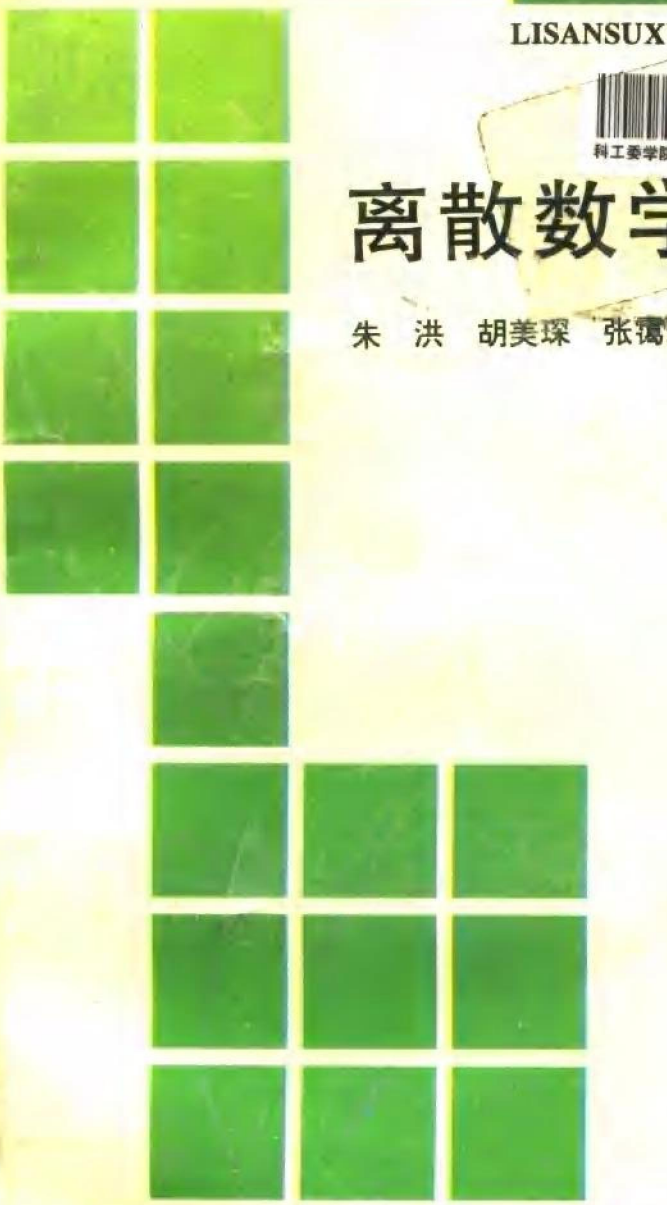
LISANSUXUEJIAOCHENG



# 离散数学教程

朱 洪 胡美琛 张霭珠 赵一鸣 编著



上海科学技术文献出版社

# 离散数学教程

朱　洪　胡美琛
张霭珠　赵一鸣　编著

上海科学技术文献出版社

离散数学教程

朱　洪　胡美琛　张鹭珠　赵一鸣　编著

*

上海科学技术文献出版社出版发行

（上海市武康路 2 号　邮政编码 200031）

全国新华书店经销

上海科技文献出版社昆山联营厂印刷

*

开本 850×1168　1/32　印张 13.75　字数 380,000

1996 年 11 月第 1 版　1996 年 11 月第 1 次印刷

印数：1—2300

ISBN 7-5439-0898-0/O・107

定　价：22.80 元

ISBN 7-5439-0898-0

9 787543 908987 >

# 序

离散数学是计算机科学与技术系的重要数学基础课之一，离散数学并不是数学中的一个独立分支，而是以离散（即非连续）对象的数量和空间关系为研究内容的数学若干个分支的总称。它包括数理逻辑、近世代数、古典概率、组合学、图论、集合论、数论、自动机和形式语言、可计算性和可判定性、离散几何等。

