引言：什么是数理逻辑?

> 数理逻辑无非是形式逻辑的精确的与完全的表述，它有着相当不同的两个方面。一方面，它是数学的一个部门，处理类、关系、符号的组合等，而不是数、函数、几何图形等。另一方面，它是先于其他科学的一门科学，包含着所有科学底部的那些思想和原则。正是在第二种意义上，莱布尼兹在他的《通用文字》中首先构想了数理逻辑，原本可作为其中的一个核心部分。
>
> ——哥德尔

就字面意思而言，“数理逻辑” 至少包含两方面的含义。一是 “使用数学”，即以数学为工具来研究逻辑；二是 “为了数学”，以数学里面出现的或是数学家常用的逻辑为研究对象。首先，我们使用数学的符号语言，这种语言本质上可定义为自然数和自然数的序列这样的数学对象。我们还频繁地使用数学中的各种工具，如数学归纳法、紧致性定理等；频繁地引用数学中的定理，如数论基本定理、中国剩余定理、佐恩引理等；并且我们的研究成果（所下的结论）也都是以数学定理的形式表述的。从这一角度来看，与用数学研究几何图形或物理方程没有太多区别，只不过我们的研究对象是逻辑而已。

其次，数理逻辑的研究目标归根到底是要指出哪些命题是真的，而且是不依赖于物理世界的事实而为真的；哪些证明或推理的形式是正确的，它们正确的依据又是什么。例如，$2+2=4$ 是真的，但这不依赖于 “两双鞋子的总数” 或 “汽车前轮加后轮的个数” 这样的物理事实。它的真必定植根于关于另外一个世界的另外一些事实中。再如，勾股定理的证明是正确的，它的正确性并不依赖于我们对任何一个直角三角形的直角边和斜边的测量结果，而必定依赖于另外一些非物理对象的属性。这些例子足以说明，为什么只有在逻辑与数学结合后才成为深刻、“伟大” ①的学科。因为究其本性，逻辑研究

① 蒯因（W. V. Quine，1908—2000）曾说：“逻辑是一门古老的科学，但 1879 年以后成为一门伟大的科学。”（W. V. Quine，*Methods of Logic*，Harvard University Press，1950，第 vii 页。）1879 年弗雷格出版了《概念文字》（*Begriffsschrift*），标志着现代数理逻辑的诞生。

的现象是超越于物理世界和物理事实之上的。在这里，没有任何物理意义上的偶然性。另外还值得一提的是，虽然这个超越物理世界的宇宙尚属于神秘之域，我们对其知之甚少，但有一点是可以肯定的：它是无穷的。而处理无穷世界带来的困难是数理逻辑发展的主要推动力之一。

以上两点综合起来，就是沙拉赫[①]所说的，数理逻辑是以“数学的方式研究数学”。[②]事实上，数理逻辑主要研究的是数学证明形式的“对错”、数学语句的真假以及数学结构的性质。所谓“以数学的方式研究数学”，就是将数学语句、数学结构、数学证明等作为数学对象，然后用已有的数学理论研究它们的性质。

当然仅停留在字面上的解读是远远不够的。例如，从以上的解读中，我们还看不出数理逻辑和哲学有什么关系，看不出为什么全世界的哲学系都要开设数理逻辑的课程。这当然很难用简短的篇幅进行解释，也不是本书要解决的问题。不过，那个逻辑事实植根于其中的、超越于物理世界的宇宙是什么样的存在呢？无穷究竟有哪些特别的性质呢？这不都是一些关乎根本的哲学问题吗？

也许，只有通过学习数理逻辑，熟练地掌握它的内容、方法和技巧以后，才能真正开始讨论“什么是数理逻辑?”这个问题。不过到那时候，你可能会想起陶潜的诗句：“此中有真意，欲辨已忘言。”

下面简单介绍数理逻辑早期发展的历史（近期的发展请参照结束语部分）。这类似于勾勒一个本学科的简明“历史地图”，也许有助于读者了解自己所处的位置和将要前进的方向。

逻辑史早期的几个重要里程碑

亚里士多德[③]

亚里士多德（见图1）是古希腊思想的集大成者（不仅限于逻辑学）。他研究了三段论和其他各种形式推理，逻辑学代表作为《工具论》[④]。在之后的两千多年中，尽管有中世纪的宗教学家和学者有零星的逻辑学研究成果，但没有重大突破。康德[⑤]曾经说过：“……从亚里士多德时代以来，逻辑在内容方面就收获不多，而就其性质来说，逻辑也不能再增加什么内容。”[⑥] 亚里士

① 沙拉赫（Saharon Shelah, 1945—　），以色列逻辑学家、数学家。

② 参见 Saharon Shelah, Logical Dreams，*Bull. Amer. Math. Soc.* 2003(40), 203-228。

③ 亚里士多德（Aristotle，前 384—前 322），古希腊哲学家。

④ 工具论，英文为“Organon”。

⑤ 康德（Immanuel Kant，1724—1804），德国哲学家。

⑥ 康德，许景行译，《逻辑学讲义》，北京：商务印书馆，1991。

图 1　柏拉图和亚里士多德（图片来自维基）

多德的形式逻辑不能称为数理逻辑。他使用自然语言，而且也没有讨论量词等概念。

莱布尼兹[①]

在人类文明史上，莱布尼兹可以与文艺复兴时代的任何一位巨匠相提并论。他 26 岁时的工作使他与牛顿[②]一起成为微积分的共同创立者。在逻辑史上，莱布尼兹被称为“数理逻辑的先驱”。他有一个伟大的设想，试图建立一个能够涵盖所有人类知识的“通用符号演算系统”，让人们讨论任何问题，包括哲学问题，都变得像数学运算那样清晰。一旦有争论，不管是科学上的还是哲学上的，只要坐下来算一算就可以毫不费力地辨明谁是对的。他的名言是：“让我们来算吧。”这一伟大的设想后来被称为“莱布尼兹之梦”。但是，莱布尼兹的许多工作在当时并不被人所知，在他死后很久才得以发表，或许这也是康德认为没人超越亚里士多德的原因吧。值得一提的是，很多哲学家研究逻辑的出发点都是试图为人类理智建立一个坚实的框架或系统，而这样的框架或系统很自然地涉及数学工具。

布尔[③]

布尔的主要贡献是把逻辑变成了代数的一部分，从而向“让我们来算吧”的方向跨出了重要一步。简单地说，布尔把逻辑中对真假的判断变成了代数

① 莱布尼兹（Gottfried Wilhelm Leibniz，1646—1716），德国数学家和哲学家。

② 牛顿（Issac Newton，1642—1727），英国物理学家、数学家。

③ 布尔（George Boole，1815—1864），英国数学家。

中符号的演算。所谓布尔代数即是以他命名的。大致上说，亚里士多德形式逻辑的所有规则都可以用布尔代数重新表述出来。

弗雷格[1]

弗雷格是莱布尼兹之梦的实现者，是现代数理逻辑的创始人。他一生致力于数学基础的研究，试图从纯逻辑的概念出发定义出全部数学，从而使数学成为逻辑的一个分支。这一纲领被称作“逻辑主义”。他的工作对分析哲学（有人称他为“分析哲学之父”）、现代逻辑和数学基础都有极其深远的影响。我们将要学习的一阶逻辑就是源自他的理论。他第一个引进了量词，同时把谓词处理为函项，这从根本上改变了逻辑的形态，使其成为一门伟大的学科。

但是，当弗雷格即将宣布他的逻辑主义成功的时候，罗素[2]于 1902 年写信给他：“只有一点我遇到些困难……”，而正是这一点困难，引发了关于数学基础的一场巨大的争论。

说到这里，需要涉及一点数学史，尤其是 19 世纪末、20 世纪初数学基础方面的争论。从古到今，数学大致是沿着从具体到抽象、从含混到准确、从庞杂到精纯的方向发展。以微积分为例，在古希腊时代，阿基米德[3]已经有了近似于现代定积分的概念。到了 17 世纪，牛顿和莱布尼兹独立发明了微积分。但用现代数学的标准来衡量，当时的微积分领域里有很多概念是不精确的。例如，莱布尼兹用无穷小量来表述导数，而无穷小量有如下性质：它可以参与所有的算术运算，小于所有的正实数但又不是零。无穷小这一概念当时即受到很多批评，其后 200 多年也一直不被人接受。[4] 尽管如此，牛顿和莱布尼兹的直观完全与物理世界吻合，微积分理论也获得了巨大成功。直到 19 世纪，柯西[5]和魏尔斯特拉斯[6]引入了数学分析中的 ε-δ 方法，才给微积分奠定了坚实的基础。首先，微积分中最根本的概念“微分”和“积分”都可以用极限来定义，而极限的概念又可以通过 ε-δ 方法建立在实数理论的基础上。之后数学家又用有理数定义实数、用整数定义有理数、用自然数定义整数。在康托尔[7]创立集合论之后，人们又用集合作为最根本的概念来定义自然数。因此，人们自然会想：也许集合论和逻辑就是莱布尼兹当年梦想的通用语言？也许整个数学（乃至整个科学，甚至人类全部精神活动）都可以归约到逻辑？这就是逻辑主义的历史背景。

[1] 弗雷格（Gottlob Frege，1848—1925），德国哲学家。

[2] 罗素（Bertrand Russell，1872—1970），英国哲学家。

[3] 阿基米德（Archimedes，约前 287—约前 212），古希腊数学家。

[4] 亚·鲁宾逊（Abraham Robinson，1918—1974）用模型论的方法，在 20 世纪 60 年代成功地为无穷小量奠定了坚实的基础，这一学科分支称为非标准分析。

[5] 柯西（Augustin-Louis Cauchy，1789—1857），法国数学家。

[6] 魏尔斯特拉斯（Karl Weierstrass，1815—1897），德国数学家。

[7] 康托尔（Georg Cantor，1845—1918），德国数学家。

让我们回到困扰罗素的那一点。罗素在弗雷格的逻辑体系中找到了一个矛盾，后来被称为“罗素悖论”。罗素悖论的具体内容这里不提。在 20 世纪初，有很多与罗素悖论类似的其他悖论。这些悖论的共同点是它们都涉及非常大的集合。这些悖论让人们怀疑人类是否越过了自己能力的极限，或者说，数学理论是不是太抽象了，抽象到人们对它的真假完全没有了直觉。因此不少人基于哲学的考虑，想给数学概念和方法加一些人为的限制，以保证数学基础的坚实，起码避免悖论。其中比较极端的主张是以布劳威尔[①]为代表的直觉主义。直觉主义者只承认潜无穷，对实无穷（起码对不可数的实无穷）持完全否定的态度。这样一来，数学里涉及实无穷的部分都将被抛弃，作为专门研究无穷的理论，康托尔的集合论也就失去了意义。

希尔伯特[②]

希尔伯特是对 20 世纪数学发展影响最大的数学家之一。对数学的许多领域都有杰出的贡献。希尔伯特强烈反对直觉主义者对数学的限制。他的名言是：“没有人能把我们从康托尔创造的乐园中赶出去。”在 20 世纪初，他提出了“希尔伯特计划”，期望一劳永逸地为数学奠定坚实的基础。纲领大致如下：首先分离出数学中那些连直觉主义者都认为无可争议的证明手段，也就是本质上有穷的那些数学证明工具。对于直觉主义者担心的，涉及无穷的数学命题，则暂时不去考虑它们的意义，而只是将其看作按照一定规则进行的纯符号操作。或者说暂时把无穷数学的语义和语法分开，只研究语法部分。这样一来，如何保证证明系统是一致[③]的就成为头等重要的大事。希尔伯特期望找到这样的形式系统，在其中能够证明这种形式化后的全部数学的一致性，而在证明过程中只使用本质上有穷数学的证明手段。

哥德尔[④]

哥德尔被称为亚里士多德以来最伟大的逻辑学家。他的主要成就包括一阶逻辑的完全性定理、一阶算术的不完全性定理（这两个定理将是本课程的主要内容），以及选择公理和连续统假设与集合论公理系统的相对一致性。哥德尔的成果遍及数理逻辑的几乎所有领域，而且对很多领域来说是开创性的。这些成果从根本上影响和推动了数理逻辑的发展，直到今天依然如此。在哥德尔所有这些惊世骇俗的成就中，不完全性定理不仅对逻辑，甚至对整个人类文明的发展都有深远的影响。我们只谈逻辑。哥德尔定理改变了逻辑发展的进程，其中一个重要的原因就是它彻底否定了（依原本设想方式的）希尔伯特计划。

① 布劳威尔（Luitzen Egbertus Jan Brouwer，1881—1966），荷兰数学家、哲学家。

② 希尔伯特（David Hilbert，1862—1943），德国数学家。

③ consistent，consistency，也常译为协调、相容、和谐、无矛盾等。

④ 哥德尔（Kurt Gödel，1906—1978），奥地利和美国数学家、哲学家。

假设皮亚诺[1]公理系统 PA[2]代表经典数论的形式化系统，按照希尔伯特计划的要求，至少要能从 PA 出发，只使用严格的“有穷主义”的手段来证明 PA 的一致性。但是，哥德尔不完全性定理告诉我们，除非 PA 是不一致的，PA 的一致性不能在 PA 中得到证明，更遑论在 PA 中证明全部数学的一致性了。

课程大纲

本书可以提供两学期课程的容量。预备知识可以根据学生的情况决定是否在一开始讲授。第一到第四部分构成一门完整的数理逻辑入门课程，（可以略去 2.9 节、4.5 节和 6.3 节）。第五、第六、第七部分可以作为进阶课程的教材，主要是针对哥德尔不完全性定理的一个相对完整的导论。

第一部分 命题逻辑

这一部分将全面讨论有关命题逻辑的内容。由于几乎所有的逻辑问题在命题逻辑中都显得十分直接和简明，因此这一部分可以看作一阶逻辑内容的简明版本，把它当作热身。主要内容包括：命题逻辑的形式语言，真值指派，合式公式的无歧义性，命题连接词的互相可定义性，命题演算的（若干）公理系统，命题逻辑的完全性定理，以及模态逻辑简介。

第二部分 一阶逻辑的语法

从这里开始正式学习一阶逻辑的内容。首先会给出一阶语言的初始符号和形成规则，然后讨论有关一阶语言的一些重要概念，包括子公式、自由和约束变元、代入和替换。读者还能学习如何用这种形式的语言翻译自然语言中的语句，主要是来自数学和哲学中的一些命题。通过练习会发现，一些传统上困难而模糊不清的哲学问题在这种翻译下会得到更好的辨析。

然后，会在定义的形式语言中建立一个形式的公理系统。还会介绍一种由根岑[3]建立的自然推演系统，对于有计算机背景或者喜欢直觉主义逻辑的读者，这样的系统会显得更为“自然”。通过这些阅读，读者可学习并掌握形式证明的概念和技巧。

第三部分 一阶语言的结构和真值理论

这一部分讨论塔斯基[4]的形式语言中的真概念。首先定义一阶语言的结构，然后解释“一阶语言的公式在一个结构中为真”这一重要概念。事实上

[1] 皮亚诺（Giuseppe Peano，1858—1932），意大利数学家。

[2] 皮亚诺公理系统的定义见后文。

[3] 根岑（Gerhard Gentzen，1909—1945），德国数学家。

[4] 塔斯基（Alfred Tarski，1901—1983），波兰和美国数学家。

这一概念是模型论建立的基石。借助这一概念可以讨论逻辑后承这一逻辑学的核心概念，以及有效式、矛盾式、可满足、不可满足等一阶逻辑语义学的核心内容。

然后会讨论结构之间的同构以及可定义性等概念，它们是对数学中常见概念的抽象，在更深入的数理逻辑研究中是经常会遇到的基本概念。

第四部分 哥德尔完全性定理

本章会证明一阶逻辑的可靠性定理和哥德尔的完全性定理，从而把语法和语义两方面联系起来。根据可靠性定理，在第二部分建立的形式系统中可证明的语句都是普遍有效的，也就是说，它们在第三部分中定义的所有结构中都真。而根据完全性定理，所有普遍有效的语句也都是在上述形式系统中可证的。

更为一般地说，一阶逻辑的形式系统作为证明手段，既是可靠的，也是完全的，形式证明可以完全正确地刻画“逻辑后承”这个关系，即：$\Gamma \vDash \sigma$ 当且仅当 $\Gamma \vdash \sigma$。这些内容大部分是 1930 年前的成果，它们可以构成一门完整的数理逻辑初阶课程。

完全性定理的一个重要推论是紧致性定理。这是模型论中最重要的定理之一，也是构造模型的基本方法之一。紧致性定理在数学和逻辑中有一些非常深刻的推论。例如，“有穷”这个概念不是一阶语言能刻画的，它不是广义初等类。再如，存在着算术的“非标准模型”，这导致了非标准分析的建立。

第五部分 递归论简介

关于什么样的函数是“可计算的”这样一个看似哲学的问题，直接导致了计算机科学的诞生。本部分将介绍哥德尔与图灵[①]各自独立发展的可计算性概念，即递归函数和图灵可计算函数。这里将证明部分递归函数与图灵机可计算函数是等价的概念，并由此引出丘奇[②]论题：直观上可计算的函数就是图灵可计算函数，也就是部分递归函数。这从某种意义上说明人们的确拥有一个客观的可计算性概念。这一部分的内容也可看作是为学习不完全性定理所作的准备，为此这一部分还介绍了“半可判定”的概念，即递归可枚举集和递归可枚举谓词。

第六部分 简化版本的自然数模型

这一部分将讨论一些“弱”版本的一阶算术结构，即标准自然数 $\mathbb{N}$ 在语言 $\mathcal{L}_S = \{0, S\}$，$\mathcal{L}_< = \{0, S, <\}$，$\mathcal{L}_+ = \{0, S, <, +\}$ 和 $\mathcal{L}_\times = \{0, S, \times\}$ 上的结构。可以证明这些结构对应的完全理论都是可判定的，因而都是可公理化

① 图灵（Alan Turing，1912—1954），英国逻辑学家、数学家。

② 丘奇（Alonzo Church，1903—1995），美国逻辑学家、数学家。

的。在证明过程中需要使用模型论的一些重要技术，这包括乌什-沃特测试、量词消去等，为此又需要勒文海姆-司寇伦定理等。

第七部分 哥德尔不完全性定理

紧接着上一部分，当语言扩张为 $\mathcal{L}_{ar}=\{0,S,+,\cdot\}$ 时，可以发现相应结构 $\mathfrak{N}=(\mathbb{N},0,S,+,\cdot)$ 的完全理论不是可判定的，因而不存在这个语言上的既是可公理化的、又是完全的理论。

这里选取鲁宾逊算术 Q 作为一阶理论的代表，证明它的任意一致的递归扩张 T 都不等于 $\mathrm{Th}\mathfrak{N}$，即总存在一个语句 σ，σ 和 $\neg\sigma$ 都不是 T 的定理。这里会展示如何通过算术的语法化在鲁宾逊算术中表示主要的语法事态。不动点引理是不完全性定理证明的核心，因而会证明不动点引理并运用它构造哥德尔句。接下来会先证明弱版本的第一不完全性定理，再介绍由罗瑟[①]改进的对强版本的第一不完全性定理的证明。

随后会给出第二不完全性定理的完整证明。这个定理是说，如果 T 是皮亚诺算术 PA 的扩张且是一致的，则 T 的一致性不能在 T 中证明。值得指出的是：一般认为，哥德尔第二不完全性定理是第一不完全性定理的推论。而实际上到第二不完全性定理的证明并不平凡。其中，对诸如皮亚诺算术满足 3 个可证性条件的证明颇费周折，本书将给出较详尽的证明过程。

本书针对的是对逻辑和数学基础有兴趣的读者。随着逻辑教育的普及，可供大家选择的逻辑学书籍也越来越多。但由于著者的动机不同，彼此的侧重点也自然有很大的不同。例如，面向计算机科学的数理逻辑可能把逻辑作为离散数学的一部分，更注重与程序有关的机械规则和形式推演；也有的课本把逻辑作为严格推理训练的一部分，因而也把重点放在逻辑演算部分；还有很多书籍把逻辑作为素质教育的一部分，因而从语言到例子都避开数学，等等。相对于以上的逻辑教科书，本书把逻辑与元数学联系在一起，更多地介绍语义部分和强调语法语义的统一。此外，本书另一个重要目的是为了继续学习逻辑学更深入的内容做准备，因此它更适合有志于从事逻辑学专门研究或对逻辑学在数学、哲学和计算机科学中那些深刻应用感兴趣的读者。数理逻辑已经发展成为一个深刻而丰富的科学部门，希望本书能为读者继续探索这个领域奠定一个初步而坚实的基础。

各章的依赖关系如图2所示。根据课程安排，可以略过对自然推演系统和模态逻辑的介绍（第二章的2.4节、2.5节、2.7节、2.9节，第四章的4.5节以及第六章的6.3节）而不影响主线。第二章作为之后内容的热身也并非必要，稍作调整后可以直接从第三章开始。第八章的内容对于哥德尔不完全性定理的证明不是必要的，但有助于理解不完全性定理的前提与意义。

① 罗瑟（J.Barkley Rosser，1907—1989），美国数学家、逻辑学家。

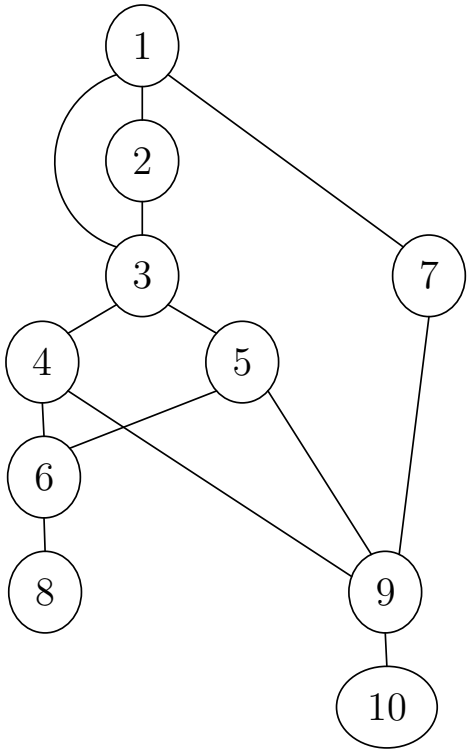

图 2　各章依赖关系

由于数理逻辑已是非常成熟的学科，本书中的大部分内容都是 1940 年以前的成果。本书作者仅仅根据教学经验，将经典内容理顺，以期减少读者学习的阻力而已。在写作过程中，作者从已有的众多的中外教科书中受益匪浅，其中对作者影响最大的是安德顿[①]的 *A Mathematical Introduction to Logic*（Enderton, 2001），该书是作者教学时选用教材的首选。事实上，安德顿一书的高水准是激励我们写好教材的动力之一。在编写过程中，陈翌佳（上海交通大学）、庄志达（新加坡国立大学）、丁德诚（南京大学）、沈恩绍（上海交通大学）、施翔晖（北京师范大学）、俞锦炯（新加坡国立大学）和喻良（南京大学）等老师和同学对初稿提出了宝贵的修改意见，在此表示深深的感谢。

