

数理逻辑

讲义，第 6.3 版，2024 年

北京大学 信息与计算科学系

林作铨

`linzuoquan@pku.edu.cn`

5 数学基础

5.1 数学系统

5.2 带等词一阶系统

5.3 群论

5.4 一阶算术

5.5 形式集论

5.6 一致性问题

- 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

一阶系统与数学

- 逻辑演算是刻画形式推理，尤其是数学中的精确推理
- 一阶语言 $\mathcal{L}$ 是普适的， $\mathcal{L}$ 中的符号可以不同方式解释
- 一阶逻辑 $K_{\mathcal{L}}$ 是足够一般的， $K_{\mathcal{L}}$ 中的定理可解释为真理
- 对任一 $\mathcal{L}$ ，有一类公式不依赖于对符号的解释，即逻辑有效的公式，亦即 $K_{\mathcal{L}}$ 中的定理
- 当 $\mathcal{L}$ 中的（非逻辑）符号用数学方式解释， $K_{\mathcal{L}}$ 中的定理可解释为数学中的真理，它们之所以为数学真理是基于逻辑的结构，而不依赖于具体的数学背景

注

数学中的逻辑主义

例 5.1

对一个算术解释, A_1^2 解释为 “=”

$\forall x_1 \forall x_2 (A_1^2(x_1, x_2) \rightarrow A_1^2(x_1, x_2))$ 是有效的, 可解释为数学真理

$\forall x_1 \forall x_2 (A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, x_1))$ 可解释为数学真理, 但不是 $K_{\mathcal{L}}$ 的定理 ($\forall x_1 \forall x_2 (\mathcal{A}(x_1, x_2) \rightarrow \mathcal{B}(x_2, x_1))$)

$\Leftarrow$ 需要补充有关 “=” 的公理

定义 5.2 (一阶理论)

一个**一阶理论** (first-order theory, 简称理论) 作为一阶系统是 $K_{\mathcal{L}}$ 的某个通过增加公理的扩充, 通过引入**合适公理**集来扩充逻辑公理 (K1-5)。一个一阶理论的模型是一个解释, 使其所有公理为真
一个数学系统作为一阶理论引入合适公理集来扩充 $K_{\mathcal{L}}$, 使得系统中的定理表示某个数学领域 (**尽可能多**) 的数学定理以及逻辑定理

注

希望一个数学系统具有完全性

例 5.3

给定一个一阶语言 $\mathcal{L}$

只有一个谓词符 A_1^2 (没有函项符和常元)

把 $A_1^2(x_i, x_j)$ 记为 $x_i < x_j$, 一个一阶理论通过增加以下合适公理

(P1) $\forall x_1 (\sim x_1 < x_1)$ (非自反性)

(P2) $\forall x_1 \forall x_2 \forall x_3 (x_1 < x_2 \wedge x_2 < x_3 \rightarrow x_1 < x_3)$ (传递性)

该一阶理论的模型称为**偏序理论**, 作为数学系统 (在数学中) 称偏序结构

一阶逻辑之外无逻辑

- 为显式地表达数学（逻辑外）的假设，所需的公理总能用一阶逻辑表达
- 数学中非形式化的证明能用一阶逻辑中形式化的证明精确地表达

注

- (1) 数学中的形式主义，Hilbert 规划
- (2) 见下例 5.20
- (3) 已有多个一阶逻辑和数学形式证明的软件 (LCF/FOL/Isabelle/Hyperproof 等)
如 Lean, Coq 是常用的交互式定理证明器，可对一阶逻辑、数学定理和程序正确性进行形式化和形式证明
- (4) E-prover (E 2.3, github.com/eprover): 带等词 FOL 证明器 (开源)
- (5) 大部分数学还没有形式化，一个 Kepler 猜想的形式化花了 20 人年

- 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

带等词一阶系统

令 $\mathcal{L}$ 为一个 (带等词的) 一阶语言, $\mathcal{L}$ 中 A_1^2 解释为 “=”

定义 5.4 (等词公理)

$$(E6) \quad A_1^2(x_1, x_1)$$

$$(E7) \quad A_1^2(t_k, u) \rightarrow A_1^2(f_i^n(t_1, \dots, t_k, \dots, t_n), f_i^n(t_1, \dots, u, \dots, t_n)),$$

