TURING 图灵计算机科学丛书

ELSEVIER

数理逻辑

（第2版）

A Mathematical Introduction to Logic

Second Edition

[美] Herbert B. Enderton 著

沈复兴 陈磊 孙运传 译

人民邮电出版社

POSTS & TELECOM PRESS

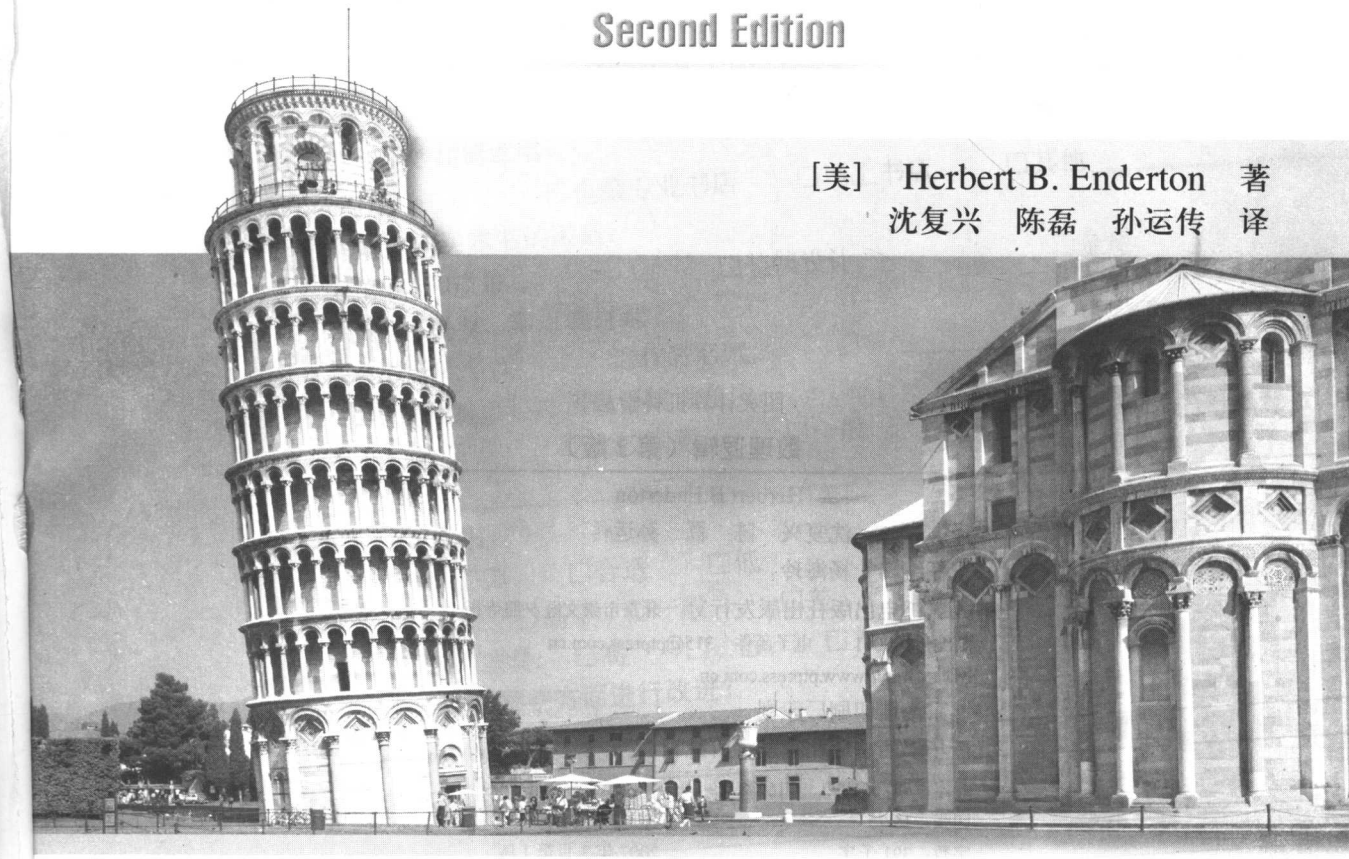
TURING 图灵计算机科学丛书

数理逻辑

（第2版）

A Mathematical Introduction to Logic

Second Edition



[美] Herbert B. Enderton 著

沈复兴 陈磊 孙运传 译

人民邮电出版社

北 京

图书在版编目（CIP）数据

数理逻辑：第2版 /（美）恩德滕著；沈复兴，陈磊，孙运传译.
—北京：人民邮电出版社，2007.3
（图灵计算机科学丛书）

ISBN 978-7-115-14311-2

Ⅰ. 数… Ⅱ. ①恩…②沈…③陈…④孙… Ⅲ. 数理逻辑—教材 Ⅳ. 0141

中国版本图书馆CIP数据核字（2006）第132105号

内 容 提 要

本书是数理逻辑方面的经典教材。书中涵盖了命题逻辑、一阶逻辑、不可判定性以及二阶逻辑等方面的内容，并且包含了与计算机科学有关的主题，如有限模型。本书特点是：内容可读性强；组织结构更灵活，授课教师可根据教学需要节选本书的内容；反映了近几年来理论计算机科学对逻辑学产生的影响；包含较多的示例和习题。本书适合作为数学、哲学、计算机科学以及其他学科需要学习数理逻辑课程的本科生和研究生的教材。

