



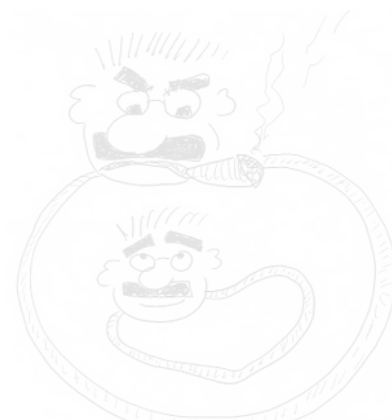
# 离散数学

## Discrete Mathematics

### 第五讲：集合论导引

吴楠

南京大学计算机学院



Would a set be a member of a set of sets that didn't accept themselves as members?

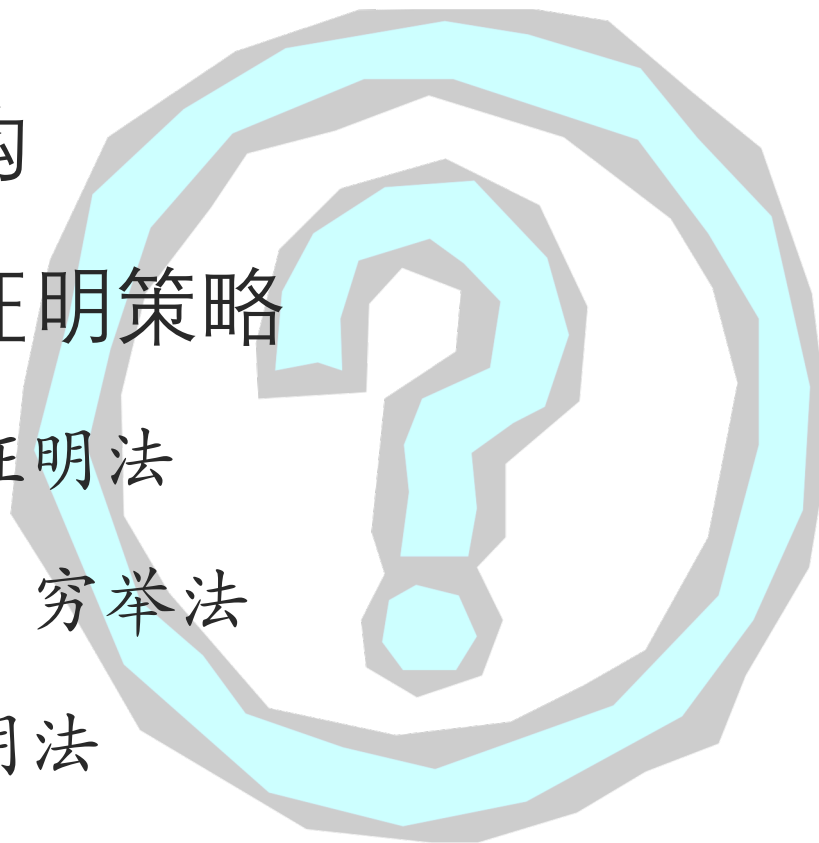
2025年3月4日



# 前情提要



- 证明的本质
- 逻辑推理的形式结构
- 常用的证明方法与证明策略
  - 直接证明法，间接证明法
  - 归谬法（反证法），穷举法
  - 空证明法，平凡证明法
  - 构造性证明法，反例证明法





# 本讲主要内容



- 引子：数学基础的危机
- 集合的概念
- 子集、空集与幂集
- 集合的运算与集合代数
- 集合公式的几种基本证明方式





# 引子：数学基础的危机



- 19世纪早期，发现数学存在缺陷
  - Н.И. Лобачёвский, G. Riemann: 非欧几何
  - A. Cauchy等：分析(微积分及其扩展)的基础
- 19世纪后期的公理化运动：去除基于直觉或经验的朴素概念所带来的模糊，使数学严密化
  - G. Peano, D. Hilbert: 算术与几何的公理化