$t_1, \dots, t_n, u$ 是 ($\mathcal{L}$ 的) 任意项, f_i^n 是任意函项符

$$(E8) \quad (A_1^2(t_k, u) \rightarrow (A_i^n(t_1, \dots, t_k, \dots, t_n) \rightarrow A_i^n(t_1, \dots, u, \dots, t_n))),$$

$t_1, \dots, t_n, u$ 是任意项, A_i^n 是任意谓词符

- 等词公理可有自由变元出现

已知：对任意公式 $\mathcal{A}$ ，它的全称闭式是 $\mathcal{A}'$

$$\mathcal{A} \vdash_{K_{\mathcal{L}}} \mathcal{A}' \text{ 且 } \mathcal{A}' \vdash_{K_{\mathcal{L}}} \mathcal{A}$$

可写成这些公理的全称闭式

- 据关于约束变元换名的 命题 4.28，在 (E6) 中用变元名 x_1 是无关紧要的

例如， $A_1^2(x_5, x_5)$ 就是 (E6) 的推论，其演算如次

$$(1) A_1^2(x_1, x_1) \quad (E6)$$

$$(2) (\forall x_1) A_1^2(x_1, x_1) \quad (1) \text{Gen}$$

$$(3) (\forall x_5) A_1^2(x_5, x_5) \quad (2)(\text{命题 4.28})$$

$$(4) (\forall x_5) A_1^2(x_5, x_5) \rightarrow A_1^2(x_5, x_5) \quad (K4)$$

$$(5) A_1^2(x_5, x_5) \quad (3)(4) \text{MP}$$

注 (续)

- (E6): 确保在任意模型中, A_1^2 的解释就是 $=$ (等号)
- (E7)(E8): 确保在任意模型中, A_1^2 的解释起到 $=$ 的作用, 即相等的东西可彼此代替
(t_k 只替换 u 一次, 重复应用可进行多个替换)
- (E7)(E8) 都是公理模式

定义 5.5 (数学系统)

数学系统 (作为一阶理论) 都是 $K_{\mathcal{L}}$ (对某个 $\mathcal{L}$) 的扩充, 它们通常包括公理 (E6), 以及 (E7)(E8) 的所有适用的 (与 $\mathcal{L}$ 有关的) 实例 ◇

定义 5.6 (等词系统)

(E6)(E7)(E8) 称为 **等词公理**

任意包括 (E6)(E7)(E8) 适当实例的 $K_{\mathcal{L}}$ 的扩充称为 **带等词一阶系统** (first-order systems with equality), 亦即一个一阶理论, 一个 (基本的) 数学系统 ◇

注 (带等词一阶逻辑)

- 把包含 (K1-5), (E6-8) 的形式系统称 **带等词 FOL**, 记 $K_{\mathcal{L}=}$
- 通常, FOL 都指带等词的

等价的带等词一阶逻辑 *

一个等价的带等词一阶逻辑：在 (K1-5) 上增加如下公理

(K6) $\forall x_1 (x_1 = x_1)$ (等词自反)

(K7) $x_1 = x_2 \rightarrow (A(x_1, x_1) \rightarrow A(x_1, x_2))$, $A(x_1, x_1)$ 是不含常元的原子公式, x_2 在 $A(x_1, x_1)$ 中对 x_1 自由 (等词替换)

注

在 (K1-5) 上, 从 (K6-7) 可推出 (E6-8) ((K6) 即 (E6)), 推导过程较长, 可作练习 (提示: 先证 (K7) 的原子 $A(x_1, x_1)$ 换成任意公式 $\mathscr{A}(x_1, x_1)$ 亦成立)

带等词一阶公理的独立性（证明思路）*

- (K1-3) 的独立性需重新考虑，因可能有 $t = s$ 实例，可把它看成形式 $A \rightarrow A$
- (K4-6) 可把量词和项去掉看成形式 $B \rightarrow B$ ，(K7) 看成形式 $(B \rightarrow B) \rightarrow (C \rightarrow C)$
- 设计多值表可证

命题 5.7

设 S 是带等词的一阶系统，则下列各式是 S 的定理

- (1) $(\forall x_1)A_1^2(x_1, x_1)$
- (2) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, x_1))$
- (3) $(\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2) \rightarrow (A_1^2(x_2, x_3) \rightarrow A_1^2(x_1, x_3)))$