18世纪以前，数学基本上是研究**离散**对象的数量和空间关系的科学，但天文学，物理学的发展，如行星轨道，牛顿三大力学定律等研究，极大地推动了**连续**数学（以微积分，数学物理方程，实、复变函数论为代表）的发展。在这段时期内，除了近世代数（又称**抽象**代数）外，属于离散数学范围的组合学（包括图论），数理逻辑等一直处于相对停滞状态。自20世纪30年代起，图灵提出计算机的理论模型**图灵机**。这种模型早于实际制造计算机十多年，但迄今为止，现实的计算机的计算能力，本质上和图灵机的计算能力一样。这是离散数学理论指导计算机实际的典型范例。由于在计算机内，机器字长总是有限的，它代表离散的数或其它离散对象。因此随着计算机科学和技术的迅猛发展，离散数学重新焕发青春。从理论计算机科学（算法、可计算性、计算复杂性、程序正确性证明、自动编程等），计算机软件（数据结构、操作系统、数据库、软件工程等），人工智能（自动推理、机器学习）和系统结构设计（网络通讯、分布式和并行计算系统）到计算机应用（模式识别，图 像处理，信号处理，数据的压缩、编码和加密）无一不以离散数学为基础，并为它提出了许多新的研

究课题。可以预见，未来计算机的模型有待于离散数学对人类计算（包括思维和推理）的形式化描述研究有重大突破，现实的计算机才会有重大进展。

由上述所见，在计算机系本科课程中设置**离散数学**不仅为计算机系的学生学习目前计算机专业课程打下坚实的离散数学基础，也为了他们的长远发展，为他们迎接未来计算机科学和技术的挑战提供必要的离散数学的理论储备。通过本书的学习，读者将具有离散数学的基本素养和得到离散数学思维方法的训练。因课时数限制，本书只讲述集合论，组合学（包括图论），近世代数和数理逻辑四个数学分支的初步知识。本书是在复旦大学计算机系原有《离散数学》教材的基础上，通过多年的教学实践编写出来的，与以往的国内离散数学教材相比，增添**范畴论**初步，因近年来计算机科学文献常常需要范畴论概念。数理逻辑是通过**泛代数**引入的，这是较为大胆的尝试，具有简洁明了的优点，和代数部分呵成一气。

本书集合论和图论部分由胡美琛编写；近世代数部分由张霭珠编写，其中范畴论一章由吴京编写第一稿，而后由朱洪完成；组合学和数理逻辑部分由赵一鸣编写；朱洪对全书制定了编写大纲并对书稿作了审定和修改。在本书初稿使用过程中，方芳，程岐，卢先捷曾提出很多宝贵意见。他们和王宇君，刘佳，张柳青，汪卫，熊鹏荣，周玉林，徐寿怀等协助作者用Latex编辑软件打印书稿，付出了大量劳动，本书才得以问世，编著者对他们表示深深的感谢。

编著者

1996年9月

# 目　录

# 第一章　集合的基本概念

集合论是现代数学的基础, 它已深入到各种科学和技术领域中, 特别是被广泛应用到数学和计算机科学的各分支中去。

集合论的创始人康托尔 (Cantor, 1845-1918), 他成功地研究了集合的理论, 为现代数学奠定了基础, 但是其理论中出现了悖论。为了解决集合论的悖论, 进一步解决集合论中自身的问题, 在本世纪初开始了集合论公理学方向的研究, 它是数理逻辑的中心问题之一。

下面完全避免用集合的公理化方法, 直观地介绍了朴素集合论。从集合的基本概念和例子着手, 对关系、函数、基数等进行讨论, 并简单介绍了集合论的悖论。

## 1.1　集合的表示

一些不同对象的总体, 称为集合, 常用大写英文字母表示, 例如 $S, A$ 等。构成一个集合中的那些对象称为该集合的元素, 用小写英文字母或数字等表示。用记号 $a \in A$ 表示 $a$ 是集合 $A$ 的元素, 读作 $a$ 属于 $A$。用记号 $a \notin A$ 表示 $a$ 不是集合 $A$ 的元素, 读作 $a$ 不属于 $A$。

通常, 集合中的元素可以是具体的事物, 也可以是抽象的符号。集合有如下表示方法:

(1) 用列出集合中元素的方法来表示。例如, 集合 $A$ 的元素为 $1, 3, 5, 7, 9$, 表示为 $A = \{1, 3, 5, 7, 9\}$。

(2) 用描述集合中元素具有共同性质的方法来表示。例如, 集合 $A$ 的元素为 $x^2 = 1$ 的根, 表示为 $A = \{x \mid x^2 - 1 = 0\}$。一般来说, 满足性质 $P$ 的元素组成的集合记为: $\{x \mid P(x)\}$, 其中 $P(x)$ 是 "$x$ 具

