数理逻辑导论

郝兆宽，杨跃

2012

录

第一章　引言：什么是数理逻辑？

就字面意思而言，“数理逻辑”可以有两种读法。一是以数学为工具来研究逻辑；二是研究数学里面出现的或是数学家常用的逻辑。这两种解读都有一定的道理。先看第一种：我们的确频繁地使用数学工具，如数学归纳法，或紧致性定理等等；并且我们的研究成果（所下的结论）都是以数学定理的形式体现的。从这一角度来看与用数学来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。再看第二种解读：我们研究的论域或所举的例子大多是从数学中来的。为什么不举日常生活里的例子呢？比如法学中，语言学中不是也有很多生动有趣的逻辑实例吗？回答是日常生活的世界有穷，数学世界无穷；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”。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”，就是把数学语句、数学结构、数学证明等等作为数学对象，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，比如，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。然而给数理逻辑下一个滴水不漏的定义几乎是不可能的，对本课程来说也是不必要的。下面我们简单介绍数理逻辑发展的历史和数理逻辑的几个重要分支，一方面让大家对数理逻辑有更多的了解，另一方面也说明数理逻辑与哲学的密切关系。

第一节　逻辑史上的几个重要里程碑

亚里士多德[2]

亚里士多德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它各种形式推理，逻辑学代表作为《工具论[3]》。之后的千多年中，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[4]曾经说过：“... 从亚里士多德以

[1]沙拉赫（Saharon Shelah, 1945 - ），以色列逻辑学家，数学家。
[2]亚里士多德，Aristotle（公元前 384 - 公元前 322），古希腊哲学家。
[3]工具论，Organon。
[4]康德，Immanuel Kant（1724 - 1804）德国哲学家。

来，它[逻辑]没能前进一步，因此它显然是尽善尽美了。”亚里士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等概念。

莱布尼茨[5]

在人类文明史上，莱布尼茨是可以与文艺复兴时代的巨匠们相提并论的一位大师。他26 岁时的工作使他与牛顿 [6] 共享发明微积分的荣誉。在逻辑史上，他被称为数理逻辑之父。他有一个伟大的设想，试图建立一个能够涵盖所有人类思维活动的“通用符号演算系统”，让人们的思维方式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，人们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“莱布尼茨的梦想”。但是，莱布尼茨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的涉及到数学工具。

布尔[7]

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。粗略地说，布尔把逻辑中对真假的判断变成了代数中符号的演算。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[8]

弗雷格一生致力于数学基础的研究，试图实现把数学当成逻辑的一个分支这一逻辑主义纲领。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。我们将要学习的谓词演算很大程度上归功于他，比如，量词的引进。当他快要成功的时候，罗素[9]于 1902 年写信给他：“只有一点我遇到些困难...”

说到这里，我们需要涉及一点点数学史，尤其是十九世纪末二十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[10] 已经有了近似于现代定积分的概念。到了十七世纪，牛顿和莱布尼茨独立发明了微积分。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。比如莱布尼茨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，其后二百多年也一直不被人接受。 [11] 尽管如此，牛顿和莱布尼茨的直观是完全与物理世界吻合的，微积分理论也获得了巨大成功。直到十九世纪，柯

[5] 莱布尼茨，Gottfried Leibniz（1646 - 1716），德国数学家，哲学家。
[6] 牛顿，Issac Newton （1642 - 1727），英国物理学家，数学家。
[7] 布尔，George Boole（1815 - 1864），英国逻辑学家，数学家。
[8] 弗雷格，Gottlob Frege（1848 - 1925），德国逻辑学家，哲学家。
[9] 罗素，Bertrand Russell （1872 - 1970），英国逻辑学家，哲学家。
[10] 阿基米德，Archimedes （公元前 287 - 公元前 212），古希腊数学家，物理学家。
[11] 亚 • 罗宾逊 [Abraham Robinson （1918 - 1974），美国逻辑学家，数学家。] 用模型论的方法，在 1960 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。

西[12] 和魏尔斯特拉斯[13]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，微积分中的最根本的概念“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[14]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茨当年梦想的通用语言？也许整个数学（甚至整个科学，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。

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我们这里不提。在二十世纪初，有很多与罗素悖论类似的其它悖论。这些悖论的共同点是它们都涉及非常大的集体。这些悖论让人们怀疑我们是否越过了我们能力的极限，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感觉了。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。当中比较极端的主张是以布劳威尔[15]为代表的直觉主义。直觉主义者只承认潜无穷，对无穷（起码对不可数的无穷）持完全否定的态度。这样一来，数学里面绝大部分内容都被摒弃掉了。康托尔的集合论也就失去意义了。

希尔伯特[16]

希尔伯特是对二十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驱逐出去”。在二十世纪初，他提出了希尔伯特纲领，期望一劳永逸地为数学奠定坚实的基础。纲领大致如下：首先分离出数学中的大家公认的手段，即本质上是有穷的数学证明。对于有争议的涉及无穷的命题，暂时不去考虑它们的意义，而只是看成机械的推导。或者说暂时把语义和语法分开，只研究语法部分。这样一来，如何保证证明系统是一致的[17]就成为头等重要的了。希尔伯特期望足够强的形式系统本身能够证明它自身的一致性，而且只使用本质上有穷的数学去证明全部数学的一致性。

哥德尔[18]

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（这将是本课程主要内容之一）、一阶算术的不完全性定理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，而且很多是开创性的，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

[12] 柯西，Augustin-Louis Cauchy（1789 - 1857），法国数学家。
[13] 魏尔斯特拉斯，Karl Weierstrass （1815 - 1897），德国数学家。
[14] 康托尔，Georg Cantor （1845 - 1918），德国数学家。
[15] 布劳威尔，L. E. J. Brouwer （1881 - 1966），荷兰数学家，哲学家。
[16] 希尔伯特，David Hilbert（1862 - 1943），德国数学家。
[17] 一致的，英文为 consistent，中文还有“无矛盾的”、“协调的”和“和谐的”等几种常见译法。本讲义把它译作“一致的”。
[18] 哥德尔，Kurt Gödel （1906 - 1978），奥地利和美国逻辑学家，数学家和哲学家。

个重要的原因就是它彻底否定了希尔伯特纲领。假设皮亚诺公理系统 PA[19] 代表经典数论的形式化系统，按照希尔伯特纲领的要求，我们必须从 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。以后的发展请看下一节。

第二节　数理逻辑的几个重要分支

哥德尔的工作完全改变了数理逻辑的面貌。人们不再追求完美无瑕的逻辑体系。集合论公理化的成功也使得悖论不再是逻辑发展的主要动力。相反地，逻辑学研究更注重探讨逻辑方法和数学工具的局限。下面我们按照数理逻辑的几个主要分支简单介绍一下 1930 年代后数理逻辑的发展。平时人们在谈论数理逻辑的内容时，在不同的场合“数理逻辑”一词所指的范围会很不一样。有时专指狭义的推理规则和基本的语义，大致上是下面经典逻辑和非经典逻辑之一部分；有时则所指的范围相当宽泛，包括下面提到的几个分支。当然这些分支可以勉强说是从狭义的数理逻辑范围内自然衍生出来的，例如，证明论研究推理规则；模型论研究语义；递归论研究计算，而计算与证明是相通的；集合论则是研究一类与数学基础有关的特殊模型。在简介之后我们还会就这些分支与逻辑的联系做更多的说明。介绍之前，务必请大家注意以下几点：首先是作者知识的局限；二是许多人名和术语缺乏标准译名，因此很多翻译会有些勉强；三是我们也意识到简介中有过多的专门术语，而这些术语显然需要专门的训练才能明白，我们也曾想过放在后记中供有兴趣进一步进修的读者参考，但基于鸟瞰领域全貌的重要性，考虑再三觉得还是放在引言中比较妥当。

经典逻辑和非经典逻辑 数理逻辑的第一个公理系统是弗雷格建立的，但是弗雷格的系统是二阶的。我们下面要学习和掌握的一阶公理系统是由希尔伯特、阿克曼[20]、罗素、怀特海[21]等人逐渐建立起来的。一阶逻辑的真值理论（或称语义系统）则归功于塔尔斯基[22] 1933 年的文章，尽管几乎可以肯定哥德尔在 1933 年之前已经了解塔尔斯基的理论和塔尔斯基关于算术真理不可定义的定理。哥德尔 1930 年的完全性定理标志着一阶逻辑的发展已经成熟。所谓的经典逻辑通常指的就是一阶逻辑的谓词演算。在哥德尔不完全性定理发表之后，人们曾经怀疑是否所有的独立命题都必须用特殊方法构造出来。在连续统假设这样的自然命题被证明为独立于集合论公理系统（见下文）之后，人们仍在寻找有没有独立于皮亚诺算术的“自然的”数论命题。1977 年，帕里斯[23]和哈灵顿[24] 在组合数学中发现了自然的独立于皮亚诺算术的命题。此后人们又陆续在数学其它分支中发现了更多的

[19] 皮亚诺，Giuseppe Peano （1858 - 1932），意大利数学家。皮亚诺公理系统的定义见后文。
[20] 阿克曼，Wilhelm Ackermann （1896 - 1962），德国逻辑学家，数学家。
[21] 怀特海，Alfred North Whitehead （1861 - 1947），英国逻辑学家，哲学家。
[22] 塔尔斯基，Alfred Tarski （1901 - 1983），波兰和美国逻辑学家，数学家。
[23] 帕里斯，Jeff Paris（1944 - ），英国逻辑学家，数学家。
[24] 哈灵顿，Leo Harrington （1946 - ），美国逻辑学家，数学家。

自然的独立于算术或集合论系统的问题，这一方面说明独立性是一个普遍现象，另一方面也促使人们寻找新的公理，因为自然的问题呼唤人们给出明确的答案。

非经典逻辑，顾名思义，包含经典逻辑之外的其它逻辑。由于范围太广，我们只列几个分支。其中有与数学基础相关的直觉主义逻辑、与哲学和认知科学相关的模态逻辑、与计算机科学有关的线性逻辑和时态逻辑等等。每一种逻辑从语言、语法与语义都非常不同，给人们带来了许多新的研究课题。这些逻辑之间，以及它们与哲学、计算机科学和语言学之间都有密切的关系。模态逻辑的参考书有 [1]。

证明论 研究对象为各种形式系统中证明，并分析各种证明的内在结构。证明论的起源与我们前面提到的二十世纪初关于数学基础的争论有很大关系。为了回应布劳威尔和外尔 [25] 等人的批评，希尔伯特提出了所谓希尔伯特纲领（见上文）。他主张数学的概念和概念间的关系是完全由公理所决定的，人们要做的是证明这些公理是一致的；因此需要一门新的学科来研究数学证明，即证明论。希尔伯特的纲领早期获得了部分的成功，人们证明了某些弱形式系统的一致性；哥德尔的完全性定理（本讲义的中心内容）也可以被视为希尔伯特纲领的一个进展。但 1931 年哥德尔的不完全性定理则彻底否定了希尔伯特纲领（见前文）。尽管如此，证明论的发展却没有停止。几乎与哥德尔不完全性定理同时，甘岑[26]利用序型为 ε_0 的良序原理证明了算术系统一致性。注意这与哥德尔定理并无矛盾，因为甘岑的证明严格说不是“有穷主义”的。事实上，甘岑证明了一致性证明中唯一非“有穷主义”的部分恰恰就是序型为 ε_0 的良序原理。甘岑的工作表明，人们可以用序数（如 ε_0）来从证明论角度衡量一个理论的强度，开创了证明论中序数分析 [27] 这一核心分支。在 1960 年代，费夫曼 [28]和舒特 [29]独立地找到了刻画直谓性的序数 Γ_0。其后，竹内外史[30]等人分析了更复杂的非直谓的二阶算术的子系统。序数分析这一分支到现在仍然相当活跃。研究一致性的另一个途径通过解释[31]，起源于哥德尔 1958 年左右的工作，斯佩科特[32] 和克雷塞尔 [33]早期做了重要工作。近年来证明论学家将解释的思想用在数学其它分支，产生了应用证明论这一分支。证明论与其它逻辑分支的联系也非常密切。许多对哲学逻辑学家的工作往往与某种模态逻辑的证明系统有关。有界算术 [34]与理论计算机科学中如 P 是否等于 NP 这样的根本问题是相关的。证明论也是解决问题 P 是否等于 NP 问题的可能途径之一。证明论参考书有 [7]。

模型论 用逻辑方法研究数学结构或模型；或者说通过研究模型的性质来研究数学理

[25] 外尔，Hermann Weyl（1885 - 1955），德国数学家，理论物理学家。
[26] 甘岑，Gerhard Gentzen （1909 - 1945），德国逻辑学家，数学家。
[27] 序数分析， ordinal analysis。
[28] 费夫曼，Solomon Feferman （1928 - ），美国逻辑学家，哲学家。
[29] 舒特，Kurt Schütte （1909 - 1998），德国逻辑学家，数学家。
[30] 竹内外史，Gaisi Takeuti （1925- ），日本逻辑学家，数学家。
[31] 解释， interpretation。
[32] 斯佩科特，Clifford Spector（1930 - 1961），美国逻辑学家，数学家。
[33] 克雷塞尔，Georg Kreisel （1923 - ），生于奥地利，工作于英国和美国，逻辑学家，数学家。
[34] 有界算术，Bounded arithmetic。

论的性质。在本课程中，我们会涉及模型论中早期的几个基本定理，如，哥德尔完全性定理、紧致性定理、勒文海姆[35]-斯寇伦[36]定理等。在数理逻辑的各个分支中，模型论同经典数学的联系最为紧密。从它的发展史上看，模型论的纯理论研究和它在其它数学领域中的应用一直相互交织在一起。例如，上世纪五、六十年代塔尔斯基实闭域[37]上的量词消去定理，及艾克斯-科申 [38] 和叶尔绍夫 [39] 在阿廷猜想 [40]上的成果。在六十年代，亚 • 罗宾逊创立了非标准分析，不仅为古典微积分提供了一个全新的理论基础，也帮助人们发现数学中新的现象和定理。1965 年，莫雷[41]证明了的范畴性定理，给模型论开创了一个全新的方向。莫雷定理及其证明在纯理论研究方面衍生出稳定性理论[42] 和沙拉赫的分类理论[43]。从这些理论中进一步发展出的很多方法和技巧也被用来解决代数及代数几何中的问题，如赫鲁绍夫斯基 [44] 在函数域上面证明了莫代尔-朗猜想 [45] 。另外序极小理论也是模型论中的课题，利用序极小模型中可定义集的良好性质，代数闭域、实数域和其它数学结构中很多新的现象被揭示出来。模型论中还有很多其它的研究领域，如关于皮亚诺算术非标准模型的研究，与计算机科学联系紧密的有限模型论等等。模型论参考书有 [2]。

集合论 是在十九世纪七十年代由康托尔创立的。初期研究对象是集合和属于关系，但把各类无穷称为现代集合论的研究对象似乎更为恰当。因为集合的概念非常简单和自然，但同时却可以描述几乎所有的数学现象，所以从一开始，集合论与数学基础就是不可分割的。然而在十九世纪末，人们发现了大量与集合有关的悖论。对悖论的消解促使公理集合论的建立。其后对数学中某些基本问题（如选择公理和连续统假设）的研究也一直推动集合论的发展。二十世纪三十年代，哥德尔引进了可构成集的类 L 并证明了连续统假设与集合论公理的协调性。哥德尔的证明中使用了大量的逻辑工具，此后集合论的研究几乎离不开逻辑。由于 L 可以算是集合论公理的一个极小模型，哥德尔猜测要想否证连续统假设恐怕需要某种极大的模型。添加各种“大基数”可以被视为向极大性方向的一种努力，因此哥德尔提出了“大基数纲领”。虽然日后的结果表明大基数并未能达到哥德尔预期的目的，但大基数纲领给集合论指出了一个新的方向。1963 年，科恩[46]发明了力迫法并证明了连续统假设的独立性。哥德尔和科恩的工作对现代的集合论研究产生了深远的影响。从哥德尔的 L 发展出了詹森 [47] 的精细结构[48] 理论，和后来包含大基数的内模型理论；

[35] 勒文海姆，Leopold Löwenheim （1878 - 1957），德国数学家。
[36] 斯寇伦，Thoralf Skolem （1887 - 1963），挪威数学家。
[37] 实闭域，real closed fields。
[38] 艾克斯，James Ax (1937 - 2006) 和科申，Simon Kochen （1934 -），都是美国数学家。
[39] 叶尔绍夫，Yuri Ershov（1940 - ）, 俄罗斯逻辑学家，数学家。
[40] 阿廷，Emil Artin （1898 -1962），奥地利和美国数学家。
[41] 莫雷，Michael Morley （1930 - ），美国逻辑学家，数学家。
[42] 稳定性理论，stability theory。
[43] 分类理论，classification theory。
[44] 赫鲁绍夫斯基，Ehud Hrushovski （1959 - ），以色列逻辑学家，数学家。
[45] 莫代尔，Louis Mordell （1888 - 1972），英国数学家；朗，Serge Lang（1927 - 2005），美国数学家。
[46] 科恩， Paul Joseph Cohen（1934 - 2007），美国逻辑学家，数学家。
[47] 詹森，Ronald Jensen （1936 - ），美国逻辑学家，数学家。工作于德国。
[48] 精细结构，Fine structure。

而科恩的力迫法带来了一系列独立性的结果。1970 年代初伊斯顿 [49] 在索洛维 [50] 结果的基础上，用力迫法确定了连续统函数在正则基数上的所有可能取值。但希尔弗 [51] 却证明了同样的方法不适用于奇异基数，所谓奇异基数假设 [52] 问题迄今仍未被解决。此外，以马丁 [53] 、斯蒂尔 [54] 和武丁 [55]，为代表的加州学派在决定性公理，大基数和内模型方面的研究上做了大量工作，例如，马丁和斯蒂尔阐明了投射决定性公理与武丁基数的关系。连续统假设和其它众多的独立性的结果显示出通常集合论公理的不足，也促使人们寻找新公理来决定像连续统假设这类自然但根本的数学问题。集合论学家也在寻找“典范宇宙”[56] 或借用武丁的话，终极的 L [57] 或终极的 V。自从科恩创立了力迫法之后，各种更强的力迫公理也成为集合论研究的对象，沙拉赫的合适力迫公理[58] 以及后来的马丁极大化公理[59]都给集合论带来很多有意义的成果，包括连续统等于 $\aleph_2$，以及图多切维奇[60]在 ω_1 的组合性质上的大量结果（其中既有假定各种力迫公理的，也有不假定任何力迫公理的结果）。集合论的研究方向还包括与经典数学和递归论都有密切联系的描述集合论等等。集合论的工具也被大量应用在集论拓扑、无穷组合和泛函分析等其它数学分支中，其中值得一提的是法拉[61]等人近来在算子代数方面的工作。集合论参考书有 [5]；或 [4]。

递归论 起源于二十世纪三十年代对可判定性的研究。由于直观上的算法概念无法满足研究的需要，哥德尔、丘奇[62]和图灵[63] 等人分别从不同的角度给出了可计算函数类的精确定义，这些定义后来被证明是等价的：直观上的可计算函数可以定义为部分递归函数，也可以定义为图灵（机）可计算函数。递归论即为递归函数论的简称。有了严格的算法定义之后，先后产生了一批不可判定性的结果，例如 1970 年代戴维斯、[64] 普特南、[65] 罗宾逊 [66] 和马蒂亚塞维奇 [67] 成功地解决了希尔伯特第十问题，证明了不存在判定整系数丢番图方程是否有根的一般算法。递归论初期特别值得一提的是 1936 年图灵的经典文章，其中图灵机的概念奠定了现代计算机的基础，文章中还提出了相对可计算的概念，可以对不

[49] 伊斯顿，William Easton，美国逻辑学家，数学家。
[50] 索洛维，Robert Solovay （1938 - ），美国逻辑学家，数学家。
[51] 希尔弗，Jack Silver （1942 - ），美国逻辑学家，数学家。
[52] 奇异基数假设，Singular Cardinal Hypothesis。
[53] 马丁，Donald A. Martin （1940 - ），美国逻辑学家，数学家，哲学家。
[54] 斯蒂尔，John Steel（1948 - ），美国逻辑学家，数学家。
[55] 武丁，W. Hugh Woodin（1955 - ），美国逻辑学家，数学家。
[56] 典范宇宙，canonical universe。
[57] 终极的 L，ultimate L。
[58] 合适力迫公理，proper forcing axiom (PFA)。
[59] 马丁极大化公理，Martin's Maximum (MM)。
[60] 图多切维奇，Stevo Todorčević，塞尔维亚和加拿大逻辑学家，数学家。
[61] 法拉，Ilijas Farah，加拿大逻辑学家，数学家。
[62] 丘奇，　Alonzo Church（1903 － 1995），美国逻辑学家，数学家。
[63] 图灵，Alan Turing （1912 - 1954），英国逻辑学家，数学家。
[64] 戴维斯，Martin Davis（1928 - ）美国逻辑学家，数学家。
[65] 普特南，Hilary Putnam（1926 - ），美国哲学家，数学家。
[66] 罗宾逊，Julia Robinson （1919 - 1985），美国数学家。
[67] 马蒂亚塞维奇，Yuri Matiyasevich （1947 - ），俄罗斯数学家，计算机学家。

可计算集合的复杂性进行比较，从而引出了归约和度的概念。1954 年克林尼 [68] 和波斯特 [69]的关于不可解度的文章使人们真正开始了对度的研究。此后的数十年，对各种归约和度的研究一直在递归论中占主导地位，尤其是对由图灵归约诱导出的图灵度这一偏序结构的研究，其中又可分为整体结构和各种局部结构如递归可枚举度两部分。在整体结构方面，1977 年，辛普森 [70] 证明了图灵度结构的理论与二阶算术的理论是递归同构的；二十世纪末，斯莱曼 [71] 和武丁利用编码和集合论的方法得到了关于图灵度整体结构的一系列结果，包括图灵度至多有可数多个自同构和每个自同构在 $\mathbf{0}''$ 之上都是恒等映射；肖尔 [72] 和斯莱曼证明了跃变算子[73] 图灵度上是可定义的。对局部结构的研究则得力于弗雷德伯格 [74] 和穆奇尼克 [75] 在 1950 年代创立的优先方法。经过哈灵顿尤其是拉克伦 [76] 等人的改进，优先方法已经成为递归可枚举度研究中不可缺少的工具。哈灵顿和斯莱曼证明了递归可枚举图灵度的理论与一阶算术理论是递归同构的；勒尔曼 [77]，索瓦 [78] 等人在格嵌入[79] 问题上也取得了一系列成果。此外对递归可枚举集合上结构 $\mathcal{E}$ 和 $\mathcal{E}^*$ 中自同构和轨道的研究也是递归论的一个重要方向。以上提到的都属于古典递归论的研究范围，即研究自然数上集合和函数的可计算性。现代递归论的口号则是研究可定义性。因为可定义性一方面包括了可计算性，同时又可以把研究范围自然地扩展到实数集合或序数集合上面。在拓广后的论域上研究可计算性或可定义性的分支称为“高层递归论”[80]。从二十世纪六十年代至今，萨克斯[81] 和所谓的萨克斯学派在高层递归论方向上做了大量的工作。近十年来，递归论与其它相关领域的交叉为递归论注入了新的活力。尤其是在反推数学和算法随机性等方面的研究已成为递归论中的热门课题。此外递归论与计算机科学一直有密切的联系，如机器学习和自动机可表示的结构理论，还有与模型论有关的递归模型论等等。递归论参考书有 [8] 或 [9]。

从我们上面大致的描述来看，数理逻辑涵盖了一个相当广的范围，各个分支表面上看似乎没有太多的联系，它们之所以都属于数理逻辑的研究范围，一方面是由于历史原因，早期出于同源；更重要的是，各科学科在思想方法上有很多共同点，例如对语言的关注，或者更广泛地说，对研究的手段和问题的表达方式的关注；又如对分类或分层的重视，对复杂性的重视等等。希望通过本课程和后续课程，大家能对此有更多的体会，也对数理逻

[68] 克林尼，Stephen Kleene（1909 - 1994），美国逻辑学家，数学家。
[69] 波斯特，Emil Post （1897 - 1954），美国逻辑学家，数学家。
[70] 辛普森，Stephen Simpson，美国逻辑学家，数学家。
[71] 斯莱曼，Theodore Slaman（1954 - ），美国逻辑学家，数学家。
[72] 肖尔，Richard Shore（1946 - ），美国逻辑学家，数学家。
[73] 跃变算子，jump operator。
[74] 弗雷德伯格，Richard Friedberg，美国逻辑学家，数学家。
[75] 穆奇尼克，Albert Muchnik （1934 - ），俄罗斯逻辑学家，数学家。
[76] 拉克伦，Alistair Lachlan，加拿大逻辑学家，数学家。
[77] 勒尔曼，Manuel Lerman（1943 - ），美国逻辑学家，数学家。
[78] 索瓦，Robert Soare，美国逻辑学家，数学家。
[79] 格嵌入，lattice embedding。
[80] 高层递归论，higher recursion theory。
[81] 萨克斯，Gerald Sacks （1933 - ），美国逻辑学家，数学家。

辑有更深的了解。最后说明一点，尽管数理逻辑被简单划分为若干个分支，但这些划分是相当人为的。我们切不可画地为牢，让这些划分把逻辑的本质割裂肢解。事实上，不仅逻辑中各个分支是相通的，逻辑与数学、逻辑与哲学也是相通的。

第三节　课程大纲

第一部分 命题逻辑

在这一部分，我们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，所以这一部分可以看做整个课程内容的简明版本，所以对命题逻辑的学习是整个课程很好的热身。主要内容包括：命题逻辑的形式语言，真值指派，形式语言的无歧义性，命题连接词的互相可定义性，一个命题演算的公理系统，以及命题逻辑的完全性定理。

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。首先我们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，这包括子公式，自由和约束变元，代入和替换。我们还会学习如何用这种形式的语言翻译自然语言中的语句，这主要是来自数学和哲学中的一些命题，通过练习我们会发现，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。

然后我们在定义的形式语言中建立一个形式的公理系统。还会介绍一种有甘岑建立的自然推演系统，对于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，读者会学习和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

这一部分讨论塔尔斯基的形式语言中的真概念。我们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。事实上这一概念是模型论建立的基石。借助这一概念我们会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。

然后我们将讨论数学中常见的同构、可定义性等概念，这些概念今后的数理逻辑课程中会被广泛地使用。对初学者或许可先放一放，等今后用到时再详细阅读。

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完全性定理，从而把语法和语义两方面联系起来。此外还会学习紧致性定理及其一些有趣的应用，从中会发现一阶逻辑的一些局限。

本书针对的是对逻辑和数学基础有兴趣的的读者。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，因而也把重点放在推演部分；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。相对于以上的逻辑书，我们的讲义把逻辑与元数学连在一起；更多地介绍语义部分和强调语法语义的统一。此外，本讲义另一个重要目的是为了后继课程做准备，因此它的确是引大家入数理逻辑之门的导论。希望读者掌握了本导论的内容之后，继续学习更深、更专门也更有意思的内容，如哥德尔不完全性定理和连续统假设的独立性等等。

由于数理逻辑已是非常成熟的学科，本讲义中的大部分内容都是 1930 年代的成果。讲义作者仅仅根据教学经验，将经典内容理顺，以期减少同学们学习的阻力而已。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[82]的[3]，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）、沈恩绍（上海交通大学）、施翔晖（北京师范大学）、杨睿之（复旦大学）、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。（定稿时会加入更多书名和为初稿提供改进意见的人名。）

[82] 安德顿，Herbert Enderton （1936 - 2010），美国逻辑学家，数学家。

第二章　预备知识

从引言可以看出本讲义会假定读者有一定的数学基础。但是我们也注意到大量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”的逻辑搞得太机械以至弄“死”。这种怀疑是有一定道理的。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。但我们要强调，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。

在本章中我们罗列一些预备知识，数学基础好的读者可以略过这一章。

第一节　证明的必要性

数学不同于实验性科学，如物理或生命科学。对实验性科学来说，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。数据（基本）吻合了，理论也就成功了。有极少数的特例问题不大。而数学则不同。数学的论证必须是“滴水不漏”或是“无可置疑”的。不允许有任何例外。注意在这一点上数学对论证的要求比思辨性科学（包括哲学）也要高。

我们看几个例子，说明大量事实不能代替数学论证。

例 2.1.1. 我们称一个正整数 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，我们能得出结论：所有形如 $33\cdots3331$ 的整数都是素数吗？

答案： 不能，例如 333333331 不是素数。

例 2.1.2. 费尔马[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

[1]费尔马，Pierre de Fermat（1601（？）- 1665），法国数学家。
[2]怀尔斯，Andrew Wiles （1953 - ），英国数学家。

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 $4{,}000{,}000$ 的 $4{,}000{,}000$ 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。我们现在考察一些与之近似的命题：方程 $x^3+y^3+z^3=w^3$ 没有 x,y,z 和 w 的正整数解。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：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，在例 2.1.1 中 333333331 就是一个反例。这是前面 7 个例子不重要了，我们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，我们从大家公认的事实出发。这些公认的事实被称为“公理”。公理是数学证明的起点。接下来我们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你承认上一步结论的正确性，你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 2.1.3. 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 $\frac{a}{b}$。我们可以进一步假定 a 和 b 没有大于 1 的公因子。

$$\sqrt{2}=\frac{a}{b}。$$

两边平方，再乘 b^2，得到

$$2b^2=a^2。$$

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，得到

$$b^2=2c^2。$$

同样的理由告诉我们 b 也是偶数。因而与 a 和 b 没有大于 1 的公因子矛盾。所以不存在这样的 a 和 b，因而 $\sqrt{2}$ 是无理数。 □

例 2.1.4. 证明存在无穷多个素数。

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

$$q = p_1 p_2 \cdots p_n + 1。$$

它不能被任何素数整除。这与任何整数都可以被分解成素数乘积这一事实矛盾。因而素数是无限多的。 □

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。

第二节　集合

在中学我们学过用 $A = \{a_0, a_1, \cdots, a_n\}$ 表示 A 是一个集合，$a_0, a_1, \ldots, a_n$ 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 $\mathbb{N} = \{0, 1, 2, \ldots\}$，但这样的写法不能表示不可数的集合，例如全体实数的集合 $\mathbb{R}$ 就不能以这种方式表示，因此更方便的是用 $A = \{x : P(x)\}$ 表示一个集合，其中 P 是一个特定的性质。例如， $\{x : x \text{ 是红的}\}$ 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，一般用 $x \notin A$ 表示 x 不是 A 的元素。

外延原理 关于集合一个最重要的性质是，它是完全由其元素决定的，而与其它的因素，如我们怎样描述集合里的元素，没有关系。比如，$\{x \in \mathbb{R} : \text{对所有的实数 } y \text{ 都满足 } x + y = y\}$ 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。所以我们有所谓 外延原理：$A = B$ 当且仅当 A 和 B 有相同的元素。一方面如果 $A = B$ 则必然有它们的元素相同，这实际上就是莱布尼茨的不可分辨原理。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，那我们就断定 $A = B$，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 $A \cup B = \{x : x \in A \text{ 或者 } x \in B\}$。类似的，同时既属于 A 又属于 B 的元素构成 A 与 B 的 交集，记作 $A \cap B$。显然， $A \cap B = \{x : x \in A \text{ 并且 } x \in B\}$。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 $A - B = \{x : x \in A \text{ 但是 } x \notin B\}$。

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，我们会以 $B \subsetneq A$ 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，

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

表示 n 个集合的族。对于集合族，我们可以定义其上的**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。[3] 特别地，

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

为了清楚表示集合族，一般需要一个下标集。虽然理论上任何集合都可以用做下标集，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。对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 $\mathcal{F} = \{F_0, F_1, \ldots, F_{n-1}\}$ 的一般交和一般并也表示为：

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

类似地，

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

[3] 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。

习题 2.1.