图灵计算机科学丛书

数理逻辑（第2版）

◆ 著 [美]Herbert B.Enderton
译 沈复兴 陈 磊 孙运传
责任编辑 杨海玲

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：15.75
字数：391千字 2007年3月第1版
印数：1-4 000册 2007年3月北京第1次印刷

著作权合同登记号 图字：01-2006-2275号

ISBN 978-7-115-14311-2/TP·5169

定价：35.00元

读者服务热线：(010)88593802 印装质量热线：(010)67129223

版 权 声 明

译 者 序

数理逻辑作为基础数学的一个重要分支，在计算机科学中起着奠基作用，在模糊数学和人工智能等方面也都有着广泛的应用，有关它的教材和参考书有许多. 我们选择 Herbert B. Enderton 教授编写的这本数理逻辑教材是因为该书以可读性强而著称，在美国大学中采用率很高，是数理逻辑方面的经典教材之一. 同时，在第 2 版的修订中，作者增加了模型论和递归论的一些基础知识，其中有限模型、解析算法、有限计算和可判定性等内容都与计算机科学密切相关，这些内容是目前多数数理逻辑教材所没有的. 而这些知识，无论对于计算机专业还是基础数学专业的学生来说都是很重要的. 通过对这些内容的学习，学生能够加深对数理逻辑的了解，更多地接触数理逻辑在可计算性理论中的一些前沿应用.

本书除了内容上的改进之外，与传统教材相比，在编排方面也很有特点. 章节组织灵活，各章节内容相对独立. 读者会发现，不少章节的脚注中都有选学提示，可以根据个人需要选择适当的部分学习，而不会影响内容的连贯性，同时学有余力的读者也可进一步扩展知识面.

本书注重数理逻辑与其他数学分支的联系，引进了非标准分析、抽象代数和数论中的一些知识和例子，但这些内容的叙述并不晦涩难懂. 作者用清晰形象的语言阐述它们，大量独具匠心的解释使枯燥的定义、定理变得容易理解和接受. 既使熟悉数学的学生感受到数理逻辑与数学其他分支的紧密联系，又使不熟悉数学的学生对这些内容有直观的认识.

作者充分了解学生学习的难点和易犯的错误，增加了不少示例和解释. 用适当的示例结合一针见血的解释以及形象易懂的图形和图表，以不多的文字点出问题的关键所在.

基于上述特点，本教材适合于数学、哲学、计算机科学以及其他学科需要学习数理逻辑的本科生和研究生，同时对于以数理逻辑为工具从事研究工作的科研工作者也是一本很好的参考书. 我们相信，第 2 版中译本的出现能够让更多的师生在愉快的教与学中得到逻辑严谨美的享受.

由于数理逻辑主要研究形式语言，这种语言不同于我们平常使用的汉语、英语等自然语言. 在翻译的过程中，为了行文的连贯，我们将“英语中的……”译成“汉语中的……”. 一部分术语翻译成数理逻辑中常用的名词，除个别词之外，尽可能与数学、计算机科学中的名词一致.

本书由北京师范大学信息科学学院、哲学与社会学学院和经济学院的三位教师合作翻译而成. 由于译者水平有限，书中难免有疏漏和不妥之处，敬请广大师生、同行和专家批评指正!

前　言

本书与第 1 版一样介绍了逻辑学中的基本概念和结果，主要包括证明、真值和可计算性. 与第 1 版相同，本书主要针对有一定数学背景知识并且对数理逻辑感兴趣的读者. 在这次修订中，我们做了许多“局部”改动，但关系到整本书的改动共有以下三处.

第一，我们力争使书中的内容容易为学生所接受. 在主要的改动中，我们不再把一些想法和知识认为是显然的，以免数学基础较薄弱的学生无法看懂.

第二，本书的结构更加灵活，以便于教师作为教材. 许多章节的开始部分都有脚注，为教师和读者的教学和学习提供可选择的方式.

第三，近年来，理论计算机科学对逻辑学产生了一定的影响. 在这次修订中，我们也突出了一些这样的影响：把可计算性问题作为重点内容之一，将有限模型的一些内容归入这一部分.

本书可以作为大学本科中、高年级学生学习数理逻辑课程的入门教材. 它涉及逻辑学中的一些重要概念和定理，并阐述了它们的重要性以及与数学其他一些分支的联系.

作为教材，本书适合用半个学期到一学年的课时来讲授. 半个学期一般能讲到一阶理论的模型 (2.6 节). 一个学期的话，富裕的时间，可以讲 3.0 节的不可判定性. 如果第二学期还有课程安排，那么就有时间讲授第 3 章的内容 (关于不可判定性).

本书适合没有学过逻辑学但有数学推理经验的读者阅读. 当然，我们希望读者还有一定程度的抽象能力. 在学习过程中，不可避免地要用到集合论的知识. 第 0 章对要用到的集合论知识做了简明概括. 读者可以先略过这一章，有需要时再回过来参考这些知识. 教师在授课时可以适当掌握集合论知识的使用，比如，基数可以完全不讲 (如果这样，一些定理也不用讲). 本书包括一些抽象代数中的例子，但它们只是例子，并不说明本质问题. 总体来说，第 3 章和第 4 章对读者能力的要求要比前两章高.

在 1.4 节中，对归纳和递归给出了更加深入的一些讨论，我们更愿意在课堂上只对这些问题给出非形式化的解释而在书中给出严格描述.