有性质 $P$" 的一个简写。

这两者表示方法都是常用的, 前者用于元素个数较少的情况, 后者用于元素个数较多 (或无限), 并且各对象具有共同性质的情况, 往往一个集合可以同时用上述两种方法表示。例如 $\{x \mid x^2 = 1\}$ 也即 $\{1, -1\}$, $\{x \mid x$ 为小于或等于 7 的质数$\}$也即 $\{1, 2, 3, 5, 7\}$。自然数集 $N$ 为 $\{1, 2, 3, \cdots\}$, 或 $\{n \mid n$ 是自然数$\}$。

(3) 可通过某规则的计算来定义集合中的元素, 在此情况下的集合常称为递归定义的集合。详细叙述见第四章。

不含有任何元素的集合称为 **空集**, 记为 $\emptyset$ 或$\{\}$。如果集合中有有限个不同元素, 则称该集合为 **有限集**, 否则称为 **无限集**。有限集 $A$ 的元素个数称为集合 $A$ 的基数 (详见第四章), 记为 $|A|$。例如 $A = \{x \mid x^2 + 1 = 0, x$ 为实数$\}$是空集 $\emptyset$, $|A| = |\emptyset| = 0$。又如 $A = \{x \mid x$ 是大于 1小于 6的质数$\}$, $|A| = 3$。

集合中的元素是不能重复出现的, 然而元素之间的次序是无关紧要的, 例如集合 $\{a, b, c\}$ 与 $\{b, a, c\}$ 是完全相同的集合。在特殊问题中, 要求考虑集合中元素可以重复出现, 这种集合称为 **多重集**, 例如 $\{a, b, b, b, c, d, d\}$, $\{1, 1, 2, 3\}$ 等。

以集合作为元素所组成的集合称为 **集合族**。例如 $S = \{\{a, b\}, \{a, b, c\}, \{d, e\}\}$ 是一个集合族。它的元素是 $\{a, b\}$, $\{a, b, c\}$, $\{d, e\}$。又如 $S = \{\emptyset, \{\emptyset\}\}$的元素是 $\emptyset$, $\{\emptyset\}$, 必须注意 $\emptyset$ 与 $\{\emptyset\}$ 是不同的, $\{\emptyset\}$ 表示以 $\emptyset$ 为元素的集合。

下面, 本书将用 $I$ 表示整数集; $I^+$ 表示正整数集; $Q$ 表示有理数集; $Q^+$ 表示正有理数集; $Q^-$ 表示负有理数集; $R$ 表示实数集; $R^+$表示正实数集; 等等。

## 1.2 集合的子集

我们可以用平面上封闭曲线包围点集的图形来表示集合, 该图形称为**文氏图**(Venn Diagrams)。例如集合 $A = \{1, 2, 3, 4\}$ 的文氏图如图 1.1 所示。文氏图还能表示集合之间的相互关系, 如集合的包含,

集合 $A$ 包含在集合 $B$ 中, 如图 1.2 所示。

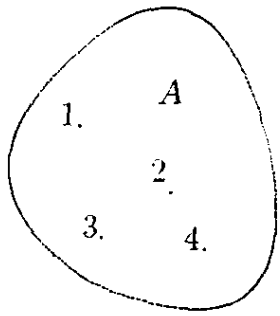



图 1.1

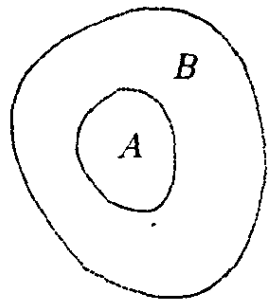



图 1.2

**定义1.1**　设 $A$ 和 $B$ 是两个集合。$A$ 的每一元素都是 $B$ 的元素, 则称 $A$ 是 $B$ 的**子集**, 记为 $A \subseteq B$ 或 $B \supseteq A$, 分别读作 $A$ 包含在 $B$ 中或 $B$ 包含 $A$。特别, $A \subseteq A$。