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

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

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

(2) 写出下列集合的元素：

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

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

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

(3) 找出三个性质 $P(x)$ 使得集合 $\{x \in \mathbb{R} : P(x)\}$ 为 $\{1\}$；找出三个性质 $Q(x)$ 使得集合 $\{x \in \mathbb{Z} : Q(x)\} = \emptyset$。

(4) 在有可能的情况下找出：

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

(b) 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。

第三节　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。比如，把自然数集 $\mathbb{N}$ 和自然数上的大小顺序放在一起，我们就有一个自然的“序结构” $(\mathbb{N}, <)$，其中：

$$0 < 1 < 2 < 3 < \cdots$$

在所有自然数的集合 $\mathbb{N}$ 上我们还可以造其它的序，比如，下面的 $\prec$

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

就给我们另外一个序结构 $(\mathbb{N}, \prec)$。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，比如第一个结构有最小元，第二个则没有。在我们继续讨论结构之前，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[4] 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。

我们称一集合 R 为集合 X, Y之间的一个 二元关系，$R \subseteq X \times Y$。这样，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。我们之所以这样定义，原因和前面提到的集合的外延原理是一样的：我们并不关心我们怎样描述 R。两个不同的描述，只要它们给出的有序对是一样的，它们就是同一个关系。比如 $R_1 = \{(x, y) \in \mathbb{N}^2 : y + 1 = x\}$ 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，尽管我们对它们的描述不同。

例 2.3.1.

(1) 我们说一个整数 m 整除 另一个整数 n 如果存在整数 k 使得 $n = m \times k$。我们用 $m \mid n$ 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，我们有 $(2, 4) \in R$ 但是 $(3, 4) \notin R$。

(2) 除了考察自然的关系之外，出于各种需要，我们经常人为地设计一些关系的例子。比如，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。我们有 $1R1$, $1Ra$, $2Rb$ 和 $3R1$，但 $1 \not R b$，$2 \not R 1$。

[4] 卡氏积，Cartesian product，因笛卡尔而得名。笛卡尔，René Descartes （1596 - 1650），法国哲学家，数学家。

以下罗列与关系有关的一些定义。

- R 的定义域定义为：$\mathrm{dom}R = \{x \mid$ 存在 y 使得 $R(x,y)\}$。
- R 的值域定义为：$\mathrm{ran}R = \{y \mid$ 存在 x 使得 $R(x,y)\}$。
- 如果 $R \subset X^2$，则称 R 是 X 中的二元关系。
- 集合 X 在关系 R 下的象定义为：

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

- 集合 Y 在关系 R 下的逆象定义为：

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

- 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：

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

例 2.3.2.

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

(2) 如果 $R = \{(x,y) \in \mathbb{R}^2 \mid y = \sqrt{x}\}$，则 $R^{-1} = \{(x,y) \mid y = x^2 \wedge x \geq 0\}$。

(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) 在前面举的 $A = \{1,2,3,4\}$，$B = \{1,a,b,c\}$ 并且 $R = \{(1,1),(1,a),(2,b),(3,1)\}$ 的例子中，$\mathrm{dom}R = \{1,2,3\} \subseteq A$；$\mathrm{ran}R = \{1,a,b\} \subseteq B$；$R$ 的逆 R^{-1} 为 $B \times A$ 的一个子集，$R^{-1} = \{(1,1),(a,1),(b,2),(1,3)\}$。

(5) 令 $R \subseteq A \times B$ 和 $S \subseteq B \times C$ 为如下关系，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。我们称 a 同余于 b 模 n，记为 $a\equiv b\pmod{n}$，如果 $n\mid(a-b)$。我们称 a 不同余于 b 模 n，记为 $a\not\equiv b\pmod{n}$，如果 n 不整除 $(a-b)$。顾名思义 $a\equiv b\pmod{n}$ 当且仅当用 n 分别去除 a 和 b 所得的余数相同。此外 $a\equiv 0\pmod{n}$ 当且仅当 $n\mid a$。同余是整数间的一个常见的关系。例如，$87\equiv 12\pmod{15}$；$83\not\equiv 5\pmod{11}$ 等等。

卡氏积和二元关系可以推广。首先，定义三元有序组

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

而四元序组

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

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

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

这是我们前面用过的“递归定义”或“归纳定义”方式。

n 个集合的卡氏积定义为：

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

同样，

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

对任意集合 R，如果 $R\subseteq X_1\times\ldots\times X_n$，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的推广到无穷多个集合上面，但我们留到以后再讲。

习题 2.2.

(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。

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

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

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

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

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

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

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

(a) （自反性） $a \equiv a \pmod{n}$。

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

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

(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。

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$。

(b) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$。

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

第四节　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发疯。

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 $(x, y) \in f$，我们常写作 $f(x) = y$，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 2.4.1. *(1) 在我们所举的关系的例子中， $\{(x, y) \mid x = y\}$ 和 $\{(x, y) \mid y = \sqrt{x}\}$ 都是函数； 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:

$$S_1(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2},$$
$$S_2(n) = 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6},$$
$$S_3(n) = 1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{2}。$$

(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 2.4.1. 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: 练习。 □

根据定义每一个函数都是一个关系，所以我们前面定义的关系的定义域、值域、象、逆等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 n 元运算。自然数上的加法是一个二元运算的例子。由于我们可以将 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 2.4.2. 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 $\mathrm{dom}(g \circ f) = \mathrm{dom}f \cap f^{-1}[\mathrm{dom}g]$。并且，对所有 $x \in \mathrm{dom}(g \circ f)$，$(g \circ f)(x) = g(f(x))$。

证明: （首先注意我们在定义 f 是函数时，只需要 f 是有序对（比如 $A \times B$）的子集，并满足“输出唯一性”；我们并没有明确给出 f 的定义域。在本题中如果我们限制好了 $f : A \to B$ 且 $g : B \to C$，那整个问题就简单多了。我们把本题当作有序对的练习好了。）

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，$z_1 = z_2$。所以 $g \circ f$ 是函数。

至于第二个命题，根据定义域的定义，我们有 $x \in \mathrm{dom}(g \circ f)$ 当且仅当存在 z 使得 $(x, z) \in g \circ f$；再根据复合的定义，我们有 $x \in \mathrm{dom}(g \circ f)$ 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 $x \in f^{-1}[\mathrm{dom}(g)]$，我们有 $\exists y (x, y) \in f$ 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**，或称 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，并且对于每一 $x \in A$，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**。

习题 2.3.

(1) 对下列集合 A 和 B 找出所有从 A 到 B 的函数。

(a) $A = \{x\}$ and $B = \{0, 1\}$。

(b) $A = \{x, y\}$ and $B = \{2\}$。

(c) $A = \{x, y\}$ and $B = \{0, 1\}$。

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

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?

(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 $f = g$。

(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。

(4) 考察函数 $f : X \to Y$。判断下列命题的对错。

(a) f 是满射当且仅当任何一个 Y 里的元素都是某个 X 里元素的像。

(b) f 是满射当且仅当任何一个 X 里的元素都有某个 Y 里元素为它的像。

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

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

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

(f) f 满射当且仅当 f 的值域等于 Y。

(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。

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

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

(c) 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 $(f + g)(x) = f(x) + g(x)$。）

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

(7) 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

$$f(x) = \frac{d - c}{b - a}(x - a) + c。$$

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

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

(9) (a) 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。

(b) 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。

(10) 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。

(a) 如果 f 是单射，则 F 也是单射。

(b) 如果 f 是满射，则 G 是满射。

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

(a) 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。

(b) 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。

(12) 考察函数 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 定义为

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

(a) 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 $f(m_1, n_1) < f(m_2, n_2)$。

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

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

(c) 证明 f 是双射。

第五节　等价关系与划分

如果有一类物体，尽管它们各不相同，但就我们关心的性质来说，它们的表现是一样的，则我们很自然地把它们等同起来，不加区分。比如，自然数 7 和 4 不相等，但如果我们只关心模 3 的算术的话，7 和 4 的性质完全一样，因为 $7 \equiv 4 \pmod 3$。因此我们完全可以把 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 2.5.1. 令 $R \subset X^2$ 为二元关系，则我们称

(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 $x, y \in X$，如果 $R(x,y)$ 则 $R(y,x)$;

(3) R 是*传递的* 如果对所有的 $x, y, z \in X$，如果 $R(x,y)$，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 $x \sim y$，则我们称 x 与 y 等价。

例 2.5.1.

(1) 如果 P 代表所有人的集合，如下定义 P 上的二元关系：

$$D = \{(x,y) \mid x \text{ 是 } y \text{ 的后代}\}; \tag{2.1}$$
$$B = \{(x,y) \mid \text{至少有一个 } x \text{ 的祖先也是 } y \text{ 的祖先}\}; \tag{2.2}$$
$$S = \{(x,y) \mid x \text{ 的父母是 } y \text{ 的父母}\}。 \tag{2.3}$$

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。让我们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 2.5.2. 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，我们常把 $[x]_\sim$ 简记为 $[x]$。

例如，在上例中相同国籍的关系下，包含姚明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 2.5.1. 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。我们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 $[0] = \{3k \mid k \in \mathbb{Z}\}$，$[1] = \{3k+1 \mid k \in \mathbb{Z}\}$，和 $[2] = \{3k+2 \mid k \in \mathbb{Z}\}$。这三个等价类的并集是所有整数集 $\mathbb{Z}$，并且由观察或用引理 2.5.1 可以得出它们彼此不相交。

定义 2.5.3. 令 X 为一集合， $S \subset \mathcal{P}(X)$ 。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 2.5.4. 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。比如代数中有商群，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 2.5.1. 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 2.5.1，如果 $[x]_\sim \neq [y]_\sim$，则 $[x]_\sim \cap [y]_\sim = \emptyset$。其次，由于对任意 $x \in X$ 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，我们可以由一个集合的划分来定义其上的等价关系。

定理 2.5.2. 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 2.5.3.

(a) 如果 S 为 X 的划分，则 $X/\sim_S = S$;

(b) 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我们留作习题。

习题 2.4.

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

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

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

(c) 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 $U \cap V \neq \emptyset$。

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

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

(2) 令 $T = \{0, 1, 2, 3, \ldots, 12\}$。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：

(a) a，b 都是偶数。

(b) a，b 都是大于 2 的素数。

(c) 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。

(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。找出等价类 $[(0, 1)]$ 和 $[(2, 4)]$。

(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 是一个等价关系并且找出 R 的所有等价类。

(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条件成立：

(a) 对所有 $x \in A$ xRx 成立。

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

(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 $x \equiv y (\mathrm{mod}\ k)$。我们已经知道 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。

(7) 对任意集合 X，如果 $\mathcal{I} \subset \mathcal{P}(X)$，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，则其上的二元关系：

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

是等价关系。

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

(9) 证明定理 2.5.2 和定理 2.5.3 。

第六节　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，我们可以添加反对称性（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。因此我们有

定义 2.6.1. 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。

例 2.6.1.

(1) 集合 $\mathbb{N}$、$\mathbb{Z}$、$\mathbb{Q}$ 和 $\mathbb{R}$ 上的自然大小关系都是都是线序。

(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。图像为 $1<3<2$。

线序的概念可以推广成所谓“偏序”的概念，人们常用 $\leq$ 来代表序。

定义 2.6.2. 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*。

我们用 $(X, \leq)$ 表示 $\leq$ 是 X 上的偏序，此时称 X 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 $x \neq y$。

例 2.6.2.

(1) 集合 $\mathbb{N}$、$\mathbb{Z}$、$\mathbb{Q}$ 和 $\mathbb{R}$ 上的自然大小关系都是序关系（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 2.5.

(1) 证明每一个有穷的偏序都可以延拓成一个线序。

第七节　结构的例子

上面的线序关系或偏序关系都是结构的例子。也是所谓用公理来“定义”结构的例子。我们再看几个数学里常见的结构的例子。

如果我们只关心所谓“算术运算”，即加减乘除，我们可以研究“域”这种结构。

定义 2.7.1. 一个 *域* 是一个集合 F，其元素间有两个运算，分别记作加法 $+$ 和乘法 $\cdot$，且满足：

(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) 存在一个元素，记作 0，满足：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 $a,b,c\in F$，$a\cdot(b\cdot c)=(a\cdot b)\cdot c$。

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

(7) 存在一个元素，记作 1，满足：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。域的典型例子有：有理数 $\mathbb{Q}$、实数 $\mathbb{R}$、复数 $\mathbb{C}$ 等等。当然还有其它不太常见的例子，我们仅举一例，其它的我们用到的时候再介绍。

例 2.7.1. 令 p 为一个素数，则 $\{0,1,\cdots,p-1\}$ 在模 p 的运算下，形成一个域。这是 *有限域* 的一个典型例子。

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；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。

有些结构关于加减乘法都有很好的性质，但不能做除法，这样的结构称为“环”。域可以被看成是特殊的环，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，所以我们才采取这样的顺序（而且暂时不谈论群）。环的精确定义如下：

定义 2.7.2. 一个 *环* 是一个集合 R，其元素间有两个运算，分别记作加法 $+$ 和乘法 $\cdot$，且满足:

(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) 存在一个元素，记作 0，满足：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 $a,b,c\in F$，$a\cdot(b\cdot c)=(a\cdot b)\cdot c$。

(6) 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：对环来说，我们不要求它满足乘法交换律，也不要求它有乘法单位元 1。环的典型例子有：整数 $\mathbb{Z}$，（实数上的）矩阵，（整系数）多项式等等。矩阵环是非（乘法）交换环的典型例子。

结构的其它例子有：图论中研究的图；代数和布尔代数；群论中研究的群等等。

最后我们看自然数。我们关注的是加法和乘法。有了加法和乘法，大部分的初等数论都包括在研究范围之内了。在后续课程中，当我们谈到哥德尔不完全定理时，我们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。我们在本节描述皮亚诺的版本。当以后我们对一阶逻辑有了一定的认识之后，我们再根据需要对皮亚诺的版本作必要的修改。皮亚诺公理中所采用的最基本函数是所谓 *后继函数* $S:\mathbb{N}\to\mathbb{N}$。有一个特殊常数 0。所谓 n 的后继就是 n 后面的那个数。[粗心的人也可以说 $S(n)$ 就是 $n+1$。但在皮亚诺版本中加法是由后继函数定义的，因此用 $n+1$ 来解释 $S(n)$ 是不恰当的。]

皮亚诺本人版本的公理如下 ：

(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，如果 $S(m)=S(n)$ 则 $m=n$。

(P5) （*归纳原理*）令 Q 为一个关于自然数的性质。如果 (1) 0 具有性质 Q；并且（2）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。

在此之上，加法被归纳地定义成对任何自然数 n 和 m：

$$n+0=n \text{ 并且 } n+S(m)=S(n+m)。$$

类似地，乘法被归纳地定义成对任何自然数 n 和 m：

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

习题 2.6.

(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。

(2) 证明每个非零的自然数都是某个自然数的后继。

(3) 证明抽屉原则 （或称鸽舍原理[5]）：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。

[5]鸽舍原理，Pigeonhole Principle，叙述为：如果把 n 个鸽子放入少于 n 个鸽舍里，则至少有一个鸽舍里面有不止一只鸽子。

(4) 证明下列命题等价：

(a) 皮亚诺公理中的归纳原理。

(b) 最小数原理：自然数的任意非空子集都有最小元。

(c) 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。

第三章　命题逻辑

第一节　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我们研究逻辑时我们用的是什么逻辑？如果我们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。我们于是造一个机器人（或用某个计算机程序来模拟），对机器人我们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我们的“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我们人脑是怎样运作的，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逻辑。只有在我们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。类似的区分还有很多，例如当我们用中文来研究语言学或计算机语言学，中文就是“元语言”而被研究的语言或计算机语言则是“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。贯穿我们课程的一个中心问题是：是否真的命题都可证。“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，我们首先要搞清楚“真”是什么意思，“证明”又是什么。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。语法一边让人想到机器，规则，算法；语义则让人想到人（脑），意义，真假等等。

事实上，一阶逻辑中“是否真的命题都可证”这个问题是我们真正想回答的。但为了分散学习难点，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。清华大学有位教授曾讲：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。

第二节　命题逻辑的语言

古典命题逻辑的语言 包括以下三部分:

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

(2) 五个 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 “)”。

注:

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。而另一方面，人们也可以研究有不可数多个命题符号的逻辑。
2. 这五个联词尽管与日常语言有关，但在数学文献中更为常见。
3. 在本节中我们强调的是语法。因此尽管我们给这五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”，但那是我们下一节讨论语义的任务。本节中，我们应把它们视为完全没有意义的字符，所以上面我们特地强调“符号”二字。
4. $\neg$ 是一元联词。其它四个是二元联词。这四个二元联词在讨论语法时区别不大，我们常用符号 $\star$ 来表示它们中任何一个联词。
5. 括号只是为了便于阅读，以后（习题 3.3）我们会看到，括号实际上是可有可无的。比如对计算机语言来说，没有括号更为简练。

规定好基本符号之后，我们就可以形成较为复杂的语句。首先我们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 3.2.1.

(a) 每个命题符号 A_i 都是合式公式。

(b) 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。

(c) 别无其它。

注:

1. 定义中的中文即是“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，我们用了“每个”这个量词，也使用了 α，β 等符号作为变元代表这个语言中任意公式。但这里的量词和符号变元都是元语言中的，显然不属于我们正在讨论的命题逻辑语言。

2. 虽然我们标准的命题符号为 $A_0, A_1, A_2, \cdots$，在实际工作中我们经常用 A、B、P、和 Q 等符号来表示任意的命题符号。

上述定义中 (a)，(b) 不难理解，(c) 有些模糊。由于我们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给习题。

“自上而下”的定义将合式公式集作为一个整体定义出来。让我们临时地把一个满足性质 (b) 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 $\star$ 代表四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”地定义为：最小的包含所有命题符号的封闭的表达式集，即

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

注意：条件 (c) 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”的定义所弥补了。“自下而上”的定义给出了公式 α 的一个构造过程。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，我们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，我们就可以构造“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

$$(\varphi_0,\varphi_1,\ldots,\varphi_n)$$

为 α 的一个 构造序列，如果最后一项 φ_n 为 α 并且对每一个 $i\le n$，或者 φ_i 是一个命题符号，或者存在 $j,k<i$ 使得 φ_i 为 $(\neg\varphi_j)$ 或 $(\varphi_j\star\varphi_k)$。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，我们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”，具体的转化过程我们留作习题。如下形式的归纳原理非常有用，利用它我们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 3.2.1 (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; 并且

(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。

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

引理 3.2.1. 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: 我们只证明第一个命题，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。我们对 $P(\alpha)$ 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，它们中的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 3.1.

(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

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

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：

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

并且令

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

证明 $C^* = C_*$。

(2) 我们称 α 是一个好公式，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。给出好公式的“自上而下”和“自下而上”的定义。

(3) 证明归纳原理，即正文中定理 3.2.1。

(4) 证明没有长度为 $2,3$ 或 6 的合式公式, 但其它长度皆有可能。

(5) 已知公式 α 中一元联词 $\neg$ 出现的次数为 m，其它四个二元联词出现的总次数为 n。找出 α 的长度。

(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 $s = c + 1$。

(7) 假定公式 φ 的长度为 n，证明 φ 有一个长度不超过 n 的构造序列。

(8) 给定公式 φ 的一个构造序列，其中 φ 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 φ 的一个构造序列。

(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。

   (a) 给出 β 是公式 α 的一个子公式的严格定义。

   (b) 用 (a) 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。

   (c) 证明在 α 的最短的构造序列中出现的都是 α 的子公式。

第三节　真值指派

我们开始探讨语义。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，$\neg$ 对应于 $f_\neg : \{\text{表达式}\} \to \{\text{表达式}\}$，$f_\neg(\alpha) = (\neg\alpha)$，同样地，每一个二元联词 $\star$ 就对应于 $f_\star : \{\text{表达式}\} \times \{\text{表达式}\}$，$f_\star(\alpha, \beta) = (\alpha \star \beta)$。$\overline{S}$ 就是表达式中由 S 经这五个函数生成的集合（见习题 3.1）。我们把真值指派 v 扩张到 $\overline{S}$ 上得到新函数 $\overline{v}$：

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

满足

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

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

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

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

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

(5)
$$\overline{v}((\alpha \leftrightarrow \beta)) = \begin{cases} T, & \text{如果 } \overline{v}(\alpha) = \overline{v}(\beta); \\ F, & \text{其它。} \end{cases}$$

我们也可以用 真值表 来表示 $\overline{v}$：

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

注：以上的真值表虽然再自然不过，但却是命题逻辑语义最根本的部分。首先注意，在我们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：我们对命题公式真值的定义是基于元语言做出的，即，只有在真值指派 v 确定以后，公式的真值才有意义。至于说，例如 v 为什么让 A_3 为假，而让 A_4 为真等等不是我们考虑的范围。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，其它的都好理解。当然，我们可以简单地说：在数学中蕴涵就是这样规定的。但我们还是给出几种解释，希望能说服初学者这样的规定是有道理的。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，我就把我鼻子吃了”。

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。），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。当我们肯定了前件时，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是一样，不管 A，B 取何值，整个公式一定为 T。现在考虑如下两种情况：（1）A 为假而 B 为真，则我们得到的是 $F \to T$；（2）B 为假，这时前件和后件都是假的，我们得到 $F \to F$。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：我们自行设计我们觉得满意的真值表：

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

首先，大家对前两行应该没有异议。剩下的是选择 X 和 Y 的值。我们选了 $X = Y = T$ 大家不满意。现在你们来选。只有三种可能，大家会发现都不合适。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 3.3.1. 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。注意在定义中 $\overline{v}$ 在定义和被定义的部分同时出现。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，比如，阶乘函数 $n!$ 就可以递归定义成 $0! = 1$ 并且对所有自然数 n, $(n+1)! = (n+1) \times n!$；又比如菲波那契[1]序列 f_n 可以递归定义为 $f_0 = f_1 = 1$ 并且对所有自然数 n, $f_{n+2} = f_n + f_{n+1}$。直观上很容易接受下述定理：

定理 3.3.1. 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) – (5)*。

定理 3.3.1 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内都有递归定义合理性的证明，有兴趣的读者可以参考，我们这里就省略了。

我们称一个真值指派 v 满足 一个公式 φ 如果 $\overline{v}(\varphi) = T$。

定义 3.3.1. 我们称一个公式集 Σ 重言蕴涵 公式 τ，记为 $\Sigma \models \tau$，如果每一个满足 Σ 中所有公式的真值指派都满足 τ。

$\Sigma \models \tau$ 也被读作 τ 是 Σ 的 语义后承 。如果我们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。$\Sigma \models \tau$ 当且仅当“对所有的真值指派 v [如果（对所有的公式 $\sigma \in \Sigma$，$\overline{v}(\sigma) = T$）则 $\overline{v}(\tau) = T$]”。

例 3.3.2.

(1) 验证 $\{(\alpha \wedge \beta)\} \models \alpha$。

(2) 公式集 $\{A, (\neg A)\}$ 重言蕴涵 B 吗？

答案：是。

我们称一个公式 τ 为一个 重言式 （记作 $\models \tau$）如果 $\emptyset \models \tau$。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 $\Sigma = \{\sigma\}$ 只含有一个公式，我们有时会把 $\{\sigma\} \models \tau$ 简写成 $\sigma \models \tau$。如果 $\sigma \models \tau$ 和 $\tau \models \sigma$ 都成立，则我们说 σ 和 τ 重言等价 。

重言式举例

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

(1) 结合律：

$$((A \vee (B \vee C)) \quad \leftrightarrow \quad ((A \vee B) \vee C))。$$
$$((A \wedge (B \wedge C)) \quad \leftrightarrow \quad ((A \wedge B) \wedge C))。$$

(2) 交换律：

$$((A \vee B) \quad \leftrightarrow \quad (B \vee A))。$$
$$((A \wedge B) \quad \leftrightarrow \quad (B \wedge A))。$$

(3) 分配律：

$$((A \wedge (B \vee C)) \quad \leftrightarrow \quad ((A \wedge B) \vee (A \wedge C)))。$$
$$((A \vee (B \wedge C)) \quad \leftrightarrow \quad ((A \vee B) \wedge (A \vee C)))。$$

(4) 双重否定：

$$((\neg(\neg A)) \leftrightarrow A)。$$

(5) 德摩根[2]定律 ：

$$((\neg(A \vee B)) \quad \leftrightarrow \quad ((\neg A) \wedge (\neg B)))。$$
$$((\neg(A \wedge B)) \quad \leftrightarrow \quad ((\neg A) \vee (\neg B)))。$$

(6) 其它：

排中律：　$(A \vee (\neg A))$。
矛盾律：　$(\neg(A \wedge (\neg A)))$。
逆否命题：　$((A \to B) \leftrightarrow ((\neg B) \to (\neg A)))$。

习题 3.2.

(1) 证明下列两公式互不重言蕴涵：

$$(A \leftrightarrow (B \leftrightarrow C)), \quad ((A \wedge (B \wedge C)) \vee ((\neg A) \wedge ((\neg B) \wedge (\neg C))))。$$

（本题说明在叙述“A 当且仅当 B 当且仅当 C”时，我们要小心。）

(2) (a) 公式 $(((P \to Q) \to P) \to P)$ 是重言式吗?

[2]德摩根，Augustus De Morgan （1806 - 1871），英国逻辑学家，数学家。

(b) 递归地定义 σ_k 如下： $\sigma_0 = (P \to Q)$ 并且 $\sigma_{k+1} = (\sigma_k \to P)$。找出所有使 σ_k 为重言式的 k。

(3) 验证下列公式为重言式：

(a) $(((\neg P) \vee Q) \leftrightarrow (P \to Q))$。

(b) $(P \to (Q \to P))$。

(c) $((P \to (Q \to R)) \to ((P \to Q) \to (P \to R)))$。

(d) $((\neg Q \to \neg P) \to ((\neg Q \to P) \to Q))$。

(e) $((P \to (Q \to R)) \leftrightarrow ((P \wedge Q) \to R))$。

(4) 证明下列命题等价：

(a) $\alpha \models \beta$。

(b) $\models (\alpha \to \beta)$。

(c) α 与 $(\alpha \wedge \beta)$ 重言等价。

(d) β 与 $(\alpha \vee \beta)$ 重言等价。

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

(6) 假定 $\Sigma \models (\alpha \to \beta)$。证明 $\Sigma \models ((\gamma \to \alpha) \to (\gamma \to \beta))$。

(7) 证明或否证（以给反例的方式）下列断言:

(a) 如果 $\Sigma \models \alpha$ 或 $\Sigma \models \beta$, 则 $\Sigma \models (\alpha \vee \beta)$;

(b) 如果 $\Sigma \models (\alpha \vee \beta)$, 则 $\Sigma \models \alpha$ 或 $\Sigma \models \beta$。

(8) 找出所有 $\{A_1, A_2, \ldots, A_n\}$ 上的分别满足下列公式的真值指派：

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

(b) $\beta = (\alpha \wedge (A_n \to A_1))$?