在每一节的末尾几乎都有习题. 如果习题的题号是黑体的，则说明这道习题的结果在前面的正文中讲评过. 通常较难的习题都标有星号.

我诚挚地感谢我所有的老师、同事和学生. 同时，我非常乐意接受任何来自读者的意见和建议. 本书的配套网址是 http://www.math.ucla.edu/~hbe/amil.

引　言

符号逻辑是演绎推理的数学模型. 应该说至少初期确实如此, 但与其他数学分支一样, 它的发展已经大大超出了最初的环境. 符号逻辑是一种模型, 很大程度上就像现代概率论是可能性和不确定性的一种模型一样.

那么, 这些模型是怎样建立起来的呢? 我们可以用建立现实生活中的具体对象的模型来解释, 比如为一架飞机建模, 那么我们选出建模的原对象要在模型中体现的一些特征, 如飞机的形状, 而忽略其他的特征, 如飞机的大小等. 接下来, 我们可以构建一个模型, 这个模型在某些方面 (本质上的) 和原对象很相像, 而在其他一些方面 (不相关的) 与原对象不同. 所建立的模型是否符合我们原来的要求, 在很大程度上取决于特征选取.

逻辑要比飞机更加抽象. 现实生活中的对象都是某种“逻辑正确”的推理. 例如,

所有的人都是要死的.
苏格拉底是人.
所以苏格拉底是要死的.

第 3 句 (结论) 是从前两句 (假设) 中推出的, 推理的正确性并不依赖于苏格拉底的特殊身份, 而是取决于命题的形式, 与“死”这个经验事实无关. 实际上,“死”是什么意思在这里并不重要, 重要的是“所有的”这个词的含义.

◎ 是 ★, 只要它是 ♦.
一个东西是 ♦, 并且它是 ◎.
那么它是 ★.

尽管我们不知道 ★、◎ 是什么, 但我们同样知道第 3 个命题可以从前两个命题中推出.

逻辑正确的推理要比上面介绍的例子有趣得多. 实际上, 公理化的数学就完全是由这样的推理组成的. 数学家实际给出的推理, 被反映在我们的模型中.

这些推理的逻辑正确性源于它们的形式, 而与它们的内容无关. 这种论断是模糊的, 而正是这种模糊性促使我们转而研究推理的数学模型. 我们的主要目标是, 在模型中, 给出这一论断的准确的描述. 我们最关心的与模型有关的问题有:

(1) 什么叫作一个命题能够从其他命题“逻辑推出”?

(2) 如果一个命题的确能够从其他命题逻辑推出, 应该采取什么样的方法来证明这个事实?

(3) 在公理系统中 (比如自然数的公理系统中), 可以证明的命题和在自然数中正确的命题是否相同?

(4) 逻辑和可计算性之间有什么联系?

实际上, 我们将涉及两种模型. 第一种是命题逻辑, 它虽然很简单却不适用于一些有趣的推理. 它的局限性使得它只能表达现实推理的一些梗概. 第二种模型是一阶逻辑, 它适用于数学中遇到的推理. 当一个数学家断定某个特殊的命题可以从集合论的公理中推出时, 他是指这个推理可以转换到我们的模型中.

本书内容的选择更侧重于与数学联系紧密的内容，而不包括多值逻辑、模态逻辑和直觉逻辑等. 这几种逻辑表现了现实推理的另一些不同的性质.

到现在为止，我们对将要研究的模型，比如一阶逻辑，并没有谈论太多. 作为简单的提示，下面我们简要地给出一些例子，看一看这种形式语言的表达能力. 第一个例子是集合论中的外延公理，“如果第一类对象中的元素和第二类对象中的元素相同，那么这两类对象相同.”我们可以把它写成一阶语言

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

第二个例子对于学过微积分的同学来说是很熟悉的. “对于所有正数 ε，存在一个正数 δ 使得对于任何与 a 的差小于 δ 的数 x，$f(x)$ 与 b 的差小于 ε.”可以写成

$$\forall \varepsilon(\varepsilon > 0 \rightarrow \exists \delta(\delta > 0 \wedge \forall x(\mathrm{d}xa < \delta \rightarrow \mathrm{d}fxb < \varepsilon))).$$

这两个例子可以大体表明本书要研究的内容. 我们还需声明：有些内容我们并不打算讨论，以免产生误解. 本书并不打算教读者如何去思考，“逻辑”这个词有时指思考训练，但在这里并不是这个意思. 读者已经知道如何思考. 我们的书给出的是一些值得思考的有趣概念.

目　录

第0章

集合基础

本书假定读者熟悉集合论的基础知识. 即便如此, 在这里我们还是要对即将用到的集合论的基础知识作一个简要的论述, 至少要说明一些记号的用法. 建议读者不要一开始就仔细阅读这部分内容, 而只需要在今后的章节中, 遇到不熟悉的集合论知识时参考一下就行了. 作者向大家推荐自己所著的《集合论基础》[1] 作为集合论方面的参考书 (参看本书最后的参考文献).

首先介绍一些对术语的说明. 贯穿全书, 我们使用了数学中标准的缩写. "■" 用于表示一个证明的结束; "如果……, 那么……" 类型的命题有时候会缩写为 "…… ⇒ ……"; 逆蕴涵则对应使用 "…… ⇐ ……" ("蕴涵" 一词在数学中有特定含义); "当且仅当" 缩写为 "iff" (这已经成为数学语言的组成部分) 或符号 "⇔"; "因此" 缩写为 "∴".