**定义1.2**　集合 $A$ 和 $B$ 的元素全相同, 则称 $A$ 和 $B$ **相等**, 记为 $A = B$, 否则称 $A$ 和 $B$ **不相等**, 记为$A \neq B$。

**定理1.1**　设 $A$ 和 $B$ 是两个集合, 则 $A = B$ 当且仅当 $A \subseteq B$, 且 $B \subseteq A$。

**证明** $\Longrightarrow$ 假设 $A = B$, 由定义, $A$ 中的每个元素是在 $B$ 中, 有 $A \subseteq B$, 同理 $B$ 中每个元素是在 $A$ 中有 $B \subseteq A$。

$\Longleftarrow$ 反之, 若 $A \neq B$, 则 $A$ 中至少有一元素不在 $B$ 中, 与 $A \subseteq B$ 矛盾; 或 $B$ 中至少有一元素不在 $A$ 中, 与 $B \subseteq A$ 矛盾。所以 $A \neq B$ 是不可能的。 □

**定义1.3**　若 $A \subseteq B$ , 且 $A \neq B$ , 则称集合 $A$ 是集合 $B$ 的**真子集**, 记为 $A \subset B$。也可以说, $A$ 是 $B$ 的子集, 并且 $B$ 中至少有一个元素不属于 $A$。

例如 $\{a\} \subset \{a, b\}$。

注意, 上面提到的记号$\in$和$\subseteq$ 是完全不同的, 表示两个不同的概念。

**定义1.4**　在取定一个集合 $U$ 以后, 对于 $U$ 的任意子集而言, 称 $U$ 为全集。

例如, 初等代数是考虑实数范围中的问题, 所以用实数全体组成的集合作为全集。又实数集对于整数集、有理数集而言是全集, 而整数集对于偶数集、奇数集而言也是全集。

**定理1.2** 对于任何集合 $A$, 必有 (1) $\emptyset \subseteq A$ , (2) $A \subseteq A$, (3) $A \subseteq U$。

**证明** (1) 假设空集 $\emptyset$ 不是集合 $A$ 的子集, 则至少有一个元素 $x$, 使得 $x \in \emptyset$ 且 $x \notin A$。又因为 $\emptyset$ 是空集, 它没有元素, 所以对任何 $x$ 必有 $x \notin \emptyset$, 导致矛盾。因此 $\emptyset$ 是集合 $A$ 的子集。

(2)、(3) 易证从略。

有时, 我们需要列出所有子集, 这些子集也可组成一个集合, 定义如下:

**定义1.5** 设 $A$ 是任意集合, $A$ 的所有子集所组成的集合, 称为集合 $A$ 的幂集, 记为 $\mathcal{P}(A)$, 或记为 $2^A$, 即 $\mathcal{P}(A) = \{B \mid B \subseteq A\}$ 。

**例1.1** 设 $A = \{a\}, \mathcal{P}(A) = \{\emptyset, \{a\}\}$,

设 $A = \{a, b\}, \mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$,

设 $A = \{a, b, c\}, \mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$。

**定理1.3** 设 $A$ 是有限集, 则 $|\mathcal{P}(A)| = 2^{|A|}$ 。

**证明** 设 $|A| = n$, 从 $n$ 个元素中选取 $i$ 个不同的元素共有 $C(n, i)$ 种取法。所以

$|\mathcal{P}(A)| = 1 + C(n,1) + C(n,2) + \cdots + C(n,n) = (1+1)^n = 2^n$, 即

$$|\mathcal{P}(A)| = 2^{|A|}$$ □

## 1.3 笛卡尔积

**定义1.6** 两个对象 $a, b$ 依一定次序组成一对, 称为**有序对**, 记为 $(a, b)$。两个有序对相等 $(a, b) = (c, d)$, 当且仅当 $a = c$ 和 $b = d$ 同时成立。

例如 $5 < 8$ 记为 $(5, 8)$, 平面上的顶点坐标为 $(x, y)$, 教师 $a$ 的学生 $b$ 记为 $(a, b)$, 这些例子说明常用有序对来表示两个对象之间的关系。

注意 $a \neq b$ 时, $(a,b) \neq (b,a)$, 但集合 $\{a,b\} = \{b,a\}$, 也就是说有序对 $(a,b)$ 中 $a,b$ 有序, 即强调次序的。$a,b$ 不一定来自同一集合。$a,b$ 可等可不等, $(a,a)$ 是有意义的。有序对概念可以推广如下。

**定义1.7**　对 $n>0$, $n$ 个对象的序列形如 $a_1,a_2,\cdots,a_n$ 组成一组称为有序 $n$ 元组, 记为 $(a_1,a_2,\cdots,a_n)$, 其中 $a_i$ 称为第 $i$ 个分量。两个有序 $n$ 元组相等当且仅当它们的每个对应分量相等。