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

[注意: (c) 中 γ 的写法不标准，但应该不妨碍对题意的理解。]

(9) 证明一个真值指派 v 满足公式

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

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

(10) 固定一个公式序列 $\alpha_1, \alpha_2, \cdots$。在每个公式 φ，对所有的 n 将命题符号 A_n 都替换成 α_n，并把所得到的公式记作 φ^*。例如，当 φ 为 $((A_2 \vee A_1) \to A_2)$ 时，φ^* 就是 $((\alpha_2 \vee \alpha_1) \to \alpha_2)$。

(a) 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 $\overline{u}(\varphi) = \overline{v}(\varphi^*)$。

(b) 证明如果 φ 是重言式，则 φ^* 也是。

第四节　唯一可读性

这一节我们重回到语法研究，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”都是一样的。或许从反面理解容易一点。像 $A \to B \leftrightarrow C$ 或 $A \wedge B \vee C$ 这样的表达式就有“歧义”，因为没有表达清楚是先处理 A 和 B 之间的运算呢，还是 B 和 C 之间的。这一节与后面的内容关系不大，除了最后的一些约定外，其它内容可以暂时跳过。

定理 3.4.1 (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 $P(\alpha)$ 用归纳很容易证明三条中至少有一条适用。

然后让我们排除重叠的情形。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；注意我们现在讨论语法，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。

最后我们检查情形 (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 3.2.1，我们有 $\alpha_1 = \beta_1$，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

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

(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 $\neg A \vee B$ 指的是 $((\neg A) \vee B)$。

(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 3.3.

(1) 给出一个算法完成如下的断句任务：输入任何表达式 α，该算法能够判定 α 是否是一个合式公式，并且在是的情况下输出 α 的一个生成序列。

(2) 在定义 3.2.1 中将所有的右括号都省略掉。例如，原来的 $((A \wedge (\neg B)) \vee (C \to D))$ 就变成了 $((A \wedge (\neg B \vee (C \to D$。证明省略后仍有唯一可读性。

(3) 假定左括号和右括号变得一样了，例如，原来的 $(\alpha \vee (\beta \wedge \gamma))$ 变成了 $\mid \alpha \vee \mid \beta \wedge \gamma \mid\mid$，唯一可读性还有吗？

(4) 将定义 3.2.1 中的 (b) 改动成

(b') 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 $((A \wedge (\neg B)) \vee (C \to D))$ 就变成了 $\vee \wedge A \neg B \to CD$。证明改动后仍有唯一可读性。（这种表示法被称为波兰记法。）

第五节　其它联词

让我们再回到语义，研究联词的性质。我们说过，我们之所以选择那五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？能不能表达其它所有的联

词？另一方面看，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？字面上看，联词就是把简单句合成复合句的方式。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。说白了，就是一个真值表。我们给它一个新的名字，称为布尔函数，即，我们称一个从 $\{T,F\}^k$ 映到 $\{T,F\}$ 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 $A_1, A_2, \cdots, A_n$ 的一个公式。那么 α 就定义了一个 n-元布尔函数 B^n_α：

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

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。

有些参考书上会提到 0-元联词 $\top$ 和 $\bot$， $\top$ 代表恒真，$\bot$ 代表恒假。如果大家觉得 0-元联词的概念不好理解，我们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；别无其它。例如，$(A\vee\bot)$ 就是新语言上的一个合式公式。在新语言上真值指派 v 自然扩展为 $v(\top)=T$ 和 $v(\bot)=F$。

例 3.5.1. 一元联词有四个：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 3.5.2. 二元联词有 *16* 个。我们分几组讨论（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” 这四个联词。

第三组是我们已经选的 $\vee$，$\wedge$，$\to$，和 $\leftrightarrow$。还有 $\leftarrow$。

第四组是 “$A\downarrow B$”（也被称为皮尔士[3]箭头）定义为 $\neg(A\vee B)$ 和 “$A\mid B$”（也被称为谢弗[4]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 $0,1$，则这三个联词的取值与 “小于” “大于” 的判断和加法结果一样（当然 $1+1=0$）。

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

[3]皮尔士，Charles Sanders Peirce （1839 - 1914），美国逻辑学家，哲学家。
[4]谢弗，Henry M. Sheffer （1882 - 1964），美国逻辑学家。

定理 3.5.1. 对任意的 n-元布尔函数 G，其中 $n \geq 1$，我们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：

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

令

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

还有

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

我们验证 $G = B^n_\alpha$。容易看出对任何 $1 \leq i \leq k$，$B^n_\alpha(\overline{X}_i) = T = G(\overline{X}_i)$。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 $B^n_\alpha(\overline{Y}) = F = G(\overline{Y})$。 □

我们称一个公式 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 3.5.1. 每一个合式公式 φ 都有一个与其重言等价的析取范式。

我们称一个联词的集合 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 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 3.5.2. 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 3.5.4. $\{\wedge, \to\}$ 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 C 功能是不完全的。常用方法是论证 C 或者不能表达 $\neg$, 或者不能表达 $\vee, \wedge, \to$ 中的一个，因为 C 要是把它们都能表达，C 就功能完全了。到底不能表达哪一个则需要好眼力，观察到 C 的缺陷。二是：假如要想论证 C 不能表达 $\neg$，只要论证任何一个由一个命题符号 A 和 C 中联词形成的公式都不重言等价 $\neg A$ 即可，也就是说，我们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（比方说）$f(A, B)$ 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 和联词 $\wedge$ 和 $\to$，则 $A \models \alpha$。） □

习题 3.4.

(1) 令 G 为下列 3-元布尔函数：

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

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

(b) 重做 (a)，要求公式中联词出现次数不超过 5 次。

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

(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 $\overline{v}(\alpha)$ 的四种可能取值里面总有偶数个 T。

(4) 令 $\mathbb{1}$ 为一个三元联词满足 $\mathbb{1}\alpha\beta\gamma$ 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 $\mathbb{1}\alpha\beta\gamma$ 等价于 $(\alpha \circ \beta) \triangle \gamma$。

(5) 我们称公式 α 是 合取范式 如果它形为

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

其中每个 γ_i 都形为

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

并且 β_{ij} 或是一个命题符号，或是命题符号的否定。

(a) 找出与 $A \leftrightarrow B \leftrightarrow C$ 重言等价的合取范式。

(b) 证明每一公式都有与其重言等价的合取范式。

(6) (a) 假定 α 为一个公式其中仅包含联词 $\rightarrow$。证明 $A \leftrightarrow B$ 不重言等价于 α。

(b) 假定 β 为一个公式其中仅包含联词 $\leftrightarrow$。证明 $A \rightarrow B$ 不重言等价于 β。

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

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

证明个 n-元布尔函数 f 是单调的当且仅当它可以被仅用联词 $\{\wedge, \vee, \top, \bot\}$ 的公式所表达。

(8) 我们称一个联词的集合 C 为 极大不完全的，如果 C 不是功能完全的，但对任意 C 表达不了的布尔函数 g，联词集 $C \cup \{g\}$ 都是功能完全的。证明联词集 $\{\wedge, \vee, \top, \bot\}$ 为极大不完全的。

第六节　命题逻辑的一个推演系统

数学中的“证明”是日常用的“推理”的严格化。在本节中我们将严格定义“证明”这一概念。有必要吗？没有证明的定义，几千年来数学不是也发展得好好的吗？不错，没有证明的定义，我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。

我们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，这个根据可以是来自假设，也可以来自逻辑公理，也可以由逻辑规则从前一环“推”到下一环。

因此我们的推演系统 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那些公式。如果 φ 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 φ 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（对象语言的）定理的

（元语言）的定理；也有关于（对象语言的）证明的（元语言）的证明。在本节中，为了强调，我们把对象语言的定理成为 内定理。日后大家熟悉了，我们再省掉“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。我们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。后面我们会介绍“甘岑式”的自然推演系统，特点是很少（例如，一条甚至没有）公理，很多规则，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。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一样的。这在后面会学到。

我们引进命题逻辑的一个推演系统 L 。为简单起见，我们假定语言中只有两个联词 $\neg$ 和 $\to$，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 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 L 中只有一条推理规则，称为 分离规则[5]：从 α 和 $\alpha\to\beta$ 可以推出 β。

定义 3.6.1. 从公式集 Γ 到公式 φ 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 $\alpha_n=\varphi$ 并且对所有 $i\le n$ 或者

(a) α_i 属于 $\Gamma\cup\Lambda$；或者

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

我们称 φ 为 Γ 的一个 *内定理*（或 *定理* ），记为 $\Gamma\vdash\varphi$，如果存在一个从 Γ 到 φ 的一个推演。

我们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. 如果 $\Gamma\subseteq\Delta$ 并且 $\Gamma\vdash\alpha$，则 $\Delta\vdash\alpha$。

[5]分离规则，modus ponens，常简记为 MP。

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

3. 如果 $\Delta \vdash \alpha$ 并且对每一 $\beta \in \Delta$，$\Gamma \vdash \beta$，则 $\Gamma \vdash \alpha$。

引理 3.6.1. 对所有的合式公式 α，都有 $\vdash \alpha \to \alpha$。

证明: 我们给出下列推演序列，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 3.6.1 (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 $\beta_n = \beta$。我们对 i 施行归纳来证明对所有的 $1 \leq i \leq n$，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 3.6.1。

假定对所有的 $k < i$ 我们已有 $\Gamma \vdash \alpha \to \beta_k$。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。前三种情形同 $i = 1$ 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，我们有 $\Gamma \vdash \alpha \to \beta_j$ 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 3.6.1.

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

习题 3.5.

(1) 证明下列公式为 L 中的内定理，其中 α 和 β 为合式公式。[注意：这是一个语法的练习，请不要使用任何有关语义的结果，当然也就不能用后面的完全性定理。]

(a) $\neg\neg\beta \to \beta$。

(b) $\beta \to \neg\neg\beta$。

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

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

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

第七节　命题逻辑的自然推演

在第 六 节，我们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。在本节我们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甘岑引进的。我们下面介绍的系统是经过后人改进的，主要是泰特[6]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。但代价是大量使用的经典逻辑中的德摩根定律，从而对直觉主义逻辑不再适用。如果大家对其它版本的自然推演系统有兴趣，比较初等的文献有 [10]，当然也可参照证明论方面的参考书。

我们本节主要目的有两个。一是提供大家一个看问题的不同角度，好与前面的“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。

首先我们重新规定语言，新的语言包括：

(1) 命题符号：$A_0, \overline{A}_0, A_1, \overline{A}_1, \cdots$ 注意：对每一个 i，A_i 和 $\overline{A}_i$ 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 $\neg A = \overline{A}$，$\neg\overline{A} = A$；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 $\neg\alpha \vee \beta$。

[6] 泰特，William W. Tait （1929 - ）美国逻辑学家，哲学家。

我们把目标从证明单个公式扩展成证明一个有穷公式集 $\Gamma = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$，即，证明 $\alpha_1 \vee \alpha_2 \vee \cdots \alpha_n$。我们用 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：

$$\Gamma, A_i, \overline{A}_i$$

规则 $(\vee)$:

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

规则 $(\wedge)$:

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

切割规则:

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

我们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。一个从（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，而树中每个节点都是某个推理规则的应用。让我们仍用 $\Delta \vdash \Gamma$ 表示存在一个从 Δ 到 Γ 的一个自然推演。由于我们对自然推演的讨论仅仅是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，我们暂不讨论。

下面举几个推演的例子。

例 3.7.1. 用自然推演证明：对所有的有穷公式集 Γ 和公式 α，我们有 $\vdash \Gamma, \neg\alpha, \alpha$。今后我们会把它称为（公理′）或直接当作公理来用。

证明: 固定 Γ，我们对公式 α 施行归纳：

如果 α 为命题符号 A_i，则 $\neg\alpha$ 为 $\overline{A}_i$。所以 $\Gamma, \neg\alpha, \alpha$ 是公理。 α 为 $\overline{A}_i$ 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 $\mathcal{D}_i$。我们有

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

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

例 3.7.2. 我们有

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

（今后我们会把它称为（$\vee'$）或直接当作规则来用。）

证明: 根据规则 $(\vee)$，我们有

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

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。

□

让我们再多看一个例子。注意，在证明过程中出于各种需要，我们会经常改变同一个集合的表达形式，如，把 $\{a, b, c\}$ 转写成 $\{a, b\}, c$ 或 $\{a\}, b, c$。反正我们要证的 $\Gamma = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ 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，我们把转写写成

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

例 3.7.3. 用自然推演证明:

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

证明: 首先我们要把 $p \to q$ 用 $\neg p \vee q$ 代替，并且用 $\neg$ 的定义把 $\neg$ 推到最里层。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：

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

□

对命题逻辑的自然推演我们先暂时介绍到此，在一阶逻辑中我们会继续这一话题。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，我们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了。

习题 3.6.

(1) 用自然推演证明以前的公理 (A1)，(A2) 和 (A3)。

(2) 用自然推演证明习题 3.5 中的公式。

第八节　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。现在我们将它们统一来看，研究两者之间的联系。

定理 3.8.1 (可靠性定理). 令 Σ 为一个公式集，并且 τ 为一个公式。如果 $\Sigma \vdash \tau$ 则 $\Sigma \models \tau$。特别地，如果 $\vdash \tau$ 则 $\models \tau$，换言之，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 $\Sigma \vdash \tau$，固定一个从 Σ 到 τ 的一个推演序列 $(\beta_1, \beta_2 \cdots, \beta_n)$，其中 $\beta_n = \tau$。令 v 为一个任意的满足 Σ 内所有公式的真值指派。我们对 i 归纳来证明：对任何 $1 \leq i \leq n$，v 都满足 β_i。

当 $i = 1$ 时，β_1 或者是逻辑公理或者是 Σ 中的一员，如果 β_1 是逻辑公理，则是重言式；如果 β_1 是 Σ 中的一员，则用对 v 的假设；无论哪种情形，v 都满足 β_1。

假设 v 满足所有的 β_k $(k < i)$，我们证明 v 满足 β_i。如果 β_i 是逻辑公理或是 Σ 中的一员，则与 β_1 的论证相同。如果 β_i 是从 β_j 和 $\beta_k = \beta_j \to \beta_i$ 经分离规则得到的，其中 $j, k < i$，则根据归纳假设，v 满足 β_j 和 β_k，因而 v 也满足 β_i。

根据归纳法，v 满足 β_n，即 v 满足 τ。 □

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 3.8.2 (完全性定理). 如果 $\Sigma \models \tau$ 则 $\Sigma \vdash \tau$.

我们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。之后我们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 3.8.1. 我们称一个公式集 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 $\Sigma \vdash \neg\alpha$。我们称 Σ 是 *一致的* 如果它不是不一致的。

引理 3.8.1. 公式集 Σ 是不一致的当且仅当对所有的公式 β，$\Sigma \vdash \beta$。

证明: 见习题 3.7。 □

引理 3.8.2. $\Sigma \vdash \tau$ 当且仅当 $\Sigma \cup \{\neg\tau\}$ 不一致。

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

($\Leftarrow$) 假设 $\Sigma \cup \{\neg\tau\}$ 不一致，则根据引理 3.8.1，$\Sigma \cup \{\neg\tau\} \vdash \tau$。所以，$\Sigma \vdash \neg\tau \to \tau$。再据公理 (A3)：

$$\vdash (\neg\tau \to \neg\tau) \to (\neg\tau \to \tau) \to \tau$$

即可得出 $\Sigma \vdash \tau$。 □

定义 3.8.2. 我们称公式集 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，我们可以给出完全性定理的一个等价叙述。

引理 3.8.3. 下列命题等价：

(a) 如果 Σ 一致，则 Σ 可满足。

(b) 如果 $\Sigma \models \tau$ 则 $\Sigma \vdash \tau$。

证明: "$(a) \Rightarrow (b)$" 假定 (a) 成立，并且前提 $\Sigma \models \tau$ 也成立，我们用反证法证 $\Sigma \vdash \tau$。如果 $\Sigma \nvdash \tau$，则根据引理 3.8.2，$\Sigma \cup \{\neg\tau\}$ 是一致的。由 (a) 它就可满足，比如被真值指派 v 所满足。一方面，我们有 $\overline{v}(\neg\tau) = T$；而另一方面，又有 $\overline{v}(\tau) = T$ 因为 $\Sigma \models \tau$ 并且 v 满足 Σ 内所有的公式。矛盾。

"$(b) \Rightarrow (a)$" 假定 (b) 成立，并且前提 Σ 一致也成立，我们用反证法证 Σ 是可满足的。如果 Σ 不可满足，则对任意公式 τ 都有 $\Sigma \models \tau$（为什么？）。根据 (b)，就有对所有公式 τ，$\Sigma \vdash \tau$，说明 Σ 不一致，矛盾。 □

这样我们就把对完全性定理的证明转化为对其等价命题 (a) 的证明。我们称一个公式集 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, $\Delta \cup \{\alpha\}$ 都是不一致的。

引理 3.8.4 (林登鲍姆[7]). 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: （基本思路是在保持一致性的前提下，把全体公式过一遍，能加的都加进去。）

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：

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

则对每一个 n，公式集 Δ_n 都一致 (见练习)。令 Δ 为 $\bigcup_{n\in\mathbb{N}} \Delta_n$。不难验证 $\Sigma \subseteq \Delta$，Δ 也一致 (请自行验证)；并且 Δ 为极大一致的，原因是对任意公式 α 或者 $\alpha \in \Delta$ 或者 $\neg\alpha \in \Delta$。所以，Δ 就是我们所要的。 □

最后我们从语法返回到语义。

引理 3.8.5. 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 $v(A) = T$ 当且仅当 $A \in \Delta$，则 v 满足 Δ 中的所有公式。

证明: 对 α 施行归纳来证明 $v(\alpha) = T$ 当且仅当 $\alpha \in \Delta$ （见习题 3.7）。 □

将引理 3.8.5 与林登鲍姆引理结合起来，我们就有：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，我们无法看出语义（即真值表）和语法（即证明）的直接联系。我们下面重新证明完全性定理的一个弱形式：如果 $\models \alpha$ 则 $\vdash \alpha$。这个证明有两点好处。一是有更强的构造性，原则上可以直接从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) 作公理是魔术。但这个魔术背后并没有太多秘密：我们选取公理的目的是达到完全性。这个新证明告诉我们哪些公式是证明完全性中需要的。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等等，从中选取我们想要的公理集。

我们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 3.5）

(3) 如果 $\Sigma \vdash \alpha$ 并且 $\Sigma \vdash \neg\beta$ 则 $\Sigma \vdash \neg(\alpha \to \beta)$。（利用习题 3.5）

[7] 林登鲍姆，Adolf Lindenbaum（1904 - 1941），波兰逻辑学家，数学家。

引理 3.8.6. 假设 α 为仅包含命题符号 $A_1, \cdots, A_k$ 的一个公式，v 是 $A_1, \cdots, A_k$ 的一个真值指派。令 A'_i 为 A_i 依照 v 的一个变形：如果 $v(A_i) = T$ 则 A'_i 为 A_i；不然则为 $\neg A_i$。同样指定 α 依照 v 的一个变形 α' 如下：如果 $\overline{v}(\alpha) = T$ 则 α' 为 α；不然则为 $\neg\alpha$。则我们有：

$$\{A'_1, \cdots, A'_k\} \vdash \alpha'。$$

证明: 令 $P(\alpha)$ 表示我们要证明的性质。我们用归纳原理证明 $P(\alpha)$ 对所有 α 都成立。为简单起见，我们将 $\{A'_1, \cdots, A'_k\}$ 暂时简记为 Σ，并用 v 代替 $\overline{v}$。

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 $\beta = \neg\alpha$，我们验证 $P(\beta)$ 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，我们有 $\vdash \alpha \to \neg\neg\alpha$。所以 $\Sigma \vdash \beta'$，因为 $\beta' = \neg\neg\alpha$。

假定 $P(\alpha)$ 和 $P(\beta)$ 成立。考察 $\gamma = \alpha \to \beta$，我们验证 $P(\gamma)$ 也成立。令 v 为一个真值指派。我们有以下三种情形。

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，我们有 $\Sigma \vdash \alpha \to \beta$，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)，我们有 $\Sigma \vdash \alpha \to \beta$，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)，我们有 $\Sigma \vdash \neg(\alpha \to \beta)$，即 $\Sigma \vdash \gamma'$。 □

定理 3.8.3 (完全性定理的弱形式)**.** 如果 $\models \alpha$，则 $\vdash \alpha$；换言之，每一个重言式都是 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 3.8.6，对任意的真值指派，我们都有 $\{A'_1, A'_2, \cdots, A'_k\} \vdash \alpha$ （因为 α 是重言式，所以 α' 总是 α）。所以 $\{A'_1, A'_2, \cdots, A'_{k-1}, A_k\} \vdash \alpha$ 还有 $\{A'_1, A'_2, \cdots, A'_{k-1}, \neg A_k\} \vdash \alpha$。由演绎定理，我们得到 $\{A'_1, A'_2, \cdots, A'_{k-1}\} \vdash A_k \to \alpha$ 和 $\{A'_1, A'_2, \cdots, A'_{k-1}\} \vdash \neg A_k \to \alpha$。根据习题 3.5，

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

使用两次分离规则，就有 $\{A'_1, A'_2, \cdots, A'_{k-1}\} \vdash \alpha$。反复上面的论证，我们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，我们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。下面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。但细节超出我们的讲义范围。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。在本节中我们点到为止。

定理 3.8.4 (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。因为右边是左边特例。

（$\Leftarrow$）假定 Σ 的每一个有穷子集都是可满足的，我们用反证法证明 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，$\Sigma \vdash A \wedge \neg A$。由于每一证明长度都是有限的，存在 Σ 的一个有穷子集 Σ_0 使得 $\Sigma_0 \vdash A \wedge \neg A$。根据可靠性定理，$\Sigma_0 \models A \wedge \neg A$，因而 Σ_0 不可满足，这就是我们要的矛盾。 □

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

例 3.8.1. 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 L 的一致性。显然可靠性的证明等等都是在系统 L 外进行的，比如，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）能够告诉我们一个公式 α 是否是 L 中的一个定理。这个算法就是列真值表来看 α 是否为重言式。这样的算法对一阶逻辑系统不存在，即，一阶逻辑的不可判定性。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。计算机科学里面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，见

  `http://www.claymath.org/millennium/P_vs_NP/`

习题 3.7.

(1) 证明引理 3.8.1，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) 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。）

(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 φ，$\overline{v}(\varphi) = T$ 当且仅当 $\varphi \in \Delta$。（这是引理 3.8.5，因而也是完全性定理证明的一部分。）

(4) 证明从可靠性和完全性定理的弱形式（即，$\models \alpha$ 当且仅当 $\vdash \alpha$）和紧致性定理，我们可以证明可靠性和完全性定理的一般形式（即，$\Gamma \models \alpha$ 当且仅当 $\Gamma \vdash \alpha$）。

(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：考虑下表：

A	$\neg A$
0	1
1	1
2	0

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

证明所有 (A2) 和 (A3) 的逻辑推论都永远取值 0。]

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

(6) 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。

(7) 令 $\mathcal{L}_1$ 为仅包含联词 $\to$ 的命题逻辑语言；并且 L_1 是语言 $\mathcal{L}_1$ 上的一个证明系统，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。我们用 $\vdash_1 \varphi$ 表示 φ 是系统 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 ψ 是重言式，则 $\vdash_1 \psi$。

提示：你可以定义“极大一致集”的概念并且模仿定理 3.8.2 的证明。更进一步，称一个集合 Y 为 φ-极大的如果 $Y \nvdash_1 \varphi$ 但对所有的 $\alpha \notin Y$, $Y \cup \{\alpha\} \vdash_1 \varphi$。你可以先证明每一个 φ-极大的集合都是“极大一致”的。

第九节　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动词进行修饰的成分，如“必须”，“可能”，“应该”，“从前”，“将来”等等。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也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[8]。由于模态逻辑的范围太广泛了，我们下面仅谈论模态逻辑中命题逻辑的很小一部分，可以说是简而又简简介。

我们这一节的目的有两个，一是模态逻辑的丰富性使得它成为哲学逻辑的热门领域，值得我们花一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[9]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，而且也适用于直觉主义逻辑等其它逻辑。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，模态逻辑指的都是命题模态逻辑。

模态逻辑的语言比古典命题逻辑的语言（见第二节）仅仅多一个一元联词 $\Box$，也称为 模态算子。为了简单起见，我们假定联词只有 $\neg, \to$ 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：

[8] 刘易斯，Clarence Irving Lewis（1883 - 1964），美国逻辑学家，哲学家。
[9] 克里普克，Saul Kripke（1940 - ），美国逻辑学家，哲学家。

- 如果 α 是一个合式公式，则 $(\Box\alpha)$ 也是。

我们很容易有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，我们假定它的“管辖范围”也是尽可能短。举例来说，$\Box p \to \Box q$ 指的是 $((\Box p) \to (\Box q))$。

接下来，我们引进一元联词 $\Diamond$ 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”。但也有其它诸多解释，仅举两例：

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

(2) 我们也可以把 $\Box$ 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，会导致我们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。我们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。

克里普克的可能世界语义学

定义 3.9.1. *(a) 我们称一个二元组 $F = (W, R)$ 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。*

(b) 我们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。

(c) 我们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 $M = (W, R, V)$。

沿袭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 可以达到 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，如果我们只关心涉及到命题符号（比方说）A, B, C 的模态公式，那我们只需考虑赋值 V 在 A, B, C 上的定义就可以了，这一点是很自然的。

定义 3.9.2. *我们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 $(M, w) \models \alpha$，如下：*

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

(2) $(M,w)\models(\neg\beta)$ 当且仅当 $(M,w)\not\models\beta$ （即，$(M,w)\models\beta$ 不成立）；

(3) $(M,w)\models(\beta\to\gamma)$ 当且仅当 $(M,w)\not\models\beta$ 或者 $(M,w)\models\gamma$；

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

自然地，如果 $(M,w)\not\models\alpha$，则称 α 在模型 M 中的世界 w 中为 假。

定义 3.9.3. 我们称 α 在 模型 $M=(W,R,V)$ 中为真，记作 $M\models\alpha$，如果对所有的 $w\in W$ 都有 $(M,w)\models\alpha$。

例 3.9.1. 考虑框架 $F=(W,R)$，其中 $W=\{u,v,w\}$ 并且 $R=\{(u,v),(u,w)\}$:

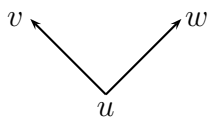

图 3.1: 框架 $F=(W,R)$ 示意图

定义赋值 $V:\{A,B\}\to\mathcal{P}(W)$ 为：$V(A)=\{u,v\}$ 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 $(M,u)\models\Box(A\to B)$ 但 $(M,u)\not\models A\to\Box B$（为什么？）。

定义 3.9.4. 我们称 α 为 普遍有效 的，记作 $\models\alpha$，如果对所有的模型 M，都有 $M\models\alpha$。

例 3.9.2. 证明：$\models\Box(\alpha\to\beta)\to(\Box\alpha\to\Box\beta)$。

证明: 给定模型 $M=(W,R,V)$ 和世界 $w\in W$，我们来验证

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

如果 $(M,w)\not\models\Box(\alpha\to\beta)$，则引用定义 3.9.2 中（3）即可。（这一点与古典命题逻辑相同。）因此我们可以假定 $(M,w)\models\Box(\alpha\to\beta)$ 来证明 $(M,w)\models\Box\alpha\to\Box\beta$。同理，只需在 $(M,w)\models\Box(\alpha\to\beta)$ 且 $(M,w)\models\Box\alpha$ 的假定下，证明 $(M,w)\models\Box\beta$ 即可。

我们验证定义 3.9.2 中的（4）：给定任意满足 wRw' 的世界 w'，根据假定，我们有 $(M,w')\models\alpha\to\beta$ 和 $(M,w')\models\alpha$，所以 $(M,w')\models\beta$。因此 $(M,w)\models\Box\beta$。 □

模态逻辑的一个推理系统 K

我们将第 六 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) 三组公理之上新添公理

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

注意：我们不仅在 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 [10]：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。自然地，我们也可以类似地定义 $\Gamma \vdash_K \alpha$。

例 3.9.3. 证明：$\vdash_K (\alpha \to \beta) \to (\Box\alpha \to \Box\beta)$。

证明: 首先注意古典命题逻辑的演绎定理仍然有效，因为演绎定理的证明只用到了(A1)和 (A2)。所以我们只需证明

$$\{\alpha \to \beta, \Box\alpha\} \vdash_K \Box\beta。$$

我们将逐项写出推理序列，而将每一步的理由留给读者：

1. $\alpha \to \beta$
2. $\Box(\alpha \to \beta)$
3. $\Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)$
4. $\Box\alpha \to \Box\beta$
5. $\Box\alpha$
6. $\Box\beta$。

□

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。但我们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：$\beta_1, \beta_2, \cdot$，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 $B_5 \to \neg B_5 \to B_{29}$。我们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的得到的关于 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 3.9.1. 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，我们有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。 □

[10] 必然化规则，Rule of Necessitation。

引理 3.9.2. 如果 $\{\alpha : \Box\alpha \in \Gamma\} \vdash_K \beta$，则 $\Gamma \vdash_K \Box\beta$。

证明: 练习。 □

仿照古典命题逻辑中的做法，我们定义 Γ 是一个 K-极大一致集 如果 Γ 是 K-一致的（定义留给读者），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起了关键的作用。

定理 3.9.1. 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$\Sigma$ 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。我们仍旧考察集合 $\Sigma = \{\alpha : \Box\alpha \in \Gamma\}$。

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，我们可以将 $\Sigma \cup \{\neg\beta\}$ 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 3.9.2，我们有 $\Gamma \vdash_K \Box\beta$，而作为 K-极大一致集，Γ 对 K 中的推理封闭。所以 $\Box\beta \in \Gamma$。 □

系统 K 的可靠性和完全性

由于是简介，我们只讨论可靠性和完全性的弱形式。

定理 3.9.2 (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: 练习。 □

定理 3.9.3 (模态逻辑 K 的完全性定理). 如果 $\models \alpha$，则 $\vdash_K \alpha$。

我们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 $(M, w) \not\models \alpha$。但在模态逻辑中，我们可以有更强的结论：我们可以找到一个模型 $M = (W, R, V)$，使得对任意 α，如果 $\nvdash_K \alpha$，则存在一个世界 $w \in W$，使得 $(M, w) \not\models \alpha$。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 3.9.5. 我们定义模态逻辑 K 的 典范模型 $M = (W, R, V)$ 为：$W = \{\Gamma : \Gamma$ 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 3.9.3. 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 $\Gamma \in W$，我们有 $(M, \Gamma) \models \alpha$ 当且仅当 $\alpha \in \Gamma$。

证明: 我们对模态公式 α 进行归纳。

我们先看 α 为命题符号 A_i 的初始情形：根据定义 3.9.2，$(M,\Gamma) \models A_i$ 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 3.9.2，$(M,\Gamma) \models \neg\beta$ 当且仅当 $(M,\Gamma) \not\models \beta$。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 $\beta \to \gamma$。我们这一条的验证留给读者。

情形 3：α 为 $\Box\beta$。假定 $(M,\Gamma) \models \Box\beta$。根据定义 3.9.2，对任意的 $\Delta \in W$，如果 $(\Gamma,\Delta) \in R$ 则 $(M,\Delta) \models \beta$；对β 和 Δ 使用归纳假定，我们有 $\beta \in \Delta$。再将 $(\Gamma,\Delta) \in R$ 按 R 的定义展开，我们有：对任意的 $\Delta \in W$，如果 $\{\alpha : \Box\alpha \in \Gamma\} \subseteq \Delta$ 则 $\beta \in \Delta$。由定理 3.9.1，$\Box\beta \in \Gamma$。反过来，假如 $\Box\beta \in \Gamma$，则由定理 3.9.1 和 R 的定义，我们有：对任意的 $\Delta \in W$，如果 $(\Gamma,\Delta) \in R$ 则 $\beta \in \Delta$。由归纳假定，$(M,\Delta) \models \beta$。所以 $(M,\Gamma) \models \Box\beta$。

这就完成了对引理的证明。 □

最后我们来证明定理 3.9.3。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 3.9.3，$(M,\Gamma) \not\models \alpha$。这与 α 的普遍有效性矛盾。

习题 3.8.

