数理逻辑

讲义，第 6.2 版，2023 年

北京大学 信息与计算科学系

林作铨

linzuoquan@pku.edu.cn

- 数学系统
- 带等词一阶系统
- 群论
- 一阶算术
- 形式集论
- 一致性问题

一阶算术

自然数和算术

数系："自然数是上帝给的，其它东西都是人造的"（Kronecker）

逻辑上，自然数也是人造的

$$\mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C} \to \mathbb{H}$$

（自然数-整数-有理数-实数-复数-四元数）

算术化：把一个理论一一对应地映射到自然数，使得关于这个理论的对象可有一个有效的计算过程（算术）通过自然数找出对象

$$\mathbb{H} \Rightarrow \mathbb{C} \Rightarrow \mathbb{R} \Rightarrow \mathbb{Q} \Rightarrow \mathbb{Z} \Rightarrow \mathbb{N}$$

注

- 直觉主义：自然数是数学的基础，数学是由此构造的（构造是不能形式化的，而是直觉）
- 逻辑主义：数学是逻辑的一部分，自然数由逻辑定义，如数“2”定义为 $(\exists x)(\exists y)(P(x) \wedge P(y) \wedge x \neq y \wedge \forall z(P(z) \rightarrow z = x \vee z = y))$
    - 人（数学家）的智能活动不是这样思考数论的，因此逻辑主义只能作为一种数学哲学
    - 但是，人工智能活动可能跟人不一样，逻辑主义可作为人工智能的基础（人工智能的逻辑基础）
- 形式主义：自然数是由公理定义的（形式系统）
    - 每个数学理论都是形式系统，但还未能做到一个统一的（或足够广泛的）数学的形式系统

（朴素）算术 N 的形式系统

N 是否可作为一个算术模型?

定义 5.23 (算术语言 $\mathscr{L}_N$)

令 $\mathscr{L}_N$ 是一个关于算术（N）的一阶语言，除变元、连接词、量词和技术性符号外，包括如下非逻辑符号

- 常元： a_1 （代表 0）
- 函项符： f_1^1, f_1^2, f_2^2 （后继、和与积）
- 谓词符： $=$ $\diamondsuit$

定义 5.24 (算术系统)

$\mathscr{N}$ 表示（一阶）算术系统（或称 Peano 算术 (PA)），它是增加了以下附加公理而得到的 $K_{\mathscr{L}_N}$ 的扩充（一阶理论）

- (E7)，(E8) 和 (E9) 的合适实例
- 下列六个公理及一个公理模式

定义（续）：算术公理

(N1) $(\forall x_1) \sim (f_1^1(x_1) = a_1)$

(N2) $(\forall x_1)(\forall x_2)(f_1^1(x_1) = f_1^1(x_2) \to x_1 = x_2)$

(N3) $(\forall x_1)(f_1^2(x_1, a_1) = x_1)$

(N4) $(\forall x_1)(\forall x_2)(f_1^2(x_1, f_1^1(x_2)) = f_1^1(f_1^2(x_1, x_2)))$

(N5) $(\forall x_1)(f_2^2(x_1, a_1) = a_1)$

(N6) $(\forall x_1)(\forall x_2)(f_2^2(x_1, f_1^1(x_2)) = f_1^2(f_2^2(x_1, x_2), x_1))$

(N7) $\mathscr{A}(a_1) \to ((\forall x_1)(\mathscr{A}(x_1) \to \mathscr{A}(f_1^1(x_1))) \to (\forall x_1)\mathscr{A}(x_1))$

对（$\mathscr{L}_N$ 的）每个公式 $\mathscr{A}(x_1)$，x_1 在其中自由出现

◇

记号

在 $\mathscr{L}_N$ 中，定义符号 $+$，$\times$ 和 $'$ 分别代替 f_1^2，f_2^2 和 f_1^1，即约定

- $t_1 + t_2$ 代表 $f_1^2(t_1, t_2)$
- $t_1 \times t_2$ 代表 $f_2^2(t_1, t_2)$
- t' 代表 $f_1^1(t)$
- 0 代表 a_1
- $f_1^1(x_1) \neq a_1$ 代表 $\sim(f_1^1(x_1) = a_1)$

$\mathscr{N}$ 中 (N1)-(N7) 可重写成如下形式

算术公理

(N1*) $x_1{}' \neq 0$

(N2*) $x_1{}' = x_2{}' \rightarrow x_1 = x_2$

(N3*) $x_1 + 0 = x_1$

(N4*) $x_1 + x_2{}' = (x_1 + x_2)'$

(N5*) $x_1 \times 0 = 0$

(N6*) $x_1 \times x_2{}' = (x_1 \times x_2) + x_1$

(N7*) $\mathscr{A}(0) \rightarrow ((\forall x_1)(\mathscr{A}(x_1) \rightarrow \mathscr{A}(x_1{}')) \rightarrow (\forall x_1)\mathscr{A}(x_1))$

