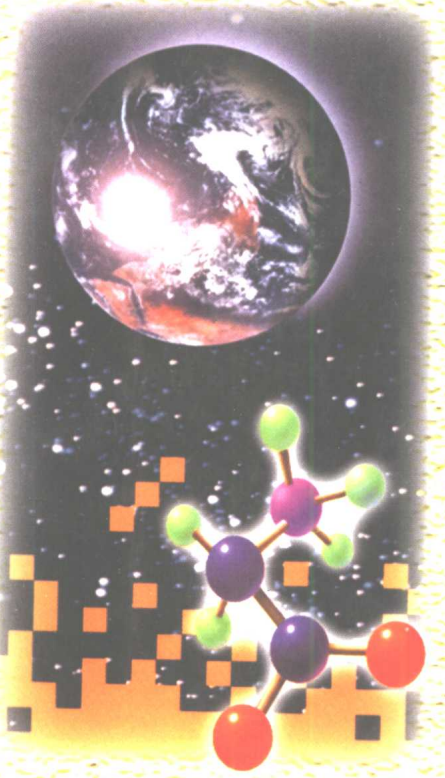


中国科学院研究生教学丛书

Gröbner 基理论及其应用

刘木兰 著

科学出版社

内 容 简 介

本书为《中国科学院研究生教学丛书》之一.

本书共四章. 第一章讲述 Gröbner 基理论和应用所需要的最基本的交换代数知识，在不长的篇幅中融入了多项式理想理论的基本内容. 第二章和第三章讲述 Gröbner 基的基本理论和基本应用. 第四章讲述 Gröbner 基理论对线性递归阵列的应用，这部分内容是本书特有的，它反映了作者和合作者近期有关的研究成果.

本书可作为数学和应用数学专业、计算机科学和信息科学专业、计算机代数和编码、密码学及系统科学专业的研究生和大学本科高年级学生的教学用书，也可作为有关科研人员、工程技术人员的参考书.

图书在版编目（CIP）数据

Gröbner 基理论及其应用/刘木兰著 . - 北京：科学出版社，2000

（中国科学院研究生教学丛书/白春礼主编）

ISBN 7-03-008085-8

Ⅰ.G… Ⅱ.刘… Ⅲ.计算数学-基（数学） Ⅳ.024

中国版本图书馆 CIP 数据核字（1999）第 67941 号

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

科地亚印刷厂印刷

科学出版社发行 各地新华书店经销

*

2000 年 6 月第 一 版 开本：850×1168 1/32

2000 年 6 月第一次印刷 印张：9 5/8

印数：1— 3000 字数：247 000

定价：20.00 元

（如有印装质量问题，我社负责调换〈新欣〉）

《中国科学院研究生教学丛书》序

在21世纪曙光初露，中国科技、教育面临重大改革和蓬勃发展之际，《中国科学院研究生教学丛书》——这套凝聚了中国科学院新老科学家、研究生导师们多年心血的研究生教材面世了，相信这套丛书的出版，会在一定程度上缓解研究生教材不足的困难，对提高研究生教育质量起着积极的推动作用.

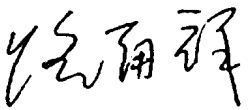
21世纪将是科学技术日新月异，迅猛发展的新世纪，科学技术将成为经济发展的最重要的资源和不竭的动力，成为经济和社会发展的首要推动力量.世界各国之间综合国力的竞争，实质上是科技实力的竞争.而一个国家科技实力的决定因素是它所拥有的科技人才的数量和质量.我国要想在21世纪顺利地实施“科教兴国”和“可持续发展”战略，实现邓小平同志规划的第三步战略目标——把我国建设成中等发达国家，关键在于培养造就一支数量宏大、素质优良、结构合理、有能力参与国际竞争与合作的科技大军.这是摆在我国高等教育面前的一项十分繁重而光荣的战略任务.

中国科学院作为我国自然科学与高新技术的综合研究与发展中心，在建院之初就明确了出成果出人才并举的办院宗旨，长期坚持走科研与教育相结合的道路，发挥了高级科技专家多、科研条件好、科研水平高的优势，结合科研工作，积极培养研究生；在出成果的同时，为国家培养了数以万计的研究生.当前，中国科学院正在按照江泽民同志关于中国科学院要努力建设好“三个基地”的指示，在建设具有国际先进水平的科学研究基地和促进高新技术产业发展基地的同时，加强研究生教育，努力建设好高级人才培养基地，在肩负起发展我国科学技术及促进高新技术产业发展重任的同时，为国家源源不断地培养输送大批高级科技人才.