# 数学基础的危机（续）



## ■ 1900年国际数学大会

- H. Poincaré: “借助集合论可以建造整个数学大厦……

今天我们可以宣称绝对的严密已经实现了！”

- 随后有人发现了Cantor集合论中的一些严重问题，  
如1901年发现的罗素悖论

- G. Frege评论：当大厦竣工时基础却动摇了





# 数学基础的危机（续）



危机的（不完美）解决：

## 公理化集合论

（以 Zermelo–Fraenkel set theory – **ZF** 为代表）





# 集合的概念

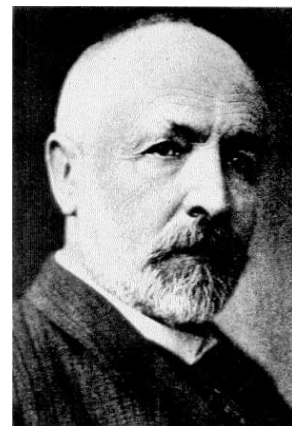


- 集合没有明确的定义，G. Cantor 给出了一种刻划：

“吾人直观或思维之对象，如为相异而确定之物，其总括之全体即谓之集合，其组成此集合之物谓之集合之元素。”

“【译注】通常用大写字母表示集合，如 $A$ 、 $B$ 、 $C$ 等，用小写字母表示元素，如 $a$ 、 $b$ 、 $c$ 等。若集合 $A$ 系由 $a$ 、 $b$ 、 $c$ 等诸元素所组成，则表如 $A = \{a, b, c, \dots\}$ ，而 $a$ 为 $A$ 之元素，亦常用 $a \in A$ 之记号表之者， $a$ 非 $A$ 之元素，则记如 $a \notin A$ 。”