**定义1.8**　设 $A$ 和 $B$ 是两个集合, 定义 $A$ 与 $B$ 的笛卡尔积为 $A \times B = \{(a,b) \mid a \in A \text{ 且 } b \in B\}$, 又称 $A \times B$ 为 $A$ 与 $B$ 的**直积**。

**例1.2**　设 $A=\{1,2\}, B=\{x,y\}, C=\{a,b,c\}$, 则

$A \times B = \{(1,x),(1,y),(2,x),(2,y)\}$;

$B \times A = \{(x,1),(x,2),(y,1),(y,2)\}$;

$B \times A \neq A \times B$;

$A \times C = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}$;

$A \times A = \{(1,1),(1,2),(2,1),(2,2)\}$。

**定义1.9**　设 $A_1,A_2,\cdots,A_n$ 是任意 $n$ 个集合, 定义**笛卡尔积** $A_1 \times A_2 \times \cdots \times A_n$ 为 $\{(a_1,a_2,\cdots,a_n) \mid a_i \in A_i,\ i=1,2,\cdots,n\}$。

例1.2中 $A \times B \times C = \{(1,x,a),(1,x,b),(1,x,c),(1,y,a),(1,y,b),(1,y,c),(2,x,a),(2,x,b),(2,x,c),(2,y,a),(2,y,b),(2,y,c)\}$。

若对所有 $i, A_i = A$, 则 $A_1 \times A_2 \times \cdots \times A_n$, 记为 $A^n$。

## 1.4　集合的运算

设 $A$ 和 $B$ 是任意两个集合, 通过下面的定义可以得到新的集合。

**定义1.10**　设 $A$ 和 $B$ 是两个集合, $U$ 是全集,

(1) $A$ 和 $B$ 的**并**, 记为 $A \cup B$, 它是由 $A$ 和 $B$ 中所有元素所组成的集合, 即 $A \cup B = \{x \mid x \in A \text{ 或 } x \in B\}$。

(2) $A$ 和 $B$ 的**交**, 记为 $A \cap B$, 它是由 $A$ 和 $B$ 中公共元素所组成的集合, 即 $A \cap B = \{x \mid x \in A \text{ 且 } x \in B\}$。