证

(1) 由 Gen 即得

证 (续)

(2)

$$(1) A_1^2(x_1, x_2) \rightarrow (A_1^2(x_1, x_1) \rightarrow A_1^2(x_2, x_1)) \quad (E8)$$

$$(2) (A_1^2(x_1, x_2) \rightarrow (A_1^2(x_1, x_1) \rightarrow A_1^2(x_2, x_1))) \rightarrow \\ ((A_1^2(x_1, x_2) \rightarrow A_1^2(x_1, x_1)) \rightarrow (A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, x_1))) \quad (K2)$$

$$(3) ((A_1^2(x_1, x_2) \rightarrow A_1^2(x_1, x_1)) \rightarrow (A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, x_1))) \quad (1)(2)MP$$

$$(4) A_1^2(x_1, x_1) \rightarrow (A_1^2(x_1, x_2) \rightarrow A_1^2(x_1, x_1)) \quad (K1)$$

$$(5) A_1^2(x_1, x_1) \quad (E6)$$

$$(6) A_1^2(x_1, x_2) \rightarrow A_1^2(x_1, x_1) \quad (4)(5)MP$$

$$(7) A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, x_1) \quad (3)(6)MP$$

$$(8) (\forall x_1)(\forall x_2)(A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, x_1)) \quad (7)Gen$$

证 (续)

(3)

$$(1) A_1^2(x_2, x_1) \rightarrow (A_1^2(x_2, x_3) \rightarrow A_1^2(x_1, x_3)) \quad (E8)$$

$$(2) (A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, x_1)) \quad (2)$$

$$(3) A_1^2(x_1, x_2) \rightarrow (A_1^2(x_2, x_3) \rightarrow A_1^2(x_1, x_3)) \quad (1)(2)HS$$

$$(4) (\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2) \rightarrow (A_1^2(x_2, x_3) \rightarrow A_1^2(x_1, x_3))) \quad (3)Gen$$



注

命题 5.7 (1-3) 的每一个在 S 的任意模型中必然为真

符号 A_1^2 在任意模型中都可用一个自反、对称和传递的关系（即等价关系）来解释

但 (E6-8) 并不能保证在 S 中 A_1^2 的解释一定是 =

例 5.8

考虑一个一阶语言 $\mathcal{L}$ ，其变元是 $x_1, x_2, \dots$ ，函项符有 f_1^2 ，谓词符有 A_1^2
定义一个解释 I 如下：

- D_I 是所有整数的集合 $\mathbb{Z}$
- $f_1^2(x, y)$ 代表 $x + y$
- $A_1^2(x, y)$ 成立 当且仅当 对 $x, y \in \mathbb{Z}$, $x \equiv y \pmod{2}$

在此解释下，等词公理都为真

例 (续)

(E6): 其解释是 $x \equiv x \pmod{2}$, 这是真的

(E7): 考虑一个特殊情形 (可推广到一般情形)

$$A_1^2(x_1, x_2) \rightarrow A_1^2(f_1^2(x_1, x_3), f_1^2(x_2, x_3))$$

可解释为

若 $x \equiv y \pmod{2}$, 则 $x + z \equiv y + z \pmod{2}$

这是真的

例 (续)

(E8): 因 $\mathcal{L}$ 只含一个谓词符, 故仅有两个实例需证

$$(A_1^2(t, u) \rightarrow (A_1^2(t, v) \rightarrow A_1^2(u, v)))$$

和

$$(A_1^2(t, u) \rightarrow (A_1^2(v, t) \rightarrow A_1^2(v, u)))$$

其解释分别为

若 $x \equiv y \pmod{2}$, 则 $x \equiv z \pmod{2}$ 蕴涵 $y \equiv z \pmod{2}$

和

若 $x \equiv y \pmod{2}$, 则 $z \equiv x \pmod{2}$ 蕴涵 $z \equiv y \pmod{2}$

它们都是真的



命题 5.9

若 S 是一致的带等词一阶系统, 则 S 有一个模型, 其对 A_1^2 的解释是 =



证

据命题 4.62, 若 S 是一致的, 则 S 有模型, 设为 M

据命题 5.7, $\bar{A}_1^2$ 是 D_M 上的等价关系, 用 $[x]$ 表示 x 的等价类

定义一个新的解释 M^* 如下

证 (续)