（肖文灿译于1939年，《集合论初步》，商务印书馆）

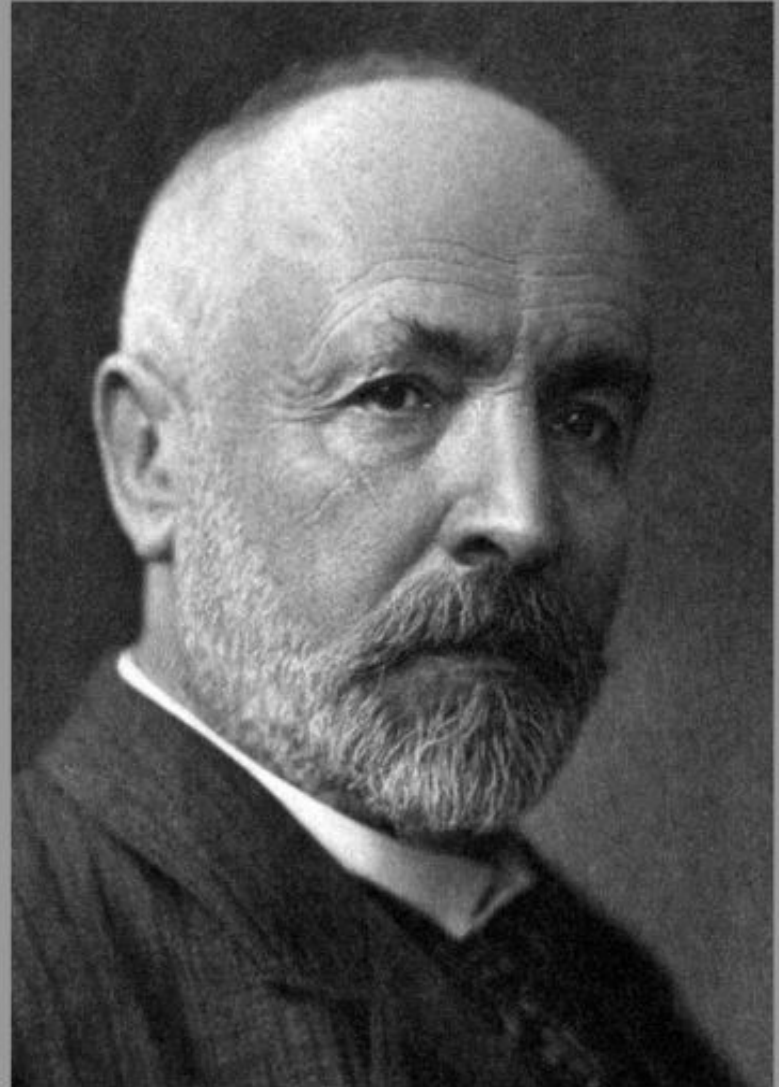


“A set is a many  
that allows itself to  
be thought of as a one”

**Georg Cantor**

German Mathematician

1845-1918

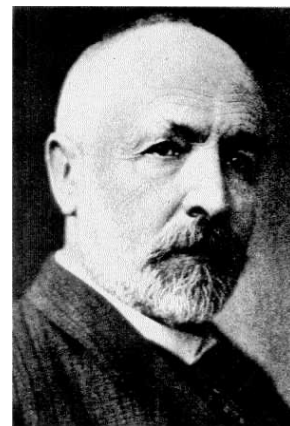




# 集合的概念（续）



- 例： $\{1,2,3\}$ 为集合，“1”为集合，“自然数之全体”为集合；但诸如“甚大之数”或“与 $P$ 点接近之点”则不能为集合，因其界限不清
- 集合中的元素互异，我们把元素的重复看作一次出现，如 $\{2,2,3,3\} = \{2,3\}$
- Cantor提到的“总括之全体”之“总括”，可由集合的外延公理和概括原则来描述





# 集合的外延公理与概括原则



- **(ZF.1) 外延公理**: 集合由其元素完全确定

$$A = B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$$

故证明集合  $A = B$  只需证明  $\forall x(x \in A \leftrightarrow x \in B)$

- **(NST.1<sup>△</sup> – Ax. of Abstraction) Cantor概括原则**: 对于人的直观或者思维之对象  $x$  的任一谓词  $P(x)$ , 存在集合  $S$  的元素恰为具有性质  $P$  的那些对象, 记为  $S = \{x | P(x)\}$ 。  
对于任何对象  $a$ ,  $a \in S \leftrightarrow P(a)$ , NST.1<sup>△</sup> 事实上继承了 Frege 的概念文字 (Begriffsschrift), 给出了概念的外延



# 罗素悖论与公理化集合论



- Cantor概括模式 (NST.1  $\Delta$  – ASc.) : 对所有谓词 $P(x)$ , 均存在集合 $\{x|P(x)\}$
- 然而, B. Russell在1901年给出反例, 即著名的罗素悖论: 令 $R = \{x|x \notin x\}$ , 则若 $R$ 为集合, 有 $R \in R \leftrightarrow R \notin R$ , 矛盾; 故 $R$ 不为集合。即任意给定的谓词 $P(x)$ 未必产生集合



# 罗素悖论与公理化集合论



■ 例\*：罗素自指涉谓词 $x \in x$ 亦可导致罗素悖论

根据朴素集合论的ASc.,  $\bar{R} = \{x | x \in x\}$ ,  $R = \{x | x \notin x\}$ , 则若 $R \in \bar{R}$ , 必有 $R \in R$ ; 根据罗素悖论,  $R \in R \rightarrow R \notin R$ ; 又因为 $\bar{R}$ 中的元素均以自身为元素, 故而 $R \notin R \rightarrow R \notin \bar{R}$ , 因此可得 $R \in \bar{R} \rightarrow R \notin \bar{R}$ , 反之亦然, 即:  $R \in \bar{R} \leftrightarrow R \notin \bar{R}$ . 因此罗素自指涉谓词同可视为罗素悖论, 即谓词 $x \in x$ 同样无法产生集合



# 罗素悖论与公理化集合论



- 罗素悖论是迄今为止最著名的悖论之一，虽形式简单却意义深远。自此人们重新审视朴素集合论，用形式化方法讨论集合论，用新的公理替代Cantor概括原则，最终形成了公理化集合论
- 进一步阅读：公理化集合论\*