(3) $A$ 和 $B$ 的**差**, 记为 $A-B$, 它是由在 $A$ 中而不在 $B$ 中的元

素所组成的集合, 即 $A-B=\{x \mid x \in A$ 且 $x \notin B\}$。

(4) $A$ 的补, 记为 $\overline{A}, \overline{A}=U-A$。

(5) $A$ 和 $B$ 的对称差, 记为 $A \oplus B, A \oplus B=(A-B) \cup(B-A)$。

集合的并, 交, 差, 补和对称差也分别称为集合的并运算, 交运算, 差运算, 补运算和对称差运算。可用文氏图表示, 如图 1.3 的斜线部分。

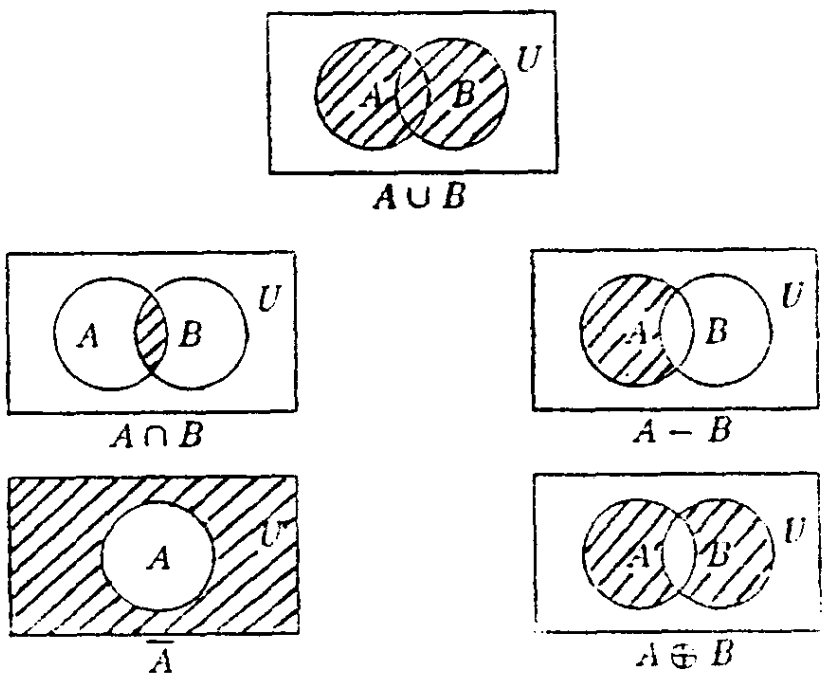



图 1.3

**例1.3** 设 $A=\{a, b, c\}$, $B=\{a, c, d\}$, $U=\{a, b, c, d, e\}$, 则 $A \cup B=\{a, b, c, d\}$, $A \cap B=\{a, c\}$, $A-B=\{b\}$, $B-A=\{d\}$, $\overline{A}=\{d, e\}$, $\overline{B}=\{b, e\}$。

若 $A \cap B=\varnothing$, 则称 $A$ 和 $B$ 不相交。集合的差与交之间是有联系的, 由定义1.10 可知 $A-B=A \cap \overline{B}$。

利用集合运算的性质和集合相等的概念, 我们可以得到一些等式。下面先介绍几个例子。

**例1.4** 证明 $A \cap(B \cup C)=(A \cap B) \cup(A \cap C)$。

**证明** 先证明 $A \cap(B \cup C) \subseteq(A \cap B) \cup(A \cap C)$。

对任一 $x \in A \cap(B \cup C)$, 则 $x \in A$ 且 $x \in B \cup C$, 即 $x \in A$ 且

$x \in B$ 或 $x \in C$。对于 $x \in A$, 如果 $x \in B$, 则 $x \in A \cap B$; 或如果 $x \in C$, 则 $x \in A \cap C$, 所以 $x \in (A \cap B) \cup (A \cap C)$, 即

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

再证明 $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$。

对任一 $x \in (A \cap B) \cup (A \cap C)$, 则 $x \in A$ 且 $x \in B$ 或 $x \in A$ 且 $x \in C$, 也就是 $x \in A$ 时有 $x \in B$ 或 $x \in C$, 所以 $x \in A \cap (B \cup C)$, 即

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

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

**例1.5**　若 $A \subseteq B$, 则有 $(A \cap B) = A, A \cup B = B$。

**证明**　若 $A \subseteq B$, 对任 $x \in A$ 有 $x \in B$, 所以 $x \in A \cap B$, 得到 $A \subseteq A \cap B$; 另一方面 $(A \cap B) \subseteq A$, 因此 $(A \cap B) = A$。

对任 $x \in A \cup B$, 于是 $x \in A$ 或 $x \in B$。若 $x \in A$ 则有 $x \in B$, 所以 $(A \cup B) \subseteq B$; 另一方面 $(A \cup B) \supseteq B$, 因此 $(A \cup B) = B$。　□

**例1.6**　证明 $\overline{A \cap B} = \overline{A} \cup \overline{B}$。

**证明**　先证明 $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$。

对任一 $x \in \overline{A \cap B}$, 则 $x \notin A \cap B$, 即 $x \in A$ 和 $x \in B$ 不同时成立。从而 $x \in \overline{A}$ 或 $x \in \overline{B}$, 也就是 $x \in \overline{A} \cup \overline{B}$, 所以 $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$。

再证明 $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$。

对任一 $x \in \overline{A} \cup \overline{B}$, 则 $x \in \overline{A}$ 或 $x \in \overline{B}$, 如果 $x \notin \overline{A \cap B}$, 则可导致矛盾。因为 $x \notin \overline{A \cap B}$, 必有 $x \in A \cap B$, 即 $x \in A$ 且 $x \in B$, 也就是说 $x \notin \overline{A}$ 且 $x \notin \overline{B}$ 同时成立, 得到矛盾, 所以 $x \in \overline{A \cap B}$。因此 $\overline{A \cap B} = \overline{A} \cup \overline{B}$。　□

集合的并、交、差和补运算的基本性质概括如下:

**定理1.4**　设 $A, B, C$ 是任意集合, $U$ 为全集, 下列等式成立:

(1) $A \cup A = A$　　(幂等律)

$A \cap A = A$

(2) $A \cup B = B \cup A$　　(交换律)

$A \cap B = A \cap B$

(3) $A \cup (B \cup C) = (A \cup B) \cup C$　　(结合律)