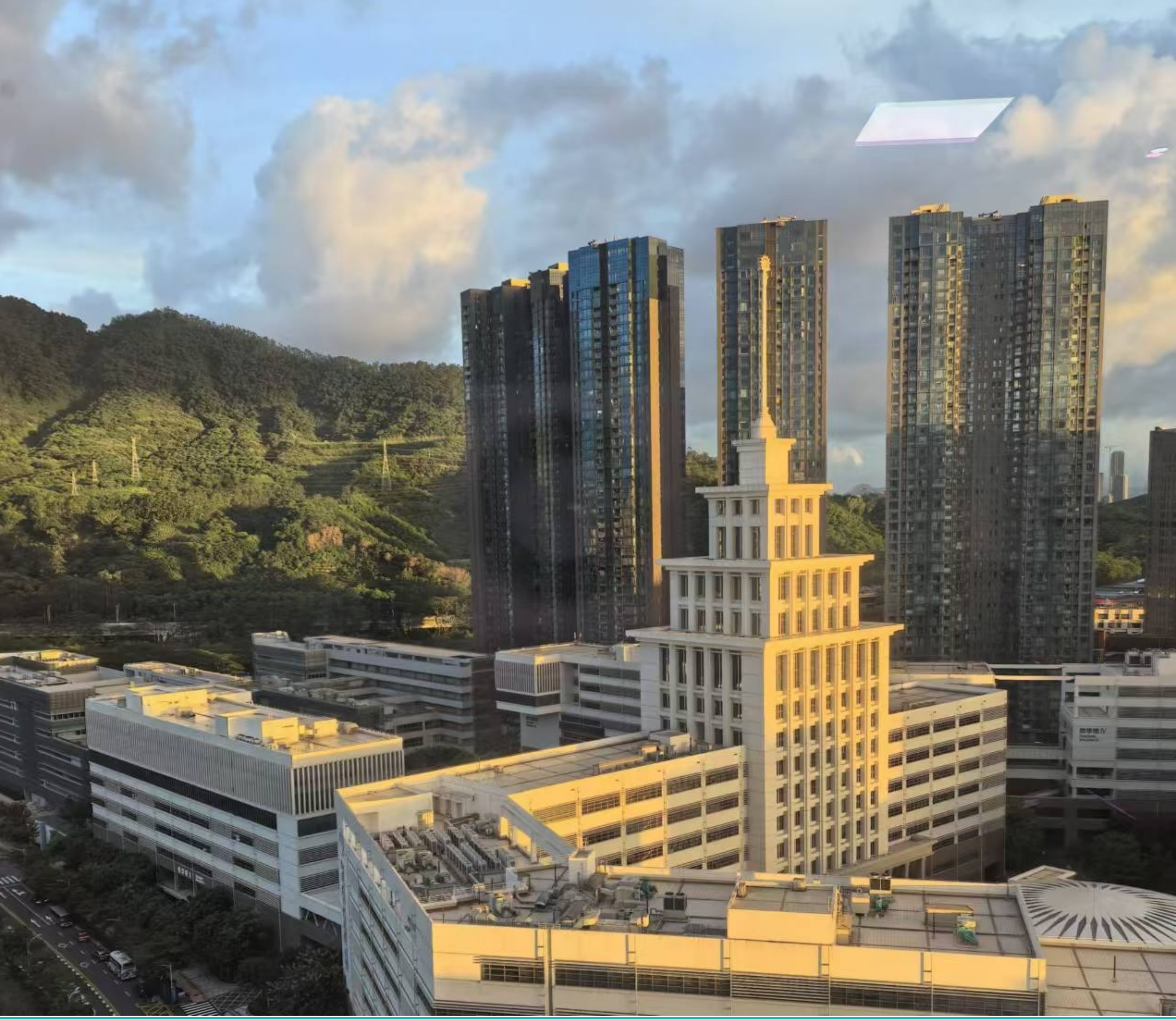

离散数学：补充阅读

作者：李修成 lixiucheng@hit.edu.cn

单位：计算机科学与技术学院

时间：2024/09/08

版本：0.1

目录

第一章 集合代数

内容提要

- 容斥原理 1.2
- 容斥原理推论 1.2

1.1 容斥原理

为证明容斥原理，我们先介绍二项式定理与其推论. 然后使用该推论计数任意元素 a 在容斥原理中被计数的次数.