<https://zh.wikipedia.org/wiki/公理化集合论>



# 子集



- $A$  为  $B$  之**子集** (记为  $A \subseteq B$ ) 指  $\forall x(x \in A \rightarrow x \in B)$ ,  $A$  为  $B$  之**真子集** (记为  $A \subset B$ ) 指  $A \subseteq B$  且  $A \neq B$ 。 $A \not\subseteq B$  是指  $\exists x(x \in A \wedge x \notin B)$
- **例:**  $\{1,2\} \subseteq \{1,2,3\}$ ,  $A \subseteq A$ ,  $\mathbb{N} \subseteq \mathbb{R}$
- **命题:**

$$A = B \leftrightarrow (A \subseteq B \wedge B \subseteq A)$$

该命题也常被用来证明集合相等



# 空集



- 集合论系统有二种：一种承认有原子（即本身不含元素但能作为别的集合的元素）；另一种不承认有原子，认为一切皆为集合，ZFC系统为后者。这样便导致“最初之元素”即为没有任何元素的集合，ZFC从这种集合出发来构成集合世界，因此这种集合是任何集合的子集
- (ZF.3)空集公理：存在一个集合其没有任何元素，称这种集合为空集（null set），记作 $\emptyset$ ，其为任何集合（包含空集）之子集（在ZFC中可由分类公理导出）



# 空集 (续)



## ■ 命题：空集是唯一的

○ 证明：设  $\emptyset_1, \emptyset_2$  皆为空集，则根据空集的定义，有  
 $\emptyset_1 \subseteq \emptyset_2 \wedge \emptyset_2 \subseteq \emptyset_1$ ，根据集合相等的定义有  $\emptyset_1 = \emptyset_2$

■ 空集本身是一个集合，也可以做为另一个集合的元素或者子集，故： $\emptyset \in \{\emptyset\}$ ， $\emptyset \subseteq \{\emptyset\}$ ；但因为空集不含任何元素，故 $\emptyset \notin \emptyset$ ， $\emptyset \neq \{\emptyset\}$

■ 定义：若集合  $A$  含有  $n$  个元素，则称  $A$  为  $n$  元集，记为  $|A| = n$ ；易见， $\emptyset$  是 0 元集， $\{\emptyset\}$  是 1 元集



# 由集合定义自然数



## ■ 在公理集合论中，自然数是集合

- **定义：** 设 $a$ 为集合，称 $a \cup \{a\}$ 为 $a$ 的**后继**，记作 $a^+$
- **定义** (von Neumann) :

$$\text{令 } 0 = \emptyset, 1 = 0^+, 2 = 0^{++}, \dots, n = \overbrace{0^{+ \cdots +}}^n$$

- **定义：** 设 $A$ 是集合，称 $A$ 为**归纳集** (inductive set) 指：

$$\emptyset \in A \wedge (\forall x \in A)(x^+ \in A)$$



# 无穷集合的存在性问题



- 若存在归纳集  $A$ ，则  $\emptyset \in A, \emptyset^+ \in A, \emptyset^{++} \cdots \in A$ ，  
从而  $A$  是**无穷集**
- Russell说：“事实上，在这个世界中是否有无穷集合，**我们还不能确定。**”
- 据此，**还不能确定归纳集是否存在**。大多数人认为宇宙是无穷的（Hilbert 则否），为了保证归纳集的存在，ZFC引入**无穷公理**



# 无穷公理



- (ZFC.7) 无穷公理 (Axiom of Infinity) :

$$\exists A(\emptyset \in A \wedge (\forall x \in A)(x^+ \in A))$$

- 以往按照 von Neumann 的定义,  $0 = \emptyset$ ,  $n + 1 = n^+$ , 从而可以定义出单个的自然数, 但不能说明全体自然数的集合  $\mathbb{N}$  的存在性。通过无穷公理可以定义  $\mathbb{N}$