[①] 安德顿（Herbert Enderton，1936—2010），美国数学家。

目录

第二版序 **i**

引言：什么是数理逻辑? **iii**

第一章 预备知识 **1**

1.1 证明的必要性 1
1.2 集合 3
1.3 关系 6
1.4 函数 11
1.5 等价关系与划分 15
1.6 序 19
1.7 结构的例子 21

第二章 命题逻辑 **25**

2.1 引言 25
2.2 命题逻辑的语言 26
2.3 真值指派 30
2.4 唯一可读性 36
2.5 其他联词 38
2.6 命题逻辑的一个推演系统 42
2.7 命题逻辑的自然推演 45
2.8 命题逻辑的可靠性和完全性定理 48
2.9 模态逻辑简介 55

第三章 一阶逻辑的语言 **63**
3.1 一阶逻辑的语言的定义和例子 63
3.2 自由出现和约束出现 70

第四章 形式证明 **73**
4.1 一阶逻辑的一个公理系统 73
4.2 推理和元定理 76
4.3 其他元定理 79
4.4 前束范式 82
4.5 自然推演 84

第五章 结构与真 **89**
5.1 一阶语言的结构 89
5.2 可定义性 96
5.3 同态和同构 99

第六章 哥德尔完全性定理 **105**
6.1 可靠性定理 105
6.2 完全性定理 107
6.3 自然推演系统的可靠性和完全性 115
6.4 紧致性定理及其应用 117

第七章 递归论的基本知识 **121**
7.1 原始递归函数 121
7.2 递归函数 128
7.3 图灵机 132
7.4 图灵可计算函数与部分递归函数 139
7.5 递归可枚举集 146

第八章 简化版本的自然数模型 **151**
8.1 紧致性定理及其应用 151
8.2 可判定的理论 156
8.3 只含后继的自然数模型 161
8.4 包含后继和序的自然数模型 165
8.5 普莱斯伯格算术模型 169

第九章　哥德尔第一不完全性定理 **175**
9.1　可表示性 175
9.2　语法的算术化 188
9.3　不动点引理和递归定理 194
9.4　不完全性、不可定义性和不可判定性 198

第十章　哥德尔第二不完全性定理 **205**
10.1 可证性条件 206
10.2 第二可证性条件 (D2) 的证明 209
10.3 第三可证性条件 (D3) 的证明 221
10.4 哥德尔第二不完全性定理 230
10.5 自然的不可判定语句 234

结束语 **237**

附录 **245**
哥德尔的生平 245
哥德尔的主要数学工作 246

参考文献 **249**

索引 **251**

第一章　预备知识

我们假定读者有一定的数学成熟度，但这个要求既不明确也非必须。通常的说法是：有一定数学背景的读者在学习本书内容时会更为顺利一些。为了便于读者检索，在本章中会罗列一些今后会用到的预备知识，主要是集合论中的一些概念。自然，对此有一定基础的读者可以略过。

稍微需要解释一下的是，我们注意到有很多对逻辑感兴趣的读者不一定对纯数学有那么强烈的兴趣。甚至有些读者会觉得太多的数学反而会与我们的目的南辕北辙，会把辩证的“活”的逻辑，或者“非形式”的逻辑搞得太过机械。这实际上是对“逻辑是什么”的一种不同的理解。我们并不声称数学方法或更广义的理性方法是研究逻辑的唯一途径。但需要强调，这一点读者在后文也会看到，数理逻辑的一个重要的特点就是它能清楚地告诉我们各种（包括数学）方法的局限，从而间接提示我们突破局限的方法和需要添加的工具。

1.1　证明的必要性

数学不同于实验科学，如物理或生命科学。对实验科学来说，重要的是设计并动手做实验，收集数据；根据观察到的事实，提出理论并作出预测，再用实验数据来检验理论的正确性。如果数据（基本）吻合，理论就算取得了成功。极少数的反例对于实验科学的理论不是致命的问题。数学则不同。数学的论证必须是“滴水不漏”或“无可置疑”，不允许有任何例外。注意，在这一点上，数学对论证的要求比任何思辨性科学（包括哲学）都要高。

下面看几个例子，说明仅仅列举大量事实不能代替数学论证。这也是经验归纳的缺陷。

例 1.1.1　称一个正整数 p 为一个**素数**，如果 $p \neq 1$ 并且 p 只能被 1 和 p 整除。观察：31 是一个素数，331 是一个素数，3331 也是一个素数，33331 和 333331 也都是素数，是不是所有形如 $33\cdots3331$ 的整数都是素数？

答案：不是。例如，333333331 不是素数。

例 1.1.2 费马[1]在 1637 年注意到：对任何整数 $n \geq 3$，方程 $x^n + y^n = z^n$ 没有 x, y 和 z 的正整数解。经过几代数学家的努力，直到 1995 年，怀尔斯[2]才证明了这一结论。在怀尔斯之前，人们验证了几乎人类计算极限内的所有整数，涉及的数字达到 4000000 的 4000000 次方，超过了整个宇宙中所有基本粒子的数目，都没有发现例外。但这些都不能成为数学证明。现在考察一些与之近似的命题：方程 $x^3 + y^3 + z^3 = w^3$ 有没有 x, y, z 和 w 的正整数解呢？方程 $x^4 + y^4 + z^4 = w^4$ 又如何呢？

答案：方程 $x^4+y^4+z^4 = w^4$ 有解 $95800^4+217519^4+414560^4 = 422481^4$。方程 $x^3 + y^3 + z^3 = w^3$ 是否有正整数解留给读者解答。

注意：首先我们没有贬低实验科学中观察及猜想的重要性。好的猜想需要深刻的洞察力，经常需要神来之笔。其次，从具体例子着手研究也是数学中普遍实行的方法。我们只不过想强调大量的个例并不构成数学证明。

在数学研究中，反例是非常重要的。错误的猜想经常是被反例推翻的。例如，例 1.1.1 中的 333333331 就是一个反例。这使前面 7 个例子不重要了，也不需要更多的反例。

那数学中怎样证实猜想呢？方法是给出数学证明。大体上说，我们从一些公认的事实出发，它们通常是直观上显然为真的。这些公认的事实被称为“公理”。公理是数学证明的起点。接下来需要一步步地列出一系列的命题，每一步都是根据逻辑规则得出的。这些逻辑规则保证如果一个人承认上一步结论的正确性，他就一定承认下一步结论的正确性。在证明中，已经被证明的事实和公理在任何时候都可以被引用。这一系列命题的终点就是我们要证实的猜想。一旦猜想被证明了，它就被称为定理。

数学证明的目的之一是让读者相信其正确性，因此证明通常都是从简单到复杂依照逻辑规则展开，与之无关的内容一概放弃。从证明中经常看不出数学家的思考过程，这也是数学证明让初学者感到困惑的地方之一。

下面给出两个经典证明的例子。它们是古希腊数学的两颗明珠，既简单又优雅。

例 1.1.3 证明 $\sqrt{2}$ 是无理数。

证明 假定 $\sqrt{2}$ 是有理数，即可以写成两个整数 a 和 b 之比：

[1] 费马（Pierre de Fermat，1601(?)—1665），法国数学家。

[2] 怀尔斯（Andrew Wiles，1953— ），英国数学家。

$$\sqrt{2} = \frac{a}{b}。 \tag{1.1}$$

可以进一步假定 a 和 b 互素，即没有大于 1 的公因子。将等式 (1.1) 两边平方，再乘 b^2，就得到

$$2b^2 = a^2。 \tag{1.2}$$

由于左边是偶数，右边必定也是，所以 a 是偶数。令 $a = 2c$ 并代入 (1.2)，得到

$$b^2 = 2c^2。$$

同样的理由告诉我们 b 也是偶数。这与 a 和 b 互素矛盾。所以不存在这样的 a 和 b，因而 $\sqrt{2}$ 是无理数。 □

例 1.1.4　证明存在无穷多个素数。

证明　假如只有有穷多个素数，如 n 个，把它们全列出来：$p_1, p_2, \cdots, p_n$。考察一个新的整数

$$q = p_1 p_2 \cdots p_n + 1。$$

q 不等于任何一个素数 p_i，$1 \leq i \leq n$，但它也不能被任何素数 p_i 整除。这与任何整数都可以被分解成素数乘积这一事实矛盾，因而素数不可能是有穷的。 □

以上两个证明也是所谓“反证法”的典型例子。反证法是这类要排除无穷多种情况或直接涉及无穷的证明的有力工具。

习题 1.1

1.1.1 是不是对所有的正整数 n，都有 $p_1 p_2 \cdots p_n + 1$ 是素数？这里 p_n 代表第 n 个素数。

1.2　集合

从本节至本章结束，有关集合、关系、函数等的内容改写自“逻辑与形而上学教科书系列”丛书中的《集合论》第二章（郝兆宽, 杨跃, 2014），更多的关于集合论的知识也请参阅此书。

在中学读者大多学过用 $A = \{a_0, a_1, \cdots, a_n\}$ 来表示 A 是一个集合，$a_0, a_1, \cdots, a_n$ 是它的元素。但集合并不总是有有穷多个元素。无穷的集合，例如，全体自然数的集合有时会记作 $\mathbb{N} = \{0, 1, 2, \cdots\}$，但这样的记法既不方便，也不适用于任何集合。例如，全体实数的集合 $\mathbb{R}$ 就不能以这种方式表示。更方便的是用 $A = \{x : P(x)\}$ 表示一个集合，其中 P 是一个特定的性质。例如，$\{x : x$ 是红的$\}$ 表示所有红色事物组成的集合。一般用 $x \in A$ 表示 x 是 A 的元素，读作 x **属于**A，用 $x \notin A$ 表示 x 不是 A 的元素。

外延原理 集合的一个最重要的性质是：每个集合都完全由其元素决定，而与其他因素，如我们描述它的方式，没有关系。例如，

$$\{x \in \mathbb{R} : \text{对所有的实数 } y \text{ 都满足} x + y = y\}$$

和

$$\{x \in \mathbb{R} : \text{对所有的实数 } z \text{ 都满足 } x \times z = x\}$$

是同一个集合，因为它们都只包含实数 0 这一个元素。所以有所谓

外延原理：$A = B$ 当且仅当 A 和 B 有相同的元素。

一方面，如果 $A = B$ 则必然它们的元素相同，这实际上就是莱布尼兹的不可分辨原理。另一方面，如果集合 A 的元素都是集合 B 的元素，反之，集合 B 的元素也都是集合 A 的元素，那就可以断定 $A = B$，这是我们证明两个集合相等的基本方法。

集合的交、并、差 如果 A, B 是集合，则将 A, B 中元素聚集在一起构成新的集合，称为 A 与 B 的**并集**，记作 $A \cup B$。所以

$$A \cup B = \big\{x : x \in A \text{ 或者 } x \in B\big\}。$$

类似地，既属于 A 又属于 B 的元素构成 A 与 B 的**交集**，记作 $A \cap B$。显然，

$$A \cap B = \big\{x : x \in A \text{ 并且 } x \in B\big\}。$$

最后，A 与 B 的**差** $A - B$ 指的是属于 A 但是不属于 B 的元素，即

$$A - B = \big\{x : x \in A \text{ 但是 } x \notin B\big\}。$$

子集、幂集和空集 如果 A 是一个集合，那么 A 中的一部分元素可以构成一个新的集合 B，称为 A 的一个**子集**，记为 $B \subset A$。因此，B 是 A 的子

集当且仅当所有 B 的元素都是 A 的元素。显然，每个集合都是自己的子集。如果 $B \subset A$ 并且 $B \neq A$，就称 B 是 A 的**真子集**。如果需要特别表明，会以 $B \subsetneq A$ 表示 B 是 A 的真子集。

A 的所有子集组成的集合称为 A 的**幂集**，记作 $\mathcal{P}(A) = \{x : x \subset A\}$。

有一个特殊的集合，它不包含任何元素，称为**空集**，一般记作 $\emptyset$。空集是任何集合的子集，怎样论证这一点对初学者是一个很好的练习。

集合族　如果集合的元素本身也是集合，则这样的集合一般称为集合的**族**。例如，

$$\mathcal{F} = \{F_0, F_1, \cdots, F_{n-1}\}$$

表示 n 个集合的族。对于集合族，可以定义其上的**一般并**：

$$\bigcup \mathcal{F} = \big\{x : \text{ 至少存在一个 } F \in \mathcal{F},\ x \in F\big\}。$$

如果 $\mathcal{F} \neq \emptyset$，则还可定义它的**一般交**：

$$\bigcap \mathcal{F} = \big\{x : \text{ 对于每一个 } F \in \mathcal{F},\ x \in F\big\}。$$

注意，如果 $\mathcal{F}$ 是空集，则它的一般并仍然是空集，但是此时它的一般交却没有定义。[①] 特别地，

$$\bigcup \{A, B\} = A \cup B, \quad \bigcap \{A, B\} = A \cap B。$$

为了清楚地表示集合族，一般需要一个下标集。虽然理论上任何集合都可以用作下标集，但最常用的下标集是全体自然数的集合 $\mathbb{N}$ 或者它的子集。因此上面的集合族也可表示为

$$\mathcal{F} = \{F_i : 0 \leq i < n\}。$$

而更一般地，

$$\mathcal{F} = \{F_i : i \in \mathbb{N}\}$$

表示一个无穷的集合族。在这种记法下，集合族 $\mathcal{F} = \{F_0, F_1, \cdots, F_{n-1}\}$ 的一般交和一般并也表示为

$$\bigcup \mathcal{F} = \bigcup_{i=0}^{n-1} F_i, \quad \bigcap \mathcal{F} = \bigcap_{i=0}^{n-1} F_i。$$

[①] 由于 $\mathcal{F}$ 是空集意味着没有 $F \in \mathcal{F}$，因此命题“对于每一个 $F \in \mathcal{F}$，$x \in F$”对任何 x 就总是真的，即所有 x 都属于 $\bigcap \mathcal{F}$，但这是不允许的，因为包含所有对象的“集合”是一个矛盾的概念。

类似地，

$$\bigcup\{F_i : i \in \mathbb{N}\} = \bigcup_{i\in\mathbb{N}} F_i, \quad \bigcap\{F_i : i \in \mathbb{N}\} = \bigcap_{i\in\mathbb{N}} F_i。$$

习题 1.2

1.2.1

(1) 列出集合 $S = \{a, b, \{c, d\}, 47\}$ 的所有子集。

(2) 回答下列问题：$c \in S$? $\{c, d\} \in S$? $\emptyset \in S$? $S \in S$?

(3) 回答更多问题：$\{c, d\} \subset S$? $\{\{c, d\}\} \subset S$? $\{b, 47\} \subset S$? $\{c, d, 47\} \subset S$? $\emptyset \subseteq S$? $S \subseteq S$?

1.2.2 写出下列集合的元素：

(1) $\{1, 2, 3, \{4, 5\}, \{6, \{7, 8\}\}\}$；

(2) $\{x \in \mathbb{N} : x^2 = 3$ 或 $x^2 = 4\}$；

(3) $\{x \in \mathbb{N} : x^2 = 3$ 并且 $x^2 = 4\}$。

1.2.3 找出 3 个性质 $P(x)$ 使得集合 $\{x \in \mathbb{R} : P(x)\}$ 为 $\{1\}$；找出 3 个性质 $Q(x)$ 使得集合 $\{x \in \mathbb{Z} : Q(x)\} = \emptyset$。这里 $\mathbb{Z}$ 指所有整数的集合。

1.2.4 在有可能的情况下找出：

(1) 两个无穷集合 A 和 B 使得 $A \cap B = \{1\}$ 并且 $A \cup B = \mathbb{Z}$；

(2) 两个集合 C 和 D 使得 $C \cup D = \{t, h, i, c, k\}$ 并且 $C \cap D = \{t, h, i, n\}$。

【**注意：**如果你认为不可能的话，请给出理由。】

1.3 关系

在数学研究中，人们关心的不仅仅是集合，在更多的时候，人们关心的是集合上的结构。用日常语言来说，一个集合就像一堆砖头，杂乱无章。我们既可以把这堆砖头建成一堵墙，又可以盖一座楼，等等。这里的墙或者楼

就是所谓的结构。砖头还是砖头，而墙和楼的不同在于砖与砖之间的关系不同。数学结构也是一样，通常是由一个集合配上若干关系或者运算所组成的。例如，把自然数集 $\mathbb{N}$ 和自然数上的大小顺序放在一起，就有一个自然的“序结构”$(\mathbb{N}, <)$，其中，

$$0 < 1 < 2 < 3 < \cdots 。$$

在所有自然数的集合 $\mathbb{N}$ 上，还可以造其他的序，如下面的 $\prec$：

$$\cdots \prec 6 \prec 4 \prec 2 \prec 0 \prec 1 \prec 3 \prec 5 \prec 7 \prec \cdots ,$$

就给出了另外一个序结构 $(\mathbb{N}, \prec)$。构成这两个结构的集合都是 $\mathbb{N}$，但作为结构它们是不同的，如第一个结构有最小元，而第二个则没有。在继续讨论结构之前，先要回顾一下关系和函数的基本概念。

最简单的关系是二元关系，它可看作一种对应或者广义的映射。每当有第一个元素时，我们总系之于第二个元素。所以，关系的要素是成对出现的对象，而且这两个对象是有顺序的，这就需要引入有序对的概念。一般用 (a, b) 表示由 a 和 b 组成的有序对。虽然 $\{a, b\} = \{b, a\}$，但除非 $a = b$，否则 $(a, b) \neq (b, a)$。因此，有序对的“有序性”就是：任何两个有序对 $(a, b), (a', b')$，$(a, b) = (a', b')$ 当且仅当 $a = a'$ 且 $b = b'$。

令 X 和 Y 为集合，则 X 和 Y 的**卡氏积**[1] 定义为

$$X \times Y = \big\{(x, y) \mid x \in X \text{ 并且 } y \in Y\big\} 。$$

如果 $X = Y$，则将 $X \times X$ 简记为 X^2。

如果 $R \subseteq X \times Y$，就称集合 R 为 X, Y 之间的一个**二元关系**。二元关系 R 的所有元素都是有序对，即：对任意 $z \in R$，存在 $x \in X$ 和 $y \in Y$ 满足 $z = (x, y)$。一般地，用 $R(x, y)$ 表示 $(x, y) \in R$，称 x 和 y 有关系 R。有时习惯地写作 xRy。把关系视为有序对的集合，初学者可能不习惯，因为它并没有直接告诉我们这个关系是什么。之所以这样定义，原因和前面提到的集合的外延原理是一样的：我们并不关心怎样描述 R。两个不同的描述，只要它们给出的有序对是相同的，它们就是同一个关系。例如，$R_1 = \{(x, y) \in \mathbb{N}^2 : y+1 = x\}$ 和 $R_2 = \{(x, y) \in \mathbb{N}^2 : x^2 = y^2 + 2y + 1\}$ 是自然数上的同一个关系，尽管对它们的描述不同。

[1] 卡氏积，英文为“Cartesian product”，因笛卡尔而得名。笛卡尔（René Descartes，1596—1650），法国哲学家、数学家。

例 1.3.1

(1) 定义一个整数 m **整除**另一个整数 n, 如果存在整数 k 使得 $n = m \times k$。可以用 $m \mid n$ 表示 m 整除 n。整除是整数间的一个关系：

$$R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : m \mid n\}。$$

例如，有 $(2, 4) \in R$，但是 $(3, 4) \notin R$。

(2) 除了考察自然的关系之外，出于各种需要，经常人为地设计一些关系的例子。例如，令 $A = \{1, 2, 3, 4\}$，$B = \{1, a, b, c\}$，并且 $R = \{(1, 1), (1, a), (2, b), (3, 1)\}$。这里 $R \subseteq A \times B$，所以 R 是集合 A 与 B 之间的一个关系，并且有 $1R1$，$1Ra$，$2Rb$ 和 $3R1$，但 $1 \not R b$，$2 \not R 1$。

以下罗列与关系有关的一些定义。

- R 的**定义域**定义为 $\text{dom}(R) = \big\{x \mid \text{存在 } y \text{ 使得 } R(x, y)\big\}$。
- R 的**值域**定义为 $\text{ran}(R) = \big\{y \mid \text{存在 } x \text{ 使得 } R(x, y)\big\}$。
- 如果 $R \subset X^2$，则称 R 是 X **中的二元关系**。
- 集合 X 在关系 R 下的**像**定义为

$$R[X] = \big\{y \in \text{ran}(R) \mid \text{存在 } x \in X \text{使得 } R(x, y)\big\}。$$

- 集合 Y 在关系 R 下的**逆像**定义为

$$R^{-1}[Y] = \big\{x \in \text{dom}(R) \mid \text{存在 } y \in Y \text{ 使得 } R(x, y)\big\}。$$

- 二元关系 R 的**逆**定义为

$$R^{-1} = \{(x, y) \mid (y, x) \in R\}。$$

- 二元关系 R 和 S 的**复合**定义为

$$S \circ R = \big\{(x, z) \mid \text{存在 } y \text{ 使得 } ((x, y) \in R \text{ 并且 } (y, z) \in S)\big\}。$$

例 1.3.2

(1) 令 $R = \{(x, y) \mid x = y\}$ 为 $\mathbb{R}$ 中的二元关系，其中 $\mathbb{R}$ 表示实数集，则 $R^{-1} = R$ 且 $R \circ R = R$。

(2) 如果 $R=\{(x,y)\in\mathbb{R}^2 \mid y=\sqrt{x}\}$，则

$$R^{-1}=\big\{(x,y)\mid y=x^2\wedge x\geq 0\big\}。$$

(3)“小于等于”关系和“大于等于”关系的复合 $\leq\circ\geq$ 等于 $\mathbb{R}\times\mathbb{R}$ 而 $\leq\circ\leq=\leq$。

(4) 在前面所举的例子中，$A=\{1,2,3,4\}$，$B=\{1,a,b,c\}$，并且 $R=\{(1,1),(1,a),(2,b),(3,1)\}$。$\mathrm{dom}(R)=\{1,2,3\}\subseteq A$；$\mathrm{ran}(R)=\{1,a,b\}\subseteq B$；$R$ 的逆 $R^{-1}\subseteq B\times A$，$R^{-1}=\{(1,1),(a,1),(b,2),(1,3)\}$。