对每个公式 $\mathscr{A}(x_1)$，x_1 在其中自由出现

注

- (N1*-N7*) 等价于它们（对变元 x_1，x_2）的全称闭式
- 由 (N7*) 用 MP 即归纳规则（导出规则，数学归纳法）

$$\mathscr{A}(0), \forall x(\mathscr{A}(x) \to \mathscr{A}(x')) \vdash_{\mathscr{N}} \forall x \mathscr{A}(x)$$

Peano 公设

(1) 0 是自然数

(2) 对每一自然数 n，存在另一自然数 n'

(3) 没有自然数 n，使得 n' 等于 0

(4) 对任意自然数 m 和 n，若 $m' = n'$，则 $m = n$

(5) 对任意包含 0 的自然数集 A，若当 $n \in A$ 时，$n' \in A$，则 A 包含每一个自然数

注

(a) 前两个 Peano 公设在 $\mathscr{N}$ 中没有任何对应的公理

因在 $\mathscr{L}_N$ 中，已包括了这些符号（0 和 $'$，或 a_1 和 f_1^1），它们在任一模型中有解释，即元素 $\bar{a}_1$ 存在，且对每个 x，元素 $\bar{f}_1^1(x)$ 存在，所以 $\mathscr{N}$ 不需要这两条公设

(b) (N7) 和 Peano 第五公设之间不是恰好对应的，它们都是数学归纳法原理的表达

- $\mathscr{N}$ 基于一阶语言 $\mathscr{L}_N$
- (N7) 是模式，有无穷个实例，因此 $\mathscr{N}$ 不是有限公理化
- Peano 第五公设包含二阶量词“对任意的自然数集 A”，这需在二阶语言中表示

$$\forall A(A(0) \wedge \forall x(A(x) \to A(x+1)) \to \forall x A(x))$$

注（续）

(N7) 的实例形成 $\mathscr{L}_N$ 的公式的能枚举集，Peano 第五公设是关于自然数的所有集的语句，而所有集的集是不能枚举的，因此 (N7) 是有更多限制的归纳法原理的形式

- Peano 第五公设需要二阶逻辑（对应的是二阶算术）
- 一般地，二阶逻辑的公式不能等价规约到一阶逻辑的公式（完整的二阶逻辑是不完全的）

能枚举的 (N7) 的实例使得在逻辑中可使用数学归纳法证明

(c) Peano 公设并没有包含“和”或“积”的概念，这些函数（项）可用后继函数应用归纳法原理来定义，但在形式语言中包括这些符号是方便的

为确保在任意模型中，这些符号的解释有需要的性质，公理 (N3)-(N6) 就是必要的

Peano 算术思想

- 朴素算术的概念不是最基本的，如“素数”“立方数”，是与一个数所具有的因子有关的，而这些因子又与乘法有关，有少数短语反复地出现，由此定义算术语言的基本成分
- 不致力于把推理的原则加以形式化，力图给出一个自然数性质的最小的集，从它出发，其余的算术性质能由推理而得

问题

PA 的元数学性质如何：完全性和一致性？ （后面讨论）

搞怪公设

Peano 公设：试用一个未经定义的术语“神怪”来替代“自然数”，用两个未定义项“怪物”与“元”

- 怪物是一个神怪
- 每个神怪有一个元（它也是一个神怪）
- 怪物不是任何神怪的元
- 不同的神怪有不同的元
- 如果怪物有 x，且每个神怪都把 x 递送给它的元，那么所有的神怪都得到 x

注

- “自然数”概念是一个设法去定义的东西，Peano 公设所施加的限制是如此之强，以至于如果两个不同的人在心里对这些概念形成意象，这两个意象会有完全同构的结构，这“神怪”就是“自然数”
- 几何公设类似，如“点”，“线”，“面”可被替换为“椅子”，“桌子”，“水瓶”，这样几何画图的直觉就可不用（虽然数学直觉是很重要的）

命题 5.25

令 t，s 是 $\mathscr{L}_N$ 的项，下列公式是 $\mathscr{N}$ 的定理

(N1′) $t' \neq 0$

(N2′) $t' = s' \to t = s$

(N3′) $t + 0 = t$

(N4′) $t + s' = (t + s)'$

(N5′) $t \times 0 = 0$

(N6′) $t \times s' = (t \times s) + t$

证

(N1′-N6′) 分别由 (N1*-N6*) 推出：首先，用 Gen 考虑其全称闭式，用变元换名使得所有约束变元不出现在 t, s 中，最后，用 R3 于 t, s 即得 □

命题 5.26

对任意（$\mathscr{L}_N$ 的）项 t，s，r，下列公式是 $\mathscr{N}$ 的定理

(a) $t = r \to (t = s \to r = s)$

(b) $t = t$

(c) $t = r \to r = t$

(d) $t = r \to (r = s \to t = s)$

(e) $r = t \to (s = t \to r = s)$

(f) $t = r \to t + s = r + s$

(g) $t = r \to s + t = s + r$

(h) $t = r \to t \times s = r \times s$

(i) $t = r \to s \times t = s \times r$

(j) $t \times (r + s) = (t \times r) + (t \times r)$ （分配律）

证

(a) (E9) 实例

(b)