(1) 给出一个模型 $M = (W,R,V)$ 和世界 $u \in W$ 使得 $(M,u) \models A \to \Box B$ 但 $(M,u) \not\models \Box(A \to B)$。

(2) 判断下列陈述的正确性并给出理由：

(a) $(M,w) \not\models \alpha$ 当且仅当 $(M,w) \models \neg\alpha$。

(b) $M \not\models \alpha$ 当且仅当 $M \models \neg\alpha$。

(3) 在 K 中证明下列公式：

(a) $\Box(\alpha \wedge \beta) \to (\Box\alpha \wedge \Box\beta)$。

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

注意：虽然我们没有正式引入 $\wedge$ 和 $\vee$，但根据引理 3.9.1 你可以使用任何关于 $\wedge$ 和 $\vee$ 的古典重言式。

(4) 证明下列公式不是普遍有效的：

(a) $\Box(\alpha \vee \beta) \to (\Box\alpha \vee \Box\beta)$。

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

(5) 证明引理 3.9.2。

(6) 证明系统 K 的可靠性定理。

(7) 证明模型 $M = (W, R, V)$ 满足 $\Box\alpha \to \alpha$ 当且仅当关系 R 是自反的。[注：本题只是模态逻辑中大量的类似对应中的一个。]

第四章　一阶逻辑的语言

第一节　一阶逻辑的语言的定义和例子

学完了命题逻辑，我们对各种联词有了充分的了解，因而可以对由联词联结的复合语句进行精确的分析。但命题逻辑语言的“最小单位”是命题符号，我们无法深入到单个命题的里面来进行更细的研究，如对主语，谓语的分析等等。我们下面讨论的一阶语言能使我们克服这一缺陷。大家将会看到，一阶语言与我们通常用的数学语言甚至自然语言非常的接近。一阶逻辑是我们本课程的中心内容。

4.1.1　一阶语言的定义

一阶逻辑的语言 L 包括

(0) 括号：“(”和“)”；

(1) 命题联词：$\neg$ 和 $\rightarrow$；

(2) （全称）量词符号：$\forall$；

(3) 变元：$v_1, v_2, \cdots$；

(4) 常数符号：若干（可以没有，也可以有无穷多个）符号；

(5) 函数符号：对每一自然数 n，都有若干（可以没有，也可以有无穷多个）符号，称为 n-元函数符号；

(6) 谓词符号：对每一自然数 n，都有若干（可以没有，也可以有无穷多个）符号，称为 n-元谓词符号；

(7) 等词符号 （可以没有）：$\approx$。

注：与命题逻辑中联词的选取类似，一阶逻辑语言中的符号也与数学有密切的关系。我们逐项解释一下符号选取的动机。（但不要忘记，我们本节讨论的是语法，因此暂时仍要认为所有的符号都是没有意义的。）

语言中的 (0) 到 (3) 被称为逻辑符号。括号只是为了阅读方便。联词我们为了精炼只挑两个，但我们知道 $\{\neg, \to\}$ 是功能完全的，不会因此而失掉一般性。量词和变元是一阶逻辑的重要组成部分，有了它们，我们可以更精细地讨论数学对象之间的关系等等，在命题逻辑中则做不到这一点。此外，量词的“控制范围”和变元的变化范围也是逻辑学所关注的。所谓“一阶”逻辑，指的就是变元仅代表“个体”，量词所控制的也是“个体”。在后继课程中我们会看到二阶逻辑，其中就有两种不同的量词和变元，一种谈论“个体”（即与一阶逻辑相同），另一种谈论“（由个体组成的）集合”或“（个体之间）的关系”（即二阶部分）。尽管二阶逻辑的语言更丰富，但一阶逻辑在逻辑学中的主导地位仍是不可动摇的，原因之一是一阶逻辑有完全性，而二阶逻辑则没有。

语言中的 (4) 到 (7) 被称为非逻辑符号，可以说是从数学中提炼出来的。比如，当人们讨论自然数的性质时，指定专门一个符号代表数字零，指定专门的运算符号来代表加法和乘法是非常自然的。又比如，当人们研究图论时，指定符号代表“边”这个顶点之间的二元关系（即二元谓词）也是顺理成章的。此外，我们有意把等词写成弯的，用来区别数学中的等号 $=$。当然如果读者能够分清对象语言和元语言中符号的区别，则完全可以采用同一个符号。最后我们把等词 (7) 同 (6) 中一般的谓词符号分开，是因为（见后文）等词必须解释成等号，而一般的谓词则允许有不同的解释。

我们看几个例子。在讨论一阶语言时，我们通常只列出非逻辑符号，而默认逻辑符号已经包含在其中了。在多数讨论数学的场合，我们还默认包含等词 $\approx$。

例 4.1.1.

(1) 公理集合论的语言 $l_{Set} = \{\approx, \in\}$，其中 $\in$ 为一个二元谓词符号。

(2) 初等数论的语言为 $L = \{\approx, <, 0, S, +, \cdot\}$，其中 $<$ 为一个二元谓词符号，0 为一个常数符号，S 为一个一元函数符号，$+$ 和 $\cdot$ 为两个二元函数符号。

(3) 序关系的语言为 $L = \{R\}$，其中 R 为一个二元谓词符号，也可以选取 $L = \{R, \approx\}$。

规定好语言之后，我们就可以定义公式。但之前我们先要定义“项”这一概念。直观上说，项在公式中扮演名词在句子扮演的角色。

定义 4.1.1. 令 L 为一个一阶语言。定义 L 中所有 项 的集合为满足下列条件的最小的表达式的集合:

(1) 每个变元 v_i 都是一个项;

(2) 每个常数符号都是一个项;

(3) 如果 $t_1, t_2 \cdots, t_n$ 是项并且 f 为一个 n 元函数符号，则 $ft_1, t_2, \cdots, t_n$ 也是一个项。

注意：这又是“自上而下”的定义方式。

例 4.1.2. $S0$，$+v_1SSS0$ 和 $\times S0+0SSS0$ 都是初等数论里的项。

定义 4.1.2. 令 L 为一个一阶语言。定义 L 中所有 合式公式 （简称 公式）的集合为满足下列条件的最小的表达式的集合:

(1) 如果 $t_1,\cdots,t_n$ 为 L 中的项，并且 P 为一个 n 元谓词符号，则 $Pt_1,\cdots,t_n$ 是一个合式公式。我们称这样的公式为 原子公式 。特别地，$\approx t_1t_2$ 是一个原子公式。

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

(3) 如果 α 是合式公式，则 $\forall v_i\ \alpha$ 也是。

注：

(1) 我们引进符号 $\vee$，$\wedge$ 和 $\leftrightarrow$ 分别作为 $((\neg\alpha)\to\beta)$，$(\neg(\alpha\to(\neg\beta)))$，和 $((\alpha\to\beta)\wedge(\beta\to\alpha))$ 的简写。

(2) 我们用 $\exists x\alpha$ 作为 $(\neg\forall x(\neg\alpha))$ 的简写，并称 $\exists$ 为 存在量词。

(3) 我们用 $u\approx t$ 作为 $\approx ut$ 的简写，对其它二元谓词也同样处理；并且用 $u\not\approx t$ 作为 $(\neg\approx ut)$ 的简写。这样做的目的是增加可读性。

(4) 同命题逻辑一样，一阶逻辑的合式公式也有唯一可读性。证明从略。

(5) 同命题逻辑类似，在不引起混乱的情况下，我们也省略掉冗余的括号。除了第二章第四节的约定外，补充上“量词 $\forall$ 和 $\exists$ 的管辖范围尽可能短”这一条。例如，$\forall v_i\alpha\to\beta$ 指的是 $(\forall v_i\alpha)\to\beta$ 而不是 $\forall v_i(\alpha\to\beta)$。

(6) 我们通常会用大写的英文字母，如 P，Q, R 等等表示谓词符号；小写字母，如 x,y,z 表示变元；用 f,g,h 表示函数符号；a,b,c 表示常数符号；t 表示项；小写希腊字母，如 α，β，φ，σ，τ 等等表示公式；用大写希腊字母，如 Γ，Δ，Σ 表示公式集。虽然我们做不到完全没有例外，但把记号固定下来是一个好的习惯。

4.1.2　一阶语言公式的例子

我们下面给出一些用一阶语言公式的例子。这些例子说明一阶逻辑的语言具有很强的表达力。事实上，几乎所有数学命题皆可在某种一阶语言中表达。事实上，几乎所有一般的语句（数学的和非数学的）都可翻译为一个形式的一阶语言的语句。这种翻译其实与后面谈到的语义方面（如可定义性）关系更密切。但因为这是学习逻辑学的学生需要掌握的技能，（加上举例的必要性）我们也把它放在本节的语法讨论当中。需要注意的是：尽管我们在把一般的语句 A 翻译成一阶公式 α 时，期望 α 表达的就是 A；但以后我们会看

到，翻译成 α 之后，它仅仅是一个字符串而已，除了还原成 A 之外，我们无法避免 α 还可能有其它的解释。这在讲语义时再详细谈。

哲学语言 由于分析哲学的原因，很多哲学家喜欢用一阶语言重述一些哲学命题。这些命题都是自然语言表达的，而自然语言的谓词和函数并无一个明确的列表，所以我们不可能把用于哲学目的的一阶语言的所有非逻辑符号都列出来。但不管怎样，自然语言的谓词和函数是有穷的，所以我们的 l 的符号总是够用。在同一语境下，我们总是可以把谓词和函数符号编上号以示区别。

1. 当今的法国国王是秃子。

   $$\forall x(P_1^1(x) \to P_2^1(x))。$$

   这里 P_1^1 的上标 1 表示 P_1^1 是一个一元谓词，下标说明它代表第一个（在我们的编号顺序下）谓词。我们把 P_1^1 和 P_2^1 的选择留给大家。注意，翻译的结果可能不唯一。

2. 金山不存在。

   $$\neg\exists x(P_3^1(x) \wedge P_4^1(x))。$$

3. 晨星即暮星。

   $$\forall x(P_5^1(x) \to \forall y(P_6^1(y) \to x \approx y))。$$

一阶算术语言 $L = \{\approx, <, 0, S, +, \cdot\}$

1. 0 不是任何自然数的后继。

   $$\forall x(Sx \not\approx 0)。$$

2. 两个自然数的后继相等当且仅当这两个自然数相等。

   $$\forall x\forall y(x \approx y \leftrightarrow Sx \approx Sy)。$$

   如果不使用省略的形式，则以上命题应该写作：

   $$\forall x\forall y(\neg((x \approx y \to Sx \approx Sy) \to \neg(Sx \approx Sy \to x \approx y)))。$$

3. 给定任意公式 $\varphi(v_1)$，数学归纳原理可以表示为以下公式：

   $$(\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(Sx))) \to \forall x(\varphi(x))。$$

4. x 是素数。

   首先，这个命题可以理解为：

   $$x > 1 \text{ 并且 } x \text{ 没有除自身和 } 1 \text{ 之外的因子。}$$

   这样我们得到如下公式：

   $$S0 < x \wedge \forall y\forall z((y < x \wedge z < x) \to y \cdot z \not\approx x)。$$

集合论语言 $l_{Set} = \{\approx, \in\}$

1. 两个集合相等当且仅当它们有共同的元素。

$$\forall x \forall y (x \approx y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y))。$$

2. x 是 y 的子集。

$$\forall z (z \in x \to z \in y)。$$

3. x 是 y 的幂集。

$$\forall z (z \in x \leftrightarrow \forall u (u \in z \to u \in y))。$$

4. 集合 z 是空集。

$$\forall x (x \notin z)。$$

5. 选择公理 选择公理有很多种等价的表述，我们找一个比较容易叙述的：

$$\begin{aligned}&\forall X ((X \neq \emptyset \wedge \emptyset \notin X) \to \\ &\exists C (\forall u \in X (\exists a (a \in u \wedge a \in C) \\ &\wedge \forall a (\forall b (a \in u \wedge a \in C \wedge b \in u \wedge b \in C) \to a = b))))。\end{aligned}$$

注意到其中 $\emptyset$ 不是我们语言 l_{Set} 中的常数符号，我们要利用它的定义来替换它。具体做法是将第一行换成：

$$\forall X (\forall z (\forall x (x \notin z) \to (X \neq z \wedge z \notin X)) \to$$

其余不变。

最后再举两个代数中的例子：

群论语言 $l_g = \{e, +\}$

群的公理可以表达如下：

1. 群的运算满足结合律。

$$\forall a \forall b \forall c (a + (b + c)) \approx (a + b) + c)。$$

2. e 是单位元。

$$\forall a (e + a \approx a)。$$

3. 每个元素都有逆元。

$$\forall a(\exists b(a+b\approx e))。$$

4. 如果群的运算还满足交换律，即

$$\forall a\forall b(a+b\approx b+a)。$$

则这样的群称为交换群或阿贝尔群。

环的语言 对群的语言扩张得到环论语言$l_R\approx\{e,+,\cdot\}$。除了以上四条公理外，环论的公理还包括：

5. 乘法结合律。

$$\forall a\forall b\forall c(a\cdot(b\cdot c))\approx(a\cdot b)\cdot c)。$$

6. 乘法对加法的分配律。

$$\forall a\forall b\forall c(a\cdot(b+c)\approx a\cdot b+a\cdot c)。$$

第二节　自由出现和约束出现

接下来我们讨论语法中另一个现象：变元的自由出现和约束出现。在数学中，一个表达式常常含有两类不同的变元，例如，$\int_0^1 f(x,t)dt$，$\sum_{i=1}^n a_i$ 等。在积分的例子中，变元 x 和 t 所起的作用是不同的；在求和的例子中，变元 n 和 i 的作用也不同。变元 t 和 i 主要起的是占位的作用，也有人管它们叫“哑元”。哑元可以被替换成任意“新的”变元而不影响公式的意义，比如 $\sum_{i=1}^n a_i$ 和 $\sum_{j=1}^n a_j$ 意义完全相同。而例中变元 x 和 n 则不能被随便替换。逻辑中，约束变元就与哑元类似。

直观上说，一个变元是自由的如果没有任何量词“管”着它。更准确地说，我们递归地定义“变元 x 在公式 α 中 **自由出现**” 如下：

1. 如果 α 是一个原子公式，则 x 在 α 中自由出现当且仅当 x 在 α 中出现。

2. 如果 α 为 $(\neg\beta)$，则 x 在 α 中自由出现当且仅当 x 在 β 中自由出现。

3. 如果 α 为 $(\beta\to\gamma)$，则 x 在 α 中自由出现当且仅当 x 在 β 中自由出现或在 γ 中自由出现。

4. 如果 α 为 $\forall v_i\beta$，则 x 在 α 中自由出现当且仅当 x 在 β 中自由出现并且 $x\neq v_i$。

在 α 中出现的变元如果不是自由出现，则被称为 **约束出现** [1] 。

如果在公式 α 中没有变元自由出现，则称 α 为一个 **闭语句** 或 **语句** 。

分清楚自由变元与约束变元之后，我们引进一个关于替换的表达式，这在后面会经常用到。我们用 α_t^x （也有的书用 $\alpha(x \mid t)$ 等不同记号）表示在公式 α 中将变元 x 在其自由出现的地方用项 t 替换后得到的公式。α_t^x 也可以用递归的方法定义如下：

(1) 如果 α 是原子公式，则 α_t^x 将 α 中所有的 x 用 t 替换所得的表达式。

(2) $(\neg\alpha)_t^x = (\neg\alpha_t^x)$。

(3) $(\alpha \to \beta)_t^x = (\alpha_t^x \to \beta_t^x)$。

(4) $(\forall y\alpha)_t^x$ is $\begin{cases} \forall y(\alpha_t^x), & \text{如果 } x \neq y; \\ \forall y\alpha, & \text{如果 } x = y。 \end{cases}$

习题 4.1.

(0) 选择一阶逻辑语言，并将下列语句转换成一阶语句。你认为推理有错误吗？为什么？

(a) 如果存在存在着的鬼，则鬼存在。

(b) 存在着的鬼当然存在。

(c) 鬼存在。

(1) 假定我们的一阶语言中有一元谓词符号 N 和 I，分别用来表示“是一个数”和“好玩的”；二元谓词符号 $<$ 表示“小于”；还有常数符号 0 表示数字零。将下列中文语句转换成该一阶语言的公式。你可能会得到不同的结果，因为语句可能会有歧义。

(a) 零小于所有的数。

(b) 要是有数好玩的话，零就好玩。

(c) 没有小于零的数。

(d) 要是一个不好玩的数满足所有比它小的数都好玩这条性质，则它本身也好玩。

(e) 不存在所有数都比它小的数。

(f) 不存在没有数不比它小的数。

[1] 约束出现，bounded occurrence，也被译作“受囿出现”

(2) 沿用上题的一阶语言，将下列一阶语句转换成日常的中文。

$$\forall x(Nx \to Ix \to \neg\forall y(Ny \to Iy \to \neg x < y)).$$

注意：虽然我们无法定义“日常中文”但“对所有的 x, 如果 Nx 则 ...”绝对不属于日常中文。

(3) 假定我们的一阶语言中有二元函数符号 $+$ 和 $\cdot$，分别用来表示“加法”和“乘法”；常数符号 $1, 2, 3, 4$ 分别表示数字一、二、三、四。再假定变元都代表整数。

(a) 将下列一阶语言的公式转换成中文语句:

$$(\forall x)[(\exists m)[x \approx 2 \cdot m + 1] \to (\exists n)[x \cdot x \approx 2 \cdot n + 1]]。$$

(b) 将下列中文语句转换成该一阶语言的公式：“没有形如 $4k + 3$ 的整数是平方和”。

(4) （下面的练习严格说与本节没有关系，请大家当作数学练习来做。）

(a) 在数学分析中，极限的定义如下：$\lim\limits_{x\to a} f(x) = l$ 当且仅当

$$(\forall \epsilon \in \mathbb{R}^+)(\exists \delta \in \mathbb{R}^+)(\forall x \in \mathbb{R})[0 <\mid x - a \mid< \delta \to \mid f(x) - l \mid< \epsilon]。$$

写出 $\lim\limits_{x\to a} f(x) \neq l$ 的定义。

(b) 在线性代数中，我们说向量组 $\vec{x}_1, \vec{x}_2, \cdots, \vec{x}_n$ 是线性相关的，如果

$$(\exists c_1 \in \mathbb{R})(\exists c_2 \in \mathbb{R}) \cdots (\exists c_n \in \mathbb{R})[(\text{不全为零}) \wedge c_1\vec{x}_1 + c_2\vec{x}_2 + \cdots + c_n\vec{x}_n = \vec{0}]。$$

写出向量组 $\vec{x}_1, \vec{x}_2, \cdots, \vec{x}_n$ 为线性无关的定义。

第五章　形式证明

第一节　一阶逻辑的一个公理系统

我们回忆一下在命题逻辑中学过的知识。令 Λ 为一个公理集，并且 Γ 为一个公式集。一个从 Γ 到 φ 的一个证明或推演是一个公式序列

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

使得 $\alpha_n = \varphi$ 并且对所有的 $i \leq n$，公式 α_i 或者属于 $\Gamma \cup \Lambda$，或者存在 $j, k < i$，α_i 是利用分离规则从 α_j 和 α_k 得到的（即 $\alpha_k = \alpha_j \to \alpha_i$）。如果存在一个从 Γ 到 φ 的一个推演，则称 φ 为 Γ 的一个定理，记为 $\Gamma \vdash \varphi$。

上述的关于证明的定义对一阶逻辑仍然适用。所不同的仅仅是我们的公理集合变得更复杂了。推理规则依然只有分离规则。

我们现在描述一个一阶逻辑的推演系统的公理集 Λ。它们被分成 6 组。首先我们称公式 φ 是公式 ψ 的一个 **全称概括** 或 **概括** 如果存在自然数 $n \geq 0$ 和变元 $x_1, x_2, \cdots, x_n$ 使得

$$\varphi = \forall x_1 \forall x_2 \cdots \forall x_n \psi。$$

注意：当 $n = 0$ 时，ψ 的全称概括 φ 就是 ψ 本身。一阶逻辑的公理集是由形如下列公式的概括所组成的，其中 x 和 y 为变元并且 α 和 β 为公式：

1. 形如命题逻辑公理中 (A1), (A2), (A3) 的一阶公式；

2. $\forall x \alpha \to \alpha_t^x$，其中项 t 可以在 α 中替代 x。

3. $\forall x(\alpha \to \beta) \to (\forall x \alpha \to \forall x \beta)$；

4. $\alpha \to \forall x \alpha$，其中 x 不在 α 中自由出现。

在语言中包含等词的情形下，还要添上

5. $x \approx x$；

6. $x \approx y \to (\alpha \to \alpha')$，其中 α 为原子公式并且 α' 是将 α 中出现若干个 x 用 y 替换所得到的，（这里若干个可以是零个，一个或多个，但不一定是全部）。

我们逐条解释。

首先看第一组公理。如果一个一阶公式 α 是一个原子公式或者是一个全称公式，即形如 $\forall x\beta$，则我们称 α 为一个 素公式 。对于任何一个一阶公式 φ，我们将它的所有的素子公式分别替换成命题符号，就得到命题逻辑中的一个公式 φ'。如果 φ' 在命题逻辑中属于公理 (A1)，(A2)，或 (A3)，或者是重言式，我们则分别称 φ 为 形如 (A1)，(A2) 或 (A3)，或是（一阶意义下的）重言式。 比如下列一阶公式 φ：

$$(\forall y \neg Py \to \neg Px) \to (Px \to \neg \forall y \neg Py)$$

就是一个一阶逻辑中的重言式，其对应的 φ' 为 $(A_1 \to \neg A_2) \to (A_2 \to \neg A_1)$。 [读了模态逻辑那一节的读者对这种想法不应该感到陌生。]

根据命题逻辑里的完全性定理，我们有

定理 5.1.1. *如果 φ 是一个一阶意义下的重言式，则 $\vdash \varphi$，即 φ 为一阶逻辑的一个内定理。*

我们再看第二组公理，通常称为 替换公理。 它的直观意义是显然的：如果 α 对所有的 x 都对，则 α 对项 t 也对。但是由于我们正在讨论语法，而 α_t^x 仅仅是机械地将 α 中自由出现的 x 换成 t，如果我们不小心的话，会出现下列我们不想要的结果：

例 5.1.1. *令 α 为一阶公式 $\exists y\ x \not\approx y$。则 $\forall x\alpha \to \alpha_z^x$ 为*

$$\forall x \exists y\ x \not\approx y \to \exists y\ z \not\approx y。$$

但是 $\forall x\alpha \to \alpha_y^x$ 则成为

$$\forall x \exists y\ x \not\approx y \to \exists y\ y \not\approx y。$$

因此我们需要加些条件以区别上例中的两个替换。仔细观察表明，问题出在项 t 里面的变元 y 在替换 α 中的 x 之后被量词 $\exists y$ “抓住了”，或者说，y 在替换前是自由的，而替换后却变成约束的了。我们需要禁止这样的 t 来替换 α 中的 x。固定项 t 和变元 x 我们通过对公式 α 递归将短语“t 在 α 中可以替换 x” 精确定义如下：

(1) 对原子公式 α，t 总可以在 α 中替换 x。

(2) t 在公式 $\neg\beta$ 中可以替换 x 当且仅当 t 在 β 中可以替换 x; t 在公式 $\beta \to \gamma$ 中可以替换 x 当且仅当 t 在 β 和 γ 中都可以替换 x。

(3) t 在公式 $\forall y\beta$ 中可以替换 x 当且仅当

(a) x 不在 $\forall y\beta$ 中自由出现；或者

(b) y 不在 t 中出现并且 t 在 β 中可以替换 x。

例 5.1.2. 变元 x 在任何公式 φ 中都可以替换自己。从而对任何公式 φ，我们有 $\forall x\varphi \vdash \varphi$。

证明: 见习题 5.1。 □

第三和第四组公理的作用是证明下列“概括定理”，也有教科书将它作为推理规则，称为“概括规则”。在数学中经常有这样的论证：假如我们不用任何关于 x 的假设就证明了命题 $\alpha(x)$，我们就可以说“因为 x 是任意的，所以我们有 $\forall x\alpha(x)$”。概括定理说的也是这个意思。

定理 5.1.2 (概括定理). 如果 $\Gamma \vdash \varphi$ 并且 x 不在 Γ 的任何公式中自由出现，则 $\Gamma \vdash \forall x\varphi$。

证明: 令 $(\varphi_1, \varphi_2, \cdots, \varphi_n)$ 为 φ 的一个推演序列。我们归纳证明对任意 $i \leq n$，$\Gamma \vdash \forall x\varphi_i$。假定对所有的 $j < i$，我们已经有 $\Gamma \vdash \forall x\varphi_j$。我们考察 φ_i。

情形 *1:* φ_i 是逻辑公理。则 $\forall x\varphi_i$ 也是逻辑公理 (为什么?)。显然 $\Gamma \vdash \forall x\varphi_i$。注意，在这种情况下，$x$ 可能在 φ_i中自由出现，但这不是问题。

情形 *2:* φ_i 属于 Γ。此时 x 不在 φ_i 中自由出现，所以 $\varphi_i \to \forall x\varphi_i$ 属于第四组公理，由分离规则， $\Gamma \vdash \forall x\varphi_i$。

情形 *3:* φ_i 由分离规则从 φ_j 和 $\varphi_k = \varphi_j \to \varphi_i$得到，其中$j, k < i$。由归纳假设，$\Gamma \vdash \forall x\varphi_j$ 和 $\Gamma \vdash \forall x(\varphi_i \to \varphi_i)$。对公理

$$\forall x(\varphi_j \to \varphi_i) \to (\forall x\varphi_j \to \forall x\varphi_i),$$

两次使用分离规则，我们就得到了 $\Gamma \vdash \forall x\varphi_i$。 □

例 5.1.3. 证明 $\forall x\forall y\alpha \vdash \forall y\forall x\alpha$。

证明: 根据例 5.1.2，$\forall x\forall y\alpha \vdash \alpha$。由于变元 x 在左端不自由出现，根据概括定理，我们有

$$\forall x\forall y\alpha \vdash \forall x\alpha。$$

同样地，

$$\forall x\forall y\alpha \vdash \forall y\forall x\alpha。$$

□

在语言中包含等词的情形下，第五条和第六组公理都不难理解。当然第六组公理实际上对任何公式 α 都成立。我们把 α 限制在原子公式上，仅仅是为了让公理更精炼，附带的一个好处是更容易证明其可靠性。更多的有关等词的内定理请见本章第三节末尾。

习题 5.1.