"$x \neq y$" 是 "$x = y$" 的否定, "$x \notin y$" 是 "$x \in y$" 的否定, 类似这样的符号记法可以推广到其他情形. 比如, 1.2 节中定义了 "$\Sigma \vDash \tau$", 那么就用 "$\Sigma \nvDash \tau$" 表示其否定.

集合(set) 是指一些对象的全体, 这些对象称为集合的元素或成员. 通常, "$t \in A$" 表示 t 是 A 的元素, "$t \notin A$" 表示 t 不是 A 的元素. "$x = y$" 表示 x 和 y 是同一个元素, 也就是说符号 x 和 y 是同一个元素的不同名字. 如果 $A = B$, 那么对于任一元素 t, 都有 "$t \in A$ iff $t \in B$", 这是因为 A 和 B 是相同的. 反之, 我们考虑其外延: 如果 A 和 B 是两个集合, 且对于任意的元素 t 都有

$$t \in A \quad \text{iff} \quad t \in B,$$

那么就有 $A = B$. 这反映了集合的基本思想: 集合是由其元素所确定的.

在集合中加入新元素是非常有用的操作. 对于集合 A, $A; t$ 表示一个新的集合, 其元素包括 (i)A 的元素和 (ii) 元素 t(可能是新的), 这里的 t 可能属于也可能不属于 A. 使用后面定义的符号, 这个过程可以表示为

$$A; t = A \cup \{t\}$$

并且

$$t \in A \quad \text{iff} \quad A; t = A.$$

空集 $\varnothing$ 是一个特殊的集合, 它不包含任何元素. 除此以外的其他集合都称为 非空的. 对于任意的对象 x, 存在单元素集合 $\{x\}$, 其唯一的元素就是 x. 更一般地, 对于任意有限个元素 $x_1, x_2, \cdots, x_n$, 都存在集合 $\{x_1, x_2, \cdots, x_n\}$, 此集合中的元素恰好就是这几个元素. 注意 $\{x, y\} = \{y, x\}$, 这是因为两个集合恰好含有相同的元素, 只不过是用不同的形式表示同一个集合. 如果一定要考虑元素的顺序, 那么可以使用有序对来表示 (稍后讨论).

1. 该书英文影印版已由人民邮电出版社出版, ISBN 7-115-14550-4/TP.5269.

集合的这种记法可以推广到某些简单的具有无限个元素的情形. 比如, $\{0,1,2,\cdots\}$ 是自然数集 $\mathbb{N}$, $\{\cdots,-2,-1,0,1,2,\cdots\}$ 是整数集 $\mathbb{Z}$.

记法 "$\{x|\_x\_\}$" 用于表示一个集合, 其元素 x 满足某种性质 $\_x\_$, 比如, $\{\langle m,n\rangle| m<n,m,n\in\mathbb{N}\}$ 表示第 1 个数比第 2 个数小的自然数的所有有序对的集合. $\{x\in A|\_\ x\_\}$ 就表示 A 中所有满足性质 $\_x\_$ 的元素的集合.

如果集合 A 的所有元素都是集合 B 的元素, 我们称 A 是 B 的子集, 记作 "$A\subseteq B$". 注意, 任何集合都是其自身的子集, 空集 $\varnothing$ 是每个集合的子集. ("$\varnothing\subseteq A$" 是 "毋庸置疑的", 因为要证明 $\varnothing$ 中的每个元素都属于 A 不需要做任何事, 或者从另外一个角度考虑, 仅当 A 的某个元素不属于 B 时 $A\subseteq B$ 才不成立, 如果 $A=\varnothing$, 这是不可能的.) 我们可以从集合 A 得到一个新的集合—— A 的 幂集(power set)$\mathcal{P}A$, 其元素是 A 的所有子集. 这样,

2

$$\mathcal{P}A=\{x|x\subseteq A\}.$$

例如,

$$\mathcal{P}\varnothing=\{\varnothing\},$$

$$\mathcal{P}\{\varnothing\}=\{\varnothing,\{\varnothing\}\}.$$

A 与 B 的 并集$A\cup B$ 是属于 A 或属于 B 的元素的集合. 比如, $A;t=A\cup\{t\}$. 类似地, A 与 B 的 交集$A\cap B$ 是所有 A 与 B 共有的元素的集合. 集合 A 与 B不相交(disjoint), 当且仅当二者的交集为空集 (即二者没有公共元素). 一组集合称为是 两两不相交的(pairwise disjoint), 当且仅当其中任意两个集合都不相交.

更一般地, 考虑集合 A, 其中的元素也是集合. 并集 $\cup A$ 可以通过将 A 中所有元素放入一个集合来获得:

$$\bigcup A=\{x|\ x\text{属于 }A\text{ 的某个元素}\}.$$

类似地, 对于非空集合 A,

$$\bigcap A=\{x|\ x\text{属于 }A\text{ 的所有元素}\}.$$

比如, 如果 $A=\{\{0,1,5\},\{1,6\},\{1,5\}\}$, 那么

$$\bigcup A=\{0,1,5,6\}\ ,$$

$$\bigcap A=\{1\}.$$

下面是另外的两个例子:

$$A\cup B=\bigcup\{A,B\}\ ,$$

$$\bigcup\mathcal{P}A=A.$$

如果对每个自然数 n, 都有一个集合 A_n 与之对应, 那么这些集合的并集 $\bigcup\{A_n|n\in\mathbb{N}\}$ 通常记作 "$\bigcup_{n\in\mathbb{N}}A_n$" 或者 "$\bigcup_n A_n$".