M^* 的论域是 $\{[x] : x \in D_M\}$, 对每一 i , a_i 用 $[\bar{a}_i]$ 解释, f_i^n 用 $\hat{f}_i^n$ 解释, 使对 $y_1, \dots, y_n \in D_M$,

$$\hat{f}_i^n([y_1], \dots, [y_n]) = [\bar{f}_i^n(y_1, \dots, y_n)]$$

A_i^n 用 $\hat{A}_i^n$ 解释, 使对 $y_1, \dots, y_n \in D_M$

$\hat{A}_i^n([y_1], \dots, [y_n])$ 成立 当且仅当 $\bar{A}_i^n(y_1, \dots, y_n)$ 成立

这里 $\bar{a}_i, \bar{f}_i^n, \bar{A}_i^n$ 是 $\mathcal{L}$ 的符号在 M 中的解释

可验证这些定义都是良定义的, 且 M^* 是 S 的模型

(处处可定义, 公理在此模型下为真)



例 5.10 (例 5.8 续)

定义一个新的模型：论域为 $\{[0], [1]\}$, f_1^2 用 $\hat{f}_1^2$ 解释, A_1^2 用 $\hat{A}_1^2$ 解释, 并给定

$$\hat{f}_1^2([x], [y]) = [\bar{f}_1^2(x, y)] = [x + y]$$

$\hat{A}_1^2([x], [y])$ 成立 当且仅当 $\bar{A}_1^2(x, y)$ 成立, 当且仅当

$$x \equiv y \pmod{2}, \text{ 当且仅当}$$

$$[x] = [y]$$

定义 5.11 (规范模型)

令 S 是带等词一阶系统, S 的 **规范模型** (normal model) 是 A_1^2 解释为 $=$ 的模型, 亦简称模型 ◇

命题 5.12

任何一致的带等词一阶系统 S (带等词一阶逻辑 $K_{\mathcal{L}_=}$) 都有有穷或能枚举无穷规范模型

证

据命题 4.65 (Löwenheim-Skolem 定理), S 有能枚举模型, S 的模型可收缩为对应的规范模型 (命题 5.9), 其能枚举论域是等价类的集, 而等价类的集是有限或能枚举的 □

推论 5.13 (推广的 Löwenheim-Skolem 定理)

对任何带等词一阶系统 S , 若 S 有一个无穷规范模型, 则它有一个能枚举无穷规范模型

证

留作练习 □

仍以 $\vdash, \models$ 表示推理关系, 考虑 FOL 是带等词的, 不会引起混淆

命题 5.14

带等词一阶系统 S (或带等词一阶逻辑 $K_{\mathcal{L}_=}$) 具有可靠与完全性定理

即 $\vdash \mathcal{A}$ 当且仅当 $\models \mathcal{A}$

证

可靠性易对等词公理验证

完全性只需考虑闭式 $\mathscr{A}$ (任一有效的 (或可证的) 公式等价于它的全称闭式), 若 $\mathscr{A}$ 是有效的, 设 $\models_S \mathscr{A}$, 据命题 4.51, 把 $\sim \mathscr{A}$ 加入 S 所得扩充 S' 是一致的, 据命题 5.12, S' 有一个规范模型 M , 因 $\sim \mathscr{A}$ 是 S' 的公理, $\sim \mathscr{A}$ 在 M 中为真, 但已设 $\mathscr{A}$ 是有效, $\mathscr{A}$ 在 M 中为真, 这是不可能的 □

注

这是证明完全性定理的另一种方式, 即先给出 Löwenheim-Skolem 定理, 再给出完全性结果

命题 5.15

带等词一阶系统 S 具有一致性

证

类似 K 一致性可证 □

记号

用 $t_1 = t_2$ 代表 $A_1^2(t_1, t_2)$

$(t_1 \neq t_2) =_{\text{def}} \sim(t_1 = t_2)$, 这里 t_1 和 t_2 是 $(\mathcal{L}_=)$ 中的项