- 定义:  $\mathbb{N} \stackrel{\text{def}}{=} \cap \{A | A \text{ 为归纳集}\} =$

$$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots\}$$



# 幂集



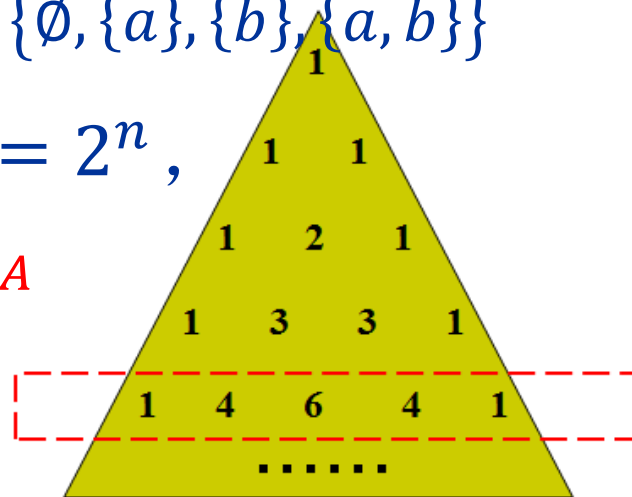
- (ZF.8) 幂集公理：集合 $A$ 的幂集 $P(A) = \{x | x \subseteq A\}$   
即由集合 $A$ 的全体子集构成的集合

○ 例：  $P(\emptyset) = \{\emptyset\}$  ,  $PP(\emptyset) = \{\emptyset, \{\emptyset\}\}$  ,  $PPP(\emptyset) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$  ,  $P(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

- 若 $|A| = n$ ，则 $|P(A)| = \sum_{k=0}^n \binom{n}{k} = 2^n$ ，

故集合 $A$ 的幂集的另一种记法为 $2^A$

- 若 $P(A) \in P(B)$ ，则 $A \in B$





# 集合运算



- 为了由已有集合产生新的集合，除幂集运算外还引入一些集合上的运算：

- 定义：

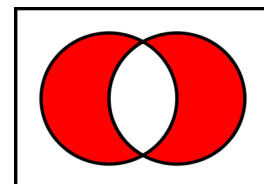
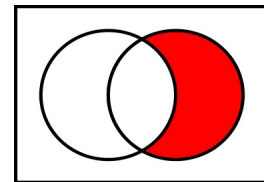
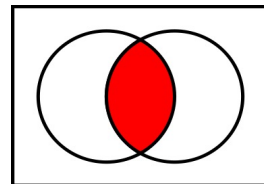
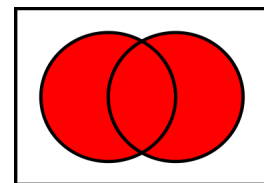
- (ZF.5) 集合的并：  $A \cup B = \{x | x \in A \vee x \in B\}$

- 集合的交：  $A \cap B = \{x | x \in A \wedge x \in B\}$

- 集合的相对补：  $A - B = \{x | x \in A \wedge x \notin B\}$

- 集合的对称差：

$$\begin{aligned} A \oplus B &= \{x | (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} \\ &= (A - B) \cup (B - A) \end{aligned}$$

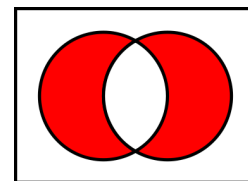




# 集合运算 (续)



■ 例：观察文氏图，试证明对称差  $A \oplus B = (A \cup B) - (A \cap B)$



证明：根据对称差定义， $A \oplus B = (A - B) \cup (B - A)$ ，任取  $x \in A \oplus B$ ，即  $x \in (A - B)$  或  $x \in (B - A)$ 。

- 1. 假设  $x \in (A - B)$ ，根据相对补定义，有  $x \in A$  且  $x \notin B$ ，故而  $x \in (A \cup B)$  但  $x \notin (A \cap B)$ ，根据相对补定义，有  $x \in (A \cup B) - (A \cap B)$ ；
- 2. 假设  $x \in (B - A)$ ，根据相对补定义，有  $x \in B$  且  $x \notin A$ ，故而  $x \in (A \cup B)$  但  $x \notin (A \cap B)$ ，根据相对补定义，亦有  $x \in (A \cup B) - (A \cap B)$ 。