(5) 令 $R\subseteq A\times B$ 和 $S\subseteq B\times C$ 为关系，其中 $A=\{1,2,3,4\}$，$B=\{a,b,c,d,e\}$，$C=\{x,y,z,w\}$，并且

$$\begin{aligned} R &= \{(1,a),(1,c),(2,b),(4,a)\},\\ S &= \{(a,y),(b,x),(a,w),(c,w),(d,z),(e,z)\},\end{aligned}$$

则 $S\circ R=\{(1,y),(1,w),(2,x),(4,y),(4,w)\}$。

(6) 假定 $a,b\in\mathbb{Z}$ 并且 n 为正整数。如果 $n\mid(a-b)$，就称a **同余于** b **模** n，记为 $a\equiv b\ (\mathrm{mod}\ n)$。顾名思义，$a\equiv b\ (\mathrm{mod}\ n)$ 当且仅当用 n 分别去除 a 和 b 所得的余数相同。此外，$a\equiv 0\ (\mathrm{mod}\ n)$ 当且仅当 $n\mid a$。同余是整数间的一个常见的关系。例如，$87\equiv 12\ (\mathrm{mod}\ 15)$，$83\not\equiv 5\ (\mathrm{mod}\ 11)$，等等。

卡氏积和二元关系可以推广。首先，定义三元有序组

$$(x_1,x_2,x_3)=_{\mathrm{df}}((x_1,x_2),x_3),$$

而四元序组

$$(x_1,x_2,x_3,x_4)=_{\mathrm{df}}((x_1,x_2,x_3),x_4)。$$

一般地，对正整数 $n>2$，假设 $(x_1,\cdots,x_{n-1})$ 已有定义，则 n 元序组定义为

$$(x_1,\cdots,x_n)=_{\mathrm{df}}((x_1,\cdots,x_{n-1}),x_n)。$$

这是经常使用的“递归定义”或“归纳定义”方式。

n 个集合的卡氏积定义为

$$X_1\times\cdots\times X_n=\{(x_1,\cdots,x_n)\mid x_1\in X_1\wedge\cdots\wedge x_n\in X_n\}。$$

同样，

$$X^n = \underbrace{X \times \cdots \times X}_{n次}。$$

对任意集合 R，如果 $R \subset X_1 \times \cdots \times X_n$，则称 R 为一个 n **元关系**。如果 $R \subset X^n$，则称 R 是 X 上的 n 元关系，并且通常将 $(x_1, \cdots, x_n) \in R$ 写作 $R(x_1, \cdots, x_n)$。

如果 R 是 X 上的 n 元关系，而 Y 是 X 的子集，则 $R' = R \cap Y^n$ 是 Y 上的 n 元关系。一般称 R' 是 R 限制，R 是 R' 扩张。

卡氏积的定义还可以进一步地推广到无穷多个集合上面，但这些留到以后再讲。

习题 1.3

1.3.1 验证下列关于整除关系的命题，其中所有字母都代表整数：

(1) 如果 $a \mid b$，则对任何 c 都有 $a \mid bc$；

(2) 如果 $a \mid b$ 并且 $b \mid c$，则 $a \mid c$；

(3) 如果 $a \mid b$ 并且 $a \mid c$，则对任何 s 和 t 都有 $a \mid (sb + tc)$；

(4) 如果 $a \mid b$ 并且 $b \mid a$，则 $a = \pm b$；

(5) 如果 $a \mid b$ 并且 $a, b > 0$，则 $a \leq b$；

(6) 如果 $m \neq 0$ 则 ($a \mid b$ 当且仅当 $ma \mid mb$)。

1.3.2 假定 $a, b, c, n \in \mathbb{Z}$ 且 $n > 0$。证明同余关系的下列性质：

(1)（自反性）$a \equiv a \pmod{n}$；

(2)（对称性）如果 $a \equiv b \pmod{n}$，则 $b \equiv a \pmod{n}$；

(3)（传递性）如果 $a \equiv b \pmod{n}$ 且 $b \equiv c \pmod{n}$，则 $a \equiv c \pmod{n}$。

1.3.3 判断下列命题是否对所有集合 A, B, C 和 D 成立，并给出理由：

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$；

(2) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$；

(3) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$。

1.4　函数

函数是一类特殊的关系。对一般的二元关系 R，R 定义域中 x 可以对应其值域中的多个元素。例如，在实数 $\mathbb{R}$ 上的关系 $\leq$ 中，0 就对应于所有大于等于 0 的实数。这种“一对多”的情形在很多情况下必须排除。设想一下，如果电脑的键盘与屏幕输出之间是一对多的话，也就是说，当你第一次敲下“a”键时，屏幕输出“a”，而下次却可能是“b”。这样的电脑一定会令人抓狂。

一个二元关系 f 如果满足：

$$\text{如果 } (x,y)\in f \text{ 并且 } (x,z)\in f \text{ ，那么 } y=z,$$

就称 f 是一个**函数**。如果 $(x,y)\in f$，通常写作 $f(x)=y$，或者 $f:x\mapsto y$，$f_x=y$ 等，并把 y 称为 f 在 x 处的值。如果 $\mathrm{dom}(f)=X$，$\mathrm{ran}(f)\subset Y$，就称f **是** X **到** Y **的函数**，记为 $f:X\to Y$。

例 1.4.1

(1) 在例1.3.2中，$\{(x,y)\mid x=y\}$ 和 $\{(x,y)\mid y=\sqrt{x}\}$ 是函数；而 $\mathbb{R}$ 上的 $\leq$ 关系不是函数；

(2) 以下都是自然数集合 $\mathbb{N}$ 上的函数：

$$\begin{aligned}
S_1(n)&=1+2+\cdots+n=\frac{n(n+1)}{2},\\
S_2(n)&=1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6},\\
S_3(n)&=1^3+2^3+\cdots+n^3=\frac{n^2(n+1)^2}{2};
\end{aligned}$$

(3) 对任意集合 X 定义 $\mathrm{id}_X:X\to X$ 为 $\mathrm{id}_X(x)=x$，则 id_X 是 X 上的函数，称为**等同函数**。

定理 1.4.2　*函数 f,g 相等当且仅当 $\mathrm{dom}(f)=\mathrm{dom}(g)$，并且对任意 $x\in\mathrm{dom}(f)$，$f(x)=g(x)$。*

证明　留给读者练习。　□

根据定义，每个函数都是一个关系，所以前面定义的关系的定义域、值域、像、逆等概念在这里仍然适用。并且与关系类似，函数可以推广到 n 元

的情形。一般来说，如果函数的定义域是一个 n 元有序组的集合，则称为 n 元函数。注意到 n 元函数是一个 $n+1$ 元关系。例如，$f : A^n \to A$ 是 A 上的 n 元函数，这样的函数经常称为 A 上的 n 元**运算**。自然数上的加法是一个二元运算的例子。由于可以将 n 元序组看作一个对象，因此以下对函数的讨论可以限制在一元函数的情形。

定理 1.4.3 *如果 f 和 g 是函数，则它们的复合 $g \circ f$ 也是函数。它的定义域为 $\mathrm{dom}(g \circ f) = f^{-1}[\mathrm{dom}(g)]$。并且对所有 $x \in \mathrm{dom}(g \circ f)$，$(g \circ f)(x) = g(f(x))$。*

证明 设 $(x, z_1), (x, z_2) \in (g \circ f)$，根据定义，存在 y_1, y_2，$(x, y_1) \in f$，$(y_1, z_1) \in g$，且 $(x, y_2) \in f$，$(y_2, z_2) \in g$。由 f 是函数，可得 $y_1 = y_2$，再由 g 是函数，有 $z_1 = z_2$。所以 $g \circ f$ 是函数。

至于第二个命题，根据定义域的定义，有 $x \in \mathrm{dom}(g \circ f)$ 当且仅当存在 z 使得 $(x, z) \in g \circ f$；再根据复合的定义，有 $x \in \mathrm{dom}(g \circ f)$ 当且仅当存在 z 和 y 使得 $(x, y) \in f$ 且 $(y, z) \in g$。因此，一方面，如果 $x \in \mathrm{dom}(g \circ f)$，则 $x \in \mathrm{dom}(f)$ 且 $f(x) \in \mathrm{dom}(g)$，也就有 $x \in \mathrm{dom}(f)$ 且 $x \in f^{-1}[\mathrm{dom}(g)]$。另一方面，如果 $x \in \mathrm{dom}(f)$ 且 $x \in f^{-1}[\mathrm{dom}(g)]$，那么有 $\exists y (x, y) \in f$ 且 $y \in \mathrm{dom}(g)$，也就有 z 和 y 使得 $(x, y) \in f$ 且 $(y, z) \in g$，所以 $x \in \mathrm{dom}(g \circ f)$。

最后，设 $x \in \mathrm{dom}(g \circ f)$，且 $(g \circ f)(x) = z$。根据复合的定义，存在 y，$f(x) = y$ 且 $g(y) = z$，因此 $g(f(x)) = g(y) = z = (g \circ f)(x)$。 □

函数 $f : X \to Y$ 称为**一一的**或**单射**，如果对所有的 $x_1, x_2 \in X$，都有 $x_1 \neq x_2$ 蕴涵 $f(x_1) \neq f(x_2)$；函数 $f : X \to Y$ 称为**满射**，如果 $\mathrm{ran}(f) = Y$；既是单射又是满射的函数称为**双射**，也称 f 为 X 和 Y 之间的一个**一一对应**。

如果 $f : X \to Y$ 是函数，A 是 X 的子集，则f **到** A **上的限制**，记作 $f \restriction A$，是由 A 到 Y 的函数，并且对于每个 $x \in A$，都有 $f \restriction A(x) = f(x)$。如果 g 是 f 的一个限制，则称 f 是 g 的一个**扩展**。

函数是数学中非常基本的概念，是数学语言不可或缺的一部分。人们经常会利用函数来描述一些其他的概念。逻辑中也是一样。下面举几个例子。

(1) 在中学一般都学过等差数列和等比数列。它们都是序列的例子。所谓序列 $a_0, a_1, a_2, \cdots$，直观上说，就是一个无穷的数串，并且人们能够分辨哪一个是它的第一项，哪个是其第二项，等等。序列的严格定义通常是用函数来完成的。例如，一个实数序列就是一个从 $\mathbb{N}$ 到 $\mathbb{R}$ 的函数 f，它的第 n 项就是 $f(n)$。

(2) 集合论中基数的比较也是利用函数来描述的。称两个集合 A 和 B 具有相同的基数，如果存在一个双射 $f : A \to B$。直观上说，A 和 B 具有相同的基数就是说 A 和 B 具有同样多的元素。至于为什么这样定义，在集合论的课程中往往会仔细讲解。在习题中，读者会看到一些例子，说明有些集合会和它的某个真子集具有相同的基数。

(3) 在后文中，经常会给一些逻辑符号指派意义，这也是利用函数来描述的。例如，S 是一个抽象符号的集合，而 A 是一个已知概念的集合，一个函数 $f : S \to A$ 可以被视为给 S 中的符号指派它们的意义，或者说 f 是一个解释。

习题 1.4

1.4.1 对下列集合 A 和 B，找出所有从 A 到 B 的函数：

(1) $A = \{x\}$ 且 $B = \{0, 1\}$；

(2) $A = \{x, y\}$ 且 $B = \{2\}$；

(3) $A = \{x, y\}$ 且 $B = \{0, 1\}$；

(4) $A = \{x, y\}$ 且 $B = \{0, 1, 2\}$。

如果集合 A 和 B 分别含有 n 和 m 个元素，有多少个从 A 到 B 的函数?

1.4.2 令 f 和 g 为从 $\{1, 2, 3\}$ 到 $\{2, 3, 4\}$ 的函数，分别定义为 $f(x) = -x + 5$ 和 $g(x) = -x^3 + 6x^2 - 12x + 11$。证明：$f = g$。

1.4.3 令 $f : \mathbb{R} \to \mathbb{R}$ 和 $g : \mathbb{Z} \to \mathbb{Z}$ 为

$$\begin{aligned} f(x) &= 4x - 1, \\ g(n) &= 4n - 1。 \end{aligned}$$

证明：f 为双射，g 为单射但不是满射。

1.4.4 考察函数 $f : X \to Y$，判断下列命题的对错：

(1) f 是满射当且仅当任何一个 Y 中的元素都是某个 X 中元素的像；

(2) f 是满射当且仅当任何一个 X 中的元素都有某个 Y 中元素为它的像；

(3) f 满射当且仅当对任何 $y \in Y$ 都存在 $x \in X$，使得 $f(x) = y$；

(4) f 满射当且仅当对任何 $x \in X$ 都存在 $y \in Y$，使得 $f(x) = y$；

(5) f 满射当且仅当存在 $y \in Y$，使得对任意 $x \in X$ 都有 $f(x) = y$；

(6) f 满射当且仅当 f 的值域等于 Y。

1.4.5 令 f 和 g 为从 $\mathbb{R}$ 到 $\mathbb{R}$ 的函数。判断下列命题的对错并给出理由：

(1) $\{x \in \mathbb{R} \mid f(x) = 0\} \cap \{x \in \mathbb{R} \mid g(x) = 0\}$
$$= \{x \in \mathbb{R} \mid f^2(x) + g^2(x) = 0\};$$

(2) $\{x \in \mathbb{R} \mid f(x) = 0\} = \{x \in \mathbb{R} \mid f^2(x) = 0\}$；

(3) 如果 f 和 g 都是双射，则 $f + g$ 也是双射。（这里函数 $f + g : \mathbb{R} \to \mathbb{R}$ 的定义是 $(f + g)(x) = f(x) + g(x)$。）

1.4.6

(1) 证明对任何函数 $f, g : \mathbb{R} \to \mathbb{R}$，如果 $f \circ g$ 是单射，则 g 是单射；

(2) 找出函数 $f, g : \mathbb{R} \to \mathbb{R}$，使得 $f \circ g$ 是单射，但 f 不是单射。

1.4.7 给定一个函数 $f : X \to Y$，定义两个新的幂集间的函数如下：

$$F : P(X) \to P(Y) \quad 和 \quad G : P(Y) \to P(X),$$

$$F(A) = \{f(a) : a \in A\} \quad 和 \quad G(B) = \{a \in X : f(a) \in B\},$$

其中 $A \subseteq X$ 并且 $B \subseteq Y$。判断下列命题是否正确并给出证明或反例。

(1) 如果 f 是单射，则 F 也是单射；

(2) 如果 f 是满射，则 G 是满射。

1.4.8 令 $a, d \in \mathbb{Z}$，$q \in \mathbb{R}$，并且 $n \in \mathbb{N}$。

(1) 找出等差数列 $a, a + d, a + 2d, \cdots, a + nd$ 的求和公式 $B(n)$，并用归纳法验证；

(2) 找出等比数列 $a, aq, aq^2, \cdots, aq^n$ 的求和公式 $C(n)$，并用归纳法验证。

下面的练习都是集合论中基数练习的翻版。建议大家把它们“翻译”成基数的语言，读出它们所暗示的有关集合大小的信息。

1.4.9 找出 $\mathbb{N}$ 和 $\mathbb{Z}$ 之间的一个一一对应。

1.4.10 假定 a, b, c, d 为实数，并且 $a < b$ 和 $c < d$。令 $f : (a, b) \to (c, d)$ 定义为

$$f(x) = \frac{d-c}{b-a}(x-a) + c。$$

这里 (a, b) 表示集合 $\{x \in \mathbb{R} : a < x < b\}$，常被称为一个**开区间**。证明：$f$ 是一个双射。

1.4.11 找出开区间 $(0, 1)$ 和 $\mathbb{R}$ 之间的一个一一对应。

1.4.12 考察函数 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$，定义为

$$f(m, n) = n + \frac{(m+n)(m+n+1)}{2}。$$

(1) 令 m_1, n_1, m_2, n_2 为自然数。证明如果 $m_1 + n_1 < m_2 + n_2$，则 $f(m_1, n_1) < f(m_2, n_2)$；

(2) 证明对任意 $y \in \mathbb{N}$，都存在唯一的 $x \in \mathbb{N}$，使得

$$\frac{x(x+1)}{2} \leq y < \frac{(x+1)(x+2)}{2}；$$

(3) 证明 f 是双射。

1.5　等价关系与划分

如果有一类物体，尽管其中每个个体各不相同，但就人们关心的性质来说，它们的表现是一样的，那么人们会很自然地把它们等同起来，不加以区分。例如，自然数 7 和 4 不相等，但如果只关心模 3 的算术的话，7 和 4 的性质完全相同，因为 $7 \equiv 4 \pmod 3$。因此完全可以把 7 和 4 当成一个数来处理。

上面的想法自然引导我们考察等价关系和等价类。

定义 1.5.1　令 $R \subset X^2$ 为二元关系，称

(1) R 是**自反的**，如果对所有的 $x \in X$，$R(x, x)$；

(2) R 是**对称的**，如果对所有的 $x, y \in X$，若 $R(x, y)$，则 $R(y, x)$；

(3) R 是**传递的**，如果对所有的 $x, y, z \in X$，若 $R(x, y)$ 且 $R(y, z)$，则 $R(x, z)$；

(4) R 是一个**等价关系**，如果 R 是自反、对称、传递的。

习惯上用 $\sim$ 表示等价关系。如果 $\sim$ 为 X 上的一个等价关系，并且 $x \sim y$，则称 x 与 y 等价。

例 1.5.2

(1) 如果 P 代表所有人的集合，考察如下定义 P 上的二元关系：

$$D = \{(x, y) \mid x \text{ 是 } y \text{ 的后代}\}; \tag{1.3}$$

$$B = \{(x, y) \mid \text{至少有一个 } x \text{ 的祖先也是 } y \text{ 的祖先}\}; \tag{1.4}$$

$$S = \{(x, y) \mid x \text{ 的父母是 } y \text{ 的父母}\}。 \tag{1.5}$$

D 不是自反的，也不是对称的，但是传递的；B 是自反的，对称的，却不是传递的；最后，S 是等价关系。

(2) 任意集合 X 上的 $=$ 是等价关系；平面上任意直线的平行关系是等价关系。

(3) 令 A 代表所有地球人的集合。考虑 A 上的关系 E，使得 xEy 当且仅当 x 和 y 有相同国籍。若忽略双重国籍等情形，则 E 是 A 上的一个等价关系。

(4) 令 $A = \mathbb{Z}$，定义 $x \equiv_3 y$ 当且仅当 $x \equiv y \pmod 3$。前面习题中证明了 $\equiv_3$ 是一个等价关系。

定义 1.5.3 令 $\sim$ 是 X 上的等价关系，$x \in X$。x 关于 $\sim$ 的**等价类** 是集合：

$$[x]_\sim = \{t \in X \mid t \sim x\}。$$

当等价关系 $\sim$ 清楚的时候，常把 $[x]_\sim$ 简记为 $[x]$。

例如，在例 1.5.2 中相同国籍的关系下，包含朱婷的等价类就是全体中国人的集合。而在 $\equiv_3$ 的关系下，$[0] = \{3k : k \in \mathbb{Z}\}$，并且 $[7] = [4]$。

引理 1.5.4 令 $\sim$ 为 X 上的等价关系，则对任意 $x, y \in X$，$[x]_\sim = [y]_\sim$ 或者 $[x]_\sim \cap [y]_\sim = \emptyset$。

证明　如果 $[x]_\sim \cap [y]_\sim \neq \emptyset$，则令 e 属于它们的交。因此 $e \sim x$ 且 $e \sim y$，由对称性和传递性，$x \sim y$。对任意 $w \in X$，$w \in [x]_\sim$ 当且仅当 $w \sim x$，当且仅当 $w \sim y$，当且仅当 $w \in [y]_\sim$，所以 $[x]_\sim = [y]_\sim$。 □

等价关系的概念常常与划分联系在一起。先看一个具体的例子：考察等价关系 $\equiv_3$，简单计算告诉我们 $[0] = \{3k \mid k \in \mathbb{Z}\}$，$[1] = \{3k+1 \mid k \in \mathbb{Z}\}$，而 $[2] = \{3k+2 \mid k \in \mathbb{Z}\}$。这 3 个等价类的并集是所有整数集 $\mathbb{Z}$，并且由观察或用引理 1.5.4 可以得出它们彼此不相交。

定义 1.5.5　令 X 为一集合，$S \subset \mathcal{P}(X) - \{\emptyset\}$。如果 S 满足：

(1) 对所有的 $a, b \in S$，如果 $a \neq b$，则 $a \cap b = \emptyset$；

(2) $\bigcup S = X$，

则称 S 是 X 的一个**划分**。

定义 1.5.6　令 $\sim$ 为 X 上的等价关系，则 $X/\sim = \{[x]_\sim \mid x \in X\}$ 称为 X 的**商集**。

仍以前面提到的相同国籍关系 E 为例，商集 A/E 中的元素为某一固定国家的全体国民。而在 $\equiv_3$ 的关系下，商集 $\mathbb{Z}/\equiv_3 = \{[0], [1], [2]\}$。

商集的概念在数学中是很常见的。例如，代数中有商群，拓扑中有商空间，等等，这些概念都是建立在商集的基础上的。$\equiv_3$ 的例子提示我们，任何一个等价关系都诱导出一个划分。

定理 1.5.7　令 $\sim$ 为 X 上的等价关系，则 $X/\sim$ 是 X 的一个划分。

证明　首先，由引理 1.5.4，如果 $[x]_\sim \neq [y]_\sim$，则 $[x]_\sim \cap [y]_\sim = \emptyset$。其次，因为对任意 $x \in X$ 都有 $x \in [x]_\sim$，所以 $\bigcup(X/\sim) = X$。由此，$X/\sim$ 是 X 上的划分。 □

反过来，也可以由一个集合的划分来定义其上的等价关系。

定理 1.5.8　令 S 为 X 的划分，定义 X 上的二元关系

$$\sim_S = \{(x, y) \in X \times X \mid \exists c \in S(x \in c \wedge y \in c)\},$$