定理 1.1 (二项式定理 Binomial Theorem)

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} \tag{1.1}$$

推论 1.1

$$\sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}=1 \tag{1.2}$$

证明 令 Eq. 1.1中 $x=-1, y=1$ 有，

$$0=\sum_{k=0}^{n}\binom{n}{k}(-1)^k \Rightarrow 1=\sum_{k=1}^{n}\binom{n}{k}(-1)^{k-1}.$$

定理 1.2 (容斥原理 Inclusion-Exclusion Principle)

令 U 为全集，$A_1, A_2, \ldots, A_n$ 为其子集，则

$$\left|\bigcup_{i=1}^{n}A_i\right|=\sum_{k=1}^{n}(-1)^{k-1}\sum_{1\le i_1<i_2<\ldots<i_k\le n}|A_{i_1}\cap A_{i_2}\cap\ldots\cap A_{i_k}|, \tag{1.3}$$

证明 对任意 a，假设其出现在集合 $A_{i_1}, A_{i_2}, \ldots, A_{i_m}$ 中，$1\le m\le n$. 由集合并的定义可知，其在 Eq. 1.3左侧被计数一次. 现只需证明其被 Eq. 1.3右侧只计数一次即可.

注意，在等式右侧 a 被 $k=1$ 项 $\sum_{i_1}|A_{i_1}|$ 计数 m 次，被 $k=2$ 项 $-\sum_{i_1<i_2}|A_{i_1}\cap A_{i_2}|$ 计数 $-\binom{m}{2}$，更一般的，被第 k 项计数 $(-1)^{k-1}\binom{m}{k}$ 次. 因此，a 被 Eq. 1.3右侧共计数，

$$\binom{m}{1}-\binom{m}{2}+\ldots+(-1)^{m-1}\binom{m}{m}=\sum_{k=1}^{m}(-1)^{k-1}\binom{m}{k}. \tag{1.4}$$

由推论 1.1可知上式值为 1.

推论 1.2 (容斥原理推论)

令 U 为全集，$A_1, A_2, \ldots, A_n$ 为其子集，则

$$|\overline{A}_1\cap\overline{A}_2\cap\ldots\cap\overline{A}_n|=|U|-\sum_{k=1}^{n}(-1)^{k-1}\sum_{1\le i_1<i_2<\ldots<i_k\le n}|A_{i_1}\cap A_{i_2}\cap\ldots\cap A_{i_k}|,\quad 1\le i_1, i_k\le n.$$

证明 由 $\overline{A}_1\cap\overline{A}_2\cap\ldots\cap\overline{A}_n=U-\bigcup_{i=1}^{n}A_i$ 可知 $|\overline{A}_1\cap\overline{A}_2\cap\ldots\cap\overline{A}_n|=|U-\bigcup_{i=1}^{n}A_i|$.

$$\begin{aligned}\left|U-\bigcup_{i=1}^{n}A_i\right| &= |U|-\left|\bigcup_{i=1}^{n}A_i\right| \\ &= |U|-\sum_{k=1}^{n}(-1)^{k-1}\sum_{1\le i_1<i_2<\ldots<i_k\le n}|A_{i_1}\cap A_{i_2}\cap\ldots\cap A_{i_k}|,\end{aligned}$$

其中，第一个等式成立由于 $\bigcup_{i=1}^{n}A_i$ 为 U 的子集，第二个等式使用定理 1.2.