(E6-8) 的简化形式

等词公理

$$(E6') \quad x_1 = x_1$$

$$(E7') \quad t_k = u \rightarrow (f_i^n(t_1, \dots, t_k, \dots, t_n) = f_i^n(t_1, \dots, u, \dots, t_n))$$

$$(E8') \quad t_k = u \rightarrow (A_i^n(t_1, \dots, t_k, \dots, t_n) \rightarrow A_i^n(t_1, \dots, u, \dots, t_n))$$

命题 5.16

令 t, s, r 为任意项

$$(1) \vdash t = t$$

$$(2) \vdash t = s \rightarrow s = t$$

$$(3) \vdash t = s \rightarrow (s = r \rightarrow t = r)$$



证

(1) 由 (E6') 和 Gen, $\vdash \forall x_1 (x_1 = x_1)$, 据 (R3), $\vdash t = t$

(2) 令 x, y 是不在 t 或 s 中出现的变元, $\mathscr{A}(x, x)$ 为 $x = x$, $\mathscr{A}(x, y)$ 为 $y = x$, 易见

$$\vdash x = y \rightarrow (x = x \rightarrow y = x)$$

是公理模式 (E8') 的实例

证 (续)

由 (1)

$$\vdash x = x$$

用重言式 $(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})) \rightarrow (\mathcal{B} \rightarrow (\mathcal{A} \rightarrow \mathcal{C}))$, 并用两次 MP, 有

$$\vdash x = y \rightarrow y = x$$

再用两次 Gen, 得到

$$\vdash (\forall x)(\forall y)(x = y \rightarrow y = x)$$

最后, 用两次 (R3) 得

$$\vdash t = s \rightarrow s = t$$

(3) 留作练习



定义 5.17 (存在唯一量词)

- 存在量词 (至少存在一个): $(\exists x_i)\mathcal{A}(x_i)$
- 存在唯一量词

$$(\exists_1 x_i)\mathcal{A}(x_i) =_{\text{def}} (\exists x_i)(\mathcal{A}(x_i) \wedge (\forall x_j)(\mathcal{A}(x_j) \rightarrow x_i = x_j))$$

亦如

$$(\exists! x_i)\mathcal{A}(x_i) =_{\text{def}} (\exists x_j)(\forall x_i)(\mathcal{A}(x_i) \leftrightarrow x_i = x_j)$$

其中 x_j 是不在 $\mathcal{A}$ 中自由出现且不同于 x_i 的 (第一个) 变元

- 至多存在一个量词 (但不一定存在)

$$(\exists!! x_i)\mathcal{A}(x_i) =_{\text{def}} (\forall x_i)(\forall x_j)(\mathcal{A}(x_i) \wedge \mathcal{A}(x_j) \rightarrow x_i = x_j)$$

注

- 验证：对任意解释 I , $I \models (\exists! x_i) \mathcal{A}(x_i)$ 当且仅当 存在唯一 $d \in D_I$ 使得 $I \models \mathcal{A}(x_i/d)$
- 可证： $\vdash \exists! x_i \mathcal{A}(x_i) \leftrightarrow \exists x_i \mathcal{A}(x_i) \wedge \exists! x_i \mathcal{A}(x_i)$

摹状 (description) 词

$\iota x A(x)$: 那个有 A 性质的 x

如 $A(x)$: x 是大于 3 的最小素数, 就有 $\iota x A(x) = 5$

规定: 对给定谓词 A , 当有唯一的 x 使得 $A(x)$ 成立时, 就说 $\iota x A(x)$ 是存在的, 即 $\iota x A(x)$ 有某种性质; 否则, 就是假的

如 $A(x)$: x 是 7 和 11 之间的素数, 说 $\iota x A(x)$ 存在或 $\iota x A(x) = 11$ 等都是假的

注

- 摹状词类似冠词有不定摹状词和定摹状词之分, 这里专指定摹状词 (存在唯一)
- 自 Frege 就通过逻辑定义引入, Russell 发展摹状词理论来解决“存在”等哲学问题 (如消除某些对象的不合理的本体论承诺)

摹状词

$\iota x A(x)$ 有性质 B , 即存在唯一的使得 $A(x)$ 成立的 x 并且这个 x 有性质 B

$$(\iota) B(\iota x A(x)) =_{\text{def}} \exists y (\forall x (A(x) \leftrightarrow x = y) \wedge B(y))$$