综上，对于任意  $x \in A \oplus B$ ，皆有  $x \in (A \cup B) - (A \cap B)$ ，反之亦然（需要加入证明内容）。由集合相等定义， $A \oplus B = (A \cup B) - (A \cap B)$ 。□



# 广义交与广义并



- 上面介绍的是两个集合的交与并，现将其推广：
- **定义（广义交与广义并）：**
  - **集合的广义并：** 设  $A$  为集合， $A$  的所有元素的并称为集合  $A$  的广义并，记为：
$$\bigcup A = \{x | \exists y (y \in A \wedge x \in y)\}$$
  - **集合的广义交：** 设  $A$  为非空集合， $A$  的所有元素的交称为集合  $A$  的广义交，记为：
$$\bigcap A = \{x | \forall y (y \in A \rightarrow x \in y)\}$$
  - **思考：** 为什么规定广义交的对象不能为  $\emptyset$ ？



# 集合代数



- 在集合的运算中，满足以下代数运算律：

- **定理：** 设 $A, B, C$ 为任意集合

- **交换律：**  $A \cup B = B \cup A, \quad A \cap B = B \cap A$

- **结合律：**  $A \cup (B \cup C) = (A \cup B) \cup C$

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

- **分配律：**  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

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

- **吸收律：**  $A \cup (A \cap B) = A, \quad A \cap (A \cup B) = A$

- **幂等律：**  $A \cap A = A \cup A = A$



# 集合代数 (续)



- 在集合的运算中，满足以下规律 (续)：

- 定理 (续)：设  $A, B, C$  为任意集合

- De Morgan 律： $A - (B \cup C) = (A - B) \cap (A - C)$

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

- 空集性质： $A \cap \emptyset = \emptyset, A \cup \emptyset = A$

- 幂集性质： $P(A \cap B) = P(A) \cap P(B)$

$$P(A \cup B) \supseteq P(A) \cup P(B)$$



# 集合公式的基本证明方式



## ■ 方法一：直接使用集合包含或相等的定义

○ **例：**  $A \cup B = B \Rightarrow A \subseteq B$

○ **分析：** 待证结论为  $A \subseteq B$ ，即  $\forall x(x \in A \rightarrow x \in B)$ ，因此，证明框架如下：

对任意  $x$ ，假设  $x \in A$ ， $\{\cdots \text{适当内容} \cdots\}$   
因此， $x \in B$ ，故  $A \subseteq B$ .  $\square$

○ **证明：** 对任意  $x$ ，假设  $x \in A$ ，根据集合并的定义有  $x \in A \cup B$ ，由已知条件  $A \cup B = B$ ，因此  $x \in B$ ，故  $A \subseteq B$ .  $\square$



# 集合公式的基本证明方式（续）



- 方法二：利用运算定义作逻辑等值式推导

**例：**试证  $A - (B \cup C) = (A - B) \cap (A - C)$

**证明：**

$$\begin{aligned} A - (B \cup C) &= \{x | x \in A, \text{ but } x \notin B \cup C\} \\ &= \{x | x \in A, \text{ but } (x \notin B \wedge x \notin C)\} \\ &= \{x | (x \in A, \text{ but } x \notin B) \wedge (x \in A, \text{ but } x \notin C)\} \\ &= (A - B) \cap (A - C) \end{aligned}$$



# 集合公式的基本证明方式（续）



## ■ 方法二：利用运算定义作逻辑等值式推导

○ 例：试证  $A - (B \cup C) = (A - B) \cap (A - C)$

另一种等价的描述方式：

$$\begin{aligned}x \in A - (B \cup C) &\Leftrightarrow (x \in A) \wedge (x \notin (B \cup C)) \\&\Leftrightarrow x \in A \wedge x \notin B \wedge x \notin C \\&\Leftrightarrow (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \\&\Leftrightarrow (x \in (A - B)) \wedge (x \in (A - C)) \\&\Leftrightarrow x \in ((A - B) \cap (A - C))\end{aligned}$$