第二章 函数

内容提要

2.1 函数的性质

回忆线性代数中关于线性函数的定义：

定义 2.1 (线性函数 Linear function)

令 V, W 为向量空间，对给定函数 $f : V \mapsto W$，如果对任意 $\mathbf{u}, \mathbf{v} \in V$，$a, b \in \mathbb{R}$ 有，

$$f(a\mathbf{u} + b\mathbf{v}) = af(\mathbf{u}) + bf(\mathbf{v}),$$

则称函数 f 为从向量空间 V 到 W 的线性函数. ♣

定理 2.1 (线性函数的单射)

向量空间 V 上的线性函数 f 为单射当且仅当 $f(\mathbf{v}) = 0 \Rightarrow \mathbf{v} = 0$. ♡

证明 （假设 f 为单射，欲证 $f(\mathbf{v}) = 0 \Rightarrow \mathbf{v} = 0$）由 f 为单射函数可知，

$$f(\mathbf{0}) = f(\mathbf{0} + \mathbf{0}) = f(\mathbf{0}) + f(\mathbf{0}) = 2f(\mathbf{0}),$$

故 $f(\mathbf{0}) = \mathbf{0}$. 又 f 为单射，因此 $f(\mathbf{v}) = 0 \Rightarrow \mathbf{v} = 0$.

（现假设 $f(\mathbf{v}) = 0 \Rightarrow \mathbf{v} = 0$，欲证 f 为单射）对任意 $\mathbf{v}_1, \mathbf{v}_2 \in V$，若 $f(\mathbf{v}_1) = f(\mathbf{v}_2)$，则有

$$\mathbf{0} = f(\mathbf{v}_1) - f(\mathbf{v}_2) = f(\mathbf{v}_1 - \mathbf{v}_2).$$

由假设条件可知，$\mathbf{v}_1 - \mathbf{v}_2 = \mathbf{0}$，即 $\mathbf{v}_1 = \mathbf{v}_2$. 故 f 为单射.

注 定理 2.1告诉我们，一个线性函数为单射的充分必要条件为 f 的零空间（null space）只包含零向量. 实际上，线性映射基本定理（fundamental theorem of linear maps）告诉我们，对于任何有限维向量空间上的线性映射 $f \in \mathcal{L}(V, W)$ 有 $\dim V = \dim \operatorname{null} f + \dim \operatorname{range} f$. 若 f 为矩阵 $\mathbf{A} \in \mathbb{R}^{m \times n}$，则有 $n = \dim \operatorname{null}(\mathbf{A}) + \dim \operatorname{range}(\mathbf{A})$. 零空间只包含零向量则意味着 $\dim \operatorname{null}(\mathbf{A}) = 0$，此时 $\dim \operatorname{range}(\mathbf{A}) = n$，即矩阵 $\mathbf{A}$ 为列满秩 column full rank. 矩阵列满秩等价于其表示的线性映射为单射.

定理 2.2 (函数与集合的势)

令 A, B 为有穷集合，

1. 若从 A 到 B 存在单射函数则 $|A| \le |B|$;
2. 若从 A 到 B 存在满射函数则 $|A| \ge |B|$;
3. 若 $|A| = |B|$ 则 f 为单射 $\iff$ f 为满射 $\iff$ f 为双射. ♡

证明 (1) 假设 $f : A \mapsto B$ 为单射函数，则 $\forall a_1, a_2 \in A, a_1 \ne a_2$ 有 $f(a_1) \ne f(a_2)$. 由于 $f(a_1), f(a_2) \in B$，故 B 至少包含与 A 一样多的元素，即 $|A| \le |B|$.

(2) 假设 $f : A \mapsto B$ 为满射函数，则 $\forall b_1, b_2 \in B, b_1 \ne b_2$ 有 $f^{-1}(b_1), f^{-1}(b_2)$ 非空. 由函数定义可知 $f^{-1}(b_1) \cap f^{-1}(b_2) = \emptyset$. 由于 $A = \cup_{b \in B} f^{-1}(b)$，故 $|A| = \cup_{b \in B} |f^{-1}(b)| \ge |B|$.

(3)（由单射证满射）若 f 为单射，则 $\forall a_1, a_2 \in A, a_1 \ne a_2$ 有 $f(a_1) \ne f(a_2)$，故 $\operatorname{range}(f) = |A| = |B|$，即 f 为满射.

（由满射证单射）若 f 为满射，则由 (2) 可知 $A = \cup_{b\in B} f^{-1}(b)$，其中 $f^{-1}(b)$ 非空且两两不相交. 若 f 不为单射，则至少存在一个 $b \in B$ 有 $|f^{-1}(b)| \geq 2$，从而 $|A| = \cup_{b\in B}|f^{-1}(b)| \geq |B|+1$，与 $|A| = |B|$ 矛盾. 故 f 为单射.