则 $\sim_S$ 是等价关系。

定理 1.5.9

(1) 如果 S 为 X 的划分，则 $X/\sim_S = S$；

(2) 如果 $\sim$ 是 X 上的等价关系且 $S = X/\sim$，则 $\sim_S = \sim$。

以上两个定理的证明留作习题1.5.9。

习题 1.5

1.5.1 判断下列关系 R 是否为 (i) 自反的；(ii) 对称的；(iii) 传递的：

(1) R 为集合 $\{a, b, c\}$ 上的关系，$R = \{(a, b), (b, a), (a, a)\}$；

(2) R 为 $\mathbb{Z}$ 上的关系，定义为 aRb 当且仅当 $a > b$；

(3) 令 X 为一非空集，A 是 X 的非空子集的集合，R 是 A 上的关系，定义为 URV 当且仅当 $U \cap V \neq \emptyset$；

(4) R 是 $\mathbb{R}$ 上的关系，使得 aRb 当且仅当 $ab \geq 0$；

(5) R 是 $\mathbb{R}$ 上的关系，使得 aRb 当且仅当 $| a - b | \leq 2$。

1.5.2 令 $T = \{0, 1, 2, 3, \cdots, 12\}$。定义 T 上的一个关系 $\sim$ 如下：对任意 a，$b \in T$，$a \sim b$ 只要下列条件之一成立：

(1) a，b 都是偶数；

(2) a，b 都是大于 2 的素数；

(3) a，$b \in \{1, 9\}$ 并且 $a = b$。

证明 $\sim$ 是一个 T 上的等价关系，并找出所有的等价类。

1.5.3 令 $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ 为非零整数集，并且 $A = \mathbb{Z} \times \mathbb{Z}^*$。在 A 上定义如下关系 R：

$$R = \{((a, b), (c, d)) \in A \times A \mid ad = bc\}。$$

证明 R 是一个等价关系，并找出等价类 $[(0, 1)]$ 和 $[(2, 4)]$。

1.5.4 令 R 为 $\mathbb{N} \times \mathbb{N}$ 上的如下关系：

$$(a, b)R(c, d) \text{ 当且仅当 } (\exists k \in \mathbb{Z})[a + b = c + d + 3k]。$$

证明 R 是一个等价关系，并找出 R 的所有等价类。

1.5.5 令 A 为一个非空集并且 R 是 A 上的一个二元关系。证明 R 是一个等价关系当且仅当下述两个条件成立：

(1) 对所有 $x \in A$，xRx 成立；

(2) 对所有 $x, y, z \in A$，如果 xRy 并且 yRz，则 zRx。

1.5.6 令 k 为一个固定的正整数。定义 $\mathbb{Z}$ 上的关系 E 使得 xEy 当且仅当 $x \equiv y(\text{mod } k)$。已经知道 E 是 $\mathbb{Z}$ 上的一个等价关系。对任意整数 $i, j \in \mathbb{Z}$，找出一个从等价类 $[i]_E$ 到等价类 $[j]_E$ 的一个双射，并验证它的确是一个双射。

1.5.7 对任意集合 X，如果 $\mathcal{I} \subset \mathcal{P}(X)$ 非空，并且满足：

$$A \subset B \in \mathcal{I} \to A \in \mathcal{I} \quad \text{且} \quad A, B \in \mathcal{I} \to A \cup B \in \mathcal{I},$$

就称 $\mathcal{I}$ 是 X 上的一个**理想**。证明：如果 $\mathcal{I}$ 是理想，则 $P(X)$ 上的二元关系

$$R = \{(A, B) \mid (A \triangle B) \in \mathcal{I}\}$$

是等价关系。其中 $(A \triangle B) = (A - B) \cup (B - A)$。

1.5.8 考察整数间的关系 E，定义为 xEy 当且仅当 $\mid x \mid = \mid y \mid$。验证 E 是一个等价关系，并找出商集 $\mathbb{Z}/E$。

1.5.9 证明定理 1.5.8 和定理 1.5.9 。

1.6　序

顾名思义，集合 X 上的一个线序就是元素之间的一个前后关系 R。根据这个关系，集合 X 的形状像一条线，即任何两个元素在这个关系下都有先后之分。把它用数学语言写出来就是：对于任意元素 $x, y \in X$，或者 xRy 或者 yRx。但仅仅这一条还不够，因为它并没有排除循环，例如，$X = \{a, b, c, d\}$ 并且 aRb, bRc, cRd, dRa，则看上去是一个圈，而不是一条线。怎样排除循环呢？仔细想想，可以添加反对称性（见下文）来排除长度是 2 的圈；再用传递性把大圈缩成小圈来排除掉。因此有下面的定义。

定义 1.6.1　令 R 为 X 上的二元关系，如果 R 满足：

(1) R 是反对称的，对所有的 $x, y \in X$，如果 xRy 且 yRx，则 $x = y$；

(2) R 是传递的，对所有的 $x, y, z \in X$，如果 xRy，yRz，则 xRz；

(3) 对所有的 $x, y \in X$，xRy 或 yRx，

就称 R 是 X 上的一个**线序**或**全序**。

注意：（3）告诉我们对所有的 $x \in X$，都有 xRx，即这里线序的定义蕴涵着自反性。

例 1.6.2

(1) 集合 $\mathbb{N}$，$\mathbb{Z}$，$\mathbb{Q}$ 和 $\mathbb{R}$ 上自然的大于等于关系 $\geq$ 和小于等于关系 $\leq$ 都是线序。

(2) 再看一个人为的例子。令 $X = \{1, 2, 3\}$ 和

$$R = \{(1,1), (2,2), (3,3), (1,3), (3,2), (1,2)\},$$

则 R 是 X 上的一个线序。

如果放弃任意两个元素都是可比的这一要求，线序可以推广为所谓“偏序”的概念。但要注意的是，此时需要将自反性单独列出。人们常用 $\leq$ 来代表偏序，所以它不再仅仅表示数上的小于等于关系。

定义 1.6.3 令 $\leq$ 为 X 上的二元关系，如果 $\leq$ 满足：

(1) $\leq$ 是自反的，即对所有的 $x \in X$，$x \leq x$；

(2) $\leq$ 是反对称的，即对所有的 $x, y \in X$，如果 $x \leq y$ 且 $y \leq x$，则 $x = y$；

(3) $\leq$ 是传递的，即对所有的 $x, y, z \in X$，如果 $x \leq y$，$y \leq z$，则 $x \leq z$，

就称 $\leq$ 是 X 上的一个**偏序**或**序**。

本书中会用 $(X, \leq)$ 表示 $\leq$ 是 X 上的偏序，此时称 $(X, \leq)$ 为**偏序集**；如果 $(X, \leq)$ 是偏序集，则用 $x \geq y$ 表示 $x \leq^{-1} y$；用 $x < y$ 表示 $x \leq y$ 且 $x \neq y$；用 $x > y$ 表示 $x \geq y$ 并且 $x \neq y$。有时也称 $<$ 为**严格偏序**。

例 1.6.4

(1) 集合 $\mathbb{N}$、$\mathbb{Z}$、$\mathbb{Q}$ 和 $\mathbb{R}$ 上的自然大小关系都是偏序关系（同时也是线序关系）；

(2) 对任意集合 X，$\subset$ 是 $\mathcal{P}(X)$ 上的序关系，但一般上不是线序；

(3) 定义 $n \mid m$ 为 “n 整除 m”，则 $\mid$ 是集合 $\{2,3,4,\cdots\}$ 上的偏序关系，也不是线序。

习题 1.6

1.6.1 给定一个偏序集 $(X,\leq)$，称其中一个元素 x_0 是一个**极大元**，如果 X 中没有严格大于 x_0 的元素。证明每一个非空有穷的偏序集中都至少有一个极大元。其中，$(X,\leq)$ 是有穷偏序集，是指 X 为一个有穷集。

1.6.2 给定一个偏序集 $(X,\leq)$，称其中一个元素 x^* 是一个**最大元**，如果对任意 $y\in X$，都有 $y\leq x^*$。证明一个偏序集中的最大元是唯一的（如果有的话）。

1.6.3 找出一个偏序集 $(X,\leq)$ 的例子，它没有最大元但有两个以上的极大元。

1.6.4 给定一个有穷的偏序集 (X,S)，证明存在一个 X 上的二元关系 R，满足 $S\subset R$ 并且 R 是一个线序。换句话说，每一个有穷偏序都可以延拓成一个线序。[①]

1.7　结构的例子

上面的线序集或偏序集都是结构的例子，也是所谓用公理来“定义”结构的例子。接下来再看几个数学里常见的结构。

如果只关心所谓“算术运算”，即加减乘除，则可以研究“域”这种结构。

定义 1.7.1　一个**域** 是一个结构 $(F,0,1,+,\cdot)$，其元素间有两个运算，分别记作加法 $+$ 和乘法 $\cdot$。有两个特殊的元素 0 和 1，分别是加法和乘法的“单位元”。它们满足：

(1) 对任意 $a,b,c\in F$，$a+(b+c)=(a+b)+c$；

(2) 对任意 $a,b\in F$，$a+b=b+a$；

(3) 对任意 $a\in F$，$a+0=a$；

(4) 对任意 $a\in F$ 存在 $b\in F$，使得 $a+b=0$；

(5) 对任意 $a,b,c\in F$，$a\cdot(b\cdot c)=(a\cdot b)\cdot c$；

[①] 事实上，在集合论中可以证明该命题对任一偏序都成立。

(6) 对任意 $a,b\in F$，$a\cdot b=b\cdot a$；

(7) 对任意 $a\in F$，$a\cdot 1=a$；

(8) 对任意 $a\in F$，$a\neq 0$, 存在 $b\in F$，使得 $a\cdot b=1$；

(9) 对任意 $a,b,c\in F, a\cdot(b+c)=a\cdot b+a\cdot c$ 并且 $(a+b)\cdot c=a\cdot c+b\cdot c$。

注意：虽然在定义中只提到了加法和乘法两个运算，但 (4) 和 (8) 实际上分别定义了它们的逆运算，即减法和除法。有理数 $\mathbb{Q}$、实数 $\mathbb{R}$、复数 $\mathbb{C}$，连带它们通常的运算是域的典型例子。

例 1.7.2 令 p 为一个素数，考虑商集 $\mathbb{Z}/\equiv_p$，记为 F_p，则

$$F_p=\{[0],[1],\cdots,[p-1]\}。\tag{1.6}$$

定义 F_p 上的加法 $+_{F_p}$ 和乘法 $\cdot_{F_p}$ 为

$$[m]+_{F_p}[n]=[(m+n)\text{ 除以 }p\text{ 的余数}],$$

$$[m]\cdot_{F_p}[n]=[(m\cdot n)\text{ 除以 }p\text{ 的余数}],$$

其中 $+$ 和 $\cdot$ 是整数上通常的加法和乘法。读者可以验证 F_p 对这样定义的 $+_{F_p}$ 和 $\cdot_{F_p}$ 构成一个域。这是**有限域**的一个典型例子。

域 F_p 满足这样的性质：

$$\underbrace{1+_{F_p}1+_{F_p}\cdots+_{F_p}1}_{p\text{-次}}=0。$$

一般地，满足 $\underbrace{1+1+\cdots+1}_{p\text{-次}}=0$ 且对任何 $q<p$，$\underbrace{1+1+\cdots+1}_{q\text{-次}}\neq 0$ 的域称为**特征为 p 的域**；如果对任何整数 p，$\underbrace{1+1+\cdots+1}_{p\text{-次}}\neq 0$，则称该域**特征为 0**。

在域中，如果不要求乘法一定有单位元，也不要求任何非 0 的元素关于乘法都有逆，就得到一类称为“环”的结构。域可以看作特殊的环，在多数代数书上都是先定义环再定义域。但在日常活动中，域的结构更为普遍。环的精确定义如下：

定义 1.7.3 一个**环**是一个结构 $(R,0,+,\cdot)$，其元素间有两个运算，分别记作加法 $+$ 和乘法 $\cdot$，0 是加法的单位元，它们满足：

(1) 对任意 $a,b,c \in R$，$a+(b+c)=(a+b)+c$；

(2) 对任意 $a,b \in R$，$a+b=b+a$；

(3) 存在一个元素，记作 0，满足：对任意 $a \in R$，$a+0=a$；

(4) 对任意 $a \in R$ 存在 $b \in F$，使得 $a+b=0$；

(5) 对任意 $a,b,c \in R$，$a \cdot (b \cdot c)=(a \cdot b) \cdot c$；

(6) 对任意 $a,b,c \in R$，$a \cdot (b+c)=a \cdot b+a \cdot c$ 并且 $(a+b) \cdot c=a \cdot c+b \cdot c$。

环的典型例子有整数 $\mathbb{Z}$、（实数上的）矩阵、（整系数）多项式等。矩阵环是非（乘法）交换环的典型例子。

结构的其他例子有图论中研究的图、布尔代数、群论中研究的群等。

最后来看自然数。我们关注的是加法和乘法。在后面谈到哥德尔不完全定理时，会特别讨论自然数的模型。自然数的公理化最初是由意大利数学家皮亚诺完成的。皮亚诺公理中所采用的最基本函数是所谓**后继函数** $S:\mathbb{N} \to \mathbb{N}$；另外有一个特殊的自然数 0。所谓 n 的后继就是直接跟在 n 后面的那个数。

皮亚诺关于自然数的公理如下：

(P1) 0 是一个自然数。

(P2) 任何自然数 n 都有一个自然数 $S(n)$ 作为它的后继。

(P3) 0 不是任何自然数的后继。

(P4) 后继函数是单一的，即：若 $S(m)=S(n)$，则 $m=n$。

(P5)（**归纳原理**）令 Q 为一个关于自然数的性质。如果 (i) 0 具有性质 Q；并且 (ii) 如果自然数 n 具有性质 Q，则 $S(n)$ 也具有性质 Q，那么所有自然数 n 都有性质 Q。

在此基础之上，可以归纳地定义加法。对任何自然数 n 和 m，

$$n+0=n \text{ 并且 } n+S(m)=S(n+m)。$$

类似地，对任何自然数 n 和 m，

$$n \times 0=0 \text{ 并且 } n \times S(m)=(n \times m)+n。$$

习题 1.7

1.7.1 验证：如果 p 是素数，则 $\{0, 1, \cdots, p-1\}$ 在模 p 的运算下满足域的所有公理。

1.7.2 证明每个非零的自然数都是某个自然数的后继。

1.7.3 证明抽屉原则（或称鸽舍原理[①]）：如果自然数 $n > m$，则不存在从 $\{0, 1, \cdots, n-1\}$ 到 $\{0, 1, \cdots, m-1\}$ 的单射。

1.7.4 证明下列命题等价：

(1) 皮亚诺公理中的归纳原理；

(2) **最小数原理**：自然数的任意非空子集都有最小元；

(3) **强归纳原理**：对任何一个自然数的性质 P，如果从所有 $m < n$，$P(m)$ 成立能推出 $P(n)$ 成立，则对所有自然数 n，$P(n)$ 都成立。

[①] 鸽舍原理（pigeonhole principle）叙述如下：如果把 n 只鸽子放入少于 n 个鸽舍里，则至少有一个鸽舍里有不止一只鸽子。

第二章　命题逻辑

2.1　引言

通常意义下的命题是指有真假值的语句。一个复杂的命题可以分解成若干简单的原子命题。这些原子命题与复合命题的关系，就是命题逻辑研究的范围。

对初学者来说，一个很自然的问题是：当人们研究逻辑时用的是什么逻辑？如果用逻辑本身来研究逻辑，那不是循环论证吗？这就引出逻辑学习中区分“元逻辑”和“对象逻辑”的重要性。打个比方来说，我们想要研究人脑的某些功能，但自己直接研究自己是很困难的。于是我们造一个机器人（或用某个计算机程序来模拟），对机器人就可以研究得清清楚楚。虽然机器人与我们相差很远，但如果我们感兴趣的功能是计算或下棋等，那么机器人或许可以很近似地模拟人脑，因此我们可以间接地通过研究机器人来了解人脑的这一部分功能。这个比方中的人脑相当于“元逻辑”，而机器人则相当于“对象逻辑”。既然计算机学家在研究机器人时完全不必问人脑是怎样运作的，我们在研究对象逻辑时也可以暂时不用考虑我们用的是什么元逻辑。只有把当前的功能研究清楚之后，我们再来思考怎样让机器人更接近人脑。

类似的还有“元语言”和“对象语言”的区分。例如，当用中文来研究英语或计算机语言时，中文就是“元语言”，而英语或计算机语言则是“对象语言”。当对象逻辑越来越像元逻辑时，两者的区别越来越小。而命题逻辑因其简单，比较容易从元逻辑中分别出来。例如，没有人会认为自然数的性质，如归纳法，是命题逻辑里面的，所以便于初学者分清元逻辑和对象逻辑，这样在学习一阶逻辑时可以减少一些困扰。这是本章的一个重要目的。

数理逻辑的一个重要方面是研究手段的局限。贯穿本课程的一个中心问题是：是否所有真命题都是可证的。“真”是我们的目的，而“证明”是我们的手段。我们的手段能达到目的吗？要想回答这个问题，首先要搞清楚“真”是什么意思，“证明”又是什么意思。在这两个重要概念中，“真”属于语义范

畴，而“证明”属于语法范畴。在学习过程中，我们常把“语法”与“语义”分开讨论，但这是暂时的，如同体育活动中分解动作一样。最终两者是不可分的。语法让人想到机器、规则、算法；语义则让人想到人（脑）、意义、真假等。

正如前面提到的，为了分散学习难点，我们在材料安排上，特意让命题逻辑与一阶逻辑沿相似的主线发展，都包含语法部分，规定好语言，研究推演系统和证明；也包含语义部分，讨论真值理论。最后以可靠性和完全性定理把语法和语义联系起来。清华大学文志英教授曾讲过：学习的过程就是不断重复、不同层次上的重复。希望我们的课程设计能够有助于读者对数理逻辑的理解。

2.2 命题逻辑的语言

古典命题逻辑的语言包括以下 3 部分:

(1) 可数多个**命题符号**: $A_0, A_1, A_2, \cdots$。

(2) **命题联词**: 否定符号 $\neg$、合取符号 $\wedge$、析取符号 $\vee$、蕴涵符号 $\rightarrow$和双蕴涵符号 $\leftrightarrow$。

(3) 括号: 左括号“(”和右括号“)”。

几点说明:

(1) 这里“可数”是一个数学专用术语，大意为同自然数一样多。在一般情况下，只要有足够（有限）多的命题符号就够用了。另一方面，人们也可以研究有不可数多个命题符号的逻辑。

(2) 这 5 个联词尽管与日常语言有关，但在数学文献中更为常见。

(3) 在本节中强调的是语法。因此尽管我们给这 5 个联词取了上述的名字，并经常把它们读成“非”、“并且”、“或”、“如果 $\cdots$ 那么 $\cdots$”和“当且仅当”，但那是下一节讨论语义的任务。在本节中，应把它们视为完全没有意义的字符，所以上面特别强调“符号”二字。

(4) $\neg$ 是一元联词。其他 4 个是二元联词。这 4 个二元联词在讨论语法时区别不大，下面会常用符号 $\star$ 来表示它们中的任何一个联词。

(5) 括号是为了消除阅读中可能出现的歧义，以后（习题 2.4）我们会看到，运用不同的语法规则实际上是可以不用括号的。对计算机语言来说，没有括号更为简练。

规定好基本符号之后，就可以形成较为复杂的语句。首先称任何一个符号串为一个**表达式**。例如，“$(\neg A_1)$”或者“$((A_1\vee$”都是表达式。表达式可以是任意的，完全不用考虑其是否有“意义”。当然我们感兴趣的是那些“合乎语法规则”的表达式。我们称它们为**合式公式**或简称为**公式**。确切定义如下。

定义 2.2.1 命题逻辑语言全体合式公式的集合是满足以下条件的表达式的最小集合：

(1) 每个命题符号 A_i 都是合式公式；

(2) 如果 α 和 β 都是合式公式，则 $(\neg\alpha)$，$(\alpha\wedge\beta)$，$(\alpha\vee\beta)$，$(\alpha\to\beta)$ 和 $(\alpha\leftrightarrow\beta)$ 也是合式公式；

(3) 别无其他。

几点说明：

(1) 定义中的中文即“元语言”，而本节一开始定义的命题逻辑语言为“对象语言”。具体地说，我们使用了“每个”这个量词，也使用了 α，β 等符号作为变元，以代表这个语言中的任意表达式。但这里的量词和符号变元都是元语言中的，显然不属于正在讨论的命题逻辑语言。

(2) 虽然定义中标准的命题符号为 $A_0, A_1, A_2, \cdots$，但在实际工作中经常用 A，B，P 和 Q 等元语言符号来表示任意的命题符号。

在定义2.2.1中，(1) 和 (2) 不难理解，(3) 有些模糊。由于以后会大量使用这类形式的定义，让我们花一些篇幅解释一下。熟悉抽象代数的读者会看出这实际上是某种“闭包”，或是“由 $\cdots$ 生成的集合”。在数学上有两种等价的方式将其严格化：“自上而下”或“自下而上”。两种方式的等价性我们留作习题。

“自上而下”的定义是将合式公式集作为一个整体定义出来。我们临时把一个满足定义 2.2.1 (2) 所述性质的表达式集 X 称为**封闭的**，即：对所有 X 中的公式 α 和 β，表达式 $(\neg\alpha)$ 和 $(\alpha\star\beta)$ 也在 X 中（其中 $\star$ 代表 4 个二元联词中的任何一个）。**全体合式公式的集合**可以“自上而下”地定义如下：最小的包含所有命题符号的封闭的表达式集，即

$$\bigcap\{X : \text{所有的 } A_i \text{ 都属于 } X \text{ 并且 } X \text{ 是封闭的}\}。$$

注意：定义2.2.1(3) 体现在“最小”里面，被符号 $\bigcap$ 精确地表达出来。

“自上而下”的定义并没有告诉我们每一个具体的合式公式是什么样子的。这一不足被“自下而上”的定义所弥补。“自下而上”的定义给出每个公式 α 的构造过程。最下面的当然是命题符号，它们相当于楼梯的第一级台阶。站在这一级上，可以构造下一级的公式，如 $(\neg A_1)$，$(A_1 \vee A_2)$；站在“第二级”上，就可以构造“第三级”的公式，如 $((\neg A_1) \to A_2)$。如此拾级而上，就会得到任意“高度”的公式。准确地说，我们称一个表达式的有穷序列

$$(\alpha_0, \alpha_1, \cdots, \alpha_n)$$

为 α 的一个**构造序列**，如果最后一项 α_n 为 α 并且对每一个 $i \leq n$，或者 α_i 是一个命题符号，或者存在 $j, k < i$ 使得 α_i 为 $(\neg\alpha_j)$ 或 $(\alpha_j \star \alpha_k)$。我们称一个表达式 α 为一个合式公式，如果存在 α 的一个构造序列。注意：构造序列并不唯一，事实上，每一个合式公式都有无穷多个不同的构造序列。

既然每一个公式都是一步步地构造出来的，就有可能把通常在自然数上的数学归纳法转化成“对公式的归纳法”。具体的转化过程留作习题。如下形式的归纳原理非常有用，利用它就可以直接讨论公式的性质，而不用每次都绕回到自然数上去做归纳。