元素 x 与 y 的有序对 $\langle x,y\rangle$ 定义如下:

$$\langle x,y\rangle=\langle u,v\rangle\ \text{ iff }\ x=u\text{且 }y=v.$$

所有具有上述性质的定义都可以作为有序对的定义, 其中, 一个标准的定义是

$$\langle x,y\rangle=\{\{x\},\{x,y\}\}.$$

有序三元组可以定义为 3

$$\langle x,y,z\rangle = \langle\langle x,y\rangle,z\rangle.$$

更一般地，对于 $n>1$ 可以如下递归地定义 n 元组：

$$\langle x_1,\cdots,x_{n+1}\rangle = \langle\langle x_1,\cdots,x_n\rangle,x_{n+1}\rangle.$$

为方便起见，对 $n=1$ 的情形，我们定义 $\langle x\rangle = x$；这样上式对于 n=1 也是成立的. 我们称 S 是 A 中元素的 **有限序列**(finite sequence)(或 **有限串**(string)) 当且仅当对某个正整数 n, $S=\langle x_1,\cdots,x_n\rangle$, 其中每个 $x_i\in A$. (有限序列常常被定义为某个特定的有限函数，但是这里的定义更方便我们今后的使用.)

有限序列 $S=\langle x_1,\cdots,x_n\rangle$ 的 **子段**(segment) 是指一个有限序列 $\langle x_k,x_{k+1},\cdots,x_{m-1},\cdots,x_m\rangle, 1\leqslant k\leqslant m\leqslant n$. 这个子段是初始段当且仅当 k=1, 一个子段是 **真子段**(proper) 当且仅当该子段与 S 不同.

如果 $\langle x_1,\cdots,x_n\rangle=\langle y_1,\cdots,y_n\rangle$, 那么容易证明 $x_i=y_i, 1\leqslant i\leqslant n$. (对 n 使用归纳法进行证明，证明的基本思想是用有序对的概念.) 但是，如果 $\langle x_1,\cdots,x_m\rangle=\langle y_1,\cdots,y_n\rangle$，那么通常不一定会得到 $m=n$. 因为每个有序三元组也是一个有序对. 不过，我们断言，只有当某个 x_i 本身是 y_j 的一个有限序列或者某个 y_j 是 x_i 的有限序列时，m 和 n 才不相等. 或者：

引理 0A 如果 $\langle x_1,\cdots,x_m\rangle=\langle y_1,\cdots,y_m,\cdots,y_{m+k}\rangle$, 那么 $x_1=\langle y_1,\cdots,y_{k+1}\rangle$.

证明 对 m 使用归纳法. 如果 m=1, 那么结论是显而易见的.

对于归纳步骤，设 $\langle x_1,\cdots,x_m,x_{m+1}\rangle=\langle y_1,\cdots,y_{m+k},y_{m+1+k}\rangle$, 那么有序对的第一部分应该是相等的，即 $\langle x_1,\cdots,x_m\rangle=\langle y_1,\cdots,y_{m+k}\rangle$. 使用归纳假设即可证明引理成立. ■

例如，设 A 是一个集合，它的任何一个元素都不是由其他元素组成的有限序列. 如果 $\langle x_1,\cdots,x_m\rangle=\langle y_1,\cdots,y_n\rangle$ 且每个元素 x_i 和 y_j 都在 A 中，那么由上述引理可得 $m=n$，于是，也有 $x_i=y_i$.

我们可以构造集合 A 与 B 的 **笛卡儿积**(Cartesian product) $A\times B$, 它是所有序对 $\langle x,y\rangle$ 的集合，其中 $x\in A$, $y\in B$. A^n 表示 A 中元素构成的所有的 n 元组组成的集合. 比如，$A^3=(A\times A)\times A$.

关系(relation)R 是有序对的集合. 例如，数字 0~3 上的大小序关系是有序对的集合：

$$\{\langle 0,1\rangle,\langle 0,2\rangle,\langle 0,3\rangle,\langle 1,2\rangle,\langle 1,3\rangle,\langle 2,3\rangle\}.$$

R 的 **定义域**(domain) 记作 dom R, 它是指所有满足 $\langle x,y\rangle\in R$ 的元素 x 的集合，其中 y 是任意的；R 的 **值域**(range) 记作 ran R, 它是指所有满足 $\langle x,y\rangle\in R$ 的元素 y 的集合，其中 x 是任意的. dom R 与 ran R 的并称为 R 的 **域**(field), 记作 fld R. 4

A 上的 n 元关系是 A^n 的子集. 若 $n>1$, 它就是一个关系；不过当 $n=1$ 时，A 上的一元关系只是 A 的一个子集. A 上的一个特殊的二元关系是恒等关系 $\{\langle x,x\rangle|\ x\in A\}$. 对于 A 上的 n 元关系 R 和 A 的一个子集 B, R 对 B 的限制是指交集 $R\bigcap B^n$. 例如，上例中的关系是 $\mathbb{N}$ 上的序关系对集合 $B=\{0,1,2,3\}$ 的限制.