注 定理 2.2-(1) 给了我们一种比较集合大小的方法. 如果能够建立从集合 A 到 B 的单射函数，则可以断定 $|A| \leq |B|$. 定理 2.2-(2) 则告诉我们，A 中只有包含足够多的元素才能覆盖集合 B（以函数映射的方式）. 矩阵 $\mathbf{A} \in \mathbb{R}^{m\times n}$ 可视为从 $\mathbb{R}^n$ 到 $\mathbb{R}^m$ 上的线性函数，若 $\mathbf{A}$ 为单射，则定理2.2要求 $n \leq m$，即矩阵的列数要足够小，保证列线性无关；若 $\mathbf{A}$ 为满射，则定理2.2要求 $n \geq m$，即矩阵的行数要足够小，保证行线性无关.

推论 2.1

令 A, B 为有穷集合，$f : A \mapsto B$ 为从 A 到 B 的函数. 若从 A 到 B 存在双射函数则 $|A| = |B|$.

笔记 对于有穷集合，$|A| = |B|$ 为其上存在双射函数的充分必要条件. 实际上，定理 2.2和推论 2.1对无穷集合亦成立. 康托（Cantor）正是借助函数的单射、双射来比较无穷集合的大小，给 19 世纪末的数学家带来了思想上的巨大冲击，并促使了人类在哲学层面上对无穷和有穷进行了更深层次的思考和讨论.

定理 2.3 (函数的像)

令 $f : A \mapsto B$，$X_1 \subseteq A, X_2 \subseteq A$，则有

1. $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$
2. $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$
3. $f(X_1) - f(X_2) \subseteq f(X_1 - X_2)$
4. 若 f 为单射，则（2）（3）为等式.

证明 (1) 对任意 $y \in f(X_1 \cup X_2)$ 有

$$\begin{aligned}
y \in f(X_1 \cup X_2) &\iff \exists x(x \in X_1 \cup X_2 \ \wedge\ f(x) = y) \\
&\iff \exists x((x \in X_1 \vee x \in X_2)\ \wedge\ f(x) = y) \qquad (2.1)\\
&\iff (\exists x \in X_1 \wedge f(x) = y) \vee (\exists x \in X_2 \wedge f(x) = y)) \qquad (2.2)\\
&\iff y \in f(X_1) \vee y \in f(X_2) \\
&\iff y \in f(X_1) \cup f(X_2).
\end{aligned}$$

(2) 对任意 $y \in f(X_1 \cap X_2)$ 有

$$\begin{aligned}
y \in f(X_1 \cap X_2) &\iff \exists x(x \in X_1 \cap X_2 \ \wedge\ f(x) = y) \\
&\iff \exists x((x \in X_1 \wedge x \in X_2)\ \wedge\ f(x) = y) \qquad (2.3)\\
&\implies (\exists x \in X_1 \wedge f(x) = y) \wedge (\exists x \in X_2 \wedge f(x) = y) \qquad (2.4)\\
&\iff y \in f(X_1) \wedge y \in f(X_2) \\
&\iff y \in f(X_1) \cap f(X_2).
\end{aligned}$$

(3) 对任意 $y \in f(X_1) - f(X_2)$ 有

$$\begin{aligned}
y \in f(X_1) - f(X_2) &\iff y \in f(X_1) \wedge y \notin f(X_2) \\
&\iff (\exists x \in X_1 \text{ s.t. } f(x) \neq y) \wedge (\forall x \in X_2 \text{ s.t. } f(x) \neq y) \qquad (2.5)\\
&\implies \exists x \in X_1 - X_2 \text{ s.t. } f(x) = y \qquad (2.6)\\
&\iff y = f(x) \in f(X_1 - X_2).
\end{aligned}$$

(4) Eq. 2.4无法推出 Eq. 2.3，因为 $\exists x_1 \in X_1, x_2 \in X_2$ s.t. $f(x_1) = f(x_2)$ 且 $x_1 \neq x_2$. 但若 f 为单射，则 $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$，此时 Eq. 2.4 $\implies$ Eq. 2.3.