质量是研究生教育的生命，全面提高研究生培养质量是当前我国研究生教育的首要任务.研究生教材建设是提高研究生培养

质量的一项重要的基础性工作.由于各种原因,目前我国研究生教材的建设滞后于研究生教育的发展.为了改变这种情况,中国科学院组织了一批在科学前沿工作,同时又具有相当教学经验的科学家撰写研究生教材,并以专项资金资助优秀的研究生教材的出版.希望通过数年努力,出版一套面向21世纪科技发展、体现中国科学院特色的高水平的研究生教学丛书.本丛书内容力求具有科学性、系统性和基础性,同时也兼顾前沿性,使阅读者不仅能获得相关学科的比较系统的科学基础知识,也能被引导进入当代科学研究的前沿.这套研究生教学丛书,不仅适合于在校研究生学习使用,也可以作为高校教师和专业研究人员工作和学习的参考书.

"桃李不言,下自成蹊."我相信,通过中国科学院一批科学家的辛勤耕耘,《中国科学院研究生教学丛书》将成为我国研究生教育园地的一丛鲜花,也将似润物春雨,滋养莘莘学子的心田,把他们引向科学的殿堂,不仅为科学院,也为全国研究生教育的发展作出重要贡献.



前　言

熟知，我们可用带余除法求一个整数被另一个非零整数除所得的商和余数，可用辗转相除法求两个整数或多个整数的最大公因子．同样地，对于有理系数多项式或者系数在一般域上的多项式，可用长除法求一个多项式被另一个非零多项式除得到的商多项式和余多项式，用欧几里得算法，即多项式的辗转相除法，求两个或多个多项式的最大公因子．实际上，这两者十分相似．用代数学中环论的观点看，整数全体组成的环和任意域 k 上单变元多项式全体组成的环 $k[x]$ 都是欧几里得环，当然也是主理想环．在这两个环中都有有效的除法算法和基于除法算法的用于求两个或多个元素的最大公因子的欧几里得算法．在主理想整环中，任意给定的 n 个元素 $a_1,a_2,\cdots,a_n$ 的最大公因子 $\gcd(a_1,a_2,\cdots,a_n)$ 就是由 $a_1,a_2,\cdots,a_n$ 这 n 个元素生成的理想 I 的生成元．特别，在整数环 Z 中，$\gcd(a_1,a_2,\cdots,a_n)$ 是由整数 $a_1,a_2,\cdots,a_n$ 生成的理想 I 中绝对值最小的整数；而在域上单变元多项式环 $k[x]$ 中，$\gcd(a_1,a_2,\cdots,a_n)$ 是由多项式 $a_1,a_2,\cdots,a_n$ 生成的理想 I 中的多项式次数最低或最小的多项式．在环 Z 中和环 $k[x]$ 中，要判断一个元素 a 是否属于由 $a_1,a_2,\cdots,a_n$ 生成的理想 I，只要检验 a 是否能被 $\gcd(a_1,a_2,\cdots,a_n)$ 整除，即余数或余项是否为零．如果余数或余项为零，说明 a 能被 $\gcd(a_1,a_2,\cdots,a_n)$ 整除，则 a 属于理想 I；如果余数或余项不为零，说明 a 不能被 $\gcd(a_1,a_2,\cdots,a_n)$ 整除，则 a 不属于理想 I．如果我们不利用 $\gcd(a_1,a_2,\cdots,a_n)$ 或者没有算法可由 $(a_1,a_2,\cdots,a_n)$ 求出 $\gcd(a_1,a_2,\cdots,a_n)$，判断元素 a 是否属于理想 I 就不会这样简单．事实上，$\gcd(a_1,a_2,\cdots,a_n)$ 作为理想 I 的生成元，它不但具有好的性质，而且又有算法保证可具体求出它，这样才使得理想成员的判定问题得以解决．用高