(1) 以下公式是公理吗？如果是，属于哪组公理？

(a) $[(\forall xPx \to \forall yPy) \to Pz] \to [\forall xPx \to (\forall yPy \to Pz)]$。

(b) $\forall y[\forall x(Px \to Px) \to (Pc \to Pc)]$。

(c) $\forall x\exists yPxy \to \exists yPyy$。

(2) 证明变元 x 在任何公式 φ 中都可以替换自己。

(3) （本练习讨论公理的独立性。）证明：如果没有第二组替换公理，则其余的公理不能证明 $\forall x(x \not\approx x) \to x \not\approx x$。*提示*：定义函数 $h : \{\text{公式}\} \to \{0, 1\}$ 满足对所有的素公式 α，$h(\alpha) = 1$；然后将其自然地扩展到 $h(\neg\alpha)$ 和 $h(\alpha \to \beta)$ 上。证明如果 σ 为其余公理的一个语法后承，则 $h(\sigma) = 1$。

第二节　推理和元定理

引理 5.2.1 (重言规则). *如果 $\Gamma \vdash \alpha_1$，$\Gamma \vdash \alpha_2$，$\cdots$，$\Gamma \vdash \alpha_n$ 并且 $\alpha_1 \to \alpha_2 \to \cdots \to \alpha_n \to \beta$ 是一阶意义下的重言式，则 $\Gamma \vdash \beta$。*

证明: 依照定理 5.1.1，$\alpha_1 \to \alpha_2 \to \cdots \to \alpha_n \to \beta$ 是一个内定理，只需对这个内定理使用 n 次分离规则即可。□

例 5.2.1. *由于 $\{\alpha \to \beta, \beta \to \alpha\}$ 重言蕴涵 $\alpha \leftrightarrow \beta$，因此若想证明 $\Gamma \vdash \alpha \leftrightarrow \beta$，则只需证明 $\Gamma \vdash \alpha \to \beta$ 并且 $\Gamma \vdash \beta \to \alpha$。*

定理 5.2.1 (演绎定理). *$\Gamma \cup \{\gamma\} \vdash \varphi$ 当且仅当 $\Gamma \vdash (\gamma \to \varphi)$。*

证明: 与命题逻辑中的演绎定理的证明相同。□

推论 5.2.1 (逆否命题). *$\Gamma \cup \{\varphi\} \vdash \neg\psi$ 当且仅当 $\Gamma \cup \{\psi\} \vdash \neg\varphi$。*

同命题逻辑一样，我们称一个公式集为 *不一致的* 如果存在公式 β，β 和 $\neg\beta$ 都是它的定理。在这种情形下，任何公式 α 都是它的定理。

推论 5.2.2 (反证法 (RAA)). *如果 $\Gamma \cup \{\varphi\}$ 不一致，则 $\Gamma \vdash \neg\varphi$。*

两个推论的证明留给读者。

例 5.2.2. $\vdash \exists x\forall y\varphi \to \forall y\exists x\varphi$。

证明（的思路）. 我们尝试以反推的方式去证明。

要证明以上命题，只需证明 $\exists x\forall y\varphi \vdash \forall y\exists x\varphi$ (为什么?)。

而这只需证明 $\exists x\forall y\varphi \vdash \exists x\varphi$ (为什么?)，即 $\neg\forall x\neg\forall y\varphi \vdash \neg\forall x\neg\varphi$。

这又只需证明 $\forall x\neg\varphi \vdash \forall x\neg\forall y\varphi$ (为什么?)。

这只需证明 $\forall x\neg\varphi \vdash \neg\forall y\varphi$ (为什么?)。

这只需证明 $\{\forall x\neg\varphi, \forall y\varphi\}$ 是不一致的 (为什么?)，而这很容易证明 (为什么?)。 □

上面的例子中鼓励我们去寻找由 Γ 证明 φ 的一般方法。我们先总结由 Γ 证明 φ 的一些有用技巧，这些技巧帮助我们利用 φ 的句法形式来寻找证明:

(1) 假设 φ 是 $(\psi \to \theta)$，则根据演绎定理，只需证明 $\Gamma \cup \{\psi\} \vdash \theta$。

这是最为常用也最为有效的方法，几乎每一个形式推演的构造都会用到。演绎定理的好处是既减少了待证结论的复杂性，又增加了可用的前提。

例 5.2.3. 令 $\Gamma = \emptyset$，$\varphi = \forall x(\alpha \to \beta) \to (\exists x\alpha \to \exists x\beta)$。根据上面的方法，要证明

$$\varnothing \vdash \forall x(\alpha \to \beta) \to (\exists x\alpha \to \exists x\beta)$$

只需证明

$$\forall x(\alpha \to \beta) \vdash \exists x\alpha \to \exists x\beta。$$

利用重言规则将右边取逆否命题，我们只需要证明

$$\forall x(\neg\beta \to \neg\alpha) \vdash \forall x\neg\beta \to \forall x\neg\alpha。$$

而再次运用以上的方法，我们只需要证明:

$$\{\forall x(\neg\beta \to \neg\alpha), \forall x\neg\beta\} \vdash \forall x\neg\alpha。 \tag{5.1}$$

而这可由分离规则以及公理容易得到。

(2) 假设 φ 是 $\forall x\psi$。如果 x 不在 Γ 中自由出现，则根据概括定理，只需证明 $\Gamma \vdash \psi$。后面（定理 5.3.2）我们会看到：即使 x 在 Γ中自由出现，仍可以找到一个变元 y 使得 $\Gamma \vdash \forall y\psi^x_y$ 且 $\forall y\psi^x_y \vdash \forall x\psi$。

依然考虑上面的例子，当我们进行到 (5.1)，根据现在的方法，我们只需证明

$$\{\forall x(\neg\beta \to \neg\alpha), \forall x\neg\beta\} \vdash \neg\alpha。$$

而由于 $\forall x(\neg\beta \to \neg\alpha) \vdash \neg\beta \to \neg\alpha$ 且 $\forall x\neg\beta \vdash \neg\beta$，根据重言规则，我们只需要证明

$$\{\neg\beta \to \neg\alpha, \neg\beta\} \vdash \neg\alpha。$$

而这又是显然的。

(3) 假设 φ 另一个公式的否定。

(a) 如果 φ 是 $\neg(\psi \to \theta)$，那就只需证明 $\Gamma \vdash \psi$ 和 $\Gamma \vdash \neg\theta$。

(b) 如果 φ 是 $\neg\neg\psi$，那就只需证明 $\Gamma \vdash \psi$。

(c) 如果 φ 是 $\neg\forall x\psi$。尝试找到项 t，它在 ψ 中可以替换 x，并且 $\Gamma \vdash \neg\psi_t^x$，这就足够了，可惜的是，这并非总是能做到。原因在于，虽然 $\Gamma \vdash \neg\alpha_t^x$ 一定蕴涵 $\Gamma \vdash \neg\forall x\alpha$，但反之并不总是成立。如果不能做到，尝试换位。然后，尝试归谬法，等等。

例 5.2.4. 证明 $\forall x\neg(\alpha \to \beta) \vdash \neg(\alpha \to \exists x\beta)$。根据 *3(a)* 中的建议，我们只需证明

$$\forall x\neg(\alpha \to \beta) \vdash \alpha \quad \text{并且} \quad \forall x\neg(\alpha \to \beta) \vdash \neg\exists x\beta。$$

根据 $\forall x\neg(\alpha \to \beta) \vdash \neg(\alpha \to \beta)$ 并且 $\neg(\alpha \to \beta)$ 重言蕴涵 α，前式成立。再看后式，$\neg\exists x\beta$ 是 $\neg\neg\forall x\neg\beta$ 的缩写，利用 *3(b)* 和概括定理，我们只需证明 $\forall x\neg(\alpha \to \beta) \vdash \neg\beta$，而这显然与前式的证明类似。

我们上面的总结不够理想。理想的情形是找到一个算法，使得对任何可证的 φ，都提供一个证明。要是有这样的算法的话，一阶逻辑就是可判定的。但在后续课程中我们会证明丘奇定理：一阶逻辑是不可判定的。因此这种理想的算法是不存在的。

习题 5.2.

(1) 给出一个从空集 $\emptyset$ 到 $\forall x\varphi \to \exists x\varphi$ 的一个推演。[注意：本题要求你给出推演序列，不准使用任何元定理。]

(2) 假设有一个从公式集 Γ 到 φ 长度为 n 的推演序列，并且 x 不在 Γ 中自由出现，概括定理告诉我们存在一个从 Γ 到 $\forall x\varphi$ 的一个推演序列，令函数 $f(n)$ 表示该序列的长度。找出一个函数增长速度尽可能慢的 f。

(3) (a) 证明如果 $\vdash \alpha \to \beta$，则 $\vdash \forall x\alpha \to \forall x\beta$。

(b) 证明 $\alpha \to \beta \models \forall x\alpha \to \forall x\beta$ 不一定总成立。

(4) 证明：

(a) $\vdash \exists x(Px \to \forall xPx)$。

(b) $\{Qy, \forall y(Qy \to \forall zPz)\} \vdash \forall xPx$。

(5) 证明内定理：

(a) $\exists x\alpha \vee \exists x\beta \leftrightarrow \exists x(\alpha \vee \beta)$。

(b) $\forall x\alpha \vee \forall x\beta \rightarrow \forall x(\alpha \vee \beta)$。

(c) $\exists x(\alpha \wedge \beta) \rightarrow \exists x\alpha \wedge \exists x\beta$。

(d) $\forall x(\alpha \wedge \beta) \leftrightarrow \forall x\alpha \wedge \forall x\beta$。

(e) $\forall x(\alpha \rightarrow \beta) \rightarrow (\exists x\alpha \rightarrow \exists x\beta)$。

(f) $\exists x(Py \wedge Qx) \leftrightarrow Py \wedge \exists xQx$。

第三节　其它元定理

我们下面介绍几个后面要用到的元定理。首先是常数概括定理，我们在一阶逻辑完全性定理的证明中会用到它。回忆一下概括定理及其证明，我们会发现变元 x 起的仅仅是占位的作用，因此如果把变元 x 换成常数 c，类似证明大概也可以通过。当然我们不能直接对常数符号使用量词，而要用另一个新的变元 y 来作为被概括的变元。

定理 5.3.1 (常数概括定理). *假设 $\Gamma \vdash \varphi$ 而 c 是一个不在 Γ 中出现常数符号，则存在变元 y，它不在 φ 中出现，使得 $\Gamma \vdash \varphi_y^c$。更进一步，存在一个从 Γ 到 $\forall y\varphi_y^c$ 的不含 c 的推演。*

证明: 令 $(\alpha_0, \alpha_1, \cdots, \alpha_n)$ 为一个由 Γ 到 φ 的推演序列，令 y 是不出现于任一 α_i 中的变元，则

$$((\alpha_0)_y^c, (\alpha_1)_y^c, \cdots, (\alpha_n)_y^c) \qquad (*)$$

是由Γ 到 φ_y^c 的推演。

情形 *1:* α_k 属于 Γ。此时 $(\alpha_k)_y^c$ 是 α_k，因为 c 不在 α_k 中出现。

情形 *2:* α_k 是逻辑公理。此时 $(\alpha_k)_y^c$ 仍是逻辑公理。例如，如果 α_k 形如 $\forall x\beta \rightarrow \beta_t^x$，则 $(\alpha_k)_y^c$ 是 $\forall x(\beta)_y^c \rightarrow (\beta_t^x)_y^c$，注意到 $(\beta_t^x)_y^c$ 正是 $(\beta_y^c)_{t_y^c}^x$，所以它仍是逻辑公理。其它组的公理也容易验证。

情形 *3:* α_k 是从 α_i 和 $\alpha_j = \alpha_i \rightarrow \alpha_k$ 施行分离规则而得到的，其中 $i, j < k$。则 $(\alpha_j)_y^c$ 为 $(\alpha_i)_y^c \rightarrow (\alpha_k)_y^c$。因而 $(\alpha_k)_y^c$ 也是从 $(\alpha_i)_y^c$ 和 $(\alpha_j)_y^c$ 施行分离规则而得到的。

我们下面验证“更进一步”部分。令 Γ_0 为推演 (*) 中用到的 Γ 中的公式的集合。Γ_0 显然是一个有穷集。我们有 $\Gamma_0 \vdash \varphi_y^c$ 并且 y 不在 Γ_0 中出现。根据概括定理，$\Gamma_0 \vdash \forall y\varphi_y^c$，所以 $\Gamma \vdash \forall y\varphi_y^c$。注意到概括定理的证明中并没有引进新的常数符号，我们就得到了一个从 Γ 到 $\forall y\varphi_y^c$ 的推演，c 不出现于其中。 □

引理 5.3.1 (循环替换引理). 如果变元 y 完全不在公式 φ 中出现，则变元 x 可以在公式 φ_y^x 中替换 y 并且 $(\varphi_y^x)_x^y = \varphi$。

证明: 见习题 5.3。 □

推论 5.3.1. 假定 $\Gamma \vdash \varphi_c^x$，其中常数符号 c 在 Γ 和 φ 中都不出现。则 $\Gamma \vdash \forall x\varphi$，并且有一个 c 完全不出现的从 Γ 到 $\forall x\varphi$ 的一个推演。

证明: 根据常数概括定理，我们有一个从 Γ 到 $\forall y(\varphi_c^x)_y^c$ 的推演，其中不出现常数符号 c。由于 c 不在 φ 中出现，$\forall y(\varphi_c^x)_y^c$ 就是 $\forall y\varphi_y^x$。再根据循环替换定理和概括定理，我们就有 $\forall y\varphi_y^x \vdash \forall x\varphi$。（为什么？） □

下面一个定理我们在前面已经间接地涉及到不止一次了。直观上很容易理解。由于我们在完全性定理的证明中也要用到它，让我们给出详细证明。

定理 5.3.2 (约束变元替换定理). 令 φ 为一公式，t 为一个项，还有 x 为一个变元。我们总可以找到一个公式 φ'，它和 φ 的差别仅在于约束变元，使得

(a) $\varphi \vdash \varphi'$ 并且 $\varphi' \vdash \varphi$;

(b) t 可以在 φ' 中替换 x。

证明: 固定项 t 和变元 x，我们递归地从 φ 构造 φ'。如果 φ 是原子公式，则令 $\varphi' = \varphi$。如果 φ 是 $\neg\psi$ 则令 $\varphi' = \neg\psi'$。如果 φ 是 $(\psi_1 \to \psi_2)$，则令 $\varphi' = \psi_1' \to \psi_2'$。

我们来看最重要的情形：即 φ 是 $\forall y\psi$。选一个在 ψ' 和 t 和 x 中都不出现的变元 z。定义 $(\forall y\psi)'$ 为 $\forall z(\psi')_z^y$。

显然（或用归纳证明）φ 和 φ' 的区别仅在于约束变元。我们对 φ 施行归纳来证明 (a) 和 (b)。我们只验证最重要的量词情形，因为其它的都很简单。根据归纳假设和变元 z 的选取，(b) 成立。（为什么？）

我们下面验证 (a)。

根据归纳假设，我们有 $\psi \vdash \psi'$。所以 $\forall y\psi \vdash \forall y\psi'$。由于 z 不在 ψ' 中出现，我们有 $\forall y\psi' \vdash (\psi')_z^y$。根据概括规则，我们得到 $\forall y\psi' \vdash \forall z(\psi')_z^y$。所以 $\forall y\psi \vdash \forall z(\psi')_z^y$。

再看另一方向。首先 $\forall z(\psi')_z^y \vdash ((\psi')_z^y)_y^z$。根据循环替换定理，后者就是 ψ'。根据归纳假设，我们有 $\psi' \vdash \psi$。所以 $\forall z(\psi')_z^y \vdash \psi$。通过分析 y 是否等于 z 很容易看出变元 y 不在左端自由出现。由概括定理，我们就有 $\forall z(\psi')_z^y \vdash \forall y\psi$。 □

最后让我们列出几个有关等词 $\approx$ 的几个内定理。这些等词的性质是很显然的，而且在证明完全性定义是也会用到。它们的证明我们留作习题。

(Eq1) $\forall x\ x \approx x$。

(Eq2) $\forall x\forall y(x \approx y \to y \approx x)$。

(Eq3) $\forall x\forall y\forall z(x \approx y \to y \approx z \to x \approx z)$。

（在下一章学了语义之后看就会看到）这三条性质说明 $\approx$ 的解释一定是一个等价关系。事实上，它还与所有的谓词和函数“相容”：

(Eq4) 对所有 n-元谓词符号 P 我们有

$$\forall x_1\cdots\forall x_n\forall y_1\cdots\forall y_n(x_1 \approx y_1 \to \cdots \to x_n \approx y_n \to Px_1\cdots x_n \to Py_1\cdots y_n)。$$

(Eq5) 对所有 n-元函数符号 f 我们有

$$\forall x_1\cdots\forall x_n\forall y_1\cdots\forall y_n(x_1 \approx y_1 \to \cdots \to x_n \approx y_n \to fx_1\cdots x_n \approx fy_1\cdots y_n)。$$

第四节　前束范式

一般说来，范式或标准型的存在会给我们的研究带来一些方便，因为我们可以只注意某种特殊的（即，规范的，或标准的）形式，从而避免处理较为杂乱的一般形式。在命题逻辑中我们讨论过所谓析取范式和合取范式。现在我们进一步讨论一阶逻辑中的前束范式。所谓前束范式，就是把所有的量词都提到前面。精确地说，我们称具有

$$Q_1x_1\cdots Q_nx_n\ \alpha,$$

形式的公式为一个 前束公式 ，其中 n 是自然数，Q_i 是量词 $\forall$ 或者 $\exists$，并且 α 不含量词。前束范式的概念在计算机科学中常常被用到。此外量词的多少（尤其是由相同量词组成的量词块的多少）天然地提供给我们一个衡量公式复杂性的度量，这在后继课程中（如集合论中的绝对性和递归论中的可计算性）会经常谈到。

定理 5.4.1 (前束范式定理). 对于任何公式我们都可以找到与之语法等价的前束公式。

证明: 我们将利用下列规则来做量词操作，规则的正确性我们留作练习：

Q1a. $\neg\forall x\alpha \vdash\dashv \exists x\neg\alpha$。

Q1b. $\neg\exists x\alpha \vdash\dashv \forall x\neg\alpha$。

Q2a. $(\alpha \to \forall x\beta) \vdash\dashv \forall x(\alpha \to \beta)$，假定 x 不在 α 中自由出现。

Q2b. $(\alpha \to \exists x\beta) \vdash\dashv \exists x(\alpha \to \beta)$，假定 x 不在 α 中自由出现。

Q3a. $(\forall x\alpha \to \beta) \vdash\dashv \exists x(\alpha \to \beta)$，假定 x 不在 β 中自由出现。

Q3b. $(\exists x\alpha \to \beta) \vdash\dashv \forall x(\alpha \to \beta)$，假定 x 不在 β 中自由出现。

我们对公式施行归纳来证明任何公式都有与之语法等价的前束公式。

(1) 如果 α 是原子公式，则它本身已经是前束公式了。

(2) 如果 α 等价于前束公式 α'，则 $\forall x\alpha$ 等价于前束公式 $\forall x\alpha'$。

(3) 如果 α 等价于前束公式 α'，则 $\neg\alpha$ 等价于 $\neg\alpha'$，再用 Q1 即可将 $\neg\alpha'$ 变为前束公式。

(4) 考察形为 $\alpha \to \beta$ 的公式。根据归纳假设，我们有分别等价于 α 和 β 的前束公式 α' 和 β'。通过适当的约束变元替换，我们可以进一步假定 α' 中的约束变元不在 β' 中出现，反之亦然。再用 Q2 和 Q3 即可得到一个与 $\alpha' \to \beta'$ 等价的前束公式，从而也与 $\alpha \to \beta$ 等价。

□

例 5.4.1. 公式 $\forall x\exists yPxy \to \exists xQx$ 的前束范式可以是 $\exists x\forall y\exists z(Pxy \to Qz)$，也可以是 $\exists x\exists z\forall y(Pxy \to Qz)$，还可以是 $\exists z\exists x\forall y(Pxy \to Qz)$。

习题 5.3.

(1) 假定 x 不在 α 中自由出现，证明 (Q2b) 和 (Q3a)：

$$\vdash \quad (\alpha \to \exists x\beta) \leftrightarrow \exists x(\alpha \to \beta)$$
$$\vdash \quad (\forall x\beta \to \alpha) \leftrightarrow \exists x(\beta \to \alpha)。$$

(2) (a) 给出两个 $(\varphi^x_y)^y_x$ 不等于 φ 的例子，要求在一个例子中 x 出现在 $(\varphi^x_y)^y_x$ 中而不出现在 φ 中；在另一个例子中 x 出现在 φ 中而不出现在 $(\varphi^x_y)^y_x$ 中。

(b) （循环替换引理）如果变元 y 完全不在公式 φ 中出现，则变元 x 可以在公式 φ^x_y 中替换 y 并且 $(\varphi^x_y)^y_x = \varphi$。

(3) 证明：

$$\forall x\forall yPxy \vdash \forall y\forall xPyx。$$

(4) 证明 (Eq3)：

$$\vdash \forall x\forall y\forall z(x \approx y \to y \approx z \to x \approx z)。$$

(5) 证明下列的等价替换定理：假定公式 φ' 是由把公式 φ 中的若干个 $\psi_1, \psi_2, \cdots, \psi_n$ 分别替换成 $\psi_1', \psi_2', \cdots, \psi_n'$ 而得到的。如果 $\vdash \psi_1 \leftrightarrow \psi_1'$，$\vdash \psi_2 \leftrightarrow \psi_2'$，$\cdots$，$\vdash \psi_n \leftrightarrow \psi_n'$，则

$$\vdash \varphi \leftrightarrow \varphi'。$$

(6) 分别找出一个与下列公式语法等价的前束公式：

(a) $(\exists x Ax \wedge \exists x Bx) \to Cx$。

(b) $\forall x Ax \leftrightarrow \exists x Bx$。

第五节　自然推演

我们见过命题逻辑中的一个自然推演系统。不难想象一阶逻辑中也有（很多）类似的系统。我们继续第 三 章第 七 节中的话题，把那里的自然推演系统扩展成为适用于一阶逻辑的系统。后面我们会用它来证明完全性定理和切割消去定理[1]。注意：我们的目的仍然是作为主线的补充，因此下面介绍的都是简化了的版本。

首先我们仍从规定语言开始，为了简单起见，我们假定语言中没有函数符号和常数符号，也没有等词。语言包括：

(0) 括号：“(”和“)”；

(1) 谓词符号：$P_0, \overline{P}_0, P_1, \overline{P}_1, \cdots$ 其中每个 P_i 可以包含若干元，并且 P_i 和 $\overline{P}_i$ 成对出现。

(2) 逻辑符号：$\vee$，$\wedge$，$\exists$，$\forall$；

(3) 变元：$v_1, v_2, \cdots$。

语言中原子公式为 $P_i(v_{i_1}, v_{i_2}, \cdots, v_{i_k})$ 和 $\overline{P}_i(v_{i_1}, v_{i_2}, \cdots, v_{i_k})$。其它公式则是由原子公式和 $\vee$，$\wedge$，$\exists x$，$\forall x$ 生成的。

注意：同命题逻辑中的做法一样，$\neg$ 和 $\to$ 仍是被定义的符号。只不过在定义 $\neg$ 时，要添上 $\neg\forall x\alpha =_{df} \exists x\neg\alpha$ 和 $\neg\exists x\alpha =_{df} \forall x\neg\alpha$。这样做的目的仍然是最大限度地利用 $\vee$ 和 $\wedge$，$\exists$ 和 $\forall$ 的对偶性，从而减少推理规则的个数。

[1] 切割消去定理，cut elimination theorem。

推理规则如下，其中 Γ 和 Δ 为任意的有穷公式集：

公理：

$$\Gamma, P(v_{i_1}, \cdots, v_{i_k}), \overline{P}(v_{i_1}, \cdots, v_{i_k})$$

规则 $(\vee)$:

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

规则 $(\wedge)$:

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

规则 $(\exists)$:

$$\frac{\Gamma, \alpha(x')}{\Gamma, \exists x \alpha(x)}$$

规则 $(\forall)$:

$$\frac{\Gamma, \alpha(x')}{\Gamma, \forall x \alpha(x)} \quad x' \text{ 不在 } \Gamma \text{ 中自由出现}$$

切割规则:

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

与命题逻辑类似，我们仍用 $\vdash \Gamma$ 表示存在 Γ 的一个自然推演。具体定义留给读者。我们仍只讨论 $\vdash \Gamma$ 这种弱形式，暂不讨论 $\Delta \vdash \Gamma$ 这样的一般形式。

与命题逻辑的情形类似，我们有

例 5.5.1. 用自然推演证明：对所有的有穷公式集 Γ 和 α，我们有 $\vdash \Gamma, \neg\alpha, \alpha$。今后我们会把它称为（公理′）或直接当作公理来用。

证明: 固定 Γ，我们对公式 α 施行归纳：

如果 α 为原子公式 $P(v_{i_1}, \cdots, v_{i_k})$，则 $\neg\alpha$ 为 $\overline{P}(v_{i_1}, \cdots, v_{i_k})$。所以 $\Gamma, \neg\alpha, \alpha$ 是公理。α 为 $\overline{P}(v_{i_1}, \cdots, v_{i_k})$ 的情形与此类似。

如果 α 形如 $\alpha_0 \vee \alpha_1$，或 $\alpha_0 \wedge \alpha_1$，则证明与命题逻辑的证明相同。

如果 α 形如 $\exists x \beta(x)$，则 $\neg\alpha$ 形如 $\forall x \neg\beta(x)$。由于 Γ 是有穷集，我们可以选一个在 Γ 中完全不出现的变元 y。根据归纳假定，存在 $\Gamma, \neg\beta(y), \beta(y)$ 的自然推演 $\mathcal{D}$。我们有

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ \vdots\\ \Gamma, \beta(y), \neg\beta(y)\end{array}}{\Gamma, \exists x \beta(x), \neg\beta(y)}}{\Gamma, \exists x \beta(x), \forall x \neg\beta(x)} \ (\forall)$$

α 为 $\forall x \beta(x)$ 的证明类似。 □

回忆一下，我们把 $\{a,b,c\}$ 转写成 $\{a,b\},c$ 或 $\{a\},b,c$ 的做法记为 (rw)。尽管转写不是推理规则，为了读者方便，我们把转写写成

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

例 5.5.2. 用自然推演证明：$\vdash \forall x\alpha(x)\to(\forall x\beta(x)\to\forall x(\alpha(x)\wedge\beta(x)))$。

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

$$\vdash \exists x\alpha(x)\vee(\exists x\beta(x)\vee(\forall x(\alpha(x)\wedge\beta(x))))。$$

固定一个新变元 y，即 $y\neq x$ 并且 y 在 α 和 β 中都不出现，推演树如下：

$$\dfrac{\dfrac{\dfrac{\dfrac{\{\exists x\neg\beta(x)\},\alpha(y),\neg\alpha(y)}{\{\exists x\neg\beta(x),\alpha(y)\},\neg\alpha(y)}\,(rw)}{\{\exists x\neg\beta(x),\alpha(y)\},\exists x\neg\alpha(x)}\,(\exists)}{\exists x\neg\alpha(x),\exists x\neg\beta(x),\alpha(y)}\,(rw) \qquad \dfrac{\dfrac{\dfrac{\{\exists x\neg\alpha(x)\},\beta(y),\neg\beta(y)}{\{\exists x\neg\alpha(x),\beta(y)\},\neg\beta(y)}\,(rw)}{\{\exists x\neg\alpha(x),\beta(y)\},\exists x\neg\beta(x)}\,(\exists)}{\exists x\neg\alpha(x),\exists x\neg\beta(x),\beta(y)}\,(rw)}{\exists x\neg\alpha(x),\exists x\neg\beta(x),\alpha(y)\wedge\beta(y)}\,(\wedge)$$
$$\dfrac{\exists x\neg\alpha(x),\exists x\neg\beta(x),\alpha(y)\wedge\beta(y)}{\exists x\neg\alpha(x),\exists x\neg\beta(x),\forall x(\alpha(x)\wedge\beta(x))}\,(\forall)$$
$$\dfrac{\exists x\neg\alpha(x),\exists x\neg\beta(x),\forall x(\alpha(x)\wedge\beta(x))}{\exists x\alpha(x)\vee(\exists x\beta(x)\vee(\forall x(\alpha(x)\wedge\beta(x))))}\,(\vee')$$

□

我们再看另一个例子。我们希望通过它一方面说明怎样对证明树进行归纳；另一方面也暗示自然推演有子公式性质，即证明中用到的公式都是所证公式的子公式。

例 5.5.3. 证明：如果 $\vdash\Gamma,(\alpha_0\wedge\alpha_1)$，则 $\vdash\Gamma,\alpha_0$ 并且 $\vdash\Gamma,\alpha_1$。

证明： 我们证明一个稍微特殊的情形，即假定 $(\alpha_0\wedge\alpha_1)\notin\Gamma$。一般情形只要进行弱化即可（见习题）。

令 $\mathcal{D}$ 为 $\Gamma,(\alpha_0\wedge\alpha_1)$ 的一个自然推演。我们对 $\mathcal{D}$ 的长度（即证明树的高度[2]）进行归纳。

如果 $\mathcal{D}$ 的长度为 1，则 $\Gamma,(\alpha_0\wedge\alpha_1)$ 是公理。因此存在原子公式 $P(v_{i_1},\cdots,v_{i_k})$ 和 $\overline{P}(v_{i_1},\cdots,v_{i_k})$ 包含在 Γ 当中。所以 Γ,α_0 和 Γ,α_1 都是公理，命题成立。

假定命题对长度小于或等于 k 的自然推演成立。考虑一个长度为 $k+1$ 的 $\Gamma,(\alpha_0\wedge\alpha_1)$ 的自然推演 $\mathcal{D}$。如果 $\mathcal{D}$ 的最后一步是公理，则与前面的证明相同。

如果 $\mathcal{D}$ 的最后一步使用了规则 $(\vee)$，或 $(\exists)$ 或 $(\forall)$ 或切割，我们以规则 $(\vee)$ 为例。假定 $\mathcal{D}$ 的最后一步为

$$\frac{\Gamma',\beta_0}{\Gamma',(\beta_0\vee\beta_1)}。$$

[2]这里我们不打算给出证明树的高度的严格定义，请大家模仿二岔树高度的定义自行补上。

注意到 $\Gamma' \cup \{(\beta_0 \vee \beta_1)\} = \Gamma \cup \{(\alpha_0 \wedge \alpha_1)\}$，如果我们令 $\Delta = \Gamma' \setminus \{(\alpha_0 \wedge \alpha_1)\}$，则 $\Delta \cup \{(\beta_0 \vee \beta_1)\} = \Gamma$。所以我们有一个长度小于或等于 k 的关于 $\Delta \cup \{\beta_0\}, (\alpha_0 \wedge \alpha_1)$ 的自然推演。根据归纳假定，$\vdash \Delta, \beta_0, \alpha_0$ 并且 $\vdash \Delta, \beta_0, \alpha_1$。再分别使用规则 $(\vee)$，我们有 $\vdash \Delta, \beta_0 \vee \beta_1, \alpha_0$ 和 $\vdash \Delta, \beta_0 \vee \beta_1, \alpha_1$。由于 $\Delta \cup \{(\beta_0 \vee \beta_1)\} = \Gamma$，我们就有 $\vdash \Gamma, \alpha_0$ 并且 $\vdash \Gamma, \alpha_1$。

剩下的情形为 $\mathcal{D}$ 的最后一步使用了规则 $(\wedge)$：

$$\frac{\Gamma', \beta_0 \quad \Gamma', \beta_1}{\Gamma', (\beta_0 \wedge \beta_1)}$$

如果对某个 $i = 0, 1$，β_i 不等于 α_i，则证明与 $(\vee)$ 情形类似。最后的可能是 $\Gamma' = \Gamma$，$\beta_0 = \alpha_0$，$\beta_1 = \alpha_1$，此时显然有 $\vdash \Gamma, \alpha_0$ 并且 $\vdash \Gamma, \alpha_1$。 □

习题 5.4.