函数 一个具有 **单值** 性质的关系 F：对于定义域 dom F 中的每一个 x, 都有唯一的一个 y 满足 $\langle x,y\rangle\in F$. 通常，这个唯一的 y 称为 F 在 x 上的值 $F(x)$. (这个记法是欧拉首先采

用的，遗憾的是，他没有使用 $(x)F$ 来表示函数的值，$(x)F$ 的记法对于复合函数的表示是非常有用的：要计算 复合(composition) 函数 $f \circ g$ 在 x 的值 $f(g(x))$，首先要计算 g 在 x 的值，再计算 f 在 $g(x)$ 的值.）

我们称 F 将 A 映射(map) 到 B 中，记作

$$F : A \to B,$$

意味着 F 是一个函数，$\mathrm{dom}\ F = A$，$\mathrm{ran}\ F \subseteq B$. 若 $\mathrm{ran}\ F = B$，则称 F 将 A 映射到 B上. F 是一个 一对一映射(one-to-one) 当且仅当对于 $\mathrm{ran}\ F$ 中的每个 y，都存在唯一的一个 x 使得 $\langle x, y\rangle \in F$. 如果 $\langle x, y\rangle$ 在定义域 $\mathrm{dom}\ F$ 中，那么记 $F(x, y) = F(\langle x, y\rangle)$. 这个记法可以推广到 n 元的情形：$F(x_1, \cdots, x_n) = F(\langle x_1, \cdots, x_n\rangle)$.

A 上的 n元运算(n-ary operation) 是一个将 A^n 映射到 A 中的函数. 比如，加法是一个 $\mathbb{N}$ 上的二元运算，而后继运算 S(这里 $S(n) = n + 1$) 是 $\mathbb{N}$ 上的一元运算. 如果 f 是 A 上的 n 元运算，那么 f 在 A 的子集 B 上的限定是一个函数 g，其定义域为 B^n，且 g 在 B^n 中的每个点上的取值都与 f 在这些点上的取值相等. 这样，

$$g = f \cap (B^n \times A).$$

这个函数 g 是 n 元运算当且仅当 B 在 f 的作用下是 封闭的，即 $f(b_1, \cdots, b_n) \in B$，只要其中的每个 b_i 都在 B 中. 在这种情况下，$g = f \cap B^{n+1}$，这与关系的限制的定义是一致的. 例如，$\mathbb{N}$ 上的加法运算 (包含类似于 $\langle\langle 3, 2\rangle, 5\rangle$ 这样的三元组) 是 $\mathbb{R}$ 上的加法运算在 $\mathbb{N}$ 上的限制，而 $\mathbb{R}$ 中所包含的三元组要多得多.

A 上的一种特殊的一元运算是 恒等(identity) 函数 Id，

$$Id(x) = x, \quad x \in A.$$

因此，$Id = \{\langle x, x\rangle | x \in A\}$.

对于关系 R，我们定义：

- R 在 A 上是 自反的，当且仅当对 A 中每个 x 都有 $\langle x, x\rangle \in R$.
- R 是 对称的，当且仅当如果 $\langle x, y\rangle \in R$，则 $\langle y, x\rangle \in R$.
- R 是 传递的，当且仅当如果 $\langle x, y\rangle \in R$ 并且 $\langle y, z\rangle \in R$(若很巧)，则 $\langle x, z\rangle \in R$.

5

R 在 A 上满足 三分律(trichotomy)，当且仅当对 A 中任意的 x 和 y，如下 3 种可能中有且仅有一种成立：$\langle x, y\rangle \in R$，$x = y$，或者 $\langle y, x\rangle \in R$.

R 是 A 上的 等价关系 当且仅当 R 是 A 上一个自反的、对称的和传递的二元关系.

R 是 A 上一个 序关系 当且仅当 R 是传递的且在 A 上满足三分律.

对于 A 上的等价关系 R 和 $x \in A$，我们定义 x 的 等价类 $[x]$ 为 $\{y | \langle x, y\rangle \in R\}$. 等价类对 A 进行了 划分，即每个等价类都是 A 的子集并且 A 的每个元素都恰好只属于一个等价类. 对 A 中的元素 x 和 y，

$$[x] = [y] \ \text{ iff } \ \langle x, y\rangle \in R.$$

自然数集 $\mathbb{N}$ 是集合 $\{0, 1, 2, 3, \cdots\}$.（自然数也可以用集合论的方法定义，见 3.7 节.）集合 A 是 有限的 当且仅当存在一个函数 f 将集合 A 一对一映射到 $\{0, 1, \cdots, n-1\}$ 上.（可以将 f 看作是对 A 中元素的一种“计数”.）

集合 A 是 **可数的** 当且仅当存在某个函数将 A 一对一映射到自然数集 $\mathbb{N}$ 中. 例如, 有限的集合显然是可数的. 现在来考虑可数无限集合 A, 从给定的把 A 一对一映射到 $\mathbb{N}$ 中的 f, 它可以扩展成从 A 到 $\mathbb{N}$ 上的一对一映射函数 f'. 对某个 $a_0 \in A$, 如果 $f(a_0)$ 是值域 $\operatorname{ran} f$ 中的最小值, 则令 $f'(a_0) = 0$. 一般地, 存在唯一的 $a_n \in A$ 使得 $f(a_n)$ 是 $\operatorname{ran} f$ 中的第 $n+1$ 个元素, 我们令 $f'(a_n) = n$. 注意 $A = \{a_0, a_1, \cdots\}$. (我们可以认为 f' 也是 A 中的元素的一种计数, 只是计数过程是无限的.)