定理 2.2.2（归纳原理） *令 $P(\alpha)$ 为一个关于合式公式的性质。假设*

(1) *对所有的命题符号 A_i, 性质 $P(A_i)$ 成立；*

(2) *对所有的合式公式 α 和 β, 如果 $P(\alpha)$ 和 $P(\beta)$ 成立，则 $P((\neg\alpha))$ 和 $P((\alpha \star \beta))$ 也成立，*

那么 $P(\alpha)$ 对所有的合式公式 α 都成立。

可以用下面的引理来说明归纳原理的用法。在以后会用该引理来证明公式的唯一可读性。

引理 2.2.3 *每一合式公式中左右括号的数目相同，而且每一合式公式的真前段中左括号多于右括号。因此合式公式的真前段一定不是合式公式。*

证明 这里只证明第一个命题，第二个命题的证明完全类似。令 $P(\alpha)$ 表示在 α 中左右括号数目相同。对 $P(\alpha)$ 施行归纳法。初始情形：对所有的命题符号 A_i, 性质 $P(A_i)$ 显然成立，因为左右括号的数目都是零。归纳情形：假设 $P(\alpha)$ 和 $P(\beta)$ 成立，即在 α 和 β 中左右括号的数目都相同。由于 $(\neg\alpha)$ 和 $(\alpha \star \beta)$ 都仅仅添加了最外端的一对括号，它们左右括号的数目依旧保持相同，即 $P((\neg\alpha))$ 和 $P((\alpha \star \beta))$ 成立。根据归纳原理，$P(\alpha)$ 对所有公式都成立。 □

习题 2.2

2.2.1 假定 E 是一个集合，B 是 E 的一个子集，$g : E \to E$ 和 $f : E \times E \to E$ 分别为 E 上的一个一元和二元函数。定义

$$C^* = \bigcap \{X : B \subseteq X \text{ 并且对所有 } x, y \in X, g(x), f(x, y) \in X\},$$

我们称 C^* 为 B 在 E 中关于 g 和 f 的**闭包**，或者称 C^* 为 E 中由 B 经 g 和 f **生成**的集合。接下来定义集合序列 $(C_n : n \in \mathbb{N})$ 如下：

$$C_0 = B;$$
$$C_{n+1} = C_n \cup \{g(x) : x \in C_n\} \cup \{f(x, y) : x, y \in C_n\}。$$

并且令

$$C_* = \bigcup_{n \in \mathbb{N}} C_n。$$

证明 $C^* = C_*$。

2.2.2 如果 α 中除了 A_3，A_{17}，$\neg$ 和 $\to$ 外没有别的命题符号和联词，称 α 是一个**好公式**。给出好公式的“自上而下”和“自下而上”的定义。

2.2.3 证明归纳原理，即定理 2.2.2。

2.2.4 证明没有长度为 $0, 2, 3$ 或 6 的合式公式, 但其他长度皆有可能。

2.2.5 已知公式 α 中一元联词 $\neg$ 出现的次数为 m，其他 4 个二元联词出现的总次数为 n。找出 α 的长度。

2.2.6 在公式 α 中，令 c 表示二元联词 $(\wedge, \vee, \to, \leftrightarrow)$ 在 α 中出现的次数；s 代表命题符号出现的次数。(例如，当 α 为 $(A \to (\neg A))$ 时，$c = 1$ 并且 $s = 2$。) 用归纳原理证明 $s = c + 1$。

2.2.7 假定公式 α 的长度为 n，证明 α 有一个长度不超过 n 的构造序列。

2.2.8 给定公式 α 的一个构造序列，其中 α 不包含命题符号 A_4。在此构造序列中删除所有包含 A_4 的项，证明删除后的序列仍是 α 的一个构造序列。

2.2.9 直观上说，β 是公式 α 的一个**子公式**，如果 β 本身是一个公式并且是 α 的一部分。

(1) 给出 β 是公式 α 的一个子公式的严格定义；

(2) 用 (1) 的定义证明：如果 β 是 α 的一个子公式，γ 是 β 的一个子公式，则 γ 也是 α 的一个子公式；

(3) 证明在 α 的最短的构造序列中出现的都是 α 的子公式。

2.3 真值指派

下面开始探讨语义。首先规定**真假值**集合为 $\{T, F\}$，其中 T 代表“真”，F 代表“假”，很多参考书也用 $\{1, 0\}$ 来代表。令 S 为一个命题符号的集合。S 上的一个**真值指派** v 就是从 S 到真假值的一个映射，

$$v : S \to \{T, F\}。$$

令 $\overline{S}$ 为只含有 S 中的命题符号的公式集。数学上更准确的说法应该是这样：每一个联词都对应于一个表达式上的函数，例如，如果令 E 表示所有表达式的集合，则 $\neg$ 对应于 $f_\neg : E \to E$，$f_\neg(\alpha) = (\neg\alpha)$。同样地，每一个二元联词 $\star$ 就对应于 $f_\star : E \to E$，$f_\star(\alpha, \beta) = (\alpha \star \beta)$。$\overline{S}$ 就是表达式中由 S 经这 5 个函数生成的集合（见习题 2.2）。再把真值指派 v 扩张到 $\overline{S}$ 上得到新函数 $\overline{v}$：

$$\overline{v} : \overline{S} \to \{T, F\},$$

使其满足：

(0) 对任意 $A \in S$，$\overline{v}(A) = v(A)$；

(1)
$$\overline{v}((\neg\alpha)) = \begin{cases} T, & \text{如果 } \overline{v}(\alpha) = F, \\ F, & \text{其他；} \end{cases}$$

(2)
$$\overline{v}((\alpha \wedge \beta)) = \begin{cases} T, & \text{如果 } \overline{v}(\alpha) = T \text{ 并且 } \overline{v}(\beta) = T, \\ F, & \text{其他；} \end{cases}$$

(3)
$$\overline{v}((\alpha \vee \beta)) = \begin{cases} T, & \text{如果 } \overline{v}(\alpha) = T \text{ 或者 } \overline{v}(\beta) = T, \\ F, & \text{其他；} \end{cases}$$

(4)
$$\overline{v}((\alpha \to \beta)) = \begin{cases} F, & \text{如果 } \overline{v}(\alpha) = T \text{ 并且 } \overline{v}(\beta) = F, \\ T, & \text{其他；} \end{cases}$$

(5)

$$\overline{v}((\alpha \leftrightarrow \beta)) = \begin{cases} T, & \text{如果 } \overline{v}(\alpha) = \overline{v}(\beta), \\ F, & \text{其他。} \end{cases}$$

也可以用**真值表**来表示 $\overline{v}$，见表2.1。

表 2.1　真值表

α	β	$(\neg\alpha)$	$(\alpha \wedge \beta)$	$(\alpha \vee \beta)$	$(\alpha \to \beta)$	$(\alpha \leftrightarrow \beta)$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

真值表是命题逻辑语义最根本的部分。首先注意，在考察命题逻辑语言时，联词都被视为无意义的符号；公式也只是按规则排列的符号串。直到现在，我们才通过定义 $\overline{v}$ 来体现联词的意义和规定公式的真假值。同时注意：对命题公式真值的定义本身是在元语言中发生的。而只有在真值指派 v 确定以后，公式的真值才有意义。至于 v 为什么让 A_3 为假、而让 A_4 为真等不是我们考虑的范围。从某种意义上来说，逻辑学关心的不是“原子事实”的真假，而是怎样处理由逻辑符号生成的复合命题的真假。我们今后会看到，这一点在一阶逻辑的真值理论中表现得更为明显。对初学者来说，除了对蕴涵式的规定外，其他的都好理解。当然，可以简单地说：在数学中蕴涵就是这样规定的。但我们还是尝试给出几种解释，以期对读者有所帮助。在专门的模态逻辑课程中对蕴涵的意义往往会有更多的讨论。

第一种解释：考察“如果中国足球队夺冠，我就把自己的鼻子吃了”。

假设我在看球时跟朋友说了这样的话，而比赛结果真的是中国队夺冠（前件为真），那朋友绝对有权利要求我把自己的鼻子吃了，因为否则我就说了假话（后件为假，所以整个命题为假，见真值表的第二行第六列），而无面目站在讲台之上。但是，更为可能的是中国队没有夺冠（前件为假，在我的记忆中，这个命题总是假），那朋友就没有权利要求我吃鼻子了，因为无论如何，我都说了真话（既然前件为假，无论后件是否为真，整个命题都真。见真值表的第三行、第四行第六列）。

第二种解释：考察 $(A \wedge B) \to B$。

在这个例子中，后件“包含”在前件中。当肯定了前件时，当然肯定了作为其一部分的后件，所以直观上这个命题无论如何都是真的。考察真值表

的结果也一样，不管 A，B 取何值，整个公式的真值一定为 T。现在考虑如下两种情况：(i) A 为假而 B 为真，则得到的是 $F \to T$；(ii) B 为假，这时前件和后件都是假的，得到的是 $F \to F$。但根据以上的讨论，整个命题依然为真。所以 $F \to T$ 和 $F \to F$ 的真值都应设为 T。

第三种解释：读者不妨自行设计让自己觉得满意的真值表，见表2.2。

表 2.2　蕴含式的真值表

α	β	$(\alpha \to \beta)$
T	T	T
T	F	F
F	T	X
F	F	Y

首先，人们对表2.2的前两行应该没有异议。剩下的是选择 X 和 Y 的值。我们选了 $X = Y = T$，有人不满意。剩下还有 3 种选项，但人们会发现都不合适。第一种可能：$X = T$，$Y = F$，这时第二列与第三列完全相同，即 $A \to B$ 与 A 的真假全无关系。第二种可能：$X = F$，$Y = T$，这与 $A \leftrightarrow B$ 相同。第三种可能：$X = Y = F$，这与 $A \wedge B$ 相同。

例 2.3.1　令 α 为下列合式公式：

$$(((B \to (A \to C)) \leftrightarrow ((B \wedge A) \to C)))。$$

假定 $v(A) = v(B) = T$ 并且 $v(C) = F$。找出 $\overline{v}(\alpha)$ 的值。

答案：$\overline{v}(\alpha) = T$。

回到 $\overline{v}$ 的定义。读者可能会注意到，在定义中 $\overline{v}$ 在定义和被定义的部分同时出现，表面看起来是一种循环定义，实则不然。这样的定义方法是递归定义的一个例子。递归定义在数学上很常见，例如，**阶乘函数** $n!$ 就可以递归定义成 $0! = 1$，并且对所有自然数 n, $(n+1)! = (n+1) \times n!$。又如，**菲波那契序列**[1] f_n 可以递归定义为 $f_0 = f_1 = 1$，并且对所有自然数 n, $f_{n+2} = f_n + f_{n+1}$。从直观上很容易接受下述定理：

定理 2.3.2　*对任意 S 上的真值指派 v，都有唯一的一个扩张 $\overline{v} : \overline{S} \to \{T, F\}$ 满足前述条件 (0) 至 (5)。*

[1] 菲波那契（Fibonacci，约 1170—约 1250），意大利数学家。

定理 2.3.2 的证明本质上是验证递归定义的合理性，即递归定义并没有犯循环定义的错误。在很多集合论的教科书中都有递归定义合理性的证明，有兴趣的读者可以参考，这里就省略了。

对任意一个真值指派 v，任意公式 α，如果 $\bar{v}(\alpha) = T$，就称 v **满足** α。

定义 2.3.3 我们称一个公式集 Σ **重言蕴涵** 公式 α，记为 $\Sigma \vDash \alpha$，如果每一个满足 Σ 中所有公式的真值指派都满足 α。

$\Sigma \vDash \alpha$ 也读作“α 是 Σ 的**语义后承**”。如果把它的定义用数学语言展开，就会发现它涉及不止一个量词。$\Sigma \vDash \alpha$ 当且仅当“对所有的真值指派 v [如果（对所有的公式 $\beta \in \Sigma$，$\bar{v}(\beta) = T$）则 $\bar{v}(\alpha) = T$]”。

例 2.3.4

(1) 验证 $\{(\alpha \wedge \beta)\} \vDash \alpha$；

(2) 公式集 $\{A, (\neg A)\}$ 重言蕴涵 B 吗?

答案：是。

我们称一个公式 α 为一个**重言式**（记作 $\vDash \alpha$）如果 $\emptyset \vDash \alpha$。这与通常的“重言式在所有真值指派下为真”或“重言式被所有真值指派满足”的说法是一致的。原因是所有的真值指派 v 都满足空集中的每一元素。不然的话，空集中就会有一个元素让 v 不满足它，而这显然是不可能的。

如果 $\Sigma = \{\beta\}$ 只含有一个公式，常常会把 $\{\beta\} \vDash \alpha$ 简写成 $\beta \vDash \alpha$。如果 $\beta \vDash \alpha$ 和 $\alpha \vDash \beta$ 都成立，则可以说 β 和 α **重言等价**。

重言式举例

(1) 结合律：

$$\begin{aligned} ((\alpha \vee (\beta \vee \gamma)) &\leftrightarrow ((\alpha \vee \beta) \vee \gamma)); \\ ((\alpha \wedge (\beta \wedge \gamma)) &\leftrightarrow ((\alpha \wedge \beta) \wedge \gamma))。 \end{aligned}$$

(2) 交换律：

$$\begin{aligned} ((\alpha \vee \beta) &\leftrightarrow (\beta \vee \alpha)); \\ ((\alpha \wedge \beta) &\leftrightarrow (\beta \wedge \alpha))。 \end{aligned}$$

(3) 分配律：

$$\begin{aligned}((\alpha \wedge (\beta \vee \gamma)) &\leftrightarrow ((\alpha \wedge \beta) \vee (\alpha \wedge \gamma)))；\\ ((\alpha \vee (\beta \wedge \gamma)) &\leftrightarrow ((\alpha \vee \beta) \wedge (\alpha \vee \gamma)))。\end{aligned}$$

(4) 双重否定：

$$((\neg(\neg\alpha)) \leftrightarrow \alpha)。$$

(5) 德摩根[1]定律：

$$\begin{aligned}((\neg(\alpha \vee \beta)) &\leftrightarrow ((\neg\alpha) \wedge (\neg\beta)))；\\ ((\neg(\alpha \wedge \beta)) &\leftrightarrow ((\neg\alpha) \vee (\neg\beta)))。\end{aligned}$$

(6) 其他：

$$\begin{aligned}\text{排中律：}&\quad (\alpha \vee (\neg\alpha))；\\ \text{矛盾律：}&\quad (\neg(\alpha \wedge (\neg\alpha)))；\\ \text{逆否命题：}&\quad ((\alpha \to \beta) \leftrightarrow ((\neg\beta) \to (\neg\alpha)))。\end{aligned}$$

习题 2.3

2.3.1 证明下列两公式互不重言蕴涵：

$$(\alpha \leftrightarrow (\beta \leftrightarrow \gamma)),\quad ((\alpha \wedge (\beta \wedge \gamma)) \vee ((\neg\alpha) \wedge ((\neg\beta) \wedge (\neg\gamma))))。$$

【**注意**：本题说明在叙述“α 当且仅当 β 当且仅当 γ”时，我们要小心。】

2.3.2 回答以下问题：

(1) 公式 $(((\alpha \to \beta) \to \alpha) \to \alpha)$ 是重言式吗?

(2) 递归地定义 γ_k 如下：$\gamma_0 = (\alpha \to \beta)$ 并且 $\gamma_{k+1} = (\gamma_k \to \alpha)$。找出所有使 γ_k 为重言式的 k。

2.3.3 验证下列公式为重言式：

(1) $(((\neg\alpha) \vee \beta) \leftrightarrow (\alpha \to \beta))$；

[1] 德摩根（Augustus De Morgan，1806—1871），英国逻辑学家、数学家。

(2) $(\alpha \to (\beta \to \alpha))$;

(3) $((\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)))$;

(4) $((\neg\beta \to \neg\alpha) \to ((\neg\beta \to \alpha) \to \beta))$;

(5) $((\alpha \to (\beta \to \gamma)) \leftrightarrow ((\alpha \wedge \beta) \to \gamma))$。

2.3.4 证明下列命题等价：

(1) $\alpha \vDash \beta$;

(2) $\vDash (\alpha \to \beta)$;

(3) α 与 $(\alpha \wedge \beta)$ 重言等价;

(4) β 与 $(\alpha \vee \beta)$ 重言等价。

2.3.5 证明 $\Sigma \cup \{\alpha\} \vDash \beta$ 当且仅当 $\Sigma \vDash (\alpha \to \beta)$。

2.3.6 假定 $\Sigma \vDash (\alpha \to \beta)$。证明 $\Sigma \vDash ((\gamma \to \alpha) \to (\gamma \to \beta))$。

2.3.7 证明或否证（以给反例的方式）下列断言：

(1) 如果 $\Sigma \vDash \alpha$ 或 $\Sigma \vDash \beta$, 则 $\Sigma \vDash (\alpha \vee \beta)$;

(2) 如果 $\Sigma \vDash (\alpha \vee \beta)$, 则 $\Sigma \vDash \alpha$ 或 $\Sigma \vDash \beta$。

2.3.8 找出所有 $\{A_1, A_2, \cdots, A_n\}$ 上分别满足下列公式的真值指派：

(1) $\alpha = ((A_1 \to A_2) \wedge (A_2 \to A_3) \wedge \cdots \wedge (A_{n-1} \to A_n))$;

(2) $\beta = (\alpha \wedge (A_n \to A_1))$;

(3) $\gamma = \bigwedge\{(A_i \to (\neg A_j)) : 1 \le i, j \le n$ 并且 $i \ne j\}$。

【**注意**：(3) 中 γ 的写法不标准，但应该不妨碍对题意的理解。】

2.3.9 证明一个真值指派 v 满足公式

$$(\cdots((A_1 \leftrightarrow A_2) \leftrightarrow A_3)\cdots \leftrightarrow A_n)$$

当且仅当在 $1 \le i \le n$ 中对偶数多个 i，$v(A_i) = F$。

2.3.10 固定一个公式的序列 $\alpha_1, \alpha_2, \cdots$。对任意公式 β，将出现在 β 中的每个命题符号 A_n 替换成以上序列中的公式 α_n，并把所得到的公式记作 β^*。例如，当 β 为 $((A_2 \vee A_1) \to A_2)$ 时，β^* 就是 $((\alpha_2 \vee \alpha_1) \to \alpha_2)$。

(1) 令 v 为一个真值指派。定义真值指派 u 为 $u(A_n) = \overline{v}(\alpha_n)$。证明 $\overline{u}(\alpha) = \overline{v}(\alpha^*)$。

(2) 证明如果 α 是重言式，则 α^* 也是。

2.4 唯一可读性

在自然语言中，相同的一句话，如果标点不同，也会表达不同的甚至相反的含义。例如，《吕氏春秋 • 察传》记载，鲁哀公曾经问孔子："乐正夔，一足，信乎?"意思是传说舜的某位叫夔的乐正只有一只脚，这可信吗? 孔子回答说："昔者舜欲以乐传教于天下，乃令重黎举夔于草莽之中而进之，舜以为乐正。夔于是正六律，和五声，以通八风，而天下大服。重黎又欲益求于人，舜曰：……若夔者一而足矣。"意思是说夔很能干，舜认为像夔这样的人，有一个就够用了。也就是说，孔子认为古籍中的"夔一足"不能断句为"夔，一足"。

虽然自然语言中的歧义也常常与语义有关，这一节要讲的则是纯语法的。我们将论证按照第一节中规则生成的合式公式没有歧义。这里的"歧义"与语义无关，指的是无论谁来把一个公式分解成子公式，其"结果"都是相同的。或许从反面理解更容易一点。像 $\alpha \to \beta \leftrightarrow \gamma$ 或 $\alpha \wedge \beta \vee \gamma$ 这样的表达式就有"歧义"，因为没有表达清楚是先处理 α 和 β 之间的运算，还是 β 和 γ 之间的运算。这一节与后面的内容关系不大，除了最后的一些约定外，其他内容可以暂时跳过。

定理 2.4.1（唯一可读性） 对任意公式 α，下列陈述有且仅有一条适用：

(1) α 是一个命题符号；

(2) α 形为 $(\neg\alpha_0)$，其中 α_0 为一合式公式；

(3) α 形为 $(\alpha_1 \star \alpha_2)$，其中 α_1 和 α_2 为合式公式，$\star$ 为某个二元联词。

不仅如此，在情形 (2) 和 (3) 中，公式 α_0，α_1 和 α_2 还有二元联词 $\star$ 都是唯一的。

证明　首先，令 $P(\alpha)$ 表示性质“(1) 或 (2) 或 (3) 对 α 适用”。对 $P(\alpha)$ 用归纳很容易证明以上 3 条中至少有 1 条适用。

然后排除重叠的情形。情形 (1) 与情形 (2) 和 (3) 都没有重叠，因为 (1) 中第一个符号是命题符号，而 (2) 和 (3) 中第一个符号都是左括号；注意现在讨论语法，α 是作为字符串来考虑的，两个字符串相等当且仅当它们长度相同，并且每一个字节上的符号都相同。同样，通过比较第二个字节，容易看出情形 (2) 和 (3) 也无重叠。

最后检查情形 (2) 和 (3) 中的唯一性。我们只看情形 (3)，因为情形 (2) 更简单。假设 $\alpha = (\alpha_1 \star_1 \alpha_2) = (\beta_1 \star_2 \beta_2)$（注意：这里 $=$ 是指作为字符串相等），则删去第一个左括号后它们仍相等，$\alpha_1 \star_1 \alpha_2) = \beta_1 \star_2 \beta_2)$。根据引理 2.2.3，有 $\alpha_1 = \beta_1$，不然的话，一个会是另外一个的真前段。继续删去相同段 α_1 和 β_1，得到 $\star_1\alpha_2) = \star_2\beta_2)$。所以 $\star_1 = \star_2$。类似地，$\alpha_2 = \beta_2$。　□

关于括号省略的一些约定

一旦知道怎样避免歧义，就可以放松一点。记住：底线是一旦有争议，就回到最初，严格遵守规则。

(1) 最外的括号总被略去；

(2) 否定词的“管辖范围”尽可能短。例如，$\neg\alpha \vee \beta$ 指的是 $((\neg\alpha) \vee \beta))$；

(3) 同一联词反复出现时，以右为先。例如，$\alpha \to \beta \to \gamma$ 指的是 $((\alpha \to (\beta \to \gamma))$。

习题 2.4

2.4.1 给出一个程序完成如下的断句任务：输入任何表达式 α，该程序能够判定 α 是否是一个合式公式，并且在是的情况下输出 α 的一个构造序列。【这里并不要求大家真的去写计算机程序（能写更好），这里所要的是一个算法，即一系列简单而清晰的指令，告诉一台机器先做什么后做什么，等等。】

2.4.2 在定义 2.2.1 中将所有的右括号都省略掉。例如，原来的 $((\alpha \wedge (\neg\beta)) \vee (\gamma \to \alpha))$ 就变成了 $((\alpha \wedge (\neg\beta \vee (\gamma \to \alpha$。证明省略后仍有唯一可读性。

2.4.3 假定左括号和右括号变得一样，例如，原来的 $(\alpha \vee (\beta \wedge \gamma))$ 变成了 $|\ \alpha \vee |\ \beta \wedge \gamma\ ||$，还有唯一可读性吗?