(1) 证明弱化定理[3]的下列弱形式：对所有的有穷公式集 Γ 和公式 α，如果 $\vdash \Gamma$ 则 $\vdash \Gamma, \alpha$。

(2) 证明：如果 $\vdash \Gamma, \forall x \alpha(x)$，则对于任意项 t （在我们简化了的版本里只有变元 v_i）$\vdash \Gamma, \alpha(t)$。[为什么我们这里没有 t 可在 α 中替换 x 的条件呢？]

[3]弱化定理，Weakening，的一般形式为 $\Delta \vdash \Delta, \Gamma$。但如何在自然推理中定义 $\Delta \vdash \Gamma$ 我们没有讲，所以暂不要求大家证明弱化定理。

第六章　一阶语言的结构和真值理论

第一节　一阶语言的结构

到现在为止我们都在讨论一阶逻辑的语法部分，所有的公式等等都可以被视为毫无意义的字符串。现在我们开始讨论它们的“意义”。首先我们要解释语言中的每一个符号的意义。粗略地说，这个解释是通过挑选“外部的”一个数学“结构”来完成的。结构挑选的过程，也就是规定量词的范围，并指定谓词、函数、和常数符号意义的过程。

定义 6.1.1. 一个一阶语言的 *结构* $\mathfrak{A}$ 是一个定义域为语言中符号的函数，并且满足下列条件:

(1) $\mathfrak{A}$ 给量词符号 $\forall$ 指定一个非空集 $|\mathfrak{A}|$，称作 $\mathfrak{A}$ 的 *论域* [1] 。

(2) 对每个 n-元谓词符号 P，$\mathfrak{A}$ 都指定一个 n-元关系 $P^{\mathfrak{A}} \subseteq |\mathfrak{A}|^n$；即 $P^{\mathfrak{A}}$ 是由论域中 n-元组所组成的集合。

(3) 对每个常数符号 c，$\mathfrak{A}$ 都指定论域 $|\mathfrak{A}|$ 中的一个元素 $c^{\mathfrak{A}}$。

(4) 对每个 n-元函数符号 f，$\mathfrak{A}$ 都指定论域 $|\mathfrak{A}|$ 上的一个 n-元函数 $f^{\mathfrak{A}}$;
即 $f^{\mathfrak{A}} : |\mathfrak{A}|^n \to |\mathfrak{A}|$。

注：选非空集作为论域是必要的，原因是我们在第五章中的有些公理对空集不适用（哪一条呢？）。当然约定论域非空并无实质的损害，因为我们并不关心空集的性质。

例 6.1.1. 考察集合论的语言 $L = \{\approx, \in\}$，其中 $\in$ 为一个二元谓词符号。尽管我们的初衷是研究“真正的”集合论，但按照以上结构的定义，我们仍有很大的自由来挑选 L 的结构。例如，令 $\mathfrak{A}$ 的论域 $|\mathfrak{A}|$ 为全体自然数的集合 $\mathbb{N}$，符号 $\in$ 在 $\mathfrak{A}$ 中的解释 $\in^{\mathfrak{A}}$ 定义为“小于”关系 $\{(m, n) : m < n\}$。下列问题会帮助我们理解后面要谈到的真值理论。在上述解释下，你怎样解读语句 $\exists x \forall y \neg y \in x$ 还有

$$\forall x \forall y \exists z \forall t (t \in z \to (t \approx x \vee t \approx y))?$$

[1] 论域，universe，也被译作“宇宙”。

下面我们将定义 “一个闭语句 σ 在结构 $\mathfrak{A}$ 中为真”，记作 $\models_{\mathfrak{A}} \sigma$。由于定义是对语句归纳完成的，我们不可避免地要处理带有自由变元的公式。但如果变元可以随便变的话，讨论公式的真假是无意义的。例如，在结构 $(\mathbb{N}, 0)$ 中如果变元 x 的值不确定，讨论 $x \approx 0$ 是否为真毫无意义。因此，我们需要一个赋值 s 告诉我们自由变元指的是哪些元素。令 V 为所有自由变元的集合。一个 赋值 s 就是一个从 V 到 $\mathfrak{A}$ 的论域的函数，即 $s : V \to |\mathfrak{A}|$。

固定一个语言 L。令 φ 为 L 中的一个公式，$\mathfrak{A}$ 为 L 的一个结构，s 为一个赋值。我们下面定义 $\mathfrak{A}$ 和 s 满足 φ 这个短语，记作 $\models_{\mathfrak{A}} \varphi[s]$。直观上说，“$\models_{\mathfrak{A}} \varphi[s]$” 的意思是：我们先把符号串 φ 里的谓词符号，函数符号和常数符号按照结构 $\mathfrak{A}$ 的规定来解释，把量词的论域限制在集合 $|\mathfrak{A}|$，把自由变元 x 解释成它的赋值 $s(x)$，从而把公式 φ 翻译成一个元语言中的数学陈述，而用我们数学知识我们知道所得到的陈述成立。精确定义如下：

定义 6.1.2.

(1) 项的解释。 我们把赋值 s 扩展到项，令 T 表示所有项的集合。我们递归定义一个项的赋值函数 $\overline{s} : T \to |\mathfrak{A}|$ 如下：

(a) 对每一个变元符号 x，$\overline{s}(x) = s(x)$。

(b) 对每一个常数符号 c，$\overline{s}(c) = c^{\mathfrak{A}}$。

(c) 如果 $t_1, t_2, \cdots, t_n$ 是项并且 f 是一个 n 元函数符号，则

$$\overline{s}(ft_1t_2\cdots t_n) = f^{\mathfrak{A}}(\overline{s}(t_1), \overline{s}(t_2)\cdots, \overline{s}(t_n))。$$

(2) 处理原子公式。

(a) $\models_{\mathfrak{A}} \approx t_1t_2[s]$ 当且仅当 $\overline{s}(t_1) = \overline{s}(t_2)$。

(b) 对 n 元谓词符号 P，$\models_{\mathfrak{A}} Pt_1t_2\cdots t_n[s]$ 当且仅当 $(\overline{s}(t_1), \overline{s}(t_2)\cdots, \overline{s}(t_n)) \in P^{\mathfrak{A}}$。

(3) 其它公式的处理。 定义

(a) $\models_{\mathfrak{A}} \neg\varphi[s]$ 当且仅当 $\mathfrak{A}$ 和 s 不满足 φ，记作 $\not\models_{\mathfrak{A}} \varphi[s]$。

(b) $\models_{\mathfrak{A}} (\varphi \to \psi)[s]$ 当且仅当或者 $\not\models_{\mathfrak{A}} \varphi[s]$ 或者 $\models_{\mathfrak{A}} \psi[s]$。

(c) $\models_{\mathfrak{A}} \forall x\varphi[s]$ 当且仅当对任何的 $d \in |\mathfrak{A}|$，我们有 $\models_{\mathfrak{A}} \varphi[s(x \mid d)]$，其中 $s(x \mid d)$ 为一个由 s、x 和 d 诱导出来新的赋值函数，定义为

$$s(x \mid d)(y) = \begin{cases} s(y), & \text{如果 } y \neq x; \\ d, & \text{如果 } y = x。 \end{cases}$$

注：

1. 符号 $s(x \mid d)$ 写法不很理想，请不要把它混成 s 在某处的取值。我们的本意是把 $\varphi(x)$ 中的变元 x 用 d 来取代，非正式的写法为 $\varphi(d)$。但严格讲这样写毫无意义，因为 d 不是我们语言中的符号。因此我们只有采用赋值的方法把变元 x 赋值为 d。有的教科书把它简记成 $\varphi[d]$。当我们概念清楚之后，例如在后面可定义性的部分也会采用这种简记。

2. 定义 6.1.2 是一阶逻辑真值理论的核心。它是由逻辑学家塔尔斯基 1933 年给出的。

3. 对初学者来说首先要搞清楚我们是用什么在定义什么，或者说它是否是循环定义。答案是我们是用数学（元语言中）的知识来定义（对象语言中）一阶语句的真假。例如，固定域的语言 $L = \{+, \cdot, 0, 1\}$。考察一阶语句 φ: $\forall x(x \cdot x \not\approx 1 + 1)$。就 φ 本身而言，它只是一个字符串，到现在为止尚不具有任何意义。只有当我们固定好 L 的一个结构 $\mathfrak{A}$ 时，我们才能决定 φ 的真假。就 φ 而言，它在有理数域 $\mathbb{Q}$ 中为真，而在实数域 $\mathbb{R}$ 中为假。至于为什么它在有理数域 $\mathbb{Q}$ 为真，则是我们的数学中背景知识告诉我们的。因此我们是用数学中关于 $\mathfrak{A}$ 的知识来定义一个形式语句（或说一阶公式）φ 在 $\mathfrak{A}$ 中的真假，即 $\models_{\mathfrak{A}} \varphi$。

4. 从上面的讨论我们可以看出用数学语言在这一点上比用自然语言要清晰。自然语言中常用的例子为 '雪是白的'为真当且仅当雪是白的。

定义 6.1.3. 令 Γ 为一个公式集并且 φ 为一个公式。我们称 Γ *语义蕴涵* φ，[2] 记作 $\Gamma \models \varphi$，如果对每一个结构 $\mathfrak{A}$ 和每个赋值函数 $s : V \to |\mathfrak{A}|$ 都有一旦 $\mathfrak{A}$ 和 s 满足 Γ 中的所有成员，则 $\mathfrak{A}$ 和 s 也满足 φ。

定义 6.1.3 是本课程中最重要的概念之一。语义蕴涵的目标是严格定义“必然地得出”这一概念。前面的语法蕴涵概念尽管非常精确，但人们多少会怀疑它是否过于依赖形式系统的选取。而语义蕴涵则没有这一缺陷。因此一个“好的”推演系统从假设集 Γ 能“推”出的命题应该不多不少恰恰是 Γ 语义蕴涵的那些命题，这就是我们后面要讲的所谓可靠性和完全性。

我们在命题逻辑中曾用符号 $\models$ 表示过重言蕴涵，但从现在起，除非特别声明，符号 $\models$ 只表示语义蕴涵。我们仍然沿用过去的一些约定，比如，我们用 $\gamma \models \varphi$ 来表示 $\{\gamma\} \models \varphi$；我们说两个公式 φ 和 ψ 是 *语义等价的* [3] 如果 $\varphi \models \psi$ 并且 $\psi \models \varphi$。一个公式 φ 被称为 *普遍有效的* 如果 $\emptyset \models \varphi$，记作 $\models \varphi$。[4] 注意：公式 φ 是普遍有效的当且仅当对所有的结构 $\mathfrak{A}$ 和所有的赋值 $s : V \to |\mathfrak{A}|$，$\mathfrak{A}$ 和 s 都满足 φ（为什么？）。因此普遍有效的公式在一阶逻辑中与重言式在命题逻辑中的地位类似。

[2] 语义蕴涵，英文为 logically imply，也被译为 逻辑蕴涵，或说 φ 是 Γ 的 语义后承。
[3] 语义等价，英文为 logically equivalent，也被译为 逻辑等价。
[4] 普遍有效的，英文为 valid。通常直译为“有效的”。

定理 6.1.1. 假定 s_1 和 s_2 为两个从 V 到 $|\mathfrak{A}|$ 的赋值函数，并且它们在公式 φ 中所有自由出现的变元上取值相同。则 $\models_{\mathfrak{A}} \varphi[s_1]$ 当且仅当 $\models_{\mathfrak{A}} \varphi[s_2]$。

证明: 固定结构 $\mathfrak{A}$。我们对公式 φ 施行归纳。假定赋值函数 s_1 和 s_2 在公式 φ 中所有自由出现的变元上取值相同。首先我们有

情形 1：φ 是一个原子公式 $Pt_1t_2\cdots t_n$ 或 $t_1 \approx t_2$。首先我们有对任意 $i \geq 1$，$\overline{s}_1(t_i) = \overline{s}_2(t_i)$。详细证明需要对项 t 施行归纳并要用到对赋值 s_1 和 s_2 的假设，我们留给读者。因此 $\models_{\mathfrak{A}} Pt_1t_2\cdots t_n[s_1]$ 当且仅当 $(\overline{s}_1(t_1), \overline{s}_1(t_2), \cdots, \overline{s}_1(t_n)) \in P^{\mathfrak{A}}$ 当且仅当 $(\overline{s}_2(t_1), \overline{s}_2(t_2), \cdots, \overline{s}_2(t_n)) \in P^{\mathfrak{A}}$ 当且仅当 $\models_{\mathfrak{A}} Pt_1t_2\cdots t_n[s_1]$。当 φ 为 $t_1 \approx t_2$ 时证明与此类似。

情形 2 和 3：φ 分别具有形式 $\neg\alpha$ 和 $\alpha \to \beta$。我们把验证留给读者。

情形 4：φ 具有形式 $\forall x\psi$。在此情形下在 ψ 中自由出现的变元至多是 x 加上在 φ 中自由出现的变元。所以对任何的 $d \in |\mathfrak{A}|$，诱导出的赋值函数 $s_1(x \mid d)$ 和 $s_2(x \mid d)$ 在 ψ 中所有自由出现的变元上取值相同。根据归纳假定 $\mathfrak{A}$ 和 $s_1(x \mid d)$ 满足 ψ 当且仅当 $\mathfrak{A}$ 和 $s_2(x \mid d)$ 满足 ψ。所以 $\mathfrak{A}$ 和 s_1 满足 φ 当且仅当 $\mathfrak{A}$ 和 s_2 满足 φ。 □

推论 6.1.1. 对任何闭语句 σ，或者

(a) 对所有函数 $s : V \to |\mathfrak{A}|$，都有 $\models_{\mathfrak{A}} \sigma[s]$；或者

(b) 对所有函数 $s : V \to |\mathfrak{A}|$，都有 $\not\models_{\mathfrak{A}} \sigma[s]$。

当情形 (a) 成立时，我们就称 σ 在 $\mathfrak{A}$ 中为真，记作 $\models_{\mathfrak{A}} \sigma$；也经常使用下列短语：$\sigma$ 在 $\mathfrak{A}$ 中成立；$\mathfrak{A}$ 满足 σ 和 $\mathfrak{A}$ 是 σ 的一个模型 。

推论 6.1.1 说明对闭语句来说，赋值函数是不重要的。

例 6.1.2. 给定一阶语言 L 包含一个二元谓词符号 P，一元函数符号 f 和一个常数符号 c，考察它的如下结构:

$$\mathfrak{A} = (\mathbb{N}, \leq, S, 0)。$$

令 $s : V \to \mathbb{N}$ 使得 $s(v_i) = i - 1$，即 $s(v_1) = 0, s(v_2) = 1$ 等等。什么是 $\overline{s}(ffv_3)$? 还有 $\overline{s}(ffc)$? 结构 $\mathfrak{A}$ 和赋值 s 满足下列公式吗?

(1) $Pcfv_1$;

(2) $\forall v_1 Pcv_1$;

(3) $\forall v_1 Pv_2v_1$。

例 6.1.3. 证明或否证下列命题:

(1) $\forall v_1 Q v_1 \models Q v_1$;

(2) $Q v_1 \models \forall v_1 Q v_1$。

习题 6.1.

(1) 前面说过，公式 $\alpha \vee \beta$，$\alpha \wedge \beta$ 和 $\exists x \alpha$ 是分别作为 $((\neg\alpha) \to \beta)$，$(\neg(\alpha \to (\neg\beta)))$ 和 $(\neg\forall x(\neg\alpha))$ 的缩写而引入的。根据定义找出 $\models_{\mathfrak{A}} (\alpha \vee \beta)[s]$，$\models_{\mathfrak{A}} (\alpha \wedge \beta)[s]$ 和 $\models_{\mathfrak{A}} \exists x \alpha[s]$ 的意义。

(2) 证明：$\models \forall x \varphi(x) \to \exists x \varphi(x)$。 [注：这似乎是“无中生有”。你在证明中用到结构是非空的吗?]

(3) 判断下列命题的对错并给出证明或反例。固定一个一阶语言 L。

(a) 对于任意 L 的结构 $\mathfrak{A}$ 和闭语句，或者 $\models_{\mathfrak{A}} \sigma$ 或者 $\models_{\mathfrak{A}} \neg\sigma$。

(b) 对任意的闭语句 σ，或者 $\models \sigma$ 或者 $\models \neg\sigma$。

(4) 证明 $\Gamma \cup \{\alpha\} \models \varphi$ 当且仅当 $\Gamma \models (\alpha \to \varphi)$。

(5) 举例说明：在 $\models \alpha$ 当且仅当 $\models \beta$ 的条件下，不一定有 $\models \alpha \leftrightarrow \beta$。

(6) 证明下列的任何语句都不被其它两个语义蕴涵。

(a) $\forall x \forall y \forall z (Pxy \to (Pyz \to Pxz))$。

(b) $\forall x \forall y (Pxy \to (Pyx \to x \approx y))$。

(c) $\forall x \exists y Pxy \to \exists y \forall x Pxy$。

（你可以构造结构，使得一个语句在该结构为假，但其它两个语句为真。）

(7) 证明

$$\models_{\mathfrak{A}} \forall v_2 Q v_1 v_2[c^{\mathfrak{A}}] \text{ 当且仅当 } \models_{\mathfrak{A}} \forall v_2 Q c v_2。$$

这里 Q 为一个二元谓词符号并且 c 为常数符号。

(8) 证明 $\{\forall x(\alpha \to \beta), \forall x \alpha\} \models \forall x \beta$。[这是后面可靠性定理证明的一部分。]

(9) 证明：如果 x 不在 α 中自由出现，则 $\alpha \models \forall x\alpha$。 [这也是后面可靠性定理证明的一部分。]

(10) 证明：公式 $x \approx y \to Pzfx \to Pzfy$ 是普遍有效的，其中 f 是一个一元函数符号并且 P 是一个二元谓词符号。

(11) 证明公式 θ 是普遍有效的当且仅当 $\forall x\ \theta$ 是普遍有效的。 [这也是后面可靠性定理证明的一部分。]

(12) 证明：$\models \exists x(Px \to \forall xPx)$。[在习题 5.2 中，我们证明了它在语法中相应的命题 $\vdash \exists x(Px \to \forall xPx)$，这种语义和语法的对应是可靠性和完全性定理的一个特例。]

第二节　可定义性

有了 $\models_{\mathfrak{A}} \sigma$ 的概念之后，我们可以利用它来讨论所谓的可定义性。一方面我们可以固定一个（或一族）公式 σ（或 Σ）来探讨什么样的结构可以满足它（或它们）；另一方面，我们也可以固定一个结构 $\mathfrak{A}$ 来探讨 $|\mathfrak{A}|$ 哪些子集或关系可以被公式 φ 描述。前者是在数学中很常见；后者则在数理逻辑中非常重要。

对一个闭语句集 Σ 我们用 Mod Σ 来表示由 Σ 的模型所组成的类。[5]如果 Σ 是单个闭语句的集合 $\{\tau\}$，我们则用“Mod τ”而不用“Mod $\{\tau\}$”。我们称（同一个一阶语言上）的结构类 $\mathcal{K}$ 为一个 *初等类* （EC）[6] 如果存在闭语句 τ 使得 $\mathcal{K}$ 是 Mod τ。我们称 $\mathcal{K}$ 为一个 *广义初等类* （EC_Δ）如果存在闭语句集 Σ，使得 $\mathcal{K}$ 是 Mod Σ。

例 6.2.1. 令一阶语言 $L = \{\approx, P\}$ 其中 P 是一个二元谓词符号。令 τ 为下列三个闭语句的合取：

$$\begin{aligned} \forall x\forall y\forall z \quad & (xPy \to yPz \to xPz); \\ \forall x\forall y \quad & (xPy \vee x \approx y \vee yPx); \\ \forall x\forall y \quad & (xPy \to \neg yPx). \end{aligned}$$

则任何 τ 的模型都是一个（严格的）线序。所以，所有非空的线序集构成的类是一个初等类。

[5]这里的类是相对集合而言，一般说来，Mod Σ 不是一个集合，不然会有悖论。但类和集合的差异对我们的讨论影响不大，初学者可以暂时忽略。

[6]初等类，英文为 elementary class；广义初等类，英文为 elementary class in a wider sense。有人也把 elementary 翻译成基本。大致上说，初等也好，基本也好，都指的是一阶逻辑所表达的性质，而非所谓的用“高阶”语言描述的“高阶”性质。

注：从上例我们可以看出：如果 Σ 是一个有穷的闭语句集，则 $\mathcal{K} = \mathrm{Mod}\ \Sigma$ 是一个初等类。

前面我们提到过“群”这个概念。我们想说明所有的群组成一个初等类，并说明我们可以选择不同的语言。在第 四 章第 一 节中，我们选的语言为 $L_0 = (e, +)$。现在我们选取 $L_1 = \{\approx, \circ, ^{-1}, e\}$，其中 $\circ$ 和 $^{-1}$ 分别是一个二元和一元函数符号，e 是一个常数符号。在 L_1 上，所有群的类可以被下列闭语句描述，因而是一个初等类：

$$\begin{aligned} \forall x\forall y\forall z \quad & (x \circ (y \circ z) \approx (x \circ y) \circ z); \\ \forall x \quad & (x \circ e \approx e \circ x \approx x); \\ \forall x \quad & (x \circ x^{-1} \approx x^{-1} \circ x \approx e)。 \end{aligned}$$

我们也可以选取 $L_2 = \{\approx, \circ\}$，其中 $\circ$ 是一个二元函数符号。在 L_2 上，所有群的类仍是一个初等类，因为它可以被下列闭语句描述（见习题）：

$$\begin{aligned} \forall x\forall y\forall z \quad & (x \circ (y \circ z) \approx (x \circ y) \circ z); \\ \forall x\forall y\exists z \quad & (x \circ z \approx y); \\ \forall x\forall y\exists z \quad & (z \circ x \approx y)。 \end{aligned}$$

注：选取不同的语言对本课程关系不大，但如果我们对句法复杂性感兴趣的话，我们会注意到在 L_1 上，我们只用到了全称量词，而在 L_2 中我们需要两种不同的量词。这样的细微差别有时会产生一些影响。

如果语言中有等词的话，我们有闭语句 $\exists_n$ 表示“结构中至少有 n 个不同的元素”，例如，$\exists_2$ 和 $\exists_3$ 分别为：

$$\begin{aligned} & \exists x\exists y(x \not\approx y), \\ & \exists x\exists y\exists z(x \not\approx y \wedge y \not\approx z \wedge x \not\approx z)。 \end{aligned}$$

这样所有的无限群组成的类就是一个广义初等类，因为它是由所有满足群的公理并且满足 $\{\exists_2, \exists_3, \cdots\}$ 的结构组成的。后面我们会证明它不是一个初等类。

我们再来讨论结构内的可定义性。这种可定义性在数理逻辑是很普遍的，比如，在哥德尔可构成集的类 L 中可定义性是最重要的概念。此外，模型论学家也经常研究可定义的集合或关系，因为同没有限制的任意集合相比，人们更愿意讨论自然的集合，而可定义的集合可以说是自然的。至少退一步说，不可定义的集合是不太自然的。熟悉集合论公理的同学可以比较分离公理和选择公理，由分离公理得到的集合是由某个公式定义出来的，而由选择公理得到的集合往往是不可定义的，因而分离公理比选择公理显得自然。

固定一个语言 L 和 L 上面的一个结构 $\mathfrak{A}$。我们先引进一个写法来避免 $s(x \mid d)$ 之类的繁琐。假定 $\varphi(v_1, v_2, \cdots, v_k)$ 为 L 的一个公式，并且 $v_1, v_2, \cdots, v_k$ 包括了 φ 中的所有自

由变元。对于 $|\mathfrak{A}|$ 中的元素 $a_1, a_2, \cdots, a_k$，我们想说 “$\varphi(a_1, a_2, \cdots, a_k)$ 成立”，但严格地说，那些 a_i 不在语言 L 里面，因此上面的写法没有意义。我们必须换一个说法。具体做法是：[7]定义

$$\models_{\mathfrak{A}} \varphi[a_1, a_2, \cdots, a_k]$$

如果存在某个赋值 $s : V \to |\mathfrak{A}|$ 满足 $s(v_i) = a_i$ （$1 \leq i \leq k$），使得 $\mathfrak{A}$ 和 s 满足 φ。注意：由于 $v_1, v_2, \cdots, v_k$ 包括了 φ 中的所有自由变元，我们有对任意满足 $s(v_i) = a_i$的赋值 s，都有 $\mathfrak{A}$ 和 s 满足 φ。

我们称 k-元关系

$$\{(a_1, a_2, \cdots, a_k) : \models_{\mathfrak{A}} \varphi[a_1, a_2, \cdots, a_k]\}$$

为公式 φ 在 $\mathfrak{A}$ 中 定义 的关系。我们称一个 $|\mathfrak{A}|$ 上的 k-元关系为 可定义的 如果存在某个公式 φ 在 $\mathfrak{A}$ 中定义它。

例 6.2.2. 考察关于数论的语言 $L = \{0, S, +, \cdot\}$。令结构 $\mathfrak{A}$ 的论域为自然数集 $\mathbb{N}$，其它的符号都按照自然的解释。则序关系 $\{(m, n) : m < n\}$ 在 $\mathfrak{A}$ 中是可定义的（为什么？）。对每一个自然数 n，单点集 $\{n\}$ 都是 $\mathfrak{A}$ 中可定义的（为什么？）。所有素数的集合在 $\mathfrak{A}$ 中是可定义的（为什么？）。

习题 6.2.