# 集合公式的基本证明方式（续）



## ■ 方法三：利用已知恒等式或等式作集合代数演算

○ **例1：**  $A \cap B = A \Leftrightarrow A - B = \emptyset$

**证明：** ( $\sim A$ 指 $A$ 的绝对补即全集 $E - A$ )  $A - B = A \cap \sim B = (A \cap \sim B) \cup (A \cap \sim A) = A \cap (\sim B \cup \sim A) = A \cap \sim(A \cap B) = A \cap \sim A = \emptyset$

○ **例2：**  $A \cup (A \cap B) = A$

**证明：** (设 $E$ 为全集)  $A \cup (A \cap B) = (A \cap E) \cup (A \cap B) = A \cap (E \cup B) = A \cap E = A$

○ **例3：** 已知 $A \oplus B = A \oplus C$ ，证明 $B = C$

**证明：** (注意 $\oplus$ 满足结合律)  $B = \emptyset \oplus B = (A \oplus A) \oplus B = A \oplus (A \oplus B) = A \oplus (A \oplus C) = (A \oplus A) \oplus C = \emptyset \oplus C = C$



# 集合公式的基本证明方式（续）



## ■ 方法四：系列逻辑等价式的方法——循环证明

○ 例：试证  $A \cup B = B \Leftrightarrow A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A - B = \emptyset$

○ 证明路径：(1)  $\rightarrow$  (2)  $\rightarrow$  (3)  $\rightarrow$  (4)  $\rightarrow$  (1)

○ 只要完成上述证明，由蕴含的循环就证明了此诸充要关系

○ 在以上例子的基础上，只要再证明  $A - B = \emptyset \Rightarrow A \cup B = B$

■ 证明：

$$\begin{aligned} A \cup B &= (A \cup B) \cap E = (A \cup B) \cap (\sim B \cup B) \\ &= (A \cap \sim B) \cup B = (A - B) \cup B = B \end{aligned}$$



# 集合公式的基本证明方式（续）



## ■ 关于充分必要条件的进一步讨论

- 若命题  $P \rightarrow Q$  为真，称命题  $P$  为命题  $Q$  的 **充分条件**（sufficient condition），命题  $Q$  为命题  $P$  的 **必要条件**（necessary condition）
- 若逻辑等价  $P \Leftrightarrow Q$  成立（即  $P \leftrightarrow Q$  永真），称命题  $P$  与命题  $Q$  **互为充分必要条件**（充要条件）
- 若要证明“命题  $P$  的 **充分必要条件是命题  $Q$** ”，则意味着证明“**结论  $P$**  成立当且仅当 **条件  $Q$**  成立”，即证两个方面：
  - **必要性**（necessity）：证明  $P \rightarrow Q$ ，即若结论成立则条件成立
  - **充分性**（sufficiency）：证明  $Q \rightarrow P$ ，即若条件成立则结论成立

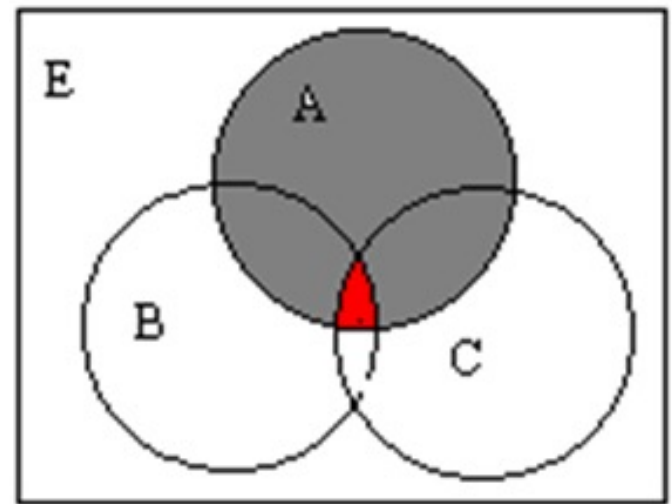


# 集合公式的基本证明方式（续）



- 其它证明方式：文氏图也可帮助推测结论（但文氏图不能完全代替证明的过程）
- 例：  $(A - B) \cup (A - C) = A$  成立的充分必要条件？