(1) $t + 0 = t$ (N3′)

(2) $(t + 0 = t) \to (t + 0 = t \to t = t)$ (a)

(3) $t + 0 = t \to t = t$ (1)(2)MP

(4) $t = t$

(j)

对 x_3 归纳证 $\vdash_{\mathcal{N}} x_1 \times (x_2 + x_3) = (x_1 \times x_2) + (x_1 \times x_3)$

其余留作练习 □

记号

$0^{(n)}$ 是 0 后面 n 个 $'$ 的缩写，数 $n \in D_N$ 是项 $0^{(n)}$ 在 N 中的解释

$0^{(0)}$ 代表 $\mathscr{N}$ 的常项 0

数字项

用 $0^{(n)}$ 代表 $\mathscr{N}$ 的项，但符号 n 本身不是 $\mathscr{L}_N$ 的符号，出现在 $0^{(n)}$ 中的 n 不能用变元代入

$0^{(n)}$ 称为数字项 ，数字项是闭项

命题 5.27

令 $m, n \in D_N$，若 $m \neq n$，则 $\vdash_{\mathscr{N}} \sim(0^{(m)} = 0^{(n)})$ $\diamondsuit$

证

不失一般性，设 $m < n$，则存在 $k > 0$，使得 $n = m + k$

由 (N2*) 可得

$$\vdash_{\mathscr{N}} 0^{(m)} = 0^{(m+k)} \to 0^{(m\text{-}1)} = 0^{(m+k\text{-}1)}$$

证 (续)

若 $m > 0$（$m = 0$ 的情形是平凡的）

反复用 (N2*)，又用规则 HS，得

$$\vdash_{\mathscr{N}} 0^{(m)} = 0^{(m+k)} \to 0^{(0)} = 0^{(k)}$$

因 $k > 0$， $k\text{-}1 \in D_N$，且

$$\vdash_{\mathscr{N}} 0^{(k)} = (0^{(k\text{-}1)})'$$

实即 $\vdash_{\mathscr{N}} 0^{\overbrace{\prime\prime\cdots\prime}^{k}} = (0^{\overbrace{\prime\prime\cdots\prime}^{k\text{-}1}})'$，有

$$\vdash_{\mathscr{N}} 0^{(m)} = 0^{(m+k)} \to 0^{(0)} = (0^{(k\text{-}1)})'$$

证 (续)

利用一个重言式，有

$$\vdash_{\mathscr{N}} \sim(0^{(0)} = (0^{(k\text{-}1)})') \to \sim(0^{(m)} = 0^{(m+k)})$$

但 (N1*) 给出

$$\vdash_{\mathscr{N}} \sim(0^{(0)} = (0^{(k\text{-}1)})')$$

由 MP $$\vdash_{\mathscr{N}} \sim(0^{(m)} = 0^{(m+k)})$$

□

命题 5.28

任何 $\mathscr{N}$ 的模型都是无穷的

证

据命题 5.27，任一 $\mathscr{N}$ 的模型中对象所对应的数字项是不同的，有（能枚举）无穷多的数字项

$\square$

注

- $t < s$ 表示 $(\exists r)(r \neq 0 \wedge r + t = s)$，类似地，可引入不等式
- 完全归纳：$\vdash_{\mathscr{N}} (\forall x)((\forall z)(z < x \rightarrow \mathscr{A}(z)) \rightarrow \mathscr{A}(x)) \rightarrow (\forall x)\mathscr{A}(x)$
- 最小数归纳：$\vdash_{\mathscr{N}} (\exists x)\mathscr{A}(x) \rightarrow (\exists y)\mathscr{A}(y) \wedge (\forall z)(z < y \rightarrow \neg\mathscr{A}(z))$
- 其它如因子分解等都容易形式化，如 $t \mid s$ 表示 $(\exists z)(s = t \times z)$，由此展开形式数论

$\mathscr{N}$ 是一个带等词一阶系统

定义 5.29

一个解释 $\mathfrak{N}$，其中

- 论域是正整数
- 0 作为符号 0 的解释
- 后继操作（+1）是函数 $'$（即 f_1^1）的解释
- 朴素算术的加和乘是 $+$ 和 $\times$ 的解释
- 相等关系是 $=$ 的解释

是 $\mathscr{N}$ 的（规范）模型，称为标准模型

注

规范模型所需的等价类论域对正整数就是自身

一致性问题：标准模型

- $\mathscr{N}$ 的公理是否在 $\mathfrak{N}$ 为真尚未验证，直观上先认为可验证为真
- 若接受 $\mathfrak{N}$ 作为 $\mathscr{N}$ 的模型，则 $\mathscr{N}$ 是具有一致性，但这种论证是成问题