Eq. 2.6无法推出 Eq. 2.5，因为 $\exists x \in X_1 - X_2$ s.t. $f(x) = y$ 亦有可能 $\exists x \in X_2$ s.t. $f(x) = y$. 但若 f 为单射，则只有一个 x s.t. $f(x) = y$，此时 Eq. 2.6 $\implies$ Eq. 2.5.

例题 2.1 考虑从集合 $A = \{a, b, c\}$ 到 $B = \{1, 2\}$ 上的函数 $f = \{(a, 1), (b, 1), (c, 1)\}$. $X_1 = \{a, b\}, X_2 = \{c\}$.

- $f(X_1 \cap X_2) = f(\emptyset) = \emptyset \subseteq \{1\} = f(X_1) \cap f(X_2)$.
- $f(X_1) - f(X_2) = \emptyset \subseteq \{1\} = f(X_1 - X_2)$.

定理 2.4 (函数的原像)

令 $f : A \mapsto B$，$Y_1 \subseteq B, Y_2 \subseteq B$，则有

1. $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$
2. $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$
3. $f^{-1}(Y_1 - Y_2) = f^{-1}(Y_1) - f^{-1}(Y_2)$

证明 (1) 对任意 $x \in f^{-1}(Y_1 \cup Y_2)$ 有

$$\begin{aligned} x \in f^{-1}(Y_1 \cup Y_2) &\iff f(x) \in Y_1 \cup Y_2 \\ &\iff f(x) \in Y_1 \vee f(x) \in Y_2 \\ &\iff x \in f^{-1}(Y_1) \vee x \in f^{-1}(Y_2) \\ &\iff x \in f^{-1}(Y_1) \cup f^{-1}(Y_2) \end{aligned} \tag{2.7}$$

(2) 对任意 $x \in f^{-1}(Y_1 \cap Y_2)$ 有

$$\begin{aligned} x \in f^{-1}(Y_1 \cap Y_2) &\iff f(x) \in Y_1 \cap Y_2 \\ &\iff f(x) \in Y_1 \wedge f(x) \in Y_2 \\ &\iff x \in f^{-1}(Y_1) \wedge x \in f^{-1}(Y_2) \\ &\iff x \in f^{-1}(Y_1) \cap f^{-1}(Y_2) \end{aligned} \tag{2.8}$$

(3) 对任意 $x \in f^{-1}(Y_1 - Y_2)$ 有

$$\begin{aligned} x \in f^{-1}(Y_1 - Y_2) &\iff f(x) \in Y_1 - Y_2 \\ &\iff f(x) \in Y_1 \wedge f(x) \notin Y_2 \\ &\iff x \in f^{-1}(Y_1) \wedge x \notin f^{-1}(Y_2) \\ &\iff x \in f^{-1}(Y_1) - f^{-1}(Y_2) \end{aligned} \tag{2.9}$$

推论 2.2

令 $f : A \mapsto B$，$Y_1, Y_2 \subseteq B$. 有

1. $f^{-1}(Y_1 \cup Y_2 \cup \ldots \cup Y_n) = f^{-1}(Y_1) \cup f^{-1}(Y_2) \cup \ldots \cup f^{-1}(Y_n)$.
2. $f^{-1}(Y_1 \cap Y_2 \cap \ldots \cap Y_n) = f^{-1}(Y_1) \cap f^{-1}(Y_2) \cap \ldots \cap f^{-1}(Y_n)$.

笔记 为何定理 2.4要比定理 2.3的结论更简洁、证明更简单？定理 2.3给定 $f(X)$，我们要分析 y 的原像 $f^{-1}(y)$，是一个集合，存在多个不同 x 映射到给定 y 的情况，除非 f 为单射. 而定理 2.4给定 $f^{-1}(Y)$，我们要分析 x 的像 $f(x)$，根据函数定义其具有唯一性，我们无需对函数做出任何额外假设.

定理 2.5

给定 $f : A \mapsto B$，则有

1. 对任意 $X \subseteq A, X \subseteq f^{-1}(f(X))$.
2. 对任意 $Y \subseteq B, Y \supseteq f(f^{-1}(Y))$.
3. 如果 f 是单射，对任意 $X \subseteq A, X = f^{-1}(f(X))$.
4. 如果 f 是满射，对任意 $Y \subseteq B, Y = f(f^{-1}(Y))$.