2.4.4 将定义 2.2.1 中的 (2) 改动如下：

(2') 如果 α 和 β 都是合式公式，则 $\neg\alpha$，$\wedge\alpha\beta$，$\vee\alpha\beta$，$\to\alpha\beta$ 和 $\leftrightarrow\alpha\beta$ 也是。

例如，原来的 $((\alpha\wedge(\neg\beta))\vee(\gamma\to\alpha))$ 就变成了 $\vee\wedge\alpha\neg\beta\to\gamma\alpha$。证明：改动后仍有唯一可读性。这种表示法被称为波兰记法。

2.5 其他联词

我们再回到语义，研究联词的性质。我们之所以选择那 5 个联词是因为它们在数学文献中最为常见。很自然的问题是它们够不够用？能不能表达其他所有的联词？另一方面，它们有没有多余？

在回答这些问题之前，先要把其中涉及的概念搞清楚。首先，什么是一个任意的联词？从字面上看，联词就是把简单句合成复合句的方式。从语义上看，每个联词都唯一确定了从简单句的真假值到复合句真假值的一个规则。其实，就是一个真值表。我们给它一个新的名字，称为“布尔函数”，即：称一个从 $\{T,F\}^k$ 到 $\{T,F\}$ 的函数 B 为一个k-**元布尔函数**。

例如，令 α 为一个仅涉及命题符号 $A_1,A_2,\cdots,A_n$ 的公式。那么 α 就定义了一个 n-元布尔函数 B^n_α：

$$B^n_\alpha(X_1,\cdots,X_n) \quad = \quad \begin{array}{l}\text{当 } A_1,\cdots,A_n \text{ 被赋予真假值 } X_1,\cdots,X_n \text{ 时}\\ \text{公式 } \alpha \text{ 所取得的真假值。}\end{array}$$

这样，每一公式 α 都表达了一个 n- 元联词，或 n-元布尔函数 B^n_α。

有些参考书会提到 0-元联词 $\top$ 和 $\bot$，$\top$ 代表恒真，$\bot$ 代表恒假。如果读者觉得 0-元联词的概念不好理解，可以换一种方式来解释。让我们在语言中添加两个常数符号 $\top$ 和 $\bot$，并且修改合式公式的定义如下：所有的命题符号和 $\top$ 还有 $\bot$ 都是合式公式；如果 α 和 β 都是合式公式，则 $(\neg\alpha)$ 和 $(\alpha\star\beta)$ 也是；别无其他。例如，$(A\vee\bot)$ 就是新语言上的一个合式公式。在新语言上，任意真值指派 v 自然扩展为 $\overline{v}(\top)=T$ 和 $\overline{v}(\bot)=F$。

例 2.5.1 一元联词有 4 个：除了本质上是 0-元联词的恒真和恒假外，还有恒同和否定。

例 2.5.2 二元联词有 16 个。可以分几组讨论（请读者自己做真值表）。

第一组是本质上是 0-元联词的恒真和恒假。

第二组是本质上是 1-元联词的“与 A 恒同”，“非 A”，“与 B 恒同”和“非 B”这 4 个联词。

第三组是已经介绍过的 $\vee$，$\wedge$，$\to$ 和 $\leftrightarrow$，还有 $\leftarrow$。

第四组是“$A \downarrow B$”（也被称为皮尔士[①]箭头）定义为 $\neg(A \vee B)$ 和“$A \mid B$”（也被称为谢弗[②]竖）定义为 $\neg(A \wedge B)$。

第五组是“$A < B$”，“$A > B$”和“$A + B$”。特点是如果把 F, T 分别看成 $0, 1$，则这 3 个联词的取值与“小于”、“大于”的判断和加法结果相同（当然这里取 $1 + 1 = 0$）。

下述定理告诉我们，每个 n-元布尔函数都可以由某个公式来表达，从而说明我们选的联词是够用的。在证明一般情形之前，先看一个典型例子。

例 2.5.3　定义 $M(A, B, C) = A, B, C$ 中的多数。例如，$M(T, F, T) = T$ 且 $M(F, F, T) = F$。找出表达 M 的公式。

答案：$(A \wedge B \wedge C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)$。

定理 2.5.4　*对任意的 n-元布尔函数 G，其中 $n \geq 1$，都可以找到一个合式公式 α 使得 α 表达函数 G，即 $G = B^n_\alpha$。*

证明　**情形 1**：函数 G 的值域为 $\{F\}$，即 G 的真值表中最末一列全是 F。在此情形下，只要令 $\alpha = (A \wedge \neg A)$ 即可。

情形 2：情形 1 不成立。假定 G 在 k 个 n-元组上取值为 T，即真值表中有 k 行结尾是 T，其中 $k \geq 1$。把它们全部列出来：

$$\begin{aligned}
\overline{X}_1 &= (X_{11}, X_{12}, \cdots, X_{1n}), \\
\overline{X}_2 &= (X_{21}, X_{22}, \cdots, X_{2n}), \\
\vdots &\qquad\qquad \vdots \\
\overline{X}_k &= (X_{k1}, X_{k2}, \cdots, X_{kn})。
\end{aligned}$$

令

$$\beta_{ij} = \begin{cases} A_j, & \text{如果 } X_{ij} = T; \\ \neg A_j, & \text{其他。} \end{cases}$$

还有

$$\begin{aligned}
\gamma_i &= \beta_{i1} \wedge \beta_{i2} \wedge \cdots \wedge \beta_{in}, \\
\alpha &= \gamma_1 \vee \gamma_2 \vee \cdots \vee \gamma_k。
\end{aligned}$$

① 皮尔士（Charles Sanders Peirce，1839—1914），美国逻辑学家、哲学家。

② 谢弗（Henry M. Sheffer，1882—1964），美国逻辑学家。

我们验证 $G = B^n_\alpha$。容易看出对任何 $1 \le i \le k$，$B^n_\alpha(\overline{X}_i) = T = G(\overline{X}_i)$。另一方面，$\{A_1, A_2, \cdots, A_n\}$ 上只有唯一的指派 $\overline{X}_i$ 能满足 γ_i，所以如果指派 $\overline{Y}$ 不同于所有的 $\overline{X}_i$，则一定不满足所有的 γ_i，于是也不满足 α。所以 $B^n_\alpha(\overline{Y}) = F = G(\overline{Y})$。 □

称一个公式 α 为**析取范式**，如果 $\alpha = \gamma_1 \vee \gamma_2 \vee \cdots \vee \gamma_k$，其中每个 $\gamma_i = \beta_{i1} \wedge \beta_{i2} \wedge \cdots \wedge \beta_{in_i}$，并且每个 β_{ij} 或者是命题符号或者是命题符号的否定。

推论 2.5.5 *每一个合式公式 α 都有一个与其重言等价的析取范式。*

称一个联词的集合 $\mathcal{C}$ 为**功能完全的**，如果任何一个布尔函数都可以用仅仅涉及 $\mathcal{C}$ 中联词的公式来表达。例如，上述推论表明集合 $\{\neg, \vee, \wedge\}$ 是功能完全的。

推论 2.5.6 *联词集合 $\{\neg, \wedge\}$ 和 $\{\neg, \vee\}$ 都是功能完全的。*

证明 （思路）反复使用德摩根定律。 □

例 2.5.7 $\{\wedge, \to\}$ 不是功能完全的。

证明之前先做些说明：一是如何论证一个联词集 $\mathcal{C}$ 不是功能完全的。常用方法是论证 $\mathcal{C}$ 或者不能表达 $\neg$, 或者不能表达 $\vee, \wedge, \to$ 中的一个，因为 $\mathcal{C}$ 要是把它们都能表达，$\mathcal{C}$ 就功能完全了。但到底不能表达哪一个，则需要好眼力来观察到 $\mathcal{C}$ 的缺陷。二是假如要想论证 $\mathcal{C}$ 不能表达 $\neg$，只要论证任何一个由一个命题符号 A 和 $\mathcal{C}$ 中联词形成的公式都不重言等价 $\neg A$ 即可，也就是说，不必担心别的命题符号（如 B）可以帮助我们表达 $\neg A$。原因是如果（打个比方）$f(A, B)$ 与 $\neg A$ 重言等价，则 $f(A, A)$ 也与 $\neg A$ 重言等价。

证明 注意如下事实：令 α 为一个用到 $\wedge$ 和 $\to$ 的公式，如果将 α 中出现的命题符号都赋予真值 T，则 α 必定取值 T。因此 α 不与 $\neg A$ 重言等价。（如果想更严格的话，可以用归纳原理证明：如果 α 仅用到命题符号 A、联词 $\wedge$ 和 $\to$，则 $A \vDash \alpha$。） □

习题 2.5

2.5.1 令 G 为下列 3-元布尔函数：

$$\begin{aligned} G(F,F,F)&=T, \qquad & G(T,F,F)&=T,\\ G(F,F,T)&=T, \qquad & G(T,F,T)&=F,\\ G(F,T,F)&=T, \qquad & G(T,T,F)&=F,\\ G(F,T,T)&=F, \qquad & G(T,T,T)&=F。 \end{aligned}$$

(1) 给出一个表达 G 但仅涉及联词 $\wedge,\vee$ 和 $\neg$ 的合式公式。

(2) 重做 (1)，要求公式中联词出现的次数不超过 5 次。

2.5.2 证明 $|$ 和 $\downarrow$ 是仅有的两个自身是功能完全的二元联词。

2.5.3 证明 $\{\top,\bot,\neg,\leftrightarrow,+\}$ 不是功能完全的。【**提示：**证明用这些联词和命题符号 A 和 B 形成的公式 α 在 $\overline{v}(\alpha)$ 的 4 种可能取值里面总有偶数个T。】

2.5.4 令 $\mathbf{1}$ 为一个三元联词满足 $\mathbf{1}\alpha\beta\gamma$ 取值 T，当且仅当 α,β,γ 中有且仅有一个赋值为 T。证明不存在二元联词 $\circ$ 和 $\triangle$ 使得 $\mathbf{1}\alpha\beta\gamma$ 等价于 $(\alpha\circ\beta)\triangle\gamma$。【**提示：**任给二元布尔函数 B_1,B_2，假设 $B_2(B_1(x_1,x_2),x_3)=B^3_{\mathbf{1}A_1A_2A_3}$。证明 $B_1(1,1),B_1(1,0),B_1(0,0)$ 两两不相等。】

2.5.5 称公式 α 是**合取范式**，如果它形如

$$\alpha=\gamma_1\wedge\gamma_2\wedge\cdots\wedge\gamma_k,$$

其中每个**合取枝** γ_i 都形为

$$\gamma_i=\beta_{i1}\vee\beta_{i2}\vee\cdots\vee\beta_{in},$$

并且每个 β_{ij} 或是一个命题符号，或是命题符号的否定。

(1) 找出与 $\alpha\leftrightarrow\beta\leftrightarrow\gamma$ 重言等价的合取范式；

(2) 证明每一公式都有与其重言等价的合取范式。

2.5.6 假定 α 为一个仅包含联词 $\rightarrow$ 的公式，证明 $A\leftrightarrow B$ 不重言等价于 α。反之，假定 β 为一个仅包含联词 $\leftrightarrow$ 的公式，证明 $A\rightarrow B$ 不重言等价于 β。【**提示：**对仅含联词 $\rightarrow$ 和命题符号 A,B 的 α，归纳证明 B^2_α 只可能是 (T,T,F,F)，(T,F,T,F)，(T,F,T,T)，(T,T,F,T)，(T,T,T,F) 或 (T,T,T,T) 中的一个。】

2.5.7 将真假值 F 和 T 分别看成 0 和 1，并规定 $0 \leq 1$。当 $n > 0$ 时，称一个 n-元布尔函数 f 为**单调的**，如果对任何 $i = 1, \cdots, n$,

$$f(x_1, \cdots, x_{i-1}, 0, x_{i+1}, \cdots, x_n) \leq f(x_1, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_n)。$$

证明：一个 n-元布尔函数 f 是单调的，当且仅当它可以被仅出现联词 $\{\wedge, \vee, \top, \bot\}$ 的公式所表达。【**提示：**令 γ 是析取范式，且 B^n_γ 是单调的。证明若 $\alpha \wedge \neg A$ 是 γ 中的一个“析取枝”，那么 $\alpha \wedge A \vDash \gamma$。因此，将 γ 中 $\alpha \wedge \neg A$ 替换为 α 得到的是重言等价的公式。】

2.5.8 称一个联词的集合 $\mathcal{C}$ 为**极大不完全的**，如果 $\mathcal{C}$ 不是功能完全的，但对任意 $\mathcal{C}$ 表达不了的布尔函数 g，联词集 $\mathcal{C} \cup \{g\}$ 都是功能完全的。证明联词集 $\{\wedge, \vee, \top, \bot\}$ 为极大不完全的。【**提示：**假设 g 不是单调的。利用 $g, \top$ 和 $\bot$ 定义 $\neg$。】

2.6 命题逻辑的一个推演系统

数学中的“证明”是日常所用的“推理”的严格化。在本节中将严格定义“证明”这一概念。这样做有必要吗？没有证明的定义，几千年来数学不是也发展得很好吗？不错，没有证明的定义，人们仍可以证明大量数学定理，但是要想说什么是不可证的就难了。我们说过，数理逻辑的一个重要方面是研究手段的局限性，包括证明的局限。因此给出严格的定义是非常必要的。

不妨回顾一下数学中证明的几个要素。形象地说，证明是从假设到结论的一根逻辑链条。首先，这根链条必须是有限长的。其次，证明从一环到下一环都要有根据，这个根据可以来自假设，也可以来自逻辑公理，还可以由逻辑规则从前一环“推”到下一环。

我们的推演系统也有一个公式集 Λ 称为“公理集”，也有一套“推理规则”告诉我们怎样能行地从已有的公式得到新的公式。（这里“能行地”是强调规则应该是简单、机械的。）这样，给定一个公式集 Γ 作为“假设集”，Γ 能推出的结论，即 Γ 的“定理集”就包括那些从 $\Gamma \cup \Lambda$ 出发经过有穷次应用推理规则所能得到的公式。如果 α 是 Γ 的一个定理，则记录整个推演过程的公式序列就被称为从 Γ 到 α 的一个“证明”。注意：这里大家要分清元语言和对象语言的区别，因为我们会有关于（对象语言）定理的（元语言）定理，也有关于（对象语言）证明的（元语言）证明。在本节中，为了强调，我们把对象语言叙述的定理称为**内定理**。以后大家熟悉了，再省掉“内”字。

所以一个推演系统由公理和规则两部分决定。公理和规则的选取有很大的自由度。在本节中采取的是所谓“希尔伯特式”的系统，其特点是有很多

公理，但只有一个规则；并且推演也是线性的。后面还会介绍“根岑式”的自然推演系统，特点是公理很少（只有一条，甚至没有），规则很多，推演是树状的。但不管公理系统怎样选取，理想的系统都是既可靠又完全的。达到这一理想的系统都是“等价的”，因为它们从同一个假设集所导出的定理集是完全相同的。这在后面会学到。

引进命题逻辑的一个推演系统 $\mathscr{L}$。为简单起见，假定语言中只有 $\neg$ 和 $\to$ 两个联词，而把 $\alpha \wedge \beta$，$\alpha \vee \beta$ 和 $\alpha \leftrightarrow \beta$ 分别视为 $\neg(\alpha \to \neg\beta)$，$\neg\alpha \to \beta$ 和 $(\alpha \to \beta) \wedge (\beta \to \alpha)$ 的缩写。

系统 $\mathscr{L}$ 内的公理集 Λ 为：

(A1) $\alpha \to (\beta \to \alpha)$；

(A2) $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$；

(A3) $(\neg\beta \to \neg\alpha) \to ((\neg\beta \to \alpha) \to \beta)$，

其中 α，β 和 γ 为合式公式。

系统 $\mathscr{L}$ 中只有一条推理规则，称为**分离规则**[①]：从 α 和 $\alpha \to \beta$ 可以推出 β。

定义 2.6.1　从公式集 Γ 到公式 α 的一个**推演**（或一个**证明**）是一个有穷的公式序列

$$(\alpha_0, \alpha_1, \cdots, \alpha_n),$$

满足 $\alpha_n = \alpha$ 并且对所有 $i \leq n$ 或者

(1) α_i 属于 $\Gamma \cup \Lambda$；或者

(2) 存在 $j, k < i$，α_i 是从 α_j 和 α_k 中由分离规则得到的（即 $\alpha_k = \alpha_j \to \alpha_i$）。

称 α 为 Γ 的一个**内定理**（或**定理**），记为 $\Gamma \vdash \alpha$，如果存在一个从 Γ 到 α 的一个推演。人们一般会用 $\vdash \alpha$ 作为 $\emptyset \vdash \alpha$ 的简写。此时，对的 α 证明只用到命题逻辑公理和分离规则，不妨称 α 是**命题逻辑内定理**。

下面叙述一些关于证明的事实，以加深理解。希望读者自行补上理由。

① 分离规则，拉丁文为 modus ponens，常简记为 MP。

(1) 如果 $\Gamma \subseteq \Delta$ 并且 $\Gamma \vdash \alpha$，则 $\Delta \vdash \alpha$。

(2) $\Gamma \vdash \alpha$ 当且仅当存在 Γ 的一个有穷子集 Γ_0，使得 $\Gamma_0 \vdash \alpha$。

引理 2.6.2 对所有的合式公式 α，都有 $\vdash \alpha \to \alpha$。

证明 这里给出下列推演序列，请读者补上每一步的依据。

(1) $(\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$,

(2) $\alpha \to (\alpha \to \alpha) \to \alpha$,

(3) $(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$,

(4) $\alpha \to (\alpha \to \alpha)$,

(5) $\alpha \to \alpha$。 □

定理 2.6.3（演绎定理） 假定 Γ 为一个公式集，α 和 β 为公式。则 $\Gamma \cup \{\alpha\} \vdash \beta$ 当且仅当 $\Gamma \vdash \alpha \to \beta$。特别地，$\{\alpha\} \vdash \beta$ 当且仅当 $\vdash \alpha \to \beta$。

证明 ($\Rightarrow$) 假定 $(\beta_1, \beta_2, \cdots, \beta_n)$ 为从 $\Gamma \cup \{\alpha\}$ 到 β 的一个推演序列，其中 $\beta_n = \beta$。对 i 施行归纳来证明对所有的 $1 \le i \le n$，都有 $\Gamma \vdash \alpha \to \beta_i$。

当 $i = 1$ 时，β_1 或者属于 Γ，或者是逻辑公理，或者是 α 本身。因为 $\beta_1 \to (\alpha \to \beta_1)$ 属于公理 (A1)，所以在前两个情形中用分离规则即可得到 $\Gamma \vdash \alpha \to \beta_1$。在最后一个情形中，我们利用引理 2.6.2。

假定对所有的 $k < i$ 已有 $\Gamma \vdash \alpha \to \beta_k$。考察 β_i，它仍是或者属于 Γ，或者是一条公理或者是 α 本身，再多一种可能：β_i 是从 β_j 和 $\beta_l = \beta_j \to \beta_i$ $(j, l < i)$ 用分离规则得到的。前 3 种情形同 $i = 1$ 一样处理，把 1 换成 i 即可。在最后一个情形中，根据归纳假设，有 $\Gamma \vdash \alpha \to \beta_j$ 和 $\Gamma \vdash \alpha \to (\beta_j \to \beta_i)$。因为

$$(\alpha \to (\beta_j \to \beta_i)) \to (\alpha \to \beta_j) \to (\alpha \to \beta_i)$$

属于公理 (A2)，使用两次分离规则即得到 $\Gamma \vdash \alpha \to \beta_i$。

($\Leftarrow$) 直接从分离规则得到。 □

推论 2.6.4 假设 α，β 和 γ 为公式，则

(1) $\{\alpha \to \beta, \beta \to \gamma\} \vdash \alpha \to \gamma$;

(2) $\{\alpha \to (\beta \to \gamma), \beta\} \vdash \alpha \to \gamma$。

习题 2.6

2.6.1 证明如果 $\Delta \vdash \alpha$ 并且对每一 $\beta \in \Delta$，$\Gamma \vdash \beta$，则 $\Gamma \vdash \alpha$。

2.6.2 证明下列公式为命题逻辑内定理，其中 α 和 β 为合式公式。【**注意**：本题为语法练习，请勿使用任何有关语义的结果，但可使用已证明的元定理。】

(1) $\neg\neg\beta \to \beta$；【**提示**：$(\neg\beta \to \neg\neg\beta) \to (\neg\beta \to \neg\beta) \to \beta$。】

(2) $\beta \to \neg\neg\beta$；【**提示**：$(\neg\neg\neg\beta \to \neg\beta) \to (\neg\neg\neg\beta \to \beta) \to \neg\neg\beta$。】

(3) $(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$；

(4) $\neg\alpha \to (\alpha \to \beta)$；【**提示**：$(\neg\beta \to \neg\alpha) \to (\neg\beta \to \alpha) \to \beta$。】

(5) $(\alpha \to \beta) \to \neg\beta \to \neg\alpha$；

(6) $(\alpha \to \beta) \to (\neg\alpha \to \beta) \to \beta$；

(7) $\alpha \to \neg\beta \to \neg(\alpha \to \beta)$。

2.7　命题逻辑的自然推演

在 2.6 节已经引进了一个推演系统。注意“一个”这个词告诉我们，它只是众多推演系统之一。本节将介绍另一个常见的系统——自然推演（或自然推理）系统。它最初是由德国数学家根岑引进的。下面介绍的系统是经过后人改进的，主要是泰特[①]的贡献。这个系统的优点是最大限度地利用 $\vee$ 和 $\wedge$ 的对偶性，而且能减少推理规则的个数。但代价是大量使用经典逻辑中的德摩根律，从而对直觉主义逻辑不再适用。如果大家对其他版本的自然推演系统有兴趣，比较初等的文献有（van Dalen, 2004），当然也可参照证明论方面的参考书。