(1) 证明满足下列闭语句的结构为一个群：

$$\begin{aligned} &\forall x \forall y \forall z \quad (x \circ (y \circ z) \approx (x \circ y) \circ z); \\ &\forall x \forall y \exists z \quad (x \circ z \approx y); \\ &\forall x \forall y \exists z \quad (z \circ x \approx y)。 \end{aligned}$$

(2) 找出一个闭语句 σ 使得对任何正整数 n，σ 都有具有恰好 $2n$ 个元素的模型；并且 σ 没有恰好奇数个元素的有穷模型。你可以假定语言中含有等词，并可随意挑选其它符号。

(3) 假定语言 L 中有等词，并且有两个二元函数符号 $+$ 和 $\times$。对下列的集合和关系，分别找出在结构 $(\mathbb{N}, +, \times)$ 中定义它的公式。

(a) $\{0\}$。

(b) $\{1\}$。

[7]另一种常见的做法是扩张语言 L 使得对每个 $|\mathfrak{A}|$ 中的元素 a, 都有常数符号 $\mathbf{a}$。当然 $\mathbf{a}^{\mathfrak{A}} = a$。

(c) $\{(m,n) : n$ 是 m 在 $\mathbb{N}$ 中的后继$\}$。

(d) $\{(m,n) : m < n\}$，其中 $<$ 是 $\mathbb{N}$ 上的自然序。

(4) 假定语言 L 中包含等词并且有一个二元谓词 P。对下列条件分别找出 L 中的闭语句 σ 使得结构 $\mathfrak{A}(= (|\mathfrak{A}|, P^{\mathfrak{A}}))$ 是 σ 的一个模型当且仅当该条件成立。

(a) $|\mathfrak{A}|$ 有且仅有两个元素。

(b) $P^{\mathfrak{A}}$ 是一个从 $|\mathfrak{A}|$ 到 $|\mathfrak{A}|$ 的函数。

(c) $P^{\mathfrak{A}}$ 是 $|\mathfrak{A}|$ 到自身的一个一一对应。

第三节　同态和同构

先看两段小故事：

> 一个女画家在飞机上被谋杀了。机上有好几个人都和她有过节。空姐和她的男朋友还有张三一起侦破。在五个小时的飞行途中，他们终于确定凶手是副驾驶员。案情明朗后，凶手试图劫机冲向大海，但在驾驶员的帮助下，大家齐心制服了凶手，成功降落。
>
> 一个雕塑家在长途车上被谋杀了。车上有好几个人都和他有仇。售票员和他的女朋友还有李四一起侦破。在八个小时的车程中，他们终于确定凶手是副司机。案情明朗后，凶手试图将车冲下悬崖，但在司机的帮助下，大家齐心制服了凶手，转危为安。

这两段故事原本是讨论创意抄袭的例子[8]。它与我们要讲的内容有什么关系留给大家去想。

定义 6.3.1. *令 $\mathfrak{A}$ 和 $\mathfrak{B}$ 为某个固定语言的两个结构。我们称一个函数 $h : |\mathfrak{A}| \to |\mathfrak{B}|$ 为一个 从 $\mathfrak{A}$ 到 $\mathfrak{B}$ 的一个同态 如果它满足下列条件:*

(a) 对每个（不是等词 $\approx$）的 n 元谓词 P，和每组 $|\mathfrak{A}|$ 中的元素 $a_1, a_2, \cdots, a_n$ 都有

$$(a_1, a_2, \cdots, a_n) \in P^{\mathfrak{A}} \Leftrightarrow (h(a_1), h(a_2), \cdots, h(a_n)) \in P^{\mathfrak{B}}。$$

(b) 对每个 n 元函数符号 f 和每组 $|\mathfrak{A}|$ 中的元素 $a_1, a_2, \cdots, a_n$ 都有

$$h(f^{\mathfrak{A}}(a_1, a_2, \cdots, a_n)) = f^{\mathfrak{B}}(h(a_1), h(a_2), \cdots, h(a_n))。$$

[8] 改编自 Mace and Vincent-Northam, *The Writer's abc checklist*, Accent Press, 2010。

(c) 对每个常数符号 c 我们有 $h(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$。

在上述定义中，如果 h 是一个双射，则称 h 为从 $\mathfrak{A}$ 到 $\mathfrak{B}$ 上的一个 同构，并称 $\mathfrak{A}$ 和 $\mathfrak{B}$ 同构，记作 $\mathfrak{A} \cong \mathfrak{B}$。

注：

1. 学过抽象代数的同学立刻可以看出这里定义的同态是群同态，环同态，偏序的同态和图的同态等等的抽象。但我们的条件（a）要求双向箭头，这比代数中通常要求的单向 $\Rightarrow$ 要强，是所谓的“强同态”。但基本思想是一样的，即，同态是“保持结构”的映射。

2. 有些参考书把是单射的同态称为同构，而把双射的同态称为映上的同构。由于我们关于同构的讨论不多，因此为了避免混乱，我们所谈的同构都是映上的同构。

下面的同态定理告诉我们公式的真假是怎样通过同态从一个结构传到另一个结构中的。

定理 6.3.1 (同态定理)**.** 假定 h 为从 $\mathfrak{A}$ 到 $\mathfrak{B}$ 的一个同态，并且 $s : V \to |\mathfrak{A}|$。则

(a) 对任意项 t，$h(\overline{s}(t)) = \overline{h \circ s}(t)$。

(b) 对任何不含量词且不含等词的公式 α，$\models_{\mathfrak{A}} \alpha[s]$ 当且仅当 $\models_{\mathfrak{B}} \alpha[h \circ s]$。

(c) 如果 h 是单射，则 *(b)* 中的公式 α 可以包含等词。

(d) 如果 h 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 的满射，则 *(b)* 中的公式 α 可以包含量词。

证明: 我们将 (a) 留作习题。

(b) 令 α 为一个不含等词和量词的公式，我们对 α 施行归纳来证：$\models_{\mathfrak{A}} \alpha[s]$ 当且仅当 $\models_{\mathfrak{B}} \alpha[h \circ s]$。

如果 α 是一个原子公式 $Pt_1t_2\cdots t_n$，其中 P 是 n-元谓词符号，$t_1, t_2, \cdots, t_n$ 是项。则

$$\begin{aligned}
& \models_{\mathfrak{A}} Pt_1t_2\cdots t_n[s] \\
\Leftrightarrow\ & (\overline{s}(t_1), \overline{s}(t_2), \cdots, \overline{s}(t_n)) \in P^{\mathfrak{A}} \\
\Leftrightarrow\ & (h(\overline{s}(t_1)), h(\overline{s}(t_2)), \cdots, h(\overline{s}(t_n))) \in P^{\mathfrak{B}} \\
\Leftrightarrow\ & (\overline{h \circ s}(t_1), \overline{h \circ s}(t_2), \cdots, \overline{h \circ s}(t_n)) \in P^{\mathfrak{B}} \\
\Leftrightarrow\ & \models_{\mathfrak{B}} Pt_1t_2\cdots t_n[h \circ s]。
\end{aligned}$$

如果 α 形为 $\neg\beta$ 或者形为 $\beta \to \gamma$，则例行地利用归纳假设即可得到证明。

(c) 无论 h 是不是单射，我们总有：

$$\begin{aligned} \models_{\mathfrak{A}} u \approx t[s] &\Leftrightarrow \overline{s}(u) = \overline{s}(t) \\ &\Rightarrow h(\overline{s}(u)) = h(\overline{s}(t)) \\ &\Leftrightarrow \overline{h \circ s}(u) = \overline{h \circ s}(t) \\ &\Leftrightarrow \models_{\mathfrak{B}} u \approx t[h \circ s]。 \end{aligned}$$

如果 h 是单射，则第二步的“$\Rightarrow$”可以逆转。

(d) 无论 h 是不是满射，我们总有：

$$\begin{aligned} \models_{\mathfrak{A}} \forall x\beta[s] &\Leftrightarrow \text{对所有的 } d \in |\,\mathfrak{A}\,| \models_{\mathfrak{A}} \beta[s(x \mid d)] \\ &\Leftrightarrow \text{对所有的 } d \in |\,\mathfrak{A}\,| \models_{\mathfrak{B}} \beta[h \circ (s(x \mid d))] \\ &\Leftrightarrow \text{对所有的 } d \in |\,\mathfrak{A}\,| \models_{\mathfrak{B}} \beta[(h \circ s)(x \mid h(d))] \\ &\Leftarrow \text{对所有的 } e \in |\,\mathfrak{B}\,| \models_{\mathfrak{B}} \beta[(h \circ s)(x \mid e)] \\ &\Leftrightarrow \models_{\mathfrak{B}} \forall x\beta[h \circ s]。 \end{aligned}$$

如果 h 是满射，则倒数第二步的“$\Leftarrow$”可以逆转。并且注意第三个“$\Leftrightarrow$”是因为赋值函数 $h \circ (s(x \mid d))$ 和 $(h \circ s)(x \mid h(d))$ 作为从 V 到 $\mathfrak{B}$ 的函数是相等的（练习）。 □

定义 6.3.2. 固定一个语言 L 和其上的两个结构 $\mathfrak{A}$ 和 $\mathfrak{B}$。我们称它们为 *初等等价的*，记作 $\mathfrak{A} \equiv \mathfrak{B}$，如果对 L 中的任何一个闭语句 σ 都有 $\models_{\mathfrak{A}} \sigma$ 当且仅当 $\models_{\mathfrak{B}} \sigma$。

注：

1. 初等等价是一个非常重要的概念，只有在数理逻辑里面，人们才会如此重视研究对象的性质对其描述语言的依赖程度。

2. 同态定理告诉我们：任何两个同构的模型都是初等等价的。这在直观上很好理解，因为同构的两个结构本质上就是同一个，只不过是“标签”不同罢了。因此在一个结构里成立的事实在它的同构体中自然也成立。

3. 有意思的是其逆命题是否成立？即是否初等等价的结构都是同构的？后面我们会给出反例说明它不成立。道理不难理解，两个结构初等等价只不过说明，用我们规定的语言我们无法描述出它们的区别，并不意味着它们没有别的区别。换句话说，初等等价但不同构的现象只说明我们语言的匮乏而已。

结构 $\mathfrak{A}$ 上的一个 *自同构* 就是从 $\mathfrak{A}$ 到 $\mathfrak{A}$ 自身的一个同构。由同态定理，我们可以得出下列推论，说明任何自同构都保持可定义的关系。

推论 6.3.1. 令 h 为结构 $\mathfrak{A}$ 上的一个自同构，并且 R 是 $|\mathfrak{A}|$ 上的一个 $\mathfrak{A}$ 中可定义的 n-元关系。则对任意 $|\mathfrak{A}|$ 中的元素 $a_1, a_2, \cdots, a_n$，

$$(a_1, a_2, \cdots, a_n) \in R \Leftrightarrow (h(a_1), h(a_2) \cdots, h(a_n)) \in R。$$

证明: 令 φ 为 $\mathfrak{A}$ 中定义 R 的公式。根据同态定理（为什么？），

$$\models_{\mathfrak{A}} \varphi[a_1, a_2, \cdots, a_n] \Leftrightarrow \models_{\mathfrak{A}} \varphi[h(a_1), h(a_2), \cdots, h(a_n)]。$$

因此，

$$(a_1, a_2, \cdots, a_n) \in R \Leftrightarrow (h(a_1), h(a_2), \cdots, h(a_n)) \in R$$

（而这正是我们“保持” R 的意思）。 □

如果一个结构上有很多自同构，我们经常用推论 6.3.1 的逆否命题来证明某些集合或关系的不可定义性。

例 6.3.1. 考察由全体实数和其上的自然序组成的结构 $(\mathbb{R}, <)$。定义 $h : \mathbb{R} \to \mathbb{R}$ 为 $h(x) = x^3$。则 h 是该结构的一个自同构（为什么？）。$h^{-1}(x) = \sqrt[3]{x}$ 也是自同构。利用 h^{-1} 我们可以证明 $\mathbb{N}$ 在结构 $(\mathbb{R}, <)$ 中是不可定义的（为什么？）。

习题 6.3.

(1) 证明同态定理中的 (a) 部分。

(2) 找出所有在结构 $(\mathbb{R}, <)$ 中可定义的 (a) $\mathbb{R}$ 的子集；(b) $\mathbb{R}$ 上的二元关系。并证明你的结论。

(3) 证明加法函数的图像 $\{(m, n, p) : p = m + n\}$（作为三元关系）在结构 $(\mathbb{N}, \cdot)$ 中不可定义。提示：找一个结构 $(\mathbb{N}, \cdot)$ 上的把两个素数“互换”的自同构。

(4) 令 $L = \{\approx, \circ\}$ 其中 $\circ$ 为一个二元函数符号。对下列 L 的结构分别给出一个闭语句，使其在一个结构内成立，而在另三个结构中不成立。因此它们两两互不初等等价。

(a) $(\mathbb{R}; \times)$ 其中 $\times$ 是实数上通常的乘法；

(b) $(\mathbb{R}^*; \times^*)$ 其中 $\mathbb{R}^*$ 是非零实数的集合，$\times^*$ 是 $\times$ 在 $\mathbb{R}^*$ 上的限制；

(c) $(\mathbb{N}; +)$ 其中 $+$ 是自然数上通常的加法；

(d) $(\mathbb{P}; +^*)$ 其中 $\mathbb{P}$ 是正整数的集合，$+^*$ 是 $+$ 在 $\mathbb{P}$ 上的限制。

(5) 令 $L=\{\approx,P\}$ 其中 P 为一个二元谓词符号。考察结构 $(\mathbb{P},|)$ 其中 $\mathbb{P}$ 是正整数的集合，并且 $|$ 为整除关系。

(a) 所有素数的集合在该结构中可定义吗？为什么？

(b) 通常的小于关系 $a<b$ 在该结构中可定义吗？为什么？

(6) (a) 假定语言 L 中除了等词之外仅有一个二元谓词 P。证明如果 $\mathfrak{A}$ 是一个 L 上的有穷结构，并且 $\mathfrak{A}\equiv\mathfrak{B}$，则 $\mathfrak{A}$ 与 $\mathfrak{B}$ 同构。

(b) 证明 (a) 对任何包含等词的语言都成立。

[注：这说明我们有能力“完全刻画”有穷的结构。]

(7) 令 $\mathcal{L}$ 为一个固定的语言、$\mathfrak{A}$ 为 $\mathcal{L}$ 的一个结构并且 B 是论域 $|\mathfrak{A}|$ 的一个子集。我们称 $|\mathfrak{A}|$ 的一个子集 D 为 $\mathfrak{A}$ 中用 B 里的参数可定义的 如果存在一个自然数 k、一个 $\mathcal{L}$-公式 $\varphi(x,y_0,y_1,\cdots,y_{k-1})$ 其中 $x,y_0,y_1,\cdots,y_{k-1}$ 为 φ 的全部自由变元和元素 $b_0,b_1,\cdots,b_{k-1}\in B$ 使得

$$D=\{a\in|\mathfrak{A}|:\models_{\mathfrak{A}}\varphi[a,b_0,b_1,\cdots,b_{k-1}]\}。$$

考察结构 $(\mathbb{R},<)$。固定 $\mathbb{R}$ 的一个子集 B。证明一个集合 A 是 $(\mathbb{R},<)$ 中用 B 里的参数可定义的当且仅当 A 是有穷多个以 B 里的元素为端点的区间的并。 注意: 这里“区间”和“端点”的定义留给读者。证明中如果需要某些自同构的性质，也希望读者自行将其表达清楚并证明。

(8) 假定 X 为 $|\mathfrak{A}|$ 的一个子集并且在结构 $\mathfrak{A}$ 的所有自同构下不变，X 一定是 $\mathfrak{A}$ 上可定义的吗?

第七章　哥德尔完全性定理

第一节　可靠性定理

定理 7.1.1 (可靠性定理). 如果 $\Gamma \vdash \varphi$，则 $\Gamma \models \varphi$。

我们把证明分成一些小的步骤。首先注意到：如果 $\Gamma \models \psi$ 并且 $\Gamma \models \psi \to \varphi$，则 $\Gamma \models \varphi$。（为什么？）换句话说，分离规则保持真确性。因此我们只需验证所有公理都是普遍有效的。

根据习题 6.1，一个公式 θ 是普遍有效的当且仅当 $\forall x\theta$ 是普遍有效的。我们得到：一个普遍有效公式的概括仍是普遍有效的。所以我们只要检查六组公理，验证每一组中的公式都是普遍有效的。

习题 6.1 还告诉我们，$\{\forall x(\alpha \to \beta), \forall x\alpha\} \models \forall x\beta$ 和当 x 不在 α 中自由出现时，$\alpha \to \forall x\alpha$。因而第三和第四组公理都是普遍有效的。

我们把第一组公理的普遍有效性留做习题。

第五组公理 $x \approx x$ 的普遍有效性是显然的。

我们再来看第六组公理的普遍有效性：$x \approx y \to (\alpha \to \alpha')$，其中 α 为原子公式并且 α' 是将 α 中出现若干个 x 用 y 替换所得到的。我们只需验证 $\{x \approx y, \alpha\} \models \alpha'$。固定一个结构 $\mathfrak{A}$ 和赋值 s 满足 $\models_{\mathfrak{A}} x \approx y[s]$，即，$s(x) = s(y)$。通过对项 t 施行归纳（具体步骤省略），我们可以证明 $\overline{s}(t) = \overline{s}(t')$ 其中 t' 是将 t 中出现若干个 x 用 y 替换所得到的。如果 α 是 $t_1 \approx t_2$，则 α' 为 $t_1' \approx t_2'$，因而 $\models_{\mathfrak{A}} \alpha[s]$ 当且仅当 $\overline{s}(t_1) = \overline{s}(t_2)$ 当且仅当 $\overline{s}(t_1') = \overline{s}(t_2')$ 当且仅当 $\models_{\mathfrak{A}} \alpha'[s]$。类似的证明对形如 $Pt_1 \dots t_n$ 的原子公式 α 也适用。

所以我们只剩下验证第二组替换公理的普遍有效性。我们先证明一个引理。

引理 7.1.1 (替换引理). 如果项 t 可以在公式 φ 中替换变元 x，则 $\models_{\mathfrak{A}} \varphi_t^x[s]$ 当且仅当 $\models_{\mathfrak{A}} \varphi[s(x \mid \overline{s}(t))]$。

证明: 我们对公式 φ 施行归纳。

初始情形：φ 是原子公式。首先利用对项 u 施行归纳，很容易证明：对任何项 u 和 t，都有 $\overline{s}(u_t^x) = \overline{s(x \mid \overline{s}(t))}(u)$。我们这里只证明当 φ 为 $Pu_1u_2 \cdots u_n$ 的情形，而把 φ 为

$u_1 \approx u_2$ 的验证留给读者。

$$\begin{aligned}
&\models_{\mathfrak{A}} (Pu_1u_2\cdots u_n)^x_t[s]\\
\text{当且仅当}\quad &(\overline{s}((u_1)^x_t), \overline{s}((u_2)^x_t), \cdots, \overline{s}((u_n)^x_t)) \in P^{\mathfrak{A}}\\
\text{当且仅当}\quad &(\overline{s(x \mid \overline{s}(t))}(u_1), \overline{s(x \mid \overline{s}(t))}(u_2), \cdots, \overline{s(x \mid \overline{s}(t))}(u_n)) \in P^{\mathfrak{A}}\\
\text{当且仅当}\quad &\models_{\mathfrak{A}} Pu_1u_2\cdots u_n[s(x \mid \overline{s}(t))]。
\end{aligned}$$

归纳情形：我们只处理量词的情形，而把 φ 为 $\neg\psi$ 或者 $\psi \to \theta$ 的情形留给读者。

如果 φ 为 $\forall y\psi$ 并且 x 不在 φ 中自由出现。只须注意 s 和 $s(x \mid \overline{s}(t))$ 在出现在 φ 中的自由变元上取值相同，还有 φ^x_t 就是 φ，立刻可得知结论成立。

剩下的情形为 φ 为 $\forall y\psi$ 并且 x 的确在 φ 中自由出现。由于 t 可以在 φ 中替换 x，我们有 y 不在 t 中出现并且 t 可以在 ψ 中替换 x。所以，对论域 $|\mathfrak{A}|$ 中的任何 d 都有 $\overline{s}(t) = \overline{s(y \mid d)}(t)$。由于 $x \neq y$，$\varphi^x_y = \forall y\psi^x_t$。所以

$$\begin{aligned}
&\models_{\mathfrak{A}} \varphi^x_t[s]\\
\text{当且仅当}\quad &\text{对所有 } d, \models_{\mathfrak{A}} \psi^x_t[s(y \mid d)],\\
\text{当且仅当}\quad &\text{对所有 } d, \models_{\mathfrak{A}} \psi[s(y \mid d)(x \mid \overline{s}(t))] \quad \text{根据归纳假定}\\
\text{当且仅当}\quad &\models_{\mathfrak{A}} \varphi[s(x \mid \overline{s}(t))]。
\end{aligned}$$

这就完成了对替换引理的归纳证明。 □

返回到对第二组公理可靠性的验证。假定 t 在 φ 中可以替换 x 并且 $\models_{\mathfrak{A}} \forall x\varphi[s]$。我们需要证明 $\models_{\mathfrak{A}} \varphi^x_t[s]$。我们知道对 $|\mathfrak{A}|$ 中的任意元素 d，都有 $\models_{\mathfrak{A}} \varphi[s(x \mid d)]$。特别地，取 d 为 $\overline{s}(t)$，我们有 $\models_{\mathfrak{A}} \varphi[s(x \mid \overline{s}(t))]$。根据替换引理，$\models_{\mathfrak{A}} \varphi^x_t[s]$。

到此可靠性定理验证完毕。我们叙述可靠性定理的两个常用推论。

推论 7.1.1. *如果 $\vdash (\varphi \leftrightarrow \psi)$，则 φ 和 ψ 语义等价。*

推论 7.1.2. *如果 Γ 是可满足的，即存在结构 $\mathfrak{A}$ 和赋值 s 满足 Γ 中的所有公式，则 Γ 是一致的。*

第二节　完全性定理

“如果一个一阶语句在所有的模型中都成立，那一定是因为有一个统一的原因（证明），而不是源于偶然让它在不同的模型内或在不同的情形下因不同的原因而成立。” – 布拉斯[1]

[1] 布拉斯，Andreas Blass （1947 - ），美国逻辑学家，数学家。

接下来我们证明可靠性定理的逆定理 – 完全性定理。最初的证明是哥德尔在 1929 年证明 1930 年发表的。我们下面采用的证明是辛钦 [2]在 1949 年给出的。我们只考虑一阶语言是可数的情形，即语言中所有的符号组成一个可数集。[3]

定理 7.2.1 (完全性定理).

(a) 如果 $\Gamma \models \varphi$，则 $\Gamma \vdash \varphi$。

(b) 任何一致的公式集都是可满足的。

根据引理 3.8.3，(a) 与 (b) 等价。（虽然引理 3.8.3 讨论的是命题逻辑，但证明稍加改动便对一阶逻辑也适用。）所以我们只证明 (b)。我们首先考虑语言中没有等词的情况。假定 Γ 是一个一致的公式集。证明的思路与命题逻辑的完全性定理相似。我们首先把 Γ 扩充成一个极大一致集 Δ 还包括一族新的“辛钦公理”，以帮助我们处理量词。所谓辛钦公理的形式如下：

$$\neg\forall x\varphi \to \neg\varphi^x_c,$$

其中 c 是“新的”常数符号。我们要做的其实是添加 $\exists x\psi \to \psi^x_c$，即对每一个存在性的语句都添加一个直接证据 c。我们写成以上的等价形式是因为后面用起来更直接。本质上说，辛钦公理其实就是量词消去，代价是添加新的常数。有了这样的 Δ 之后，我们很容易“读出”一个满足 Δ 中（除了带等词的）所有公式的结构和赋值。

首先我们向语言 L 中添加可数多个新的常数符号 $C = \{c_0, c_1, \cdots\}$。把扩展后的语言记作 L_C。我们验证 Γ 在新的语言中仍然是一致的。这听起来是显然的，但添加了常数符号后，公理变多了，我们还是有必要验证一下。（这实际上是后面归纳验证辛钦公理的一致性的一部分。）假如在扩张语言之后 Γ 变得不一致了，则存在（L_C 内的）公式 β 和某个（L_C 内的）从 Γ 到 $\beta \wedge \neg\beta$ 的证明序列。注意到证明序列中包含的新常数符号为有穷多。我们可以用常数概括定理把它们都替换成变元，从而得到一个从 Γ 到 $(\beta' \wedge \neg\beta')$（在 L 中的）证明序列，其中 β' 是从 β 中把新常数符号替换成变元而得到的。由于 β' 是 L 中的公式，这与 Γ 的一致性矛盾。

接下来我们添加所谓 辛钦公理 ，即对所有（L_C 中的）公式 φ 和所有的变元 x，我们都向 Γ 中添加公式

$$\neg\forall x\varphi \to \neg\varphi^x_c,$$

其中 c 是某个新常数符号。具体做法如下[4]：固定一个（L_C 中）公式和变元有序对 (φ, x) 的枚举：

$$(\varphi_1, x_1), (\varphi_2, x_2), \cdots$$

[2]辛钦，Leon Henkin (1921 - 2006)，美国逻辑学家。

[3]完全性定理对不可数语言也成立，只不过证明要用到选择公理等集合论工具。

[4]另一种常见的做法是：从语言 $L_0 = L$ 出发，添加可数多常数 C_0 使得 L_0 中的公式都有辛钦公理相配，但语言扩展成 $L_1 = L_0 \cup C_0$ 之后，我们还要添新的常数 C_1 使得 L_1 中的公式都有辛钦公理相配，如此下去，我们需要扩充 ω 步才能达到目的。

枚举存在性是由语言的可数性保证的。令 θ_1 为

$$\neg\forall x_1\varphi_1 \to \neg(\varphi_1)^{x_1}_{c_{i_1}},$$

其中 c_{i_1} 为第一个不在 φ_1 中出现的新常数符号。假如我们已经处理完了前 k 个有序对，并且定义了辛钦公理 $\{\theta_1, \theta_2, \cdots, \theta_k\}$，则令 θ_{k+1} 为

$$\neg\forall x_{k+1}\varphi_{k+1} \to \neg(\varphi_{k+1})^{x_{k+1}}_{c_{i_{k+1}}},$$

其中 $c_{i_{k+1}}$ 为第一个在 $\varphi_1 \cdots, \varphi_k, \varphi_{k+1}, \theta_1, \cdots, \theta_k$ 中都不出现的新常数符号。这样不断地做下去，我们最终得到一个公式集 $\Theta = \{\theta_1, \theta_2, \cdots\}$。我们验证 $\Gamma \cup \Theta$ 仍然是一致的：如果不一致的话，则根据证明序列的有限性和前面验证的 Γ 的一致性，就存在某个 $m \geq 0$，使得

$$\Gamma \cup \{\theta_1, \cdots, \theta_{m+1}\}$$

为不一致的。选取最小的这样的 m。根据（RAA）

$$\Gamma \cup \{\theta_1, \cdots, \theta_m\} \vdash \neg\theta_{m+1}。$$

假设 θ_{m+1} 为

$$\neg\forall x\varphi \to \neg\varphi^x_c。$$

根据重言规则，我们有

$$\Gamma \cup \{\theta_1, \cdots, \theta_m\} \vdash \neg\forall x\varphi,$$

并且

$$\Gamma \cup \{\theta_1, \cdots, \theta_m\} \vdash \varphi^x_c。$$

注意到 c 在表达式左边不出现，根据常数概括定理，我们有

$$\Gamma \cup \{\theta_1, \cdots, \theta_m\} \vdash \forall x\varphi,$$

这与 m 的极小性矛盾。

我们在一致公式集 $\Gamma \cup \Theta$ 继续扩张，以得到一个极大一致的公式集 Δ，即对任何公式 φ 或者 $\varphi \in \Delta$ 或者 $(\neg\varphi) \in \Delta$。具体做法与命题逻辑中林登鲍姆引理的证明完全类似，这里不再重复。注意任何的极大一致集 Δ 都对语法后承（或说对推导）封闭：如果 $\Delta \vdash \varphi$，则一致性告诉我们 $\Delta \nvdash \neg\varphi$ 所以 $(\neg\varphi) \notin \Delta$，在根据极大性，就有 $\varphi \in \Delta$。

小结：我们扩充了语言，添加了辛钦公理集 Θ，并把 $\Gamma \cup \Theta$ 扩充成一个极大一致集 Δ。

下一步我们将从 Δ 中“读出”一个新语言 L_C 上的结构 $\mathfrak{A}$，但把等词 $\approx$ 暂时替换成一个新的二元谓词 E。（等词的处理将使我们下一步的工作。）结构 $\mathfrak{A}$ 的定义如下：

(a) 论域 $|\mathfrak{A}|$ 为语言 L_C 上所有项的集合。

(b) 定义二元关系 $E^{\mathfrak{A}}$ 为 $(u,t)\in E^{\mathfrak{A}}$ 当且仅当公式 $u\approx t$ 属于 Δ。

(c) 对每个 n-元谓词符号 P，定义 n-元关系 $P^{\mathfrak{A}}$ 为

$$(t_1,t_2,\cdots,t_n)\in P^{\mathfrak{A}} \text{ 当且仅当 } Pt_1t_2\cdots t_n\in\Delta。$$

(d) 对每个 n-元函数符号 f，定义 $f^{\mathfrak{A}}$ 为 $f^{\mathfrak{A}}(t_1,t_2,\cdots,t_n)=ft_1t_2\cdots t_n$。

(e) 对每个常数符号 c，定义 $c^{\mathfrak{A}}=c$。

定义赋值函数 $s:V\to|\mathfrak{A}|$ 为等同函数，即对所有的变元 v，$s(v)=v$。

引理 7.2.1. 对任意项 t，$\overline{s}(t)=t$。对任意公式 φ，$\models_{\mathfrak{A}}\varphi^*[s]$ 当且仅当 $\varphi\in\Delta$，其中 φ^* 是将 φ 中的等词用 E 替换而得到的。

证明: 通过对项 t 施行归纳，不难证明 $\overline{s}(t)=t$。细节我们留给读者。

我们下面对公式 φ 中出现的联词和量词的个数 k 施行归纳，证明 $\models_{\mathfrak{A}}\varphi^*[s]$ 当且仅当 $\varphi\in\Delta$。

初始情形：$k=0$ 则 φ 为原子公式。如果 φ 为 $Pt_1t_2\cdots t_n$，则

$$\begin{aligned}
&\models_{\mathfrak{A}}\varphi^*[s]\\
\text{当且仅当}\quad&\models_{\mathfrak{A}}Pt_1t_2\cdots t_n[s]\\
\text{当且仅当}\quad&(\overline{s}(t_1),\overline{s}(t_2),\cdots,\overline{s}(t_n))\in P^{\mathfrak{A}}\\
\text{当且仅当}\quad&(t_1,t_2,\cdots,t_n)\in P^{\mathfrak{A}}\\
\text{当且仅当}\quad&Pt_1t_2\cdots t_n\in\Delta。
\end{aligned}$$

如果 φ 为 $u\approx t$，则

$$\begin{aligned}
&\models_{\mathfrak{A}}\varphi^*[s]\\
\text{当且仅当}\quad&\models_{\mathfrak{A}}uEt[s]\\
\text{当且仅当}\quad&(\overline{s}(u),\overline{s}(t))\in E^{\mathfrak{A}}\\
\text{当且仅当}\quad&(u,t)\in E^{\mathfrak{A}}\\
\text{当且仅当}\quad&u\approx t\in\Delta。
\end{aligned}$$

归纳情形：假定我们已经证明了引理对联词和量词个数为 k 的公式成立。考察某个联词和量词个数为 $k+1$ 的公式 φ。φ 有三种可能性：$\neg\psi$，$\alpha\to\beta$ 和 $\forall x\psi$，其中 ψ,α 和 β 的联词和量词个数小于或等于 k。

假如 φ 为 $\neg\psi$，则通常的归纳可以走通，我们略去细节。

假如 φ 为 $\alpha \to \beta$，则

$$\begin{aligned} \models_{\mathfrak{A}} (\alpha \to \beta)^*[s] \quad & \text{当且仅当} \quad \not\models_{\mathfrak{A}} \alpha^*[s] \text{ 或者 } \models_{\mathfrak{A}} \beta^*[s], \\ & \text{当且仅当} \quad \alpha \notin \Delta \text{ 或者 } \beta \in \Delta, \\ & \text{当且仅当} \quad \neg\alpha \in \Delta \text{ 或者 } \beta \in \Delta。 \end{aligned}$$