斯消去法解有理系数或系数在一般域上的线性方程组也是大家熟悉的. 高斯消去法的本质就是将原始的线性方程组化成一组等价的容易求解的线性方程组. 从代数学的观点来看，这也是属于从理想的一组生成元出发，设法求出一组具有好的性质的理想的另一组生成元. 这里边有两个问题，一是具有好的性质的理想生成元的代数含意是什么；二是如何求出它. 要解决这两个问题，当然不能只局限于环 Z 和$k[x]$，我们希望对基环为一般的交换环，甚至包括非交换环的多变元多项式环都能解决上述问题. 但是，即使是域上，例如有理数域上的多变元（变元个数≥2）的多项式环，问题变得复杂得多，因为这时的环不再是主理想整环. 关于环中的理想，除了知道它们是有限生成之外，再作进一步的刻画就十分困难. 虽然多项式除法可以形式上进行，但是所得商多项式和余多项式没有唯一性，当然也就更谈不上直接推广欧几里得算法了. 然而在实际中有大量问题都要求我们能够对环中理想有进一步的刻画，不只单纯回答与存在性相关的问题，更重要的是能够具体求解. 例如，我们要有办法判断环中一个元素是否属于给定的理想，在代数编码中码字的判别就属这类问题；如何检验一个理想是否素理想，它的解决可用于判断一个代数簇是否可约；如何计算环中理想的维数及给出理想准素分解的有效算法，因为通常的诺特环中理想准素分解的理论并没有解决如何将一个理想具体分解；如何求解环上，例如整数环 Z 和同余类环Z/mZ上的线性方程组，这是我们常遇到的问题. 此外，在计算机代数、计算代数、计算代数数论、计算代数几何、多维系统理论、代数编码和密码学、乃至整数规划等诸多领域的许多问题，最后都可归结为对系数取自某个环的多项式组成的多项式环中理想的计算. 确切地说，首先需要一个可执行的有效算法，用它找到一组具有良好性质的理想生成元，进而利用这组生成元，使得我们进而能够具有有效的算法解决与理想相关的各种问题. Gröbner 基理论就是为解决这些问题而产生和发展起来的.

Gröbner 基理论的形成，可以说是经历了几十年的时间. 最

早我们可追溯到 1927 年 F.S.Macauly 的工作. 他首先将全序的概念引入到多变元多项式环中单项式全体组成的集合中，他的目的是研究理想的某些不变量. 经历了将近 40 年，H.Hironaka 于 1964 年在研究关于奇性分解（resolution of singularities）时，引进了多变元多项式的除法算法. 在 1965 年，B.Buchberger 使用除法算法系统地研究了域上多变元多项式环的理想生成元问题. 他的基本思想是在单项式的集合中引入保持单项式的乘法运算的全序，称为项序，以保证多项式相除后所得余多项式唯一. 他引进了 S -多项式，使得对多项式环中的任一给定的理想，从它的一组生成元出发，可计算得到一组特殊的生成元，即现在通常称之的 Gröbner 基（这是 Buchberger 用他的导师的名字命名的），在某些文章中也称为 Standard 基，它具有“唯一性”的良好性质. 利用 Gröbner 基，理想成员的判断及许多问题都可得到解决. 因此它一出现，不只受到代数学界人士的重视，而且受到数学界、应用数学界、计算机科学界、系统科学界等许多领域的研究人员的重视，理论方面和应用方面都得到迅速发展. Gröbner 基理论最重要的，或者说 Buchberger 的最大贡献，是在于 Gröbner 基可以计算，可以真正求出来. 此后，H.Grauert 于 1972 年研究了域上形式幂级数环的相应问题. G.Bergman 于 1978 年对结合（非交换）代数和更一般的代数系统研究了 Gröbner 基的形式，再次发现 Buchberger 在交换情形下的算法. 1983 年，D.Lazard 提出了用 Gröbner 基解代数方程组的思想. 1986 年，L.Robbiano 发展了比较抽象的 Gröbner 基理论. Buchberger 在 1985 年的文章“Recent trends in multidimensional system theory”中系统地研究了算法，已成为这个领域必引的文献. 其后，人们将域上多项式环的 Gröbner 基理论先推广到整数环 Z 上的多项式环上，进而推广到主理想整环上的多元多项式环上以及有零因子的基环，如模 m 的整数同余类环 Z/mZ（其中 m 是任一给定的整数）上的多元多项式环. Buchberger 和他的学生还将 Gröbner 基理论公理化. V.Weispfenning 等人研究了非交换代

数的情形.