  因 $\mathfrak{N}$ 包含（朴素）集论（其论域及有关推理），这样证明的一致性是不牢靠的（依赖于集论的一致性）
- 若 $\mathfrak{N}$ 是一个模型，即 $\mathscr{N}$ 是一致的，对 $\mathscr{N}$ 任意（算术）公式 $\mathscr{A}$，$\mathscr{A}$ 或 $\sim\mathscr{A}$ 为真；若 $\mathscr{A}$ 或 $\sim\mathscr{A}$ 在 $\mathscr{N}$ 可证，则 $\mathscr{N}$ 就是完全的

$\mathscr{N}$ 有完全性定理与否取决于一致性

一致性问题：朴素模型

（朴素）算术 N 应是一个算术模型，但 N 是算术系统 $\mathscr{N}$ 的（规范）模型吗？

若 N 是一个模型，即 $\mathscr{N}$ 是一致的，则 $\mathscr{N}$ 就是完全的

注

设 N 是算术模型，则可由 N 生成一个完全的一阶（算术）系统（定义 4.68），当然这个一阶系统不能有限公理化，亦不是 Peano 算术系统

没人怀疑算术的一致性，怎么办？

思路

算术系统 $\mathscr{N}$ 是不完全的（Gödel 不完全性定理）

若 $\mathscr{N}$ 是不完全的，则存在一个算术公式 $\mathscr{B}$，使得 $\mathscr{B}$ 或 $\sim\mathscr{B}$ 都不是定理，即 $\mathscr{B}$ 是不可判定的

注

设若 $\mathscr{N}$ 是完全的，则如同一阶逻辑，算术系统也是半可判定的，数论专家就得赋闲了：只要有足够的时间（姑且不考虑 NP 难解问题），他们领域里的任何问题都能够用机器证明

算术系统的一致性问题依赖于集论的一致性，而朴素集论发现了 Russell 悖论 $\Rightarrow$ 数学基础（危机）问题

- 数学系统
- 带等词一阶系统
- 群论
- 一阶算术
- 形式集论
- 一致性问题

形式集论

朴素集论（naive set theory）

一个集（合）是具有一定性质的对象的全体（相当于没定义的直观概念）

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

隶属关系：$x \in S$

子集关系：若 $\forall x,\ x \in S \Rightarrow x \in S'$，则 S 包含于 S'，即 $S \subseteq S'$

S 是 S' 的子集

集中成员（元素）可以是集

问题

包含所有集的集是个什么集？

注

Cantor 不能枚举集和 Russell 悖论揭示存在非常大的对象，之前数学尚未能观察其结构

悖论 5.30 (Russell 悖论)

令 $R = \{x \mid x \notin x\}$，则 $R \in R \iff R \notin R$ $\diamondsuit$

R 定义为一个所有不含自身作为成员的集的集

若 $R \in R$，即 R 包含自身作为成员，按 R 的定义 $\Rightarrow$

R 为不含自身作为成员的集，即 R 不属于 R

则 $R \notin R$

若 $R \notin R$，即 R 不含自身作为成员，按 R 的定义 $\Rightarrow$

R 为不含自身作为成员的集，即 R 属于 R

则 $R \in R$

Russell 悖论

设 $\mathscr{R}(x)$ 为任一（含一个自由变元 x 的）公式

考虑 $\quad \vdash \exists y \forall x (x \in y \leftrightarrow \mathscr{R}(x))$

令 $\quad \mathscr{R}(x)$ 为 $x \notin x$ $(\sim x \in x)$，即 Russell 集

演算：消去存在量词和全称量词，可推出矛盾

$$y \in y \leftrightarrow y \notin y$$

语义：由 $\forall x (x \in y \leftrightarrow x \notin x) \models y \in y \leftrightarrow y \notin y \qquad [\forall x \mathscr{A}(x) \models \mathscr{A}(x/y)]$

显然 $\quad y \in y \leftrightarrow y \notin y$ 是不可满足的

因此 $\quad \forall x (x \in y \leftrightarrow x \notin x)$ 亦不可满足

故 $\quad \models \sim \exists y \forall x (x \in y \leftrightarrow x \notin x)$

即 Russell 集不存在

悖论反证 *

反证法：可通过构造一个悖论，如 Russell 悖论，证明不存在性结果

例

任何集不与它的幂集双射

证

设若一集 X 其幂集能从 X 枚举，即 $2^X = \{A_x \mid x \in X\}$

考虑集 $Y = \{x \in X \mid x \notin A_x\}$ 由所有不被包含在所枚举的 X 的子集的 X 中元素组成

因 Y 是 X 的子集，就有对某个 $y \in X$，$A_y = Y$

这样，若 $y \in Y$ 则 $y \notin Y$，若 $y \notin Y$ 则 $y \in Y$ $\square$

取代 Cantor 对角线证法

注

- 符号 $\in$ 可不做隶属关系，以上证明就不只针对朴素集论，这个悖论具有普遍意义
- 自谓：语言的一种自指，即能陈述语言表达式自身的一种性质；否则，称为非自谓（“它谓”）