充要条件：  $A \cap B \cap C = \emptyset$





# Georg Cantor



- 23岁获数学博士学位
- 集合论“公认为全部数学的基础”
- 关于无限的若干论断：
  - 集合论是一种“疾病”
  - “雾中之雾”、“疯子”
- 可能是这个时代所能夸耀的最巨大的工作。

——罗素





# 本次课后作业



- 教材内容: [Rosen] 2.1–2.2 节
- 课后习题:
  - Problem Set 5
- 提交时间: 3月11日 10:00 前





# ZFC公理化集合系统\*



- Ax. 1 外延公理
- Ax. 2 正则公理
- Ax. 3 分类公理
- Ax. 4 配对公理
- Ax. 5 并集公理
- Ax. 6 替代公理
- Ax. 7 无穷公理
- Ax. 8 幂集公理
- Ax. 9 选择公理 (AC, 或良序公理)



# ZFC公理化集合系统\* (续)



## ■ ZFC.1 外延公理 (Axiom of extensionality)

- 如果两个集合含有同样的元素，则它们是相等的：

$$\forall x \forall y [\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y]$$

## ■ ZFC.2 正则公理 (Axiom of regularity/foundation)

- 任意非空集合 $x$ 包含一个元素 $y$ ， $x$ 与集合 $y$ 是不相交的：

$$\forall x [\exists a (a \in x) \rightarrow \exists y (y \in x \wedge \neg \exists z (z \in y \wedge z \in x))]$$

## ■ ZFC.3 分类公理 (Axiom schema of separation)

- 对任意集合 $z$ 和任意对 $z$ 的元素 $x$ 有定义的逻辑谓词 $\phi(x)$ ，存在 $z$ 的子集 $y$ ，使 $x \in y$ 当且仅当 $x \in z$ 且 $\phi(x)$ 为真：

$$\forall z \forall w_1 \dots w_n \exists y \forall x [x \in y \leftrightarrow (x \in z \wedge \phi(x))]$$



# ZFC公理化集合系统\* (续)



## ■ ZFC. 4 配对公理 (Axiom of pairing)

$$\forall x \forall y \exists z (x \in z \wedge y \in z)$$

## ■ ZFC. 5 并集公理 (Axiom of union)

$$\forall \mathcal{F} \exists A \forall Y \forall x [(x \in Y \wedge Y \in \mathcal{F}) \rightarrow x \in A]$$

## ■ ZFC. 6 替代公理 (Axiom schema of replacement)

$$\forall A \forall w_1 \dots w_n \left[ \forall x (x \in A \rightarrow \exists! y: \phi) \right. \\ \left. \rightarrow \exists B \forall x (x \in A \rightarrow \exists y (y \in B \wedge \phi(y))) \right]$$



# ZFC公理化集合系统\* (续)



## ■ ZFC. 7 无穷公理 (Axiom of infinity)

$$\exists X[\emptyset \in X \wedge \forall y(y \in X \rightarrow y^+ \in X)]$$

## ■ ZFC. 8 幂集公理 (Axiom of power set)

$$\forall x \exists y \forall z [z \subseteq x \rightarrow z \in y]$$

## ■ ZFC. 9 选择公理 (Axiom of choice)

- 任一非空集合族  $(S_i)_{i \in I}$  均存在元素族  $(s_i)_{i \in I} : \forall i \in I (s_i \in S_i)$
- 或良序定理 (Well-ordering theorem) :

$$\forall X \exists R (R \text{ well-orders } X)$$