- $\iota x A(x)$: 摹状词
- ιx : 摹状算子
- $A(x)$ 是 ιx 的辖域
- ι : 摹状符
- x : 摹状变元
- $B(\iota x A(x))$ 为 $\iota x A(x)$ 的辖域
- (ι) 为 $\iota x A(x)$ 的 (辖域的) 标志符, 根据 (ι) 在公式中用以上定义式把摹状词替除后, x 在其中是约束的

摹状词演算 *

- 摹状词可用来定义项，如 $a =_{\text{def}} \iota x A(x)$
- 由此可进行演算

$$E! \iota x A(x) =_{\text{def}} \exists y (\iota x A(x) = y)$$

其中 y 不在 A 中出现

$$E! \iota x A(x) \text{ 当且仅当 } \exists! x A(x)$$

注

在一阶系统中，摹状词不是必要的，可通过引入新的函项和常元取代

函项符的消去 *

在带等词的一阶语言 $\mathcal{L}$ 中, 函项符可消去 (即不是必要的), 一个 n 元函项符可用一个 $n+1$ 元谓词符来表示

如 $\langle t_1, \dots, t_n, s \rangle \in \bar{P}$ iff $\bar{f}(t_1, \dots, t_n) = s$

如 $\mathcal{A}^*$ 是把 $\mathcal{A}$ 中函项符替换为相应的谓词符中变元

$$\forall x_1 \dots \forall x_n \exists! x_{n+1} P(x_1, \dots, x_n, x_{n+1}) \wedge \mathcal{A}^*$$

- 反过来看, 就是引入新的函项符
- 消去或引入常元可看成函项符的特殊情况

纯谓词演算*

纯谓词演算

不含函项符和常元的谓词演算

n 元谓词符 (有时只用一元谓词符) 可能无穷多个

斯科伦前束范式: 全部 $\exists$ (若有) 在 $\forall$ (若有) 之前的前束范式

命题 (等价性定理): 在纯谓词演算中, 对任一公式 $\mathscr{A}$ 与其斯科伦前束范式 $\mathscr{A}^S$, 有 $\vdash \mathscr{A}$ 当且仅当 $\vdash \mathscr{A}^S$ ($\models \mathscr{A}$ 当且仅当 $\models \mathscr{A}^S$)

注

- 数学中, 如算术运算, 使用函项符 (函数) 比较方便, 也是必要的
- 可计算性上, 不含函项符的一阶理论计算复杂度较低, 但把一个含函项符的一阶理论通过消去函项符得到的等价的一阶理论需要考虑新引入替换公式的计算, 计算复杂性是一样的

等词的消去 *

在带等词的一阶语言 $\mathcal{L}_=$ 中, 等词可消去: 可在不带等词的一阶语言 $\mathcal{L}'$ 中通过引入一个 (特殊的) 谓词符 E , 对任一 $\mathcal{L}_=$ 的公式 $\mathcal{A}$ 中每次出现的 $=$ 都用 E 替换得到对应 $\mathcal{L}'$ 的公式 $\mathcal{A}^*$, 并令 $\mathcal{A}^\#$ 为

$$\forall x_1 E(x_1, x_1) \wedge \mathcal{P}_1 \wedge \cdots \wedge \mathcal{P}_k \wedge \mathcal{A}^*$$

设 P_i 为 $\mathcal{A}$ 中出现的 (有限个) n_i 元谓词符, 令 $\mathcal{P}_i$ 为如下公式

$$\begin{aligned} & \forall x_1 \cdots \forall x_{2n_i} (E(x_1, x_{n_i+1}) \rightarrow E(x_2, x_{n_i+2}) \rightarrow \cdots \rightarrow E(x_{n_i}, x_{2n_i}) \\ & \rightarrow P_i(x_1, \cdots, x_{n_i}) \rightarrow P_i(x_{n_i+1}, \cdots, x_{2n_i})) \end{aligned}$$

则一个 $\mathcal{L}_=$ 的解释 $I \models \mathcal{A}$ 当且仅当一个 $\mathcal{L}'$ 的一个解释 $I' \models \mathcal{A}^\#$

- 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

定义 5.18 (群语言 $\mathcal{L}_G$)