  如，“汉语”是自谓的，而“英语”是非自谓的

  “这个句子有九个汉字”是自谓的

  一般地，否定的自谓表达式会导致悖论

  如，“这个句子没有十个汉字”
- Russell 悖论与语义悖论是相通的

注

Russell（1901，Zermelo 1900）提出的悖论引发了第三次数学危机

Cantor 提出集论，即成为数学基础概念，Russell 悖论表明集的概念是不一致的，因此数学基础的危机本质上就是不能保证一致性

消除 Russell 悖论（1908）

- Russell 的类型论（type theory）
  1. 保留朴素集论：对集的抽象有所限制
  2. 改变语言：对象语言涉及自指需在元语言表达，从而避免悖论；元语言涉及自指需在元元语言表达，依次类推
- Zermelo 的公理化集论（axiomatic set theory）
  1. 公理化集的概念：对集的抽象不加限制
  2. 保留一阶语言：公理集论作为一阶系统（形式集论，描述集论）

公理化集论：ZF（Zermelo-Fraenkel）系统

定义 5.31 (一阶 ZF 语言)

ZF 的一阶语言 $\mathscr{L}_{ZF}$：变元、连接词、量词和技术性符号外

- 谓词符：$=$（A_1^2），A_2^2
- 没有函项符和常元

A_2^2 解释为隶属关系 $\in$，记 $t_1 \in t_2$ 表示 $A_2^2(t_1, t_2)$，$t_1 \notin t_2$ 表示 $\sim A_2^2(t_1, t_2)$

$\vdash_{ZF}$ 是 $\mathscr{L}_{ZF}$ 上的推理关系（简记 $\vdash$） $\diamondsuit$

注

- 没有常元和函项符意味着变元是唯一的项
- 变元 x_i 解释为集

  (有时用名称类以区分含悖论的朴实集论的集，即类是不会导致 Russell 悖论的集)
- 原子公式只有形式 $x_i = x_j$ 或 $x_i \in x_j$

定义 5.32 (*ZF*)

ZF 作为 $K_{\mathscr{L}}$ 的扩充（带等词一阶理论）

- (E7)，(E9) 的所有合适的实例

  （(E8) 没有非平凡实例）

- 下述的公理 (ZF1) 到 (ZF8)

外延公理 （Axiom of Extensionality）

(ZF1) $(x_1 = x_2 \leftrightarrow (\forall x_3)(x_3 \in x_1 \leftrightarrow x_3 \in x_2))$

两集相等 当且仅当 它们有相同的元素

注

从左到右的蕴涵其实已由 (E9) 给出

记号

引入 $\subseteq$ 作为缩写符号

$t_1 \subseteq t_2$： $(\forall x_1)(x_1 \in t_1 \to x_1 \in t_2)$

t_1 和 t_2 是任意（$\mathscr{L}_{ZF}$ 的）项

$t_1 \subset t_2$： $t_1 \subseteq t_2 \wedge t_1 \neq t2$

注

易证如 $\vdash_{ZF} x_1 = x_2 \leftrightarrow (x_1 \subseteq x_2 \wedge x_2 \subseteq x_1)$ 等朴实集论命题（子集）

空集公理 （Null Set Axiom）

(ZF2) $\quad (\exists x_1)(\forall x_2) \sim (x_2 \in x_1)$

存在没有元素的集

注

在任何（规范）模型中，空集只有一个，这是作为 (ZF1) 的直接推论

记号

引入符号 $\varnothing$ 记空集，它起着常项的作用

(ZF2)：$\quad (\forall x_2) \sim (x_2 \in \varnothing)$。

对集公理 (Axiom of Pairing)

$(ZF3)\quad (\forall x_1)(\forall x_2)(\exists x_3)(\forall x_4)(x_4 \in x_3 \leftrightarrow (x_4 = x_1 \vee x_4 = x_2))$

给定任意集 x 和 y，存在其元素是 x 或 y 的集 z

注

该公理断言存在性（$\exists x_3$），易证

$$(\forall x_1)(\forall x_2)(\exists_1 x_3)(\forall x_4)(x_4 \in x_3 \leftrightarrow (x_4 = x_1 \vee x_4 = x_2))$$

可引入符号 $\{,\}$，$\{x_1, x_2\}$ 看作是项（无序对）

$(\mathrm{ZF3})$：$\quad x_4 \in \{x_1, x_2\} \leftrightarrow (x_4 = x_1 \vee x_4 = x_2)$

有序对 $\langle x_1, x_2\rangle$ 表示为 $\{\{x_1\}, \{x_1, x_2\}\}$

并集公理 （Axiom of Unions）

(ZF4) $(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow (\exists x_4)(x_4 \in x_1 \wedge x_3 \in x_4))$

给定任意集 x，存在一个集 y，它以 x 的元素的所有元素为元素

记号

用 $\cup x_1$ 表示 (ZF4) 中断言存在的对象，把它看作一个项，引入 $\cup$ 作为函项 $(t_1 \cup t_2)$ 代表 $\cup\{t_1, t_2\}$