近十几年来，关于 Gröbner 基的应用研究发展十分迅速，这包括给出切实可行的域上多项式环中理想的准素分解算法，其中零维理想的准素分解的研究比较彻底. 虽然早在 van der Waerden 的 50 年代出版的《代数学》一书中就讲述了理想的准素分解，但那只是理论上可行，并没有具体的算法去实现. Gröbner 基的应用研究还包括代数方程组的求解，多项式的因子分解，多项式在代数扩域和代数函数域中的因子分解，素理想的检验，代数流型的分解，纠错编码中循环码和代数几何码的译码，密码学中多条序列的综合和高维线性递归阵列的分析与综合，多维系统理论等诸多领域. 计算机代数、计算代数、计算代数几何、计算代数数论等都是近些年发展起来的计算机科学与数学的交叉学科分支，而 Gröbner 基在其中占有重要地位. 随着计算机的小型化、大容量、高速度，可以断言，Gröbner 基的应用前景将愈来愈广泛，同时 Gröbner 基理论和算法的研究将会吸引更多的人.

本书可作为计算代数和相关领域的学习和研究用书. 读者对象是数学、应用数学、计算机科学、信息理论、系统科学和编码理论等系或专业的硕士研究生和博士研究生，大学本科高年级学生，及相关领域的研究人员. 本书由 4 章组成. 第一章讲述学习 Gröbner 基理论和应用所需要的代数学中的关于群、环、理想和域的基础知识，特别用一些篇幅讲述多项式的理想论，这些内容基本上保证了本书的自封性的要求. 第二章是本书的核心内容，讲述 Gröbner 基的基本理论，包括除法算法，S -多项式和 Buchberger 算法. 我们先讲述域上的 Gröbner 基的基本概念和算法，指出关键所在，然后将其自然地推广到一般交换环上去，并详细地研究了主理想整环上的 Gröbner 基的标准型. 在这章我们没有像其他书中那样放许多例子，而是侧重分析解决问题的基本思想. 我们希望通过尽可能少的篇幅使读者掌握 Gröbner 基的基本理论. 对算法有兴趣的读者可参阅 [28, 8]. 第三章除了包括 Gröbner 基理论的最典型和最基本的应用，例如理想成员的判

定，理想包含关系和相等与否的判定，多项式同余类环的陪集代表元的计算，理想的交、理想的商和根理想的 Gröbner 基的计算，还包括理想的消元定理和扩张定理，它们主要用于求解代数方程组，以及投射空间的消元与扩张定理，它们具有十分重要的几何意义．此外，我们还介绍了三色问题和整数规划问题，这部分取材于 [1]，讲述它们的目的是使读者体会到，许多问题如果能够转化为与代数方程组相关的问题，Gröbner 基就可能成为解决问题的工具．第四章讲述 Gröbner 基理论对线性递归阵列的应用．这部分内容是本书特有的．众所周知，线性递归序列的研究已有悠久的历史．由于密码学和编码学的应用背景，域上的，特别是有限域上的线性递归序列已有丰硕的研究成果．近些年来，线性递归阵列和 Galois 环上线性递归序列的研究已经颇为活跃．Gröbner 基理论对于研究环上的线性递归序列和阵列提供了一个十分有力的工具．在这章，我们将侧重应用 Gröbner 基的性质和多项式理想论分析线性递归阵列的结构，包括线性递归阵列的迹表示，模结构和循环模的判定等．这章内容是作者与合作者近年的部分研究成果．

在阅读本书时，已具有交换代数基础知识的读者，或者只对 Gröbner 基本身的概念及算法感兴趣的读者可跳过第一章而直接进入第二章．要想了解 Gröbner 基理论的应用，则第三章是必读的．读第三章需要一些交换代数方面的知识．对代数编码和密码学有兴趣的读者，通过第四章可接触到线性递归阵列的较深刻的研究结果，也可进一步体会到 Gröbner 基的应用价值．Gröbner 基理论是处理与多项式有关问题的一个有力工具，掌握 Gröbner 基的基本概念、算法和性质并不困难，除了要进一步研究如何改进已有的算法和发现新的性质之外，问题的关键之一是如何将它用于解决相关问题和用好它，希望本书在这方面能对读者有所启发．

最后，作者在此衷心感谢中国科学院院士吴文俊先生和万哲先先生对作者的鼓励与指导，感谢中国科学技术大学研究生院冯

克勤教授的支持，感谢香港城市大学郝刚教授的帮助和支持．感谢吴新文博士、陈佩忠博士、韩阳博士和吴清泉同学，他们阅读了本书的部分初稿并提出了许多好的意见和建议．由于作者的水平有限，文中定有谬误之处，敬请读者批评和指正．