定理 0B　设 A 是一个可数集, 则所有由 A 的元素组成的有限序列的集合也是可数的.

证明　所有有限序列的集合 S 可用如下式子表示:

$$S = \bigcup_{n \in \mathbb{N}} A^{n+1}.$$

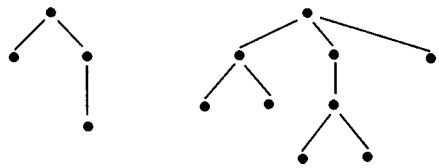
由于 A 是可数的, 因此存在函数 f 将 A 一对一映射到 $\mathbb{N}$ 中.

基本思路是通过将 $\langle a_0, a_1, \cdots, a_m \rangle$ 指派给自然数 $2^{f(a_0)+1}3^{f(a_1)+1} \cdot \cdots \cdot p_m^{f(a_m)+1}$ 来建立一个从 S 到 $\mathbb{N}$ 中的一对一映射, 其中 p_m 是第 $m+1$ 个素数. 这样做的缺点是这种指派的定义不明确. 我们可以想像, 可能会出现 $\langle a_0, a_1, \cdots, a_m \rangle = \langle b_0, b_1, \cdots, b_n \rangle$, 且 a_i 和 b_j 属于 A, 但是 $m \neq n$ 的情况. 然而, 问题不大, 只要给 S 中的每个元素指派具有上述形式的 最小(smallest) 的一个数即可. 这就能够得到一个良定义的映射, 并且容易看出它是一对一映射的. ■

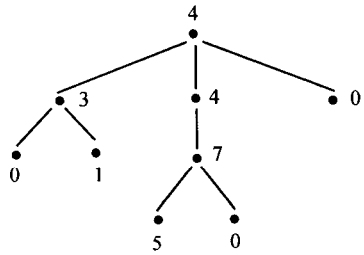
6

有些情况下, 可能会用 树 (tree) 的方法来给出某些问题的直观图形表示. 可是, 本书对树的说法是非正规的, 定理和证明不会依赖于树. 相应地, 在这里我们对树的讨论也是非正规的.

每棵树都是一种潜在的有限偏序, 我们可以给出这种偏序关系 R 的图形表示; 如果 $\langle a, b \rangle \in R$, 那么我们把 a 放在 b 的下面, 并且用线将它们连起来. 下面是两棵典型的树. (数学中的树是向下长的, 而不是向上的.) 树中总会有一个最高点 (称之为 树根(root)). 另外, 尽管允许某个顶点向下分叉, 一个顶点 上 面的点都在一条连线上.



除了这种向下的有限偏序树外, 在一棵树上也可以定义一个标记函数, 其定义域是顶点的集合. 比如, 一棵树可以用自然数进行标记, 如下图所示.



本书有些地方会用到选择公理. 但是, 当问题中所用的定理只涉及可数语言时, 我们可以不使用选择公理. 选择公理有很多等价的命题, 其中佐恩引理是非常有用的一个命题.

我们说一组集合 C 是一个 **链**(chain) 当且仅当对于 C 中任意的元素 x 和 y, 要么 $x \subseteq y$ 要么 $y \subseteq x$.

佐恩引理 设 A 是一个集合, 且满足对于任意的链 $C \subseteq A$, 有集合 $\bigcup C$ 在 A 中. 那么
7 A 中存在极大元 m, 即 m 不是 A 中其他任意元素的子集.

基数

所有的无限集合都很大, 但是其中某些集合会比另外一些更大. (例如, 实数集大于整数集.) 基数是一种度量集合大小的方便方法, 当然, 这种方法并非必不可少.

自然地, 我们说两个集合 A 与 B 大小相同, 当且仅当存在一个函数将 A 一对一地映射到 B 上. 如果 A 与 B 都是有限的, 这个概念就等价于通常的一个说法: 如果对 A 和 B 的元素分别计数, 那么得到的结果是相同的. 但是, 这个方法还可以用到当 A 和 B 是无限集合的时候, 尽管它们是难以计数的.

规范地说, A 与 B**大小相等**(记作 $A \sim B$) 当且仅当存在一个从 A 到 B 上的一对一映射. 例如, 自然数集 $\mathbb{N}$ 和整数集 $\mathbb{Z}$ 是大小相等的. 显然, 集合大小相等的关系是自反的、对称的和传递的.

对于有限集合, 我们可以使用自然数来度量其大小. 同一个自然数可以同时表示两个有限集合的大小, 当且仅当这两个集合大小相等. 基数的引入使我们可以将这种方法推广到无限集合.

一个集合 A 的 **基数** (cardinal number)(或称为 **基** (cardinality), 记作 $\operatorname{card} A$) 是给集合 A 指定的一个特定的对象, 其意义为, 两个集合的基数相等当且仅当它们大小相等:

$$\operatorname{card} A = \operatorname{card} B \quad \text{iff} \quad A \sim B. \tag{K}$$

定义集合的基数的方法有很多种; 目前, 标准的方法是用与 A 大小相等的最小序数作为 $\operatorname{card} A$. (这种定义的成功依赖于选择公理.) 这里并不讨论序数, 因为, $\operatorname{card} A$ 的实质是什么与我们的课程内容关系不大, 它并不比数字 2 的本质是什么有更多的意义. 对于我们来说, 最重要的是 (K) 式是成立的. 然而对于一个有限集合 A 而言, $\operatorname{card} A$ 指明了集合 A 中有多少个元素, 就已经够用了. **基数**, 或简称 **基**, 就是指某个集合 A 的 $\operatorname{card} A$.