证明 留作练习.

笔记 定理 2.5告诉我们，定义域 A 中的集合在经过 $X \xrightarrow{f} \xrightarrow{f^{-1}}$ 推、拉回来之后可能会膨胀，这是由于函数 f 非单

射，在被 f^{-1} 拉回来后会引入额外元素；而陪域 B 中的集合在经过 $X \xrightarrow{f^{-1}} \xrightarrow{f}$ 推、拉回来之后可能会收缩，这是由于 f 非满射，在被 f 推出去时，有些元素没有原像，只能被丢弃.

例题 2.2 考虑从集合 $A = \{a, b, c\}$ 到 $B = \{1, 2\}$ 上的函数 $f = \{(a, 1), (b, 1), (c, 1)\}$. $X = \{a, b\}, Y = \{1, 2\}$.

- $X \subseteq f^{-1}(f(X)) = \{a, b, c\}$.
- $Y \supseteq f(f^{-1}(Y)) = \{1\}$.

2.2 函数的复合

定理 2.6 (函数的复合与态射)

令 $f : A \mapsto B, g : B \mapsto C$.

1. 若 f, g 都是单射的，则 $g \circ f : A \mapsto C$ 也是单射的.
2. 若 f, g 都是满射的，则 $g \circ f : A \mapsto C$ 也是满射的.
3. 若 f, g 都是双射的，则 $g \circ f : A \mapsto C$ 也是双射的.

证明 (1) 由 f 为单射可知 $\forall a_1, a_2 \in A, a_1 \neq a_2$ 有 $f(a_1) \neq f(a_2)$；由 g 为单射可知 $g(f(a_1)) \neq g(f(a_2))$. 因此，我们有 $\forall a_1, a_2 \in A, a_1 \neq a_2 \Rightarrow g \circ f(a_1) \neq g \circ f(a_2)$.

(2) 对任意 $c \in C$，由 g 为满射可知 $\exists b \in B$ s.t. $c = g(b)$. 又由 f 为满射可知 $\exists a \in A$ s.t. $b = f(a)$. 因此，对任意 $c \in C, \exists a \in A$ s.t. $c = g(f(a)) = g \circ f(a)$.

(3) 由 (1)(2) 可知，$g \circ f$ 既为单射亦为满射，即双射.

定理 2.7 (函数的复合与态射)

令 $f : A \mapsto B, g : B \mapsto C$.

1. 若 $g \circ f : A \mapsto C$ 是单射的，则 f 是单射的.
2. 若 $g \circ f : A \mapsto C$ 是满射的，则 g 是满射的.
3. 若 $g \circ f : A \mapsto C$ 是双射的，则 f 是单射的，g 是满射的.

证明 (1) 若 f 不为单射，则 $\exists a_1, a_2 \in A, a_1 \neq a_2$ s.t. $f(a_1) = f(a_2)$. 故 $g \circ f(a_1) = g(f(a_1)) = g(f(a_2)) = g \circ f(a_2)$, 与 $g \circ f$ 为单射矛盾. 因此假设不成立，即 f 为单射.

(2) 由 $g \circ f : A \mapsto C$ 为满射可知 $\forall c \in C, \exists a \in A$ s.t. $c = g \circ f(a)$. 令 $b = f(a)$, 由 $g \circ f(a) = g(f(a)) = g(b)$ 可知 $b \in g^{-1}(c)$, 故 g 为满射.

(3) 由 (1)(2) 可知.

定理 2.8

令 $f : A \mapsto B, g : B \mapsto C$ 均为双射函数，则

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

证明 根据复合函数和逆函数的定义，$(g \circ f)^{-1}$ 与 $f^{-1} \circ g^{-1}$ 均为从 C 到 A 的函数，故定义域相同.

任取 $a \in A$，令 $b = f(a), c = g(b) = g(f(a))$. 根据逆函数定义，

$$(g \circ f)^{-1}(c) = a = f^{-1}(b) = f^{-1}(g^{-1}(c)) = f^{-1} \circ g^{-1}(c).$$