注

$x_1 \cap x_2$ 可定义为 $(\forall x_3)x_3 \in x_1 \cap x_2 \Leftrightarrow x_3 \in x_1 \wedge x_3 \in x_2$, $\bar{x_1}$ 可定义为 $(\forall x_2)x_2 \in \bar{x_1} \Leftrightarrow x_2 \notin x_1$，由此可推出有关集的并、交、补等运算

幂集公理 (Power Set Axiom)

(ZF5) $(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow x_3 \subseteq x_1)$

给定任意集 x，存在以 x 的所有子集作为元素的集 y

注

Cartesian 积 $x_1 \times x_2$ 可定义为

$$(\forall x_3)\left(x_3 \in x_1 \times x_2 \Leftrightarrow (\exists x_4)(\exists x_5)\left(x_3 = \langle x_4, x_5\rangle \wedge x_4 \in x_1 \wedge x_5 \in x_2\right)\right)$$

x_1^n 表示 $x_1^{n\text{-}1} \times x_1$，余如集上关系等可引入

替换公理模式（Axiom Scheme of Replacement）

(ZF6) $(\forall x_1)(\exists_1 x_2)\mathscr{A}(x_1,x_2) \rightarrow$

$$(\forall x_3)(\exists x_4)(\forall x_5)(x_5 \in x_4 \leftrightarrow (\exists x_6)(x_6 \in x_3 \wedge \mathscr{A}(x_6,x_5)))$$

对每个公式 $\mathscr{A}(x_1,x_2)$，x_1,x_2 在其中自由出现

（不失一般性，假定量词 $(\forall x_5)$ 和 $(\forall x_6)$ 不在其中出现）

若公式 $\mathscr{A}$ 确定一个函项，则对任意集 x，存在一个集 y，它以所有 x 的元素在这函项下的象作为元素

无穷公理 (Axiom of Infinity)

(ZF7) $(\exists x_1)(\varnothing \in x_1 \wedge (\forall x_2)(x_2 \in x_1 \rightarrow x_2 \cup \{x_2\} \in x_1))$

$\{x_2\}$ 是 $\{x_2, x_2\}$ 的缩写

在任意模型中，无穷集存在

注

- 假若不把 (ZF7) 包括在公理组中，就无法保证形式系统与包括无穷集在内的朴素集合论有任何关系
- $\{\varnothing\} \in x_1, \{\varnothing, \{\varnothing\}\} \in x_1, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \in x_1 \cdots$
- 令 0 表示 $\varnothing$，1 表示 $\{\varnothing\}$，2 表示 $\{\varnothing, \{\varnothing\}\} \cdots$，则对 $n \geq 0$，$\varnothing \neq 1$，$\varnothing \neq 2, 1 \neq 2$，$\varnothing \neq 3$，$1 \neq 3$，$2 \neq 3 \cdots$

  (von Neumann 定义自然数)

基础公理 （Axiom of Foundation）

(ZF8) $(\forall x_1)(\sim x_1 = \varnothing \rightarrow (\exists x_2)(x_2 \in x_1 \wedge \sim(\exists x_3)(x_3 \in x_2 \wedge x_3 \in x_1)))$

每一非空集 x 包含一个与 x 不相交的元素

注

这是为避免反直观的悖论，排除集以自身作为其元素的可能性而列入的技术性公理（排除 Russell 悖论，即 $\{x_1 \mid x_1 \in x_1\}$ 不合法）

进一步，形式化基数、序数等，可证明如超限归纳等，展开形式集论

ZF 在排除 Russell 悖论前提下，保留了数学中所需用的（朴素）集论

注

ZF 变元解释为集，集中元素都是集，不能处理元素为非集的个体（如人、分子、公司等个体），但有推广的 *ZF* 系统可处理个体作为元素

ZFA（ZF with Atoms）：对象可为原子（atoms/urelements），原子可是集的元素，但不能是由其它元素组成

问题

ZF 是否还包含其它未发现的悖论？

数学基础

集 (论) 作为数学基础

⇒ 一个代数结构（如群）是一个集，其上有一些操作，满足一些公理

⇒ 一个空间（如拓扑）是一个集，其上有一些操作，满足一些公理

$\cdots\ \cdots$

ZF 作为数学（公理化）基础

假若 ZF 具有一致性，则它有（规范）模型

⇒ 算术系统 $\mathcal{N}$ 的模型可定义为 ZF 模型的子集

⇒ 自然数、后继函数和算术公理基于 ZF 模型的解释定义

⇒ 由自然数基于代数分析定义有理数、实数和复数

⇒ （可测集 ⇒Lebesgue 测度论 ⇒ 概率论

Dedekind 分割 ⇒ 实数 ⇒ 极限理论 ⇒ 微积分）

ZF 的模型包含一个复数集，亦包含实数集作为子集

选择公理 (Axiom of Choice)