令 $\mathcal{L}_G$ 是具有下述字符表的一阶语言

- 变元 $x_1, x_2, \dots$
- 个体常元 a_1 (单位元)
- 函项符 f_1^1, f_1^2 (逆, 积)
- 谓词符 $=$
- 技术性符号 $(,), ,$
- 逻辑符 $\forall, \sim, \rightarrow$

定义 5.19 (群系统 $\mathcal{G}$)

$\mathcal{G}$ 为 $K_{\mathcal{L}_G}$ 的扩充, 其合适公理包含 (E6-8) 的所有适当实例, 并增加以下公理

群公理

$$(G1) \quad f_1^2(f_1^2(x_1, x_2), x_3) = f_1^2(x_1, f_1^2(x_2, x_3)) \quad (\text{结合律})$$

$$(G2) \quad f_1^2(a_1, x_1) = x_1 \quad (\text{左单位元})$$

$$(G3) \quad f_1^2(f_1^1(x_1), x_1) = a_1 \quad (\text{左逆元})$$

这些公理中的变元可考虑等价的全称闭式

注

$$(G4) \quad f_1^2(x_1, x_2) = f_1^2(x_2, x_1) \quad (\text{交换律})$$

增加 (G4) 即 Abel 群

定义 (群)

一个非空集 G 称为一个群, 如果下列条件成立

- 给定一个运算法则, 对 G 中的每对元素 a 和 b , 都有集合中的第三个元素与之对应, 这个元素通常称为 a 和 b 积, 记作 ab 或 $a \cdot b$

- 结合律 对 G 中的任意三个元素 a, b 和 c , 等式

$$ab \cdot c = a \cdot bc$$

- G 中存在 (至少) 一个 (左) 单位元素 e , 它具有下列性质:
对 G 中所有元素 a

$$ea = a$$

- 对 G 中每个元素 a , G 中存在 (至少) 一个 (左) 逆元素 a^{-1} , 它具有性质

$$a^{-1}a = e,$$

在这个等式中, 出现于右端的总是同一个 (左) 单位元素 e

代数学 (p.24), [荷] 范德瓦尔登著 (1930-1931), 丁石孙等译 (1963)

注

- 数学中（基本）群（论） G 的定义是群公理的非形式陈述，对照上述定义
 - 第一点由 $\mathcal{L}_G$ 规定
 - 其余三点即 (G1-3)
- “代数学”书由 Van der Waerden 据 Noether & Artin 讲稿而撰，其时正逢一阶逻辑成熟，其后公理化方法教科书由 Bourbaki 继承

例 5.20

在任何有单位元 e 的群 G 中, $e(ee) = e$

在 $\mathcal{G}$ 中形式化为公式

$$f_1^2(a_1, f_1^2(a_1, a_1)) = a_1$$

形式证明如下

注

在群论中（非形式）证明 $e(ee) = e$ 是简单的，但严格的证明步骤可通过形式证明验证

复杂的群论（数学）定理及证明同样可被形式化（Hilbert 论题）

例 (续)

$$(1) \quad f_1^2(a_1, x_1) = x_1 \quad (G2)$$

$$(2) \quad \forall x_1 (f_1^2(a_1, x_1) = x_1) \quad (1)Gen$$

$$(3) \quad \forall x_1 (f_1^2(a_1, x_1) = x_1) \rightarrow (f_1^2(a_1, a_1) = a_1) \quad (K4)$$

$$(4) \quad f_1^2(a_1, a_1) = a_1 \quad (2)(3)MP$$

$$(5) \quad \forall x_1 (f_1^2(a_1, x_1) = x_1) \rightarrow (f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1)) \quad (K4)$$

$$(6) \quad (f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1)) \quad (2)(5)MP$$

$$(7) \quad (f_1^2(a_1, a_1) = a_1) \rightarrow (f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1) \rightarrow f_1^2(a_1, f_1^2(a_1, a_1)) = a_1) \quad (E8')$$

$$(8) \quad f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1) \rightarrow f_1^2(a_1, f_1^2(a_1, a_1)) = a_1 \quad (4)(7)MP$$

$$(9) \quad f_1^2(a_1, f_1^2(a_1, a_1)) = a_1 \quad (6)(8)MP$$

解释

若 a_1 解释为 (任意群 G 的) 单位元, f_1^1 解释为逆, f_1^2 解释为群的运算, $=$ 解释为相等, 则任意群 G 都是群系统 $\mathcal{G}$ 的一个模型