(康托尔 (Georg Cantor) 于 1895 年最早采用基数这一概念, 他认为集合 M 的基数是从集合中抽象而得到的有助于人们理解的一个一般的概念, 而不考虑组成集合的元素的不同和集合中元素的排列次序.)

我们称 A **受控于** B (记作 $A \preccurlyeq B$) 当且仅当 A 与 B 的一个子集大小相等. 换句话说, $A \preccurlyeq B$ 当且仅当存在一个从 A 到 B 中的一对一映射. 对应的基数的关系是

$$\operatorname{card} A \leqslant \operatorname{card} B \quad \text{iff} \quad A \preccurlyeq B.$$

(易见, $\leqslant$ 是良定义的, 即 $\kappa \leqslant \lambda$ 是否成立仅取决于基数 κ 和 λ 本身, 而与集合的选择
8 无关.) 受控性是自反的和传递的. 集合 A 受控于 $\mathbb{N}$ 当且仅当 A 是可数的. 下述定理是有关这方面内容的常用结果.

Schröder-Bernstein 定理　(a) 对于集合 A 和 B, 如果 $A \preccurlyeq B$ 并且 $B \preccurlyeq A$, 那么 $A \sim B$; (b) 对于任意的基数 κ 和 λ, 如果 $\kappa \leqslant \lambda$ 并且 $\lambda \leqslant \kappa$, 那么 $\kappa = \lambda$.

(b) 是从基数的角度对 (a) 的简单描述. 下面的定理等价于选择公理, 只是描述方式不同而已.

定理 0C　(a) 对于任意的集合 A 和 B, $A \preccurlyeq B$ 或者 $B \preccurlyeq A$ 必有一个成立; (b) 对任意的基数 κ 和 λ, $\kappa \leqslant \lambda$ 或者 $\lambda \leqslant \kappa$ 必有一个成立.

这样, 任意两个基数都可以比较大小. (事实上, 任意非空的基数的集合都有一个最小的元素.) 最小的一类基数是有限集合的基数: 0, 1, 2, …, 其次小的是无限基数 card $\mathbb{N}$, 称为 $\aleph_0$. 这样就有

$$0, 1, 2, \cdots, \aleph_0, \aleph_1, \cdots,$$

这里的 $\aleph_1$ 是大于 $\aleph_0$ 的最小基数. 实数的基数, card $\mathbb{R}$, 称作 "$2^{\aleph_0}$", 由于 $\mathbb{R}$ 是不可数的, 我们有 $\aleph_0 < 2^{\aleph_0}$.

常用于有限基数的加法与乘法运算也可以推广到所有的基数. 计算 $\kappa + \lambda$, 我们要选择两个不相交的集合 A 与 B, 其基数分别为 κ 和 λ, 那么,

$$\kappa + \lambda = \operatorname{card}(A \cup B).$$

这个定义是良定义的, 即 $\kappa + \lambda$ 仅依赖于 κ 和 λ, 而不依赖于两个不相交集合 A 与 B 的选择. 对乘法, 有

$$\kappa \cdot \lambda = \operatorname{card}(A \times B).$$

显然, 这些定义对有限基数都是正确的. 无限基数的算术运算都是相当简单的 (根据选择公理). 两个无限基数的和与积只是它们中较大的那个.

基数算术定理　对基数 κ 和 λ, 如果 $\kappa \leqslant \lambda$ 并且 λ 是无限的, 那么 $\kappa + \lambda = \lambda$. 另外, 如果 $\kappa \neq 0$, 那么 $\kappa \cdot \lambda = \lambda$. 特别地, 对于无限基数 κ, 9

$$\aleph_0 \cdot \kappa = \kappa.$$

定理 0D　对无限集合 A, 由 A 中元素组成的有限序列的集合 $\bigcup_n A^{n+1}$ 与 A 具有相同的基数 card A.

我们已经证明了这个定理对可数集合 A 是正确的 (参见定理 0B).

证明　根据基数算术定理 (使用 n 次), 每个 A^{n+1} 的基数等于 card A. 于是, 我们得到 $\aleph_0$ 个大小相等的集合的并集, 其基数为 $\aleph_0 \cdot \operatorname{card} A = \operatorname{card} A$. ■

例　代数数集合的基数为 $\aleph_0$. 首先, 我们把每个整系数的一元多项式看作其系数的序列; 然后, 由上述定理知, 共有 $\aleph_0$ 个多项式, 每个多项式都只有有限多个根. 为了给出一个充分大的上界, 注意到即使每个多项式都有 $\aleph_0$ 个根, 我们也只能得到 $\aleph_0 \cdot \aleph_0 = \aleph_0$ 个代数数. 同时, 至少也应该有这么多个, 于是结论成立.

由于实数是不可数的 (事实上, 有 $2^{\aleph_0}$ 个), 因此超越数也是不可数的 (也有 $2^{\aleph_0}$ 个). 10