本节的主要目的有两个：一是为大家提供一个看问题的不同角度，可以与前面的“希尔伯特式”的系统相比较；二是在模态逻辑和证明论的文献中，通常会采用自然推演系统，因为自然推演有很多好的性质，如子公式性质等，这在后续课程中会讲到。由于我们的目的只是介绍，下面的叙述会简略一些。

首先需要重新规定语言。新的语言包括：

[①] 泰特（William W. Tait，1929—　），美国逻辑学家、哲学家。

(1) 命题符号：$A_0, \bar{A}_0, A_1, \bar{A}_1, \cdots$，注意：对每一个 i，A_i 和 $\bar{A}_i$ 都成对出现；

(2) 逻辑符号：$\vee$，$\wedge$；

(3) 括号："(" 和 ")"。

注意：$\neg$ 和 $\to$ 不再是原始符号。$\neg\alpha$ 的定义如下：对任意的命题符号 A，定义 $\neg A = \bar{A}$，$\neg\bar{A} = A$；定义 $\neg(\alpha \vee \beta) = \neg\alpha \wedge \neg\beta$ 和 $\neg(\alpha \wedge \beta) = \neg\alpha \vee \neg\beta$。$\alpha \to \beta$ 定义为 $\neg\alpha \vee \beta$。

在自然推演系统中，目标从证明单个公式扩展成证明一个公式的有穷集合 $\Gamma = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$，即：证明 $\alpha_1 \vee \alpha_2 \vee \cdots \vee \alpha_n$。这里用 Γ, α 表示集合 $\Gamma \cup \{\alpha\}$。推理规则如下：其中 Γ 和 Δ 为任意的有穷公式集，横线表明其下面的公式集可由其上面的推出。

公理：

$$\Gamma, A_i, \bar{A}_i;$$

规则 ($\vee$):

$$\frac{\Gamma, \alpha_i}{\Gamma, (\alpha_0 \vee \alpha_1)} \quad , \quad i = 0, 1;$$

规则 ($\wedge$):

$$\frac{\Gamma, \alpha_0 \quad \Gamma, \alpha_1}{\Gamma, (\alpha_0 \wedge \alpha_1)} \quad ;$$

切割规则:

$$\frac{\Gamma, \alpha \quad \Gamma, \neg\alpha}{\Gamma} \quad 。$$

这里不打算给出推演的精确定义，而只给出下列描述和一些例子。从（可以是无穷的）公式集 Δ 到有穷公式集 Γ 的一个自然推演是一个有穷二岔树，树根为公式集 Γ，树叶中的公式都来自 Δ，而树中的每个节点都是某个推理规则的应用。这里仍用 $\Delta \vdash \Gamma$ 表示存在从 Δ 到 Γ 的一个自然推演。由于对自然推演的讨论仅仅作为对证明系统的一个补充，我们只讨论 $\vdash \Gamma$ 这种弱形式，至于 $\Delta \vdash \Gamma$ 这样的一般形式，暂不讨论。

下面举几个推演的例子。

例 2.7.1 用自然推演证明：对所有的有穷公式集 Γ 和公式 α，有 $\vdash \Gamma, \neg\alpha, \alpha$。今后会把它称为（公理′）或直接当作公理来用。

证明　固定 Γ，对公式 α 施行归纳。

如果 α 为命题符号 A_i，则 $\neg\alpha$ 为 $\bar{A}_i$。所以 $\Gamma, \neg\alpha, \alpha$ 是公理。α 为 $\bar{A}_i$ 的情形类似。

如果 α 形如 $\alpha_0 \vee \alpha_1$，则 $\neg\alpha$ 形如 $\neg\alpha_0 \wedge \neg\alpha_1$。根据归纳假定，对 $i = 0, 1$ 分别存在 $\Gamma, \neg\alpha_i, \alpha_i$ 的自然推演 $\mathcal{D}_i$。有

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}_0\\ \vdots\\ \Gamma, \alpha_0, \neg\alpha_0\end{array}}{\Gamma, \alpha_0 \vee \alpha_1, \neg\alpha_0} \quad \dfrac{\begin{array}{c}\mathcal{D}_1\\ \vdots\\ \Gamma, \alpha_1, \neg\alpha_1\end{array}}{\Gamma, \alpha_0 \vee \alpha_1, \neg\alpha_1}}{\Gamma, \alpha_0 \vee \alpha_1, \neg\alpha_0 \wedge \neg\alpha_1} \ ,$$

α 为 $\alpha_0 \wedge \alpha_1$ 的证明类似。 □

例 2.7.2　我们有

$$\dfrac{\Gamma, \alpha_0, \alpha_1}{\Gamma, \alpha_0 \vee \alpha_1} \ 。$$

（今后会把它称为 $(\vee')$ 或直接当作规则来用。）

证明　根据规则 $(\vee)$，有

$$\dfrac{\dfrac{\Gamma, \alpha_0, \alpha_1}{\Gamma, \alpha_0, \alpha_0 \vee \alpha_1}}{\Gamma, \alpha_0 \vee \alpha_1, \alpha_0 \vee \alpha_1} \ ,$$

但作为集合，$\Gamma, \alpha_0 \vee \alpha_1, \alpha_0 \vee \alpha_1$ 等于 $\Gamma, \alpha_0 \vee \alpha_1$，都等于 $\Gamma \cup \{\alpha_0 \vee \alpha_1\}$，所以结论成立。 □

我们再多看一个例子。注意：在证明过程中出于各种需要，会经常改变同一个集合的表达形式。例如，把 $\{a, b, c\}$ 转写成 $\{a, b\}, c$ 或 $\{a\}, b, c$。反正要证的 $\Gamma = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ 指的是 $\alpha_1 \vee \alpha_2 \vee \cdots \vee \alpha_n$，因此问题不大。另外，尽管转写不是推理规则，为了读者方便，可以把**转写**写成

$$\dfrac{\{a, b, c\}}{\{a, b\}, c} \ (rw)。$$

例 2.7.3　用自然推演证明：

$$\vdash ((\alpha \to \beta) \wedge (\beta \to \gamma)) \to (\alpha \to \gamma)。$$

证明 首先要用 $\neg p \vee q$ 代替 $p \to q$，并且用 $\neg$ 的定义把 $\neg$ 推到最里层。由此，我们要证的是：

$$\vdash ((\alpha \wedge \neg\beta) \vee (\beta \wedge \neg\gamma)) \vee (\neg\alpha \vee \gamma)。$$

推演树如下：

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\{\gamma,\beta\},\alpha,\neg\alpha}{\{\gamma,\beta,\neg\alpha\},\alpha}\,(rw) \quad \dfrac{\{\neg\alpha,\gamma\},\neg\beta,\beta}{\{\gamma,\beta,\neg\alpha\},\neg\beta}\,(rw)}{\{\gamma,\neg\alpha,\beta\},\alpha\wedge\neg\beta}\,(\wedge)}{\{\gamma,\neg\alpha,\alpha\wedge\neg\beta\},\beta}\,(rw) \quad \dfrac{\{\neg\alpha,\alpha\wedge\neg\beta\},\gamma,\neg\gamma}{\{\gamma,\neg\alpha,\alpha\wedge\neg\beta\},\neg\gamma}\,(rw)}{\{\gamma,\neg\alpha,\alpha\wedge\neg\beta\},\beta\wedge\neg\gamma}\,(\wedge)}{(\alpha\wedge\neg\beta),(\beta\wedge\neg\gamma),\neg\alpha,\gamma}\,(rw)}{((\alpha\wedge\neg\beta)\vee(\beta\wedge\neg\gamma)),(\neg\alpha\vee\gamma)}\,(\vee')}{((\alpha\wedge\neg\beta)\vee(\beta\wedge\neg\gamma))\vee(\neg\alpha\vee\gamma)}\,(\vee')$$

□

对命题逻辑的自然推演先暂时介绍到此，在一阶逻辑中会继续这一话题。由于推理规则少了，在系统变得精炼的同时，读者可能会觉得对具体公式的证明反而不那么“自然”了。不过不要紧，在后面讲到一阶逻辑的自然推演系统的完全性定理时，会给出寻找证明的系统方法。那时大家就能体会自然推演自然在哪里。

习题 2.7

2.7.1 用自然推演证明以前的公理 (A1)，(A2) 和 (A3)。

2.7.2 用自然推演证明习题 2.6 中的公式。

2.8 命题逻辑的可靠性和完全性定理

我们已经分别研究了“硬币的两面”，即语法和语义。现在要将它们统一起来，研究两者之间的联系。

定理 2.8.1（可靠性定理） 对任意公式集 Σ、任意公式 α，如果 $\Sigma \vdash \alpha$，则 $\Sigma \vDash \alpha$。特别地，如果 $\vdash \alpha$，则 $\vDash \alpha$，换言之，$\mathscr{L}$ 的每一个内定理都是重言式。

证明 首先请读者自行验证每一个 (A1)，(A2) 和 (A3) 中的公理都是重言式。

假定 $\Sigma \vdash \alpha$，固定一个从 Σ 到 α 的一个推演序列 $(\beta_1, \beta_2, \cdots, \beta_n)$，其中，$\beta_n = \alpha$。令 v 为一个任意的满足 Σ 内所有公式的真值指派。对 i 施行强归纳来证明：对任何 $1 \leq i \leq n$，v 都满足 β_i。

假设 v 满足所有的 β_k $(k < i)$，可以证明 v 满足 β_i。考察 β_i 的所有 3 种可能性：如果 β_i 是逻辑公理，则它是重言式；如果它是 Σ 中的一员，则根据对 v 的假设，v 都满足 α_i；如果 β_i 是从 α_j 和 $\alpha_k = \alpha_j \to \alpha_i$ 经分离规则得到的，其中 $j, k < i$，则根据归纳假设，v 满足 α_j 和 α_k，因而 v 也满足 α_i。

根据归纳法，v 满足 α_n，即 v 满足 α。 □

可靠性定理的逆命题被称为**完全性定理**，其证明要复杂得多。从前面的练习里大家也有体会，想寻找合适的证明并不是那么容易。

定理 2.8.2（完全性定理）　如果 $\Sigma \vDash \alpha$ 则 $\Sigma \vdash \alpha$。

下面先引入一致性和可满足性的概念，然后用它们给出完全性定理的一个等价形式。之后再证明完全性定理的这个等价形式。注意：后面对一阶逻辑完全性定理的证明也利用了类似的想法。

定义 2.8.3　称一个公式集 Σ 是**不一致的**（或**矛盾的**），如果存在某个公式 α，使得 $\Sigma \vdash \alpha$ 并且 $\Sigma \vdash \neg\alpha$。称 Σ 是**一致的**，如果它不是不一致的。

引理 2.8.4　公式集 Σ 是不一致的当且仅当对所有的公式 α，$\Sigma \vdash \alpha$。

证明　见习题 2.8。 □

引理 2.8.5　$\Sigma \vdash \alpha$ 当且仅当 $\Sigma \cup \{\neg\alpha\}$ 不一致。

证明　($\Rightarrow$) 如果 $\Sigma \vdash \alpha$，则添上任何公式（如 $\neg\alpha$）后，依然有 $\Sigma \cup \{\neg\alpha\} \vdash \alpha$。另一方面，显然有 $\Sigma \cup \{\neg\alpha\} \vdash \neg\alpha$。所以 $\Sigma \cup \{\neg\alpha\}$ 不一致。

($\Leftarrow$) 假设 $\Sigma \cup \{\neg\alpha\}$ 不一致，则根据引理 2.8.4，$\Sigma \cup \{\neg\alpha\} \vdash \alpha$。所以，$\Sigma \vdash \neg\alpha \to \alpha$。再据公理 (A3)：

$$\vdash (\neg\alpha \to \neg\alpha) \to (\neg\alpha \to \alpha) \to \alpha,$$

即可得出 $\Sigma \vdash \alpha$。 □

定义 2.8.6　称公式集 Σ 为**可满足的**，如果存在一个真值指派满足 Σ 中的所有公式；称 Σ 为 **不可满足的**，如果 Σ 不是可满足的。

有了这些概念之后就可以给出完全性定理的一个等价叙述。

引理 2.8.7 下列命题等价：

(1) 如果 Σ 一致，则 Σ 可满足；

(2) 如果 $\Sigma \vDash \alpha$，则 $\Sigma \vdash \alpha$。

证明 “(1) $\Rightarrow$ (2)”。假定 (1) 成立，并且前提 $\Sigma \vDash \alpha$ 也成立，我们用反证法证 $\Sigma \vdash \alpha$。如果 $\Sigma \nvdash \alpha$，则根据引理2.8.5，$\Sigma \cup \{\neg\alpha\}$ 是一致的。由 (1) 它就可满足，不妨设被真值指派 v 所满足。一方面，有 $\bar{v}(\neg\alpha) = T$；而另一方面，又有 $\bar{v}(\alpha) = T$，因为 $\Sigma \vDash \alpha$ 并且 v 满足 Σ 内所有的公式。矛盾。

“(2) $\Rightarrow$ (1)”。假定 (2) 成立，并且前提 Σ 一致也成立，可以用反证法证明 Σ 是可满足的。如果 Σ 不可满足，则对任意公式 α 都有 $\Sigma \vDash \alpha$。（为什么？）根据 (2)，就有对所有公式 α，$\Sigma \vdash \alpha$，说明 Σ 不一致，矛盾。 □

这样，就把对完全性定理的证明转化为对其等价命题——引理 2.8.7(1) 的证明。称一个公式集 Δ 为**极大一致的**，如果 Δ 一致，并且对任何不在 Δ 中的公式 α, $\Delta \cup \{\alpha\}$ 不一致。

引理 2.8.8（林登鲍姆[①]引理） 每一个一致的公式集 Σ 都可以扩张成一个极大一致集 Δ。

证明 固定一个全体公式的枚举 $\alpha_1, \alpha_2, \cdots$。递归地定义一个公式集的序列 $\{\Delta_n\}_{n\in\mathbb{N}}$ 如下：

$$\begin{aligned} \Delta_0 &= \Sigma; \\ \Delta_{n+1} &= \begin{cases} \Delta_n \cup \{\alpha_{n+1}\}, & \text{如果 } \Delta_n \cup \{\alpha_{n+1}\} \text{ 一致}, \\ \Delta_n \cup \{\neg\alpha_{n+1}\}, & \text{如果 } \Delta_n \cup \{\alpha_{n+1}\} \text{ 不一致}, \end{cases} \end{aligned}$$

不难验证，对每一个 n，公式集 Δ_n 都一致（见习题2.8.2）。

令 Δ 为 $\bigcup_{n\in\mathbb{N}} \Delta_n$，则 $\Sigma \subseteq \Delta$。接下来验证 Δ 为极大一致集。如果 Δ 不一致，则存在 β，$\Delta \vdash \beta \wedge \neg\beta$。而这又意味着存在 Δ 的一个有穷子集 Δ'，$\Delta' \vdash \beta \wedge \neg\beta$。根据 Δ 的定义，这个 Δ' 一定包含在某个 Δ_n 之中，因此这个 Δ_n 也不一致，与所有 Δ_n 一致相矛盾。

其次，根据 Δ 的构造，对任意公式 α，如果 $\alpha \notin \Delta$，则 $\neg\alpha \in \Delta$，所以 $\Delta \cup \{\alpha\}$ 不一致，因而 Δ 是极大一致集。 □

最后，让我们从语法返回到语义。

① 林登鲍姆（Adolf Lindenbaum，1904—1941），波兰逻辑学家、数学家。

引理 2.8.9　任何极大一致集 Δ 都是可满足的。事实上，定义真值指派 v，使得对任意命题符号 A_i，$v(A_i)=T$ 当且仅当 $A_i\in\Delta$，则 v 满足 Δ 中的所有公式。

证明　对 α 施行归纳来证明 $\bar{v}(\alpha)=T$ 当且仅当 $\alpha\in\Delta$（见习题 2.8.3）。□

将引理 2.8.9 与林登鲍姆引理结合起来就有：任何一致集都是可满足的。这就完成了对完全性定理的证明。

从上述证明中难以看出语义（真值表）和语法（证明）的直接联系。为此，下面重新证明完全性定理的一个弱形式：如果 $\vDash\alpha$，则 $\vdash\alpha$。这个证明有两点好处。

一是有更强的构造性，原则上可以直接把重言式的真值表转化成证明；二是间接提供一些公理挑选的信息。对初学者来说，为什么选 (A1)，(A2) 和 (A3) 作公理像是个魔术，但这个魔术背后并没有太多秘密：选取公理的目的是为了证明完全性的需要。这个新证明告诉我们哪些公式是证明完全性所必需的。有了这个大的并且足以证明完全性的公式范围之后，就可以进一步地剔除冗余的公式，或用更简练的公式来替代，从中选取我们想要的公理集。

下面先罗列几个证明中会用到的事实：

(1) 如果 $\Gamma\vdash\alpha$，则对任何公式 β，都有 $\Gamma\vdash\beta\to\alpha$。（因为 $\alpha\to\beta\to\alpha$ 是公理。）

(2) $\vdash\neg\alpha\to(\alpha\to\beta)$（见习题 2.6）。

(3) 如果 $\Sigma\vdash\alpha$，并且 $\Sigma\vdash\neg\beta$，则 $\Sigma\vdash\neg(\alpha\to\beta)$（利用习题 2.6.2）。

引理 2.8.10　假设 α 为仅包含命题符号 $A_1,\cdots,A_k$ 的一个公式，v 是 $A_1,\cdots,A_k$ 上的一个真值指派。令 A_i' 为 A_i 依照 v 的一个变形：若 $v(A_i)=T$，则 A_i' 为 A_i；否则，A_i' 为 $\neg A_i$。同样指定 α 依照 v 的一个变形 α' 如下：若 $\bar{v}(\alpha)=T$，则 α' 为 α；否则，α' 为 $\neg\alpha$。那么有

$$\{A_1',\cdots,A_k'\}\vdash\alpha'。$$

证明　令 $P(\alpha)$ 表示需要证明的性质被公式 α 满足。用归纳原理证明 $P(\alpha)$ 对所有 α 都成立。为简单起见，不妨将 $\{A_1',\cdots,A_k'\}$ 暂时简记为 Σ，并用 v 代替 $\bar{v}$。

容易看出，对任意命题符号 A_i，$P(A_i)$ 成立。

假定 $P(\alpha)$ 成立。考察 $\beta = \neg\alpha$，可以验证 $P(\beta)$ 也成立。令 v 为一个真值指派。

情形 1：$v(\beta) = T$。则 $v(\alpha) = F$，所以变形 α' 为 $\neg\alpha$。根据归纳假设，$\Sigma \vdash \alpha'$。于是有 $\Sigma \vdash \beta'$，因为 $\beta' = \beta = \neg\alpha = \alpha'$。

情形 2：$v(\beta) = F$。则 $v(\alpha) = T$，所以变形 α' 为 α。根据归纳假设，$\Sigma \vdash \alpha$。又根据习题 2.6.2，有 $\vdash \alpha \to \neg\neg\alpha$。所以 $\Sigma \vdash \beta'$，因为 $\beta' = \neg\neg\alpha$。

假定 $P(\alpha)$ 和 $P(\beta)$ 成立。考察 $\gamma = \alpha \to \beta$，需要验证 $P(\gamma)$ 也成立。令 v 为一个真值指派。有以下 3 种情形。

情形 1：$v(\alpha) = F$。则 $v(\gamma) = T$。根据归纳假设，$\Sigma \vdash \neg\alpha$ 因为 α' 为 $\neg\alpha$。根据罗列的事实 (2) 和分离规则，有 $\Sigma \vdash \alpha \to \beta$，所以 $\Sigma \vdash \gamma'$。

情形 2：$v(\beta) = T$。则 $v(\gamma) = T$。根据归纳假设，$\Sigma \vdash \beta$ 因为 β' 为 β。根据罗列的事实 (1)，有 $\Sigma \vdash \alpha \to \beta$，即 $\Sigma \vdash \gamma'$。

情形 3：$v(\alpha) = T$ 并且 $v(\beta) = F$。则 $v(\gamma) = F$。根据归纳假设，$\Sigma \vdash \alpha$ 并且 $\Sigma \vdash \neg\beta$。根据罗列的事实 (3)，有 $\Sigma \vdash \neg(\alpha \to \beta)$，即 $\Sigma \vdash \gamma'$。 □

定理 2.8.11（完全性定理的弱形式） *如果 $\vDash \alpha$，则 $\vdash \alpha$；换言之，每一个重言式都是 $\mathscr{L}$ 中的内定理。*

证明 （概要）假定 α 是一个重言式并且 $A_1, A_2, \cdots, A_k$ 是 α 中出现的命题符号。根据引理 2.8.10，对任意的真值指派，都有 $\{A'_1, A'_2, \cdots, A'_k\} \vdash \alpha$（因为 α 是重言式，所以 α' 总是 α）。所以 $\{A'_1, A'_2, \cdots, A'_{k-1}, A_k\} \vdash \alpha$，并且 $\{A'_1, A'_2, \cdots, A'_{k-1}, \neg A_k\} \vdash \alpha$。由演绎定理，可以得到 $\{A'_1, A'_2, \cdots, A'_{k-1}\} \vdash A_k \to \alpha$ 以及 $\{A'_1, A'_2, \cdots, A'_{k-1}\} \vdash \neg A_k \to \alpha$。根据习题 2.6.2，

$$\vdash (A_k \to \alpha) \to (\neg A_k \to \alpha) \to \alpha。$$

使用两次分离规则，就有 $\{A'_1, A'_2, \cdots, A'_{k-1}\} \vdash \alpha$。重复上面的论证，可以把命题符号一个个消去，最终得到 $\vdash \alpha$。 □

一旦有了完全性定理，很容易得出下面的紧致性定理。紧致性是拓扑学中的一个概念，逻辑中的紧致性定理可以看成拓扑中紧致性定理的一个特殊情形，但细节超出了本书的范围。在后面的一阶逻辑中，也有紧致性定理，并且会给我们带来许多重要的推论。

定理 2.8.12（紧致性定理） *公式集 Σ 是可满足的当且仅当 Σ 的每一个有穷子集都是可满足的。*

证明　($\Rightarrow$) 显然。因为右边是左边的特殊情况。

($\Leftarrow$) 假定 Σ 的每一个有穷子集都是可满足的，用反证法证明 Σ 也是可满足的。如果 Σ 不可满足，则根据完全性定理，Σ 也不一致。所以，存在公式 α，$\Sigma \vdash \alpha \wedge \neg\alpha$。这又蕴涵存在 Σ 的一个有穷子集 Σ_0，使得 $\Sigma_0 \vdash \alpha \wedge \neg\alpha$。根据可靠性定理，$\Sigma_0 \vDash \alpha \wedge \neg\alpha$，因而 Σ_0 不可满足，与前提矛盾。 □