(AC) 对任一由互不相交的非空集组成的集 x，存在至少一个集 y，它与 x 的每一元素（非空集）恰好有一个公共元素

与以下两个等价陈述

Zorn 引理

若一个偏序集的每条链存在一个上确界，则该偏序集存在一个极大元

良序原理

每个集都是良序的（所有非空子集在全序关系下都存在最小元素）

注

- (AC) 独立于 ZF

注

- 选择公理被普遍使用，但有争议，如用选择公理可构造不可测集，但测度论需要（Lebesgue）可测集
- Banach-Tarski 悖论（分球问题）：把一个单位球体分成有限个点集(最少可分成五份)，通过一些刚体运动（旋转和平移）再重新组合后可成为两个单位球体

  ——存在不可测集的结果

ZFC

公理化集论 $ZFC = ZF + (AC)$

注

- 若 ZF 是一致的，则 ZFC 也是一致的
- (AC) 不会产生悖论，但可能导致反直觉的结果(如 Banach-Tarski 悖论)

类 *

- 基于形式集论，集不会导致 Russell 悖论，作为数学中集的概念
- 数学中（如布尔巴基学派），认为集作为数学基础是没危机的，一旦发现悖论总能通过引入新的公理加以限制或消除
- 朴素集改称为类（class），这样，类包含集；把不能作为（*ZFC*）集的类称为真（proper）类，这样，全体集是一个真类（类似地，全体代数结构（群）/空间（拓扑）是真类）（这种大对象通过范畴论处理）
- NGB 系统（von Neumann–Bernays–Gödel）通过排除真类的公理定义集，从而避免 Russell 悖论
- 计算机科学中，如程序语言，用类的概念（不需 ZFC 作为基础），通常不是真类，并引入过程机制（如 Python 类中方法），但有时需要处理真类的悖论问题（如 OWL (Web Ontology Lanuguage)），并与（数据）类型相关

Hilbert 无穷旅馆悖论

假设有一个拥有无穷（能枚举）多个房间的旅馆，且所有的房间均已客满。设想此时这一旅馆将可再接纳新的客人

一个新客人：由于旅馆拥有无穷个房间，因而可将在 1 号房间原有的客人安置到 2 号房间、2 号房间原有的客人安置到 3 号房间，以此类推，这样就空出了 1 号房间留给新的客人

类推之

有穷个新客人

无穷个新客人

无穷个客车且每个客车有无穷客人

有穷对无穷

该“悖论”事实上并不矛盾，仅是与直觉相悖

无穷集的性质与有穷集的性质并不相同

注（实无穷与潜无穷）

Hilbert 悖论常被用于反对实无穷的存在

哲学家 William Lane Craig 证明上帝的存在

"尽管在数学上这种旅馆（或任何无穷的事物）并非是不可能的，但从直觉上这样的事物永远不可能存在，不仅如此，任何实无穷都不可能存在。如果一个时间序列能够无穷地回退到过去那就会建立起一个实无穷，既然实无穷不存在，那时间就必然有个"起点"。每个事物都有其发生的原因，而时间起始的原因不可能是其他事物，只能是上帝。"

基数

基数：集中包含元素的“个数”（大小，通过映射定义）

自然数集 $\mathbb{N}$：与 $\mathbb{N}$ 能一一对应的集为能枚举集

$\mathbb{N}$ 的所有无穷子集都能与 $\mathbb{N}$ 一一对应

$\mathbb{N}$ 的基数记 $\aleph_0$（最小的无穷集基数）

实数集是不能枚举的（Cantor 对角证法或悖论反证）

实数集的基数，记作 c，代表连续统（直线）

构作逐个大的集，而这些巨集的元素已不可如实数描述

$\Rightarrow$ 需要集论

基数序列：$\aleph_0, \aleph_1, \cdots, \aleph_n \cdots$

注意 $c = 2^{\aleph_0}$

猜想

$c = \aleph_1$

连续统假设

(*CH*) 每个实数的无穷集或是能枚举的，或与全部实数有相同的基数

推广之，$\aleph_{n+1} = 2^{\aleph_n}$

广义连续统假设

(*GCH*) 对所有无穷基数 $\aleph$ ，都不存在介乎 $\aleph$ 与 $2^{\aleph}$ 之间的基数

注

Cantor（1874）提出，亦是 Hilbert（1900）提出的 23 个数学问题中的第一个

结果

- 一致性（Gödel 1938，内模型法）：(*AC*) 和 (*CH*) 都与 *ZF* 一致
- 独立性（Cohen 1963，力迫法）：(*AC*) 和 (*CH*) 都与 *ZF* 独立

- 数学系统
- 带等词一阶系统
- 群论
- 一阶算术
- 形式集论
- 一致性问题

一致性问题

任何一阶系统是一致的 当且仅当 它有一个模型

数学系统的一致性 $\Leftrightarrow$ 模型 ?

算术系统 $\mathcal{N}$ 的一致性 $\Leftrightarrow$ 算术模型 N ??