目　录

第一章　代数学基础

在本章，我们将讲述 Gröbner 基理论和应用所需要的最基本的代数学知识，特别是多项式理想理论. 在前面 3 节中，我们给出群、环和理想的基本定义和性质. 在第 4 节，讲述多项式环，特别是多项式环的唯一因子分解性质. 第 5 节到第 9 节，主要内容是多项式理想理论. 为此，交换代数中的一些最基本的概念，例如，分式环和分式模，理想的扩张和局限，理想的准素分解等都一一讲述. 虽然交换代数（乃至非交换代数）方面的知识对 Gröbner 基理论和应用起着至关重要的作用，但是，我们并没有在这里系统地介绍它们，而只是讲述最基础的、在本书中所必须的、非讲不可的内容，因为我们希望读者尽快地了解和学习 Gröbner 基理论本身.

§1.1　么半群和 Dickson 引理

这节的主要目的是通过对么半群基本概念和性质的讨论给出 Dickson 引理. Dickson 引理是建立 Gröbner 基理论的基石之一，尽管它并不复杂和深奥.

定义 1.1.1（半群、么半群）　一个**半群**(semigroup) 是指一个非空集合 M 和 M 上满足结合律的二元运算“$\cdot$”，记为$(M, \cdot)$，即 $M \neq \varnothing$，对任何 $a, b \in M$，有 $a \cdot b \in M$，为简单起见记 $a \cdot b = ab$，并对任何 $a, b, c \in M$，有 $a(bc) = (ab)c$. M 中的一个元素 e 称为**么元素**或**单位元**(unit)，如果对任何 $a \in M$，都有 $ea = ae = a$. 如果半群 M 含有么元素，则称 M 为**么半群**(monoid). 如果对任何 $a, b \in M$，都有 $ab = ba$，则称 M 为交换半群. 对交换半群，二元运算常用“+”表示，即用 $a + b$ 代替 $a \cdot b (= ab)$. 如果对任何 $a, b, c \in M$ 和 $ab = ac$，可推出 $b = c$，则称 M 为满足消去律的半

群.

例 1.1.1 正偶数全体,在通常的数的加法运算之下成一半群,但不是么半群.而正偶数全体再添加数 0,就成为么半群,0 就是么元素.

例 1.1.2 令 $\mathbb{N}$ 表示非负整数全体组成的集合,和 $\mathbb{N}^n = \underbrace{\mathbb{N}\times\cdots\times\mathbb{N}}_{n} = \{(a_1,\cdots,a_n) \mid \forall\, i, a_i \in \mathbb{N}\}$ 为 $\mathbb{N}$ 的笛卡尔积.

$\mathbb{N}^n$ 中的二元运算用分量定义,即 $(a_1,\cdots,a_n)+(b_1,\cdots,b_n) = (a_1 + b_1,\cdots,a_n + b_n)$. 于是 $\mathbb{N}^n$ 是以 $(0,\cdots,0)$ 为么元素的交换么半群.

习题 1.1.1 证明:如果 M 是么半群,则么元素是唯一的.

定义 1.1.2(么半群理想) 令 M 是交换么半群. M 的子集 I 称为**么半群理想**(monoideal),简称为理想,如果 $I \cdot M \subseteq I$(或 $I + M \subseteq I$). 如果 $E \subseteq M$ 是 M 的子集,则 $I(E) = \langle E\rangle$ 表示由 E 生成的 M 中的理想.实际上,$I(E) = \{a \cdot m \mid \forall\, a \in E, m \in M\}$. 如果 E 是 M 中的有限子集,则称 $I(E)$ 是有限生成的.

例 1.1.3 设 M 是所有自然数的集合,M 上的二元运算由通常的数乘给出.设 I 是所有偶数的集合.则 I 是交换么半群 M 中的理想,而且 I 是由 2 生成,即 $I(\{2\}) = I$.

习题 1.1.2 证明:设 M 是交换么半群,则 M 中任何二个理想的并仍是 M 中的一个理想.

定义 1.1.3 设 M 为任意给定的一个交换么半群.那么 M 中序列 $\{a_n\}_{n\in\mathbb{N}}$ 称为**有限型**(finite type)是指存在一个数 $N \in \mathbb{N}$,其中 $\mathbb{N}$ 是非负整数集合,使得 $I(\{a_n\}_{n\in\mathbb{N}}) = I(\{a_0,a_1,\cdots,a_N\})$,即由集合 $\{a_0,a_1,\cdots\} = \{a_n\}_{n\in\mathbb{N}}$ 在 M 中生成的理想等于有限集合 $\{a_0,a_1,\cdots,a_N\}$ 在 M 中生成的理想.