紧致性定理有许多重要的应用，在一阶逻辑的相关部分会有更多讨论。这里仅举一个不太重要的例子。

例 2.8.13　证明任何集合都可以被线序化，即：对任何一个集合 M，都存在 M 上的一个二元关系 R 满足非自反性、传递性，并且对 M 中的任何两个元素 x 和 y，xRy，$x = y$，yRx 三者有且仅有一个成立。

证明　给定集合 M，指定命题符号集 S 为 $\{p_{ab} : a, b \in M\}$，其脚标为 M 中的有序对。考察 S 的下列公式集 Γ：

$$\begin{aligned}\Gamma &= \{\neg p_{aa} : a \in M\} \cup \{p_{ab} \to p_{bc} \to p_{ac} : a, b, c \in M\} \\ &\cup \{p_{ab} \vee p_{ba} : a, b \in M, a \neq b\},\end{aligned}$$

则 Γ 的任意有穷子集都可满足（请读者自行验证）。根据紧致性定理，Γ 也可满足。任何一个满足 Γ 的真值指派中都给出 M 上的一个线序（自行验证）。 □

结束古典命题逻辑之前，让我们指出如下几点：

• 根据可靠性定理，公理系统 L 所能证明的都是重言式，从而证明了系统 $\mathscr{L}$ 的一致性。可靠性的证明等都是在系统 $\mathscr{L}$ 外进行的，例如，数学归纳法等自然数的性质都是命题逻辑中没有的。这就给我们一个很好的“用数学方法研究逻辑”和“用元逻辑来研究对象逻辑”的例子。

• 命题逻辑的定理集是可判定的，即存在一个算法（或计算机程序），能够告诉我们公式 α 是否是 $\mathscr{L}$ 中的一个定理。这个算法就是通过列真值表来判断 α 是否为重言式。这样的算法对一阶逻辑系统不存在，即：一阶逻辑是不可判定的。这是命题逻辑和一阶逻辑的一个重要区别。

• 尽管有算法来判定一个命题逻辑的公式 α 是否是重言式或是否可满足，但列真值表的算法效率很低，是所谓指数时间算法。计算机科学中的一个重要的尚未解决的问题是所谓“P 是否等于 NP”的问题，即有没有多项式时间算法来判定一个公式的可满足性。参见 http://www.claymath.org/millennium-problems/p-vs-np-problem。

习题 2.8

2.8.1 证明引理 2.8.4，即：公式集 Σ 是不一致的当且仅当对所有的公式 β，$\Sigma \vdash \beta$。

2.8.2 假定公式集 Σ 一致，证明对任意公式 α，$\Sigma \cup \{\alpha\}$ 与 $\Sigma \cup \{\neg\alpha\}$ 中有一个一致。（这是林登鲍姆引理证明的一部分。）

2.8.3 假定 Δ 为一个极大一致集。定义真值指派 v 如下：对任意命题符号 A，

$$v(A) = \begin{cases} T, & \text{如果 } A \in \Delta; \\ F, & \text{如果 } A \notin \Delta。 \end{cases}$$

证明对任意公式 α，$\overline{v}(\alpha) = T$ 当且仅当 $\alpha \in \Delta$。（这是引理 2.8.9，因而也是完全性定理证明的一部分。）

2.8.4 证明从可靠性和完全性定理的弱形式（$\vDash \alpha$ 当且仅当 $\vdash \alpha$）以及紧致性定理，可以证明可靠性和完全性定理的一般形式（$\Gamma \vDash \alpha$ 当且仅当 $\Gamma \vdash \alpha$）。

2.8.5 （独立性证明）证明某些公理 (A1) 的实例不能由公理 (A2) 和 (A3) 导出。【**提示**：考虑表2.3。证明所有 (A2) 和 (A3) 的逻辑推论都永远取值 0。】

表 2.3　独立性证明

A	$\neg A$	A	B	$A \to B$
0	1	0	0	0
1	1	1	0	2
2	0	2	0	0
		0	1	2
		1	1	2
		2	1	0
		0	2	2
		1	2	0
		2	2	0

2.8.6 $\alpha \to \alpha$ 可以仅用公理 (A2) 和 (A3) 证明吗?

2.8.7 证明皮尔士定律

$$(((p \to q) \to p) \to p)$$

不能从公理组 (A1) 和 (A2) 中导出。

2.8.8 令 $\mathcal{L}_1$ 为仅包含联词 $\to$ 的命题逻辑语言；并且 $\mathscr{L}_1$ 是语言 $\mathcal{L}_1$ 上的一个证明系统，$\mathscr{L}_1$ 的公理为 (A1), (A2) 和皮尔士定律，推理规则仍只有一条分离规则。用 $\vdash_1 \alpha$ 表示 α 是系统 $\mathscr{L}_1$ 的一个内定理。证明：$\vdash_1$ 是完全的，即如果 $\mathcal{L}_1$ 中的公式 α 是重言式，则 $\vdash_1 \alpha$。

【**提示**：可以重新定义“极大一致集”的概念，并且模仿定理 2.8.2 的证明。更进一步，称一个公式集 Γ 为 α-极大的，如果 $\Gamma \nvdash_1 \alpha$，并且对所有的 $\beta \notin \Gamma$，$\Gamma \cup \{\beta\} \vdash_1 \alpha$。可以先证明每一个 α-极大的公式集都是“极大一致”的。】

2.9　模态逻辑简介

古典命题逻辑中研究的联词可以说是从数学文献中提炼出来的。为了更好地反映研究日常语言的丰富性，人们往往在逻辑中也添加对模态动词进行修饰的成分，如“必然”、“可能”、“应该”、“从前”、“将来”等。这就把我们引导到模态逻辑（包括时态逻辑）的范畴。对模态逻辑的研究最早可以追溯到亚里士多德，但对模态形式系统的研究恐怕要归功于刘易斯[①]。由于模态逻辑的范围太广泛了，下面仅谈论模态逻辑中命题逻辑的很小一部分，可以说是简而又简的简介。

本节的目的有两个：一是模态逻辑的丰富性使得它成为哲学逻辑的热门领域，值得我们花些时间哪怕是粗略地看一下；二是介绍可能世界语义学，它是 1959 年由克里普克[②]引进的，当时他年仅 19 岁。可能世界语义学不仅适用于模态逻辑，也适用于直觉主义逻辑等其他逻辑。这一节的内容与后面一阶逻辑是独立的，即使大家暂时略过，也不会影响后面的学习。在本节中，模态逻辑指的都是只含有一个模态算子的模态命题逻辑。

基本的模态逻辑的语言比古典命题逻辑的语言（见2.2节）仅仅多一个一元联词 $\Box$，也称为**模态算子**。为了简单起见，假定联词只有 $\neg, \to$ 和 $\Box$。合式公式的形成规则也是在前面的规则中添上下面这条：

- 如果 α 是一个合式公式，则 $(\Box\alpha)$ 也是。

我们很容易得到类似的唯一可读性定理。也沿用前面关于括号省略的约定。就 $\Box$ 而言，同样假定它的“管辖范围”尽可能短。举例来说，$\Box p \to \Box q$ 指的是 $((\Box p) \to (\Box q))$。

① 刘易斯（Clarence Irving Lewis，1883—1964），美国逻辑学家、哲学家。

② 克里普克（Saul Kripke，1940—　），美国逻辑学家、哲学家。

接下来，引进一元联词 $\Diamond$ 作为 $\Box$ 的对偶：对任意公式 α，定义

$$\Diamond\alpha = \neg\Box\neg\alpha,$$

并且约定它的管辖范围也是尽可能短。

联词 $\Box$ 和 $\Diamond$ 通常被分别解释成“必然”和“可能”。但也有其他诸多解释，仅举两例如下：

(1) 可以把 $\Box$ 和 $\Diamond$ 分别解释成“已经知道”和“不与目前所知矛盾”。

(2) 也可以把 $\Box$ 和 $\Diamond$ 分别解释成道义上的“应该”和“允许”。

自然地，对模态算子 $\Box$ 的解释不同，会导致对模态公式的真假判断和模态推理规则的选取的不同。因而就有不同的模态语义和推理系统。本书只介绍克里普克语义和推理系统 K。它们可以说是最简单且适用范围最广的语义和语法系统。

2.9.1 克里普克的可能世界语义学

定义 2.9.1

(1) 称一个二元组 $F = (W, R)$ 为一个**框架**，如果 W 为一个非空集合并且 R 为 W 上的一个二元关系；

(2) 称一个从命题符号的集合到 W 的幂集的一个映射 V 为一个**赋值**；

(3) 称一个由框架和赋值形成的二元组 $M = (F, V)$ 为一个（**克里普克**）**模型**。模型 M 也常被写作 $M = (W, R, V)$。

沿用克里普克本人的解释，人们习惯上称 W 中的元素为一个**可能世界**或**世界**；并且称 xRy 为**从** x **可以通达** y（甚至可以更富有暗示性地读作“y 是 x 的一个将来世界”，尽管这种暗示有它的片面性）；对每个命题符号 A，赋值 V 指派给 A 的集合 $V(A)$ 就是那些 A 在其中成立的可能世界的集合。

在实际应用中，如果只关心涉及命题符号（比方说）A, B, C 的模态公式，那么只需考虑赋值 V 在 A, B, C 上的定义就可以了，这一点是很自然的。

定义 2.9.2 归纳地定义一个模态公式 α 在**模型** M **中的世界** w **中为真**，记作 $(M, w) \vDash \alpha$，

(1) 对命题符号 A_i，$(M, w) \vDash A_i$，当且仅当 $w \in V(A_i)$；

(2) $(M,w)\vDash(\neg\beta)$，当且仅当 $(M,w)\nvDash\beta$（即：$(M,w)\vDash\beta$ 不成立）；

(3) $(M,w)\vDash(\beta\to\gamma)$，当且仅当 $(M,w)\nvDash\beta$ 或者 $(M,w)\vDash\gamma$；

(4) $(M,w)\vDash\Box\beta$，当且仅当对任意的 $w'\in W$，如果 Rww'，则 $(M,w')\vDash\beta$。

自然地，如果 $(M,w)\nvDash\alpha$，则称 α **在模型** M **中的世界** w **中为假**。

定义 2.9.3　称 α 在**模型** $M=(W,R,V)$ **中有效**，记作 $M\vDash\alpha$，如果对所有的 $w\in W$ 都有 $(M,w)\vDash\alpha$。

例 2.9.4　考虑框架 $F=(W,R)$（见图2.1），其中 $W=\{u,v,w\}$，$R=\{(u,v),(u,w)\}$：定义赋值 $V:\{A,B\}\to\mathcal{P}(W)$ 为 $V(A)=\{u,v\}$

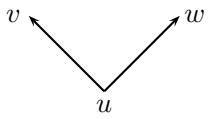

图 2.1　框架 $F=(W,R)$ 示意

和 $V(B)=\{v\}$，即：A 在世界 u,v 中成立，且 B 仅在世界 v 中成立。则 $(M,u)\vDash\Box(A\to B)$ 但 $(M,u)\nvDash A\to\Box B$。（为什么？）

定义 2.9.5　称 α 为**普遍有效**的，记作 $\vDash\alpha$，如果对所有的模型 M，都有 $M\vDash\alpha$。

例 2.9.6　证明：$\vDash\Box(\alpha\to\beta)\to(\Box\alpha\to\Box\beta)$。

证明　给定模型 $M=(W,R,V)$ 和世界 $w\in W$，验证

$$(M,w)\vDash\Box(\alpha\to\beta)\to(\Box\alpha\to\Box\beta)。$$

如果 $(M,w)\nvDash\Box(\alpha\to\beta)$，则引用定义 2.9.2 中 (3) 即可。这一点与古典命题逻辑相同。因此可以假定 $(M,w)\vDash\Box(\alpha\to\beta)$，并证明 $(M,w)\vDash\Box\alpha\to\Box\beta$。同理，只需在 $(M,w)\vDash\Box(\alpha\to\beta)$ 且 $(M,w)\vDash\Box\alpha$ 的假定下，证明 $(M,w)\vDash\Box\beta$ 即可。

验证定义 2.9.2 中的 (4)：给定任意满足 Rww' 的世界 w'，根据假定，有 $(M,w')\vDash\alpha\to\beta$ 和 $(M,w')\vDash\alpha$，所以 $(M,w')\vDash\beta$。因此 $(M,w)\vDash\Box\beta$。□

2.9.2 模态逻辑的一个推理系统 K

将 2.6 节引入的古典命题逻辑的推理系统进行如下的扩张。首先，在 (A1)，(A2)，(A3) 这 3 组公理之上新添公理

$$K : \Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)。$$

注意：不仅在 K 中，而且在 (A1)，(A2)，(A3) 中，都允许将 α, β, γ 被任何的模态公式替换。

其次，在原有的分离规则之上新添**必然化规则** RN[①]：从 α 可以得到 $\Box\alpha$。我们把 α 是**系统 K 中的内定理**（记作 $\vdash_K \alpha$）的定义留给读者练习。自然地，也可以类似地定义 $\Gamma \vdash_K \alpha$。

注意：由于系统 K 增加了必然化规则，演绎定理不一定成立。例如，$\alpha \vdash_K \Box\alpha$，但 $\alpha \to \Box\alpha$ 未必是系统 K 的内定理。

由于 K 是古典命题逻辑推演系统 L 的一个扩张，因此 K 自然可以证明所有的重言式。但这里需要澄清在模态语言中重言式的概念。首先把所有的命题符号和形如 $(\Box\alpha)$ 的模态公式全部列出来：$\beta_1, \beta_2, \cdots$，并且给它们中的每一个都指派一个新的命题符号，例如，用 B_i 代表 β_i。这样，每个模态公式都成为关于命题符号 B_i 的古典公式。例如，假定 A_3 和 $\Box\Box(A_1 \to \Box A_2)$ 分别是 B_5 和 B_{29}，则模态公式 $A_3 \to (\neg A_3) \to \Box\Box(A_1 \to \Box A_2)$ 就是 $B_5 \to \neg B_5 \to B_{29}$。称一个模态公式为一个（模态的）**重言式**，如果经过上述变换后得到的关于 B_i 的公式是古典意义下的重言式。下面的事实会给我们带来很大的方便：

引理 2.9.7 *如果 α 是一个模态的重言式，则 $\vdash_K \alpha$。*

证明概述 令 α' 为 α 经上述变换后所得到的古典公式。首先根据古典命题逻辑的完全性，可以在古典命题逻辑中证明 α'。只要将古典证明序列中每一个 B_i 再代换为 β_i，即可得到 α 在系统 K 中的证明。 □

引理 2.9.8 *如果 $\{\alpha : \Box\alpha \in \Gamma\} \vdash_K \beta$，则 $\Gamma \vdash_K \Box\beta$。*

证明 留给读者练习。 □

仿照古典命题逻辑中的做法，定义 Γ 是一个K- **极大一致集**。如果 Γ 是 K-一致的（定义留给读者练习），且对于任意模态公式 α，或者 $\alpha \in \Gamma$ 或者 $\neg\alpha \in \Gamma$。注意：同古典逻辑一样，K-极大一致集 Γ 对 K 中的推理是封闭的，即：如果 $\Gamma \vdash_K \alpha$，则 $\alpha \in \Gamma$。而且模态逻辑 K 也有相应的林登鲍姆引理：任

① 必然化规则，英文为 rule of necessitation。

何一个 K-一致的公式集都可以扩张成一个 K- 极大一致集。下面的定理在后面证明完全性的时候会起到关键的作用。

定理 2.9.9　假定 Γ 为一个 K-极大一致集。则 $\Box\beta \in \Gamma$ 当且仅当对每个满足 $\{\alpha : \Box\alpha \in \Gamma\} \subseteq \Delta$ 的 K-极大一致集 Δ, β 都属于 Δ。

证明　($\Rightarrow$) 假定 $\Box\beta \in \Gamma$。考察集合 $\Sigma = \{\alpha : \Box\alpha \in \Gamma\}$。根据 Σ 的定义，显然 $\beta \in \Sigma$。所以对于任何包含 Σ 的集合 Δ（无论是不是 K- 极大一致集），β 都属于 Δ。

($\Leftarrow$) 固定 β 和 Γ。仍旧考察集合 $\Sigma = \{\alpha : \Box\alpha \in \Gamma\}$。

断言：$\Sigma \vdash_K \beta$。不然的话，即 $\Sigma \nvdash_K \beta$；则 $\Sigma \cup \{\neg\beta\}$ 是 K-一致的。根据林登鲍姆引理，可以将 $\Sigma \cup \{\neg\beta\}$ 扩张成一个 K-极大一致集 Δ。而根据假设，$\beta \in \Delta$，这与 Δ 的 K-一致性矛盾。因此断言成立。

现在应用引理 2.9.8，有 $\Gamma \vdash_K \Box\beta$，而作为 K-极大一致集，Γ 对 K 中的推理封闭。所以 $\Box\beta \in \Gamma$。　□

2.9.3　系统 K 的可靠性和完全性

由于是简介，这里只讨论可靠性和完全性的弱形式。

定理 2.9.10（模态逻辑 K 的可靠性定理）　如果 $\vdash_K \alpha$，则 α 是普遍有效的。

证明　留给读者练习。　□

定理 2.9.11（模态逻辑 K 的完全性定理）　如果 $\vDash \alpha$，则 $\vdash_K \alpha$。

这里仍旧模仿古典命题逻辑中的做法，试图证明：如果 $\nvdash_K \alpha$，则找到一个模型 M 和世界 w，使得 $(M, w) \nVdash \alpha$。但在模态逻辑中，可以有更强的结论：可以找到一个模型 $M = (W, R, V)$，使得对任意 α，如果 $\nvdash_K \alpha$，则存在一个世界 $w \in W$，使得 $(M, w) \nVdash \alpha$。这个能够给所有的非定理提供“反例”的模型称为**典范模型**。

定义 2.9.12　定义模态逻辑 K 的**典范模型** $M = (W, R, V)$ 如下：$W = \{\Gamma : \Gamma$ 是一个 K- 极大一致集 $\}$；$(\Gamma, \Gamma') \in R$ 当且仅当 $\{\alpha : \Box\alpha \in \Gamma\} \subseteq \Gamma'$；$V(A_i) = \{\Gamma \in W : A_i \in \Gamma\}$。

引理 2.9.13　令 $M = (W, R, V)$ 为模态逻辑 K 的典范模型。则对任意的模态公式 α，对任意的 $\Gamma \in W$，有 $(M, \Gamma) \vDash \alpha$ 当且仅当 $\alpha \in \Gamma$。

证明 对模态公式 α 进行归纳。

先看 α 为命题符号 A_i 的初始情形：根据定义 2.9.2，$(M,\Gamma)\vDash A_i$ 当且仅当 $\Gamma\in V(A_i)$。再根据 V 的定义，$\Gamma\in V(A_i)$ 当且仅当 $A_i\in\Gamma$。引理成立。

再看归纳情形。

情形 1：α 为 $\neg\beta$。根据定义 2.9.2，$(M,\Gamma)\vDash\neg\beta$ 当且仅当 $(M,\Gamma)\nvDash\beta$。根据归纳假设，后者成立当且仅当 $\beta\notin\Gamma$，再根据 K-极大一致性，就得到引理所要的结论。

情形 2：α 为 $\beta\to\gamma$。这一条的验证留给读者练习。

情形 3：α 为 $\Box\beta$。假定 $(M,\Gamma)\vDash\Box\beta$。根据定义 2.9.2，对任意的 $\Delta\in W$，如果 $(\Gamma,\Delta)\in R$，则 $(M,\Delta)\vDash\beta$；对 β 和 Δ 使用归纳假定，有 $\beta\in\Delta$。再将 $(\Gamma,\Delta)\in R$ 按 R 的定义展开：对任意的 $\Delta\in W$，如果 $\{\alpha:\Box\alpha\in\Gamma\}\subseteq\Delta$，则 $\beta\in\Delta$。由定理 2.9.9，$\Box\beta\in\Gamma$。反过来，假如 $\Box\beta\in\Gamma$，则由定理 2.9.9 和 R 的定义，对任意的 $\Delta\in W$，如果 $(\Gamma,\Delta)\in R$，则 $\beta\in\Delta$。由归纳假设，$(M,\Delta)\vDash\beta$。所以 $(M,\Gamma)\vDash\Box\beta$。

这就完成了对引理的证明。 □

最后来证明定理 2.9.11。假如 $\nvdash_K\alpha$，则 $\{\neg\alpha\}$ 是 K-一致的。将其扩张成一个 K-极大一致集 Γ。考察典范模型 $M=(W,R,V)$ 中的世界 Γ。显然 $\alpha\notin\Gamma$。根据引理 2.9.13，$(M,\Gamma)\nvDash\alpha$，所以 $\nvDash\alpha$。

习题 2.9

2.9.1 给出一个模型 $M=(W,R,V)$ 和世界 $u\in W$，使得 $(M,u)\vDash A\to\Box B$ 但 $(M,u)\nvDash\Box(A\to B)$。

2.9.2 判断下列陈述的正确性并给出理由：

(1) $(M,w)\nvDash\alpha$ 当且仅当 $(M,w)\vDash\neg\alpha$；

(2) $M\nvDash\alpha$ 当且仅当 $M\vDash\neg\alpha$。

2.9.3 在 K 中证明下列公式：

(1) $\Box(\alpha\wedge\beta)\to(\Box\alpha\wedge\Box\beta)$；

(2) $(\Diamond\alpha\vee\Diamond\beta)\to\Diamond(\alpha\vee\beta)$。

【**注意**：虽然书中没有正式引入 $\wedge$ 和 $\vee$，但根据引理 2.9.7 可以使用任何关于 $\wedge$ 和 $\vee$ 的古典重言式。】

2.9.4 证明下列公式不是普遍有效的：

(1) $\Box(\alpha \vee \beta) \to (\Box\alpha \vee \Box\beta)$；

(2) $(\Diamond\alpha \wedge \Diamond\beta) \to \Diamond(\alpha \wedge \beta)$。

2.9.5 证明引理 2.9.8。

2.9.6 证明系统 K 的可靠性定理。

2.9.7 证明：给定框架 (W, R)，关系 R 是自反的，当且仅当对任意赋值 V 和任意公式 α，$\Box\alpha \to \alpha$ 都在模型 $M = (W, R, V)$ 中真。【**注意：**本题只是模态逻辑中大量类似对应中的一个。】