问题

考虑 ZF 的模型（解释）需要集的概念（解释的论域），如何回避由此引起的循环？

悖论 5.33 (Skolem 悖论)

按 Löwenheim-Skolem 定理，ZF 具有能枚举模型，而不能枚举集存在，ZF 似应有不能枚举模型 □

命题 5.34 (相对一致性)

令 S 是一个一阶系统，S^* 是 S 的扩充，若 S^* 是一致的，则 S 也是一致的 $\diamondsuit$

证

设 S^* 是一致的，但 S 是不一致的

对 S 的某个公式 $\mathscr{A}$，$\vdash_S \mathscr{A}$ 且 $\vdash_S \sim\mathscr{A}$

$\mathscr{A}$ 也是 S^* 的公式

且 S 中证明也是 S^* 的证明

$\vdash_{S^*} \mathscr{A}$ 且 $\vdash_{S^*} \sim\mathscr{A}$

这与 S^* 的一致性矛盾 $\square$

例 5.35

由 ZF 的一致性可推出 $\mathscr{N}$ 的一致性

数学基础问题：绝对一致性

一阶逻辑具有绝对一致性，作为一阶系统是否有某个数学系统（如最基本的 *ZF*）具有一致性？

注

- Euclud 几何（经 Hilbert 改正）被认为有“几乎接近”完全性（因此有“几乎接近”一致性）

未解问题

尚未知 *ZF* 是否具有一致性

数学基础危机问题

- 数学第三次危机仍未解决
- 至今尚未发现明确的思想和技术路线解决 ZF 一致性问题（或其它数学系统的绝对一致性问题）
- 不建议在没有充分准备条件下立志解决这个数学的根本问题

数学基础问题 *

随堂讨论

范畴作为数学基础？

- 范畴（category）论（Eilenberg & Mac Lane，1942–45）：一个范畴包含对象和箭头（arrow，态射），其公理系统

  (1) 箭头的复合具有结合性

  (2) 有一个单（位）箭头

  范畴之间的映射称函子（functor），函子亦箭头，由范畴和函子可构造新范畴，函子亦对象，函子之间态射称自然变换。集（作为对象）范畴仅考虑结构（同构），而不需朴素集的构造（因此一致性是无关的）

- Topos （理）论：对集范畴，其公理系统

  (1) A 的子集 B 与其特征函数 $X: A \mapsto \{Truen, False\}$ 之间一一映射且对 A 中元素 a，$X(a) = true$ 当且仅当 a 在 B 中

  (2) 给定一个 A 中的 a 和一个函数 $h: A \mapsto A$，存在唯一一个函数 $f: \mathbb{N} \mapsto A$ 使得 $f(n) = h^n(a)$

范畴作为数学基础？

- 集、群、自然数、序、序数等都定义为各种范畴
- 范畴论研究不同抽象数学结构之间的联系，需要全体对象（如幺半群）的结构性质，不可避免地会遇到大量的真类（因此一致性是有关的）
- 所有类放在一起不再是一个类，而是一个更高一级的类，以此类推，类似类型论，但用 Grothendieck 全集（universe）概念
- Grothendieck 全集是一个满足下列条件的集 U:
  - 若 $x \in u$ 且 $u \in U$，则 $x \in U$
  - 若 $u \in U$ 且 $v \in U$，则 $\{u, v\} \in U$
  - 若 $x \in u$，则 $P(x) \in U$（幂集）
  - 全体自然数集 $N \in U$
  - 若 $I \in U$ 且对任意 $x_i \in I$，则 $\cup_i x_i \in U$

  可证 U 是 ZFC 的模型

范畴作为数学基础？

- 基于 U，满足 $x \in U$ 的 x 称为（U）小集；满足 $x \subset U$ 但 $x \notin U$ 的 x（不是 U 的元素的子集）称为（U）大集(取代真类)，这样，在小集上可定义几乎一切数学结构（群、空间等)，而全体对象（群、空间等）归为大集
- 全集公理：对任意集 x，存在一个 Grothendieck 全集 U 使得 $x \in U$
  例如，"全体大集"超出了 U 自身的范围，把它放到另一个更大的 Grothendieck 全集 V 中（类似于更高一层的类型）

范畴作为数学基础？

- Lawvere 基于 Grothendieck 的代数几何（范畴 + 拓扑，1950-1960）提出范畴论（尤其是 Topos）作为数学基础，Topos 论与直觉主义类型论直接相关（每个 Topos J 的内部语言 $\mathscr{L}(J)$ 是直觉主义类型论，每个直觉主义类型论 $\mathscr{L}$ 生成一个 topos $T(\mathscr{L})$，通过范畴摹状词描述，它们之间构成不交的函子），而 Gödel 完全性定理和不完全性定理 仍然成立（逻辑 $\Leftrightarrow$ 范畴）
- Langlands 纲领（1967/1979）企图建立数学的统一理论，仍致力于解决一些基本数学问题（素数分类算术，猜想），未涉及元数学问题
- 无穷范畴（Jacob Lurie：Higher topos theory (pp.944, arxiv, 2006)，Higher algebra (pp.1553, 2011)）是一个新的数学基础（如，用等价取代相等），被认为是继代数几何后数学最大的进展之一，是近二十来数学的新发展，但未涉及数学基础危机问题
- 数学仍是诸侯（分支）封建，（统一的）数学基础尚未形成