但还存在着其它的模型

例 5.21

构造 $\mathcal{G}$ 的一个解释 I 如下

- D_I 是整数集 $\mathbb{Z}$,
- a_1 解释为 0,
- $f_1^1(x) = -x, \quad x \in \mathbb{Z},$
- $f_1^2(x, y) = x + y, \quad x, y \in \mathbb{Z};$
- $=$ 解释为 $(\text{mod } m)$ 同余, 这里 m 是一个确定的正整数

I 是 $\mathcal{G}$ 的模型

证

需证 $\mathcal{G}$ 的每一公理在 I 下为真

(K1-5) 为真, 因它们是有效的

(E6-8) 为真 (见例 5.8)

需考察 (G1-3) 在 I 下为真

(G1) 解释为 $(x + y) + z \equiv x + (y + z) \pmod{m}$

(G2) 解释为 $0 + x \equiv x \pmod{m}$

(G3) 解释为 $-x + x \equiv 0 \pmod{m}$

对任意 $x, y, z \in \mathbb{Z}$, 上面语句都是真的

故 I 是 $\mathcal{G}$ 的模型



例 (续)

但 I 不是一个群 (包含了额外的同余关系)

对模型 I 用 命题 5.9 的方法, 构造一个规范模型 I^* 如下

- 论域是整数的同余类 $(\text{mod } m)$ 的集
- a_1 解释作 0_m (含 0 的类)
- f_1^2 用 $+$ 解释
- f_1^1 解释作 “加性逆元”
- $=$ 解释作相等

I^* 是一个规范模型, 且是一个群

定义 5.22 (群解释)

任意群 G 是群系统 $\mathcal{G}$ 的一个规范模型，群系统 $\mathcal{G}$ 的任一规范模型是一个群 G

问题

群系统 $\mathcal{G}$ 是否具有完全性定理？

计算系统 *

类似于数学系统，一个**计算系统**（关于可计算或计算机的形式系统）亦可作为一阶系统，扩充为某个领域的计算机理论

程序语言

设 P 是一个包含**赋值**、**条件**和**迭代**语句的程序设计语言

给出 $\mathcal{L}_P$ 作为关于 P 的一阶语言

扩充关于三个程序语句的公理的一阶系统是一个**程序语言系统** $\mathcal{P}$

$\mathcal{P}$ 可作为 P 的公理化语义 (Hoare 逻辑)

问题

P 与 $\mathcal{P}$ 之间的关系 (如完全性定理)?

应用

(数学) 定理自动证明和 (计算机) 程序 (正确性) 自动验证

非标准分析 *

无穷小：标准分析通过极限理论严格使用无穷小（无穷小缺乏直观意义）

实无穷小：非标准分析严格定义存在无穷小，并通过构造模型，使之（基本）等价（但不同构）于实数的有序域

令 R 是实数集， $\mathcal{K}_R$ 是广义带等词 FOL，其一阶语言 $\mathcal{L}_R$ 规定

- 对任一实数 r ，有一个常元 a_r
- 对 R 任一 n 元操作 ϕ ，有一个函项符 f_ϕ
- 对 R 任一 n 元关系 Φ ，有一个谓词符 A_Φ

R 作为 $\mathcal{K}_R$ 的模型 $\mathcal{R}$ 的论域，这样的 $\mathcal{R}$ 可被构造获得（非标准）实数（包含无穷小和无穷大）

分析可逐次展开, 如 $\lim s_n = c$, c 是一个实数

$$(\forall \varepsilon) (\varepsilon > 0 \rightarrow (\exists n) (n \in \omega \wedge (\forall k) (k \in \omega \wedge k \geq n \rightarrow |s_k - c| < \varepsilon)))$$

如实数集 B 上函数 f 在 $c \in B$ 连续

$$(\forall \varepsilon) (\varepsilon > 0 \rightarrow (\exists \delta) (\delta > 0 \wedge (\forall x) (x \in B \wedge |x - c| < \delta \rightarrow |f(x) - f(c)| < \varepsilon)))$$

许多标准分析的定理可在非标准分析得到更简单的证明, 甚至得到更强的结果

非标准分析方法可推广到现代分析领域