无论 $\neg\alpha \in \Delta$ 还是 $\beta \in \Delta$，我们都有 $\Delta \vdash (\alpha \to \beta)$。根据 Δ 对推导的封闭性，我们有 $(\alpha \to \beta) \in \Delta$。另一方面，如果 $(\alpha \to \beta) \in \Delta$，则或者 $\alpha \notin \Delta$ 或者 $[\alpha \in \Delta$ 并且 $\Delta \vdash \beta]$。因而或者 $\neg\alpha \in \Delta$ 或者 $\beta \in \Delta$，再反向倒溯上文的论证，就得到 $\models_{\mathfrak{A}} (\alpha \to \beta)^*[s]$。

假如 φ 为 $\forall x\psi$，我们证明：$\models_{\mathfrak{A}} \forall x\psi^*[s]$ 当且仅当 $\forall x\psi \in \Delta$ （注意我们用了 $\forall x\psi^*$ 为 $(\forall x\psi)^*$ 这一事实。）从左向右，我们先选好 c 为辛钦公理 $\neg\forall x\psi \to \neg\psi^x_c$ 中的常数 c，然后有：

$$\begin{aligned} \models_{\mathfrak{A}} \forall x\psi^*[s] \quad & \Rightarrow \quad \models_{\mathfrak{A}} \psi^*[s(x \mid c)] \\ & \Rightarrow \quad \models_{\mathfrak{A}} (\psi^*)^x_c[s] \qquad \text{由替换引理} \\ & \Rightarrow \quad \models_{\mathfrak{A}} (\psi^x_c)^*[s] \\ & \Rightarrow \quad \psi^x_c \in \Delta \\ & \Rightarrow \quad \neg\psi^x_c \notin \Delta \\ & \Rightarrow \quad (\neg\forall x\psi) \notin \Delta \qquad \text{因为 } \theta \in \Delta \text{ 并且 } \Delta \text{ 对推导封闭} \\ & \Rightarrow \quad \forall x\psi \in \Delta。 \end{aligned}$$

从右向左，首先利用约束变元替换先选一个公式 ϕ 使得 ϕ 和 ψ 的差别仅在于约束变元（因而联词和量词的个数不变）并且 t（t 的选法见下文）在 ϕ 中可以替换 x。我们有

$$\begin{aligned} \not\models_{\mathfrak{A}} \forall x\psi^*[s] \quad & \Rightarrow \quad \not\models_{\mathfrak{A}} \psi^*[s(x \mid t)] \qquad \text{对某个 } t\text{，选好并固定} \\ & \Rightarrow \quad \not\models_{\mathfrak{A}} \phi^*[s(x \mid t)] \qquad \text{因为 } \psi^* \text{ 和 } \phi^* \text{ 语义等价} \\ & \Rightarrow \quad \not\models_{\mathfrak{A}} (\phi^x_t)^*[s] \qquad \text{根据替换引理} \\ & \Rightarrow \quad \phi^x_t \notin \Delta \qquad \text{根据归纳假设} \\ & \Rightarrow \quad \forall x\phi \notin \Delta \\ & \Rightarrow \quad \forall x\psi \notin \Delta \qquad \text{根据约束变元替换引理。} \end{aligned}$$

这就完成了对归纳情形的证明。 □

小结：我们得到了一个结构 $\mathfrak{A}$ 和一个赋值 s，它们满足 Δ 里面所有不含等词 $\approx$ 的公式。

我们下面处理等词。首先看看等词到底带来什么问题。回忆一下我们对等词的解释的特殊要求。例如，假定我们的语言中本来有常数符号 d，我们在添加辛钦公理时，会把 $\exists x(x \approx d) \to c \approx d$ 添加进去，其中 c 是一个新的常数符号，特别地，$c \neq d$。所以

$c \approx d \in \Delta$。可是在我们的结构 $\mathfrak{A}$ 中，$\models_{\mathfrak{A}} c \approx d$ 当且仅当 $c^{\mathfrak{A}} = d^{\mathfrak{A}}$ 即 $c = d$，也就是 c 和 d 是同一个常数符号，这显然是不对的。

我们解决方案是考虑商结构 $\mathfrak{A}/E$，它的定义为 $\mathfrak{A}$ 模掉等价关系 $E^{\mathfrak{A}}$。大致上说，就是把像 c, d 这样的满足 $c \approx d \in \Delta$ 的项等同起来，看成一个东西。问题就解决了。具体细节如下：

引理 7.2.2. *$E^{\mathfrak{A}}$ 是论域 $|\mathfrak{A}|$ 上的一个合同关系，也就是说，*

(1) $E^{\mathfrak{A}}$ 是论域 $|\mathfrak{A}|$ 上的一个等价关系。

(2) 对语言中的任何一个不是等词的 n-元谓词符号 P，任何的项 t_i 和 u_i （$i = 1, 2, \cdots, n$）如果对所有的 $i \leq n$，$t_i E^{\mathfrak{A}} u_i$，则

$$(t_1, t_2, \cdots, t_n) \in P^{\mathfrak{A}} \text{ 蕴涵 } (u_1, u_2, \cdots, u_n) \in P^{\mathfrak{A}}。$$

(3) 对语言中的任何一个 n-元函数符号 f，任何的项 t_i 和 u_i （$i = 1, 2, \cdots, n$）如果对所有的 $i \leq n$，$t_i E^{\mathfrak{A}} u_i$，则

$$f^{\mathfrak{A}}(t_1, t_2, \cdots, t_n) E^{\mathfrak{A}} f^{\mathfrak{A}}(u_1, u_2, \cdots, u_n)。$$

证明: 引理的证明本质上是第 五 章中那些关于等词的内定理。我们留作习题。 □

对每个 $|\mathfrak{A}|$ 中的元素 t，令 $[t]$ 表示包含它的等价类。定义 商结构 $\mathfrak{A}/E$ 如下：

(a) 论域 $|\mathfrak{A}/E| = \{[t] : t \in |\mathfrak{A}|\}$，即由 t 的等价类 $[t]$ 形成的集合。

(b) 对每个 n-元谓词符号 P，

$$([t_1], [t_2], \cdots, [t_n]) \in P^{\mathfrak{A}/E} \text{当且仅当} (t_1, t_2, \cdots, t_n) \in P^{\mathfrak{A}}。$$

(c) 对每个 n-元函数符号 f，

$$f^{\mathfrak{A}/E}([t_1], [t_2], \cdots, [t_n]) = [f^{\mathfrak{A}}(t_1, t_2, \cdots, t_n)]。$$

(d) 对每个常数符号 c，$c^{\mathfrak{A}/E} = [c^{\mathfrak{A}}]$。

引理 7.2.3. *对任意公式 φ，$\models_{\mathfrak{A}/E} \varphi[S]$ 当且仅当 $\varphi \in \Delta$，其中赋值 S 为 $S(v) = [v]$。*

我们可以把 S 看成由等同赋值 s 诱导出的赋值。更一般地，每一个赋值 r 都自然诱导出一个商结构的赋值 R，即对每一个变元 v，$R(v) = [r(v)]$。证明的思路是依照引理 7.2.1 和商结构的定义，进行惯常的归纳验证。

证明: 根据引理 7.2.1，只需证明：$\models_{\mathfrak{A}/E} \varphi[S]$ 当且仅当 $\models_{\mathfrak{A}} \varphi^*[s]$。

我们对 φ 施行归纳，证明下列略微强一点的命题：对任意赋值 r，$\models_{\mathfrak{A}/E} \varphi[R]$ 当且仅当 $\models_{\mathfrak{A}} \varphi^*[r]$，其中 R 为由 r 诱导出的赋值。

首先，通过对项 t 施行归纳，很容易证明：对任意项 t，$\overline{R}(t) = [\overline{r}(t)]$。而且对所有项 u，$r(x \mid u)$ 诱导出的赋值为 $R(x \mid [u])$。

初始情形：φ 为原子公式。如果 φ 为 $Pt_1t_2\cdots t_n$，其中 P 为不是等词的 n-元谓词符号。则

$$\begin{aligned}
& \models_{\mathfrak{A}/E} Pt_1t_2\cdots t_n[R] \\
\text{当且仅当}\quad & (\overline{R}(t_1), \overline{R}(t_2), \cdots, \overline{R}(t_n)) \in P^{\mathfrak{A}/E} \\
\text{当且仅当}\quad & ([\overline{r}(t_1)], [\overline{r}(t_2)], \cdots, [\overline{r}(t_n)]) \in P^{\mathfrak{A}/E} \\
\text{当且仅当}\quad & (\overline{r}(t_1), \overline{r}(t_2), \cdots, \overline{r}(t_n)) \in P^{\mathfrak{A}} \\
\text{当且仅当}\quad & \models_{\mathfrak{A}} Pt_1t_2\cdots t_n[r]。
\end{aligned}$$

如果 φ 是原子公式 $t \approx t'$，则

$$\begin{aligned}
& \models_{\mathfrak{A}/E} t \approx t'[R] \\
\text{当且仅当}\quad & \overline{R}(t) = \overline{R}(t') \\
\text{当且仅当}\quad & [\overline{r}(t)] = [\overline{r}(t')] \\
\text{当且仅当}\quad & \overline{r}(t) E^{\mathfrak{A}} \overline{r}(t') \\
\text{当且仅当}\quad & \models_{\mathfrak{A}} (t \approx t')^*[r]。
\end{aligned}$$

归纳情形：我们把联词 $\neg$ 和 $\to$ 的处理留给读者，只考察 φ 为 $\forall x\psi$ 的情形：

$$\begin{aligned}
& \models_{\mathfrak{A}/E} \varphi[R] \\
\text{当且仅当}\quad & \text{对每一个项 } u,\quad \models_{\mathfrak{A}/E} \psi[R(x \mid [u])] \\
\text{当且仅当}\quad & \text{对每一个项 } u,\quad \models_{\mathfrak{A}} \psi^*[r(x \mid u)] \quad \text{归纳假定} \\
\text{当且仅当}\quad & \models_{\mathfrak{A}} \forall x\psi^*[r] \\
\text{当且仅当}\quad & \models_{\mathfrak{A}} \varphi[r]。
\end{aligned}$$

这就完成了对引理的归纳证明。 □

引理 7.2.3 似乎完成了完全性定理的证明。但实际上我们做过头了。我们需要的是一个语言 L 的结构，即一个定义域为 L 中符号的（解释）函数，我们得到的是一个扩充后的语言 L_C 上的结构。因此我们把结构 $\mathfrak{A}/E$ 限制在扩充前的语言 L 上，所得到的结构就是完全性定理所要的。

习题 7.1.

(1) (a) 令 $\mathfrak{A}$ 为一个结构并且 $s : V \to |\mathfrak{A}|$ 为一个给变元的赋值。由此诱导出一个真值指派 v 定义在素公式（所形成的命题符号）上：

$$v(\alpha) = T \text{ 当且仅当 } \models_{\mathfrak{A}} \alpha[s]。$$

证明对任意公式 α （不一定为素公式）都有：

$$\overline{v}(\alpha) = T \text{ 当且仅当 } \models_{\mathfrak{A}} \alpha[s]。$$

(b) 由 (a) 导出：如果 φ 是第一组公理中的公式（事实上，对任何一阶意义下的重言式 φ），则 $\models \varphi$。[这是可靠性定理证明的一部分。]

(2) 证明引理 7.2.2。

(3) 令 Λ 为我们前面选定了一阶逻辑的公理集。我们下面对 Λ 进行一些改动，看看它对语法和语义有什么影响。

(a) 假如我们向 Λ 添加一个非普遍有效的公式 ψ，证明可靠性定理不再成立。

(b) 假如我们走向另一个极端，令 $\Lambda = \emptyset$，即没有任何的逻辑公理。证明完全性定理不再成立。

(c) 假如我们向 Λ 添加一个新的普遍有效公式 ψ，证明此时可靠性定理和完全性定理都依然成立。

(4) （本练习讨论存在量词例化规则的两种形式，请不要用可靠性和完全性定理。）

(a) 规则的语法形式：假定常数符号 c 在公式 φ，ψ，和公式集 Γ 中都不出现，并且 $\Gamma \cup \{\varphi_c^x\} \vdash \psi$。则 $\Gamma \cup \{\exists x\varphi\} \vdash \psi$。

(b) 规则的语义形式：假定常数符号 c 在公式 φ，ψ，和公式集 Γ 中都不出现，并且 $\Gamma \cup \{\varphi_c^x\} \models \psi$。则 $\Gamma \cup \{\exists x\varphi\} \models \psi$。

第三节　自然推演系统的可靠性和完全性

我们沿用第 五 章第 五 节的自然推演系统。其可靠性是不难证明的，我们留作练习。我们下面证明它的弱完全性，即它可以证明所有的普遍有效式。至于自然推演中一般形式的完全性定理也是成立的，有兴趣的读者可以参考 [7] 或其它证明论的参考书。

我们已经有了辛钦的证明，该证明在模型论中非常有用，因为利用常数符号来构造模型是模型论中最基本的方法。在后面谈到紧致性定理和它的应用时，用到的方法本质上都是辛钦构造。我们下面给出的搜寻证明树的构造模型方法虽然也利用了项，但它提供给我们一些新的信息。一是可以得到一些证明论学家关心的性质，如，切割消去和所谓子公式性质，即如果一个公式是可证的，则存在一个（自然推演系统的）证明，其中出现的都是它的子公式。二是它提供给我们一些能行性的信息。这一点有些超前，我们点到为止。有些读者可能会关心哥德尔的完全性定理是否等在“有穷数学”中得到证明。从下面的证明我们清楚地看到，我们需要在某棵树上拿到一个无穷支。因此完全性定理不能在“有穷数学”中得到证明。精确的版本是反推数学中如下的定理：完全性定理等价于弱的柯尼西引理[5]。

我们证明：如果 $\nvdash \Gamma$，则 Γ 不是普遍有效的。证明思路是：我们试图从 Γ 出发，寻找它的一个证明树。在寻找过程中，我们不用切割规则，而把其它推理规则倒过来用，并把 Γ 里的公式分解成其子公式。由于 Γ 不是可证的，我们的寻找注定失败，但从失败当中我们可以读出一个让 Γ 不成立的模型（反模型）。细节如下：

首先把 Γ 中的公式排成一个序列，原子公式（如果有的话）在前。令 α 为序列中第一个非原子公式，Δ 为其余部分，则序列 Γ 形如：

$$\Gamma = \text{若干原子公式}, \alpha, \Delta。$$

然后我们用下述规则把 α 拆成其子公式，从而产生新的公式序列 Γ'，在 $(\wedge)$ 情形中我们会得到两个新序列 Γ'_0 和 Γ'_1。

$(\vee)$ $\Gamma =$ 若干原子公式，$(\alpha_0 \vee \alpha_1), \Delta$，则 $\Gamma' =$ 同样原子公式，$\alpha_0, \alpha_1, \Delta$；

$(\wedge)$ $\Gamma =$ 若干原子公式，$(\alpha_0 \wedge \alpha_1), \Delta$，则对 $i = 0, 1$，$\Gamma'_i =$ 同样原子公式，α_i, Δ。

$(\forall)$ $\Gamma =$ 若干原子公式，$\forall x \beta(x), \Delta$，则 $\Gamma' =$ 同样原子公式，$\beta(v_j), \Delta$，其中 v_j 为一个迄今为止没有用到过的变元；

$(\exists)$ $\Gamma =$ 若干原子公式，$\exists x \beta(x), \Delta$，则 $\Gamma' =$ 同样原子公式，$\beta(v_k), \Delta, \exists x \beta(x)$，其中 v_k 为 $v_0, v_1, v_2, \cdots$ 中第一个迄今为止没有用来当成 $\exists x \beta(x)$ 证据的变元。

重复上述过程，我们就得到一个序列 $\Gamma, \Gamma', \Gamma'', \cdots$，并且可以排成树状，将 Γ 排在最下面，然后自下而上，依次添加 $\Gamma', \Gamma'', \cdots$ 等等。例如，它有可能是：

$$\dfrac{\dfrac{\Gamma''_0 \quad \Gamma''_1}{\Gamma'}}{\Gamma} \quad 。$$

注意到我们的生成规则恰好是把推理规则倒过来，因此在这棵树上，排在下面的 Γ^* 可以视为从排在它上面的 Γ^{**} 按照自然推演规则导出的，（在 $(\wedge)$ 情形中则是从 Γ_0^{**} 和 Γ_1^{**} 中

[5] 弱的柯尼西引理，Weak König Lemma (WKL_0)，柯尼西，Dénes König （1884 - 1944），匈牙利数学家。

导出的)。如果发现树的某个节点上的公式集是一个公理，则停止这一支的构造。根据 Γ 不可证的假定，这棵树至少有一支，记为 p，或者 (a) 终结于一个由原子公式组成的但不是公理的序列；或者 (b) 永不终结，即形成一个无穷支。

从分支 p 中我们定义一个 Γ 的“反模型” $\mathfrak{A}$ 如下：论域 $|\mathfrak{A}|$ 为自然数集 $\mathbb{N}$；对每个谓词符号 P_j 定义：

$(i_1, i_2, \cdots, i_n) \in P_j^{\mathfrak{A}}$ 当且仅当 原子公式 $P_j(v_{i_1}, v_{i_2}, \cdots, v_{i_n})$ 不在分支 p 中出现。

引理 7.3.1. *令赋值函数 s 为 $s(v_i) = i$。对任意在分支 p 中出现的公式 α，都有 $\not\models_{\mathfrak{A}} \alpha[s]$。*

证明: 对公式 α 施行归纳。注意：根据序列的构造，每一个 p 中出现的非原子公式都会有机会被处理到，因此它的子公式都会在 p 中出现。

初始情形：α 为原子公式 $P_j(v_{i_1}, v_{i_2}, \cdots, v_{i_n})$，则根据定义，$\not\models_{\mathfrak{A}} \alpha[s]$。

归纳情形：我们分成如下子情形来讨论：

子情形 1：α 为 $\overline{P}_j(v_{i_1}, v_{i_2}, \cdots, v_{i_n})$。由于 p 中不含公理，因此公式 $P_j(v_{i_1}, v_{i_2}, \cdots, v_{i_n})$ 在 p 中不出现，所以 $\models_{\mathfrak{A}} P_j(v_{i_1}, v_{i_2}, \cdots, v_{i_n})[s]$，因而 $\not\models_{\mathfrak{A}} \alpha[s]$。

子情形 2：α 为 $\alpha_0 \vee \alpha_1$。当我们处理 α 时，α_0 和 α_1 都被添进 p 中。根据归纳假定，我们有 $\not\models_{\mathfrak{A}} \alpha_0[s]$ 和 $\not\models_{\mathfrak{A}} \alpha_1[s]$。所以 $\not\models_{\mathfrak{A}} \alpha[s]$。

子情形 3：α 为 $\alpha_0 \wedge \alpha_1$。当我们处理 α 时，α_0 和 α_1 至少有一个被添进 p 中。根据归纳假定，我们至少有 $\not\models_{\mathfrak{A}} \alpha_0[s]$ 或 $\not\models_{\mathfrak{A}} \alpha_1[s]$。所以 $\not\models_{\mathfrak{A}} \alpha[s]$。

子情形 4：α 为 $\forall x \beta(x)$。当我们处理 α 时，某个 $\beta(v_j)$ 被添进 p 中。根据归纳假定，我们有 $\not\models_{\mathfrak{A}} \beta(v_j)[s]$。所以 $\not\models_{\mathfrak{A}} \alpha[s]$。

子情形 5：α 为 $\exists x \beta(x)$。根据构造，我们会处理 α 无穷多次，在每次处理它时，j-最小的那个还不在 p 中的 $\beta(v_j)$ 被添进 p 中。所以，对每一个自然数 i，$\beta(v_i)$ 都在 p 中出现。根据归纳假定，对每一个自然数 i，我们有 $\not\models_{\mathfrak{A}} \beta(v_i)[s]$。所以 $\not\models_{\mathfrak{A}} \alpha[s]$。

这就完成了引理的归纳证明。 □

推论 7.3.1 (甘岑 1936). *如果 Γ 是自然推演系统的一个定理，则有一个 Γ 的证明树其中没有用到切割规则。*

证明: 假定 $\vdash \Gamma$。根据可靠性定理，$\models \Gamma$。所以如果我们用完全性定理证明中的方法来搜索，结果一定找不到 Γ 的反模型。因此一定得到 Γ 的一个证明树。根据构造，这棵证明树显然没有用到切割规则。 □

习题 7.2.

(1) 证明自然推演系统的可靠性。

(2) 证明自然推演系统的子公式性质：如果 $\vdash \Gamma$，则存在一个证明树，其中出现的公式都是 Γ 的子公式。

第四节　紧致性定理及其应用

定理 7.4.1 (紧致性定理). *(a)* 如果 $\Gamma \models \varphi$，则存在 Γ 的某个有穷子集 Γ_0 使得 $\Gamma_0 \models \varphi$。

(b) 如果 Γ 的每个有穷子集 Γ_0 都是可满足的，则 Γ 也是可满足的。

证明: 见习题 7.3。 □

下面我们看一些紧致性定理的应用。

定理 7.4.2. 假定语言中包含等词。如果一个闭语句集 Σ 有任意大的有穷模型，则它一定有一个无穷模型。

证明: 回忆一下，在第 六 章第 二 节中，对任意整数 $k \geq 2$ 我们都给出了一个闭语句 $\exists_k$ 表达“至少存在 k 个元素”。例如，

$$\begin{aligned} \exists_2 &=_{df} \exists v_1 \exists v_2 \; v_1 \not\approx v_2, \\ \exists_3 &=_{df} \exists v_1 \exists v_2 \exists v_3 \; (v_1 \not\approx v_2 \wedge v_2 \not\approx v_3 \wedge v_1 \not\approx v_3)。 \end{aligned}$$

考察公式集 $\Gamma = \Sigma \cup \{\exists_2, \exists_3, \cdots\}$。根据假定，$\Gamma$ 的任何一个有穷子集都是可满足的。紧致性定理告诉我们，Γ 本身也是可满足的。显然任何满足 Γ 的模型都必须是 Σ 的一个无穷模型。 □

推论 7.4.1. 固定一个有等词的语言 L。L 上的所有有穷结构形成的类不是广义初等类 EC_Δ。所有无穷结构形成的类不是初等类 EC。

注：

1. 定理 7.4.2 和推论 7.4.1 很好地阐明了逻辑学是研究手段的极限的主旨。虽然在数学内所有的有穷结构显然是可以表述的，但如果我们把语言限制在一阶语言上，则我们无法划清有穷与无穷的界限，哪怕我们允许用无穷多条描述。在习题中我们还会看到一些一阶逻辑无法表达的概念，它们多少多有些“有穷对无穷”的影子在里面。

2. 推论 7.4.1 也回答了前面欠下的问题：即所有的无限群不形成一个初等类。

我们再看一个紧致性定理另外一个重要应用，非标准算术模型的存在性，它也回答了前面欠下的另一个问题，即存在初等等价但不同构的模型。

例 7.4.1. *考察 标准 算术模型* $\mathfrak{A} = (\mathbb{N}, 0, S, <, +, \cdot)$。*存在一个可数模型* $\mathfrak{B}$ *与* $\mathfrak{A}$ *初等等价但不同构。*

这样的与 $\mathfrak{A}$ 初等等价但不同构的（可数或不可数）模型称为 非标准算术模型 。

让我们先引入一个后续课程中常用的概念。对任何一个结构 $\mathfrak{A}$，我们称所有在 $\mathfrak{A}$ 中成立的闭语句为 $\mathfrak{A}$ 的理论， 记作 Th $\mathfrak{A}$，即

$$\text{Th } \mathfrak{A} = \{\sigma : \models_{\mathfrak{A}} \sigma\}。$$

下面的简单命题提供给我们一个构造初等等价模型的方法：

引理 7.4.1. 如果（同一个语言上的）结构 $\mathfrak{B}$ 满足 Th $\mathfrak{A}$，则 $\mathfrak{B} \equiv \mathfrak{A}$。

证明: 见习题。 □

回到非标准模型的构造。

证明: 首先扩展语言：添加一个新的常数符号 c。令

$$\Sigma = \{0 < c, S0 < c, SS0 < c, \cdots\}。$$

我们验证任何一个 $\Sigma \cup \text{Th } \mathfrak{A}$ 的有穷子集 Σ_0 都是可满足的：注意到 Σ_0 最多只有有穷条 Σ 中的语句，我们可以找一个充分大的自然数 k，并在标准模型中添上 c 的解释为 k 即可。Th $\mathfrak{A}$ 中的语句不牵扯到 c，因此在标准模型中依然成立。

依照紧致性定理，$\Sigma \cup \text{Th } \mathfrak{A}$ 也有一个模型。完全性定理的证明告诉我们这个模型可以取为可数的。我们所要的模型 $\mathfrak{B}$ 就是该模型在算术语言上的限制。由于 $\mathfrak{B}$ 是 Th $\mathfrak{A}$ 的模型，$\mathfrak{A} \equiv \mathfrak{B}$。剩下验证 $\mathfrak{B}$ 和 $\mathfrak{A}$ 不同构。假定存在一个同构 $h : \mathfrak{B} \to \mathfrak{A}$。令 $m = h(c^{\mathfrak{A}})$。由于 $0 < c, S0 < c, \cdots, \underbrace{SS\cdots S}_{m \text{ 多个}}0 < c$ 在模型 $\mathfrak{B}$ 中成立，因此 h 诱导出一个从 $m+1$ 到 m 的一个单一映射，这与抽屉原则（习题 2.6）矛盾。 □

紧致性定理还有更深刻的应用，例如，林德斯特罗姆[6]利用紧致性定理（和一些其它性质）给出了一个对一阶逻辑的完全刻画。虽然我们这里把紧致性定理当作完全性定理的一个推论，但从某种意义上讲，林德斯特罗姆定理告诉我们，紧致性定理才是一阶逻辑中更根本的特征。

习题 7.3.

(1) 证明紧致性定理。

(2) 证明引理 7.4.1。

[6] 林德斯特罗姆，Per Lindström（1936 - 2009），瑞典逻辑学家，数学家。

(3) 假定闭语句 σ 在 Γ 的所有无穷模型中都成立。证明：存在一个自然数 k 使得 σ 在 Γ 的所有多于 k 个元素的模型中都成立。

(4) 假定语言中有一个二元谓词符号 $<$。令结构 $\mathfrak{A} = (\mathbb{N}, <)$ 为自然数集和其上的通常的序。证明存在一个与 $\mathfrak{A}$ 初等等价的模型 $\mathfrak{B}$ 使得 $<^{\mathfrak{B}}$ 有一个无穷降链，即，存在 $|\mathfrak{B}|$ 中的元素 $a_0, a_1, \cdots$ 使得对任意自然数 i，$(a_{i+1}, a_i) \in <^{\mathfrak{B}}$。[注：本题可以解读成：良序不是一个一阶的概念。]

(5) 考察一阶逻辑可靠性和完全性的下列弱形式：$\vdash \alpha$ 当且仅当 $\models \alpha$。利用紧致性定理，从上述弱形式推导出一阶逻辑可靠性和完全性的一般形式。

第八章　结束语

先总结一下我们做了什么：我们精确定义了一些数理逻辑中的基本概念，如真和可证。并且建立了它们之间如下的联系：$\Gamma \models \sigma$ 当且仅当 $\Gamma \vdash \sigma$。用通俗语言说，如果我们把真解释成放之四海而皆准，那么真的就刚刚好是可证的。从中我们可以领会形式化方法的强大。然而，在将概念精确化之后，紧致性定理马上告诉我们形式化方法的局限。

但紧致性定理揭露的还只是冰山的一角。我们接下来的课程将会证明哥德尔的两个不完全性定理，从而更深刻地揭示了逻辑方法的局限。在不完全性定理的证明中，大家可以更深的体会到把基本概念精确化的必要性。毕竟，只说明真的刚好是可证的并没有什么令人惊奇的地方。我们将会看到：恰恰是揭示了逻辑方法的局限的不完全性定理才充分体现了数理逻辑的真正精髓！

参考文献

[1] Patrick Blackburn, Maarten de Rijke and Yde Venema. *Modal Logic*, Cambridge University Press, 2001.

[2] Chang and Keisler. *Model Theory* (third edition), Elsevier, 1990.

[3] Herbert Enderton. *A Mathematical Introduction to Logic*, 2nd ed. Harcourt, 2001. 有中译本及影印本。

[4] Thomas Jech. *Set Theory*, the third Millennium edition, Springer, 2002.

[5] Kenneth Kunen. *Set Theory*, College Publications, 2011.

[6] Elliott Mendelson. *Introduction to Mathematical Logic*, 5th ed. CRC, 2009.

[7] Wolfram Pohlers. *Proof Theory - The First Step into Impredicativity*, Springer, 2009.

[8] Hartley Rogers, Jr. *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, 1967.

[9] Robert Soare. *Recursively Enumerable Sets and Degrees - A Study of Computable Functions and Computably Generated Sets*, Springer, 1987. 目前正在写第二版，可以通过邮件索取初稿。

[10] Dirk van Dalen. *Logic and Structure*, 4th ed. Springer, 2004.

[11] 邢滔滔. 数理逻辑, 北京大学出版社，2008。

[12] 徐明. 符号逻辑讲义, 武汉大学出版社，2008。

[13] 叶峰. 一阶逻辑与一阶理论, 中国社会科学出版社，1994。

索引