定义 1.1.4 设 $\{I_\lambda\}_{\lambda\in\Lambda}$ 是交换么半群 M 中的理想的集合,其中 Λ 是指标集.那么 $\{I_\lambda\}_{\lambda\in\Lambda}$ 称为理想链,是指对任何 $\lambda,\lambda' \in \Lambda$,都有包含关系 $I_\lambda \subseteq I_{\lambda'}$ 或者 $I_\lambda \supseteq I_{\lambda'}$(这里的包含关系是指集合的包含关系). 理想链 $\{I_\lambda\}_{\lambda\in\Lambda}$ 称为**平稳的**(stationary),是指存在

$\lambda_0 \in \Lambda$,使得对任何 $\lambda \in \Lambda$, $I_\lambda \supseteq I_{\lambda_0}$,都有 $I_{\lambda_0} = I_\lambda$. 特别地,可数理想升链是指满足下面条件的理想链

$$\{I_\lambda\}_{\lambda \in \Lambda}, I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots.$$

定理 1.1.1 设 M 是交换么半群. 则下列叙述是等价的:

(1) M 中的每个理想链都是平稳的;

(2) M 中的每个可数理想升链都是平稳的;

(3) M 中的每个非空的理想的集合有极大元;

(4) M 中的每个序列都是有限型;

(5) M 中的每个序列都包含一个有限型子序列;

(6) M 中的每个理想都是有限生成的.

证明 (1)⇒(2). 显然.

(2)⇒(3). 设 S 为 M 中的非空的理想集合. 如果 S 中没有极大元,则我们可得到 S 中的无限长的理想严格升链

$$I_1 \subsetneq I_2 \subsetneq I_3 \cdots.$$

这与(2) 中的假设条件矛盾,因此 S 中必有极大元,(3) 成立.

(3)⇒(4). 设 $\{a_n\}_{n \in N}$ 是 M 中的一个任意给定的序列. 考虑下面的理想链

$$\langle a_0 \rangle \subseteq \langle a_0, a_1 \rangle \subseteq \langle a_0, a_1, a_2 \rangle \subseteq \cdots,$$

其中 $\langle a_0, a_1, \cdots, a_{i-1} \rangle$ 表示由集合 $\{a_0, a_1, \cdots, a_{i-1}\}$ 生成的理想. 在链中出现的理想全体构成一个非空理想集合 S. 根据(3), S 含有一个极大元,设为 $\langle a_0, a_1, \cdots, a_N \rangle$. 于是 $I(\{a_0, a_1, \cdots, a_N\}) = I(\{a_n\}_{n \in N})$,即 $\{a_n\}_{n \in N}$ 是有限型,(4) 成立.

(4)⇒(5). 显然.

(5)⇒(6). 设 I 是 M 中的一个任意给定的理想. 如果 $I = \{0\}$,其中 0 是 M 的么元素,则(6) 成立. 故我们可设 $I \neq \{0\}$. 如果 I 不是有限生成的,则在 I 中有序列 $\{a_n\}_{n \in N}$,其中 $a_0 \neq 0$,

$$\langle a_0 \rangle \subsetneq \langle a_0, a_1 \rangle \subsetneq \langle a_0, a_1, a_2 \rangle \subsetneq \cdots.$$

显然,这个序列的任何子序列都不是有限型,这与(5) 矛盾,因此 I 是有限生成的,(6) 成立.

(6)⇒(1). 设$\{I_\lambda\}_{\lambda\in\Lambda}$,其中$\Lambda$是指标集,是$M$中的理想链,和令$I=\bigcup_{\lambda\in\Lambda}I_\lambda$. 由习题1.1.1,$I$是$M$中的理想. 根据条件(6),$I$是有限生成的. 因此存在有限个元素$a_1,a_2,\cdots,a_N\in I$,使得

$$I=\langle a_1,a_2,\cdots,a_N\rangle.$$

设$a_i\in I_{\lambda_i}$. 于是$I=\bigcup_{i=1}^{N}I_{\lambda_i}$. 因此,由于$\{I_\lambda\}_{\lambda\in\Lambda}$是理想链,故存在$\lambda_0\in\Lambda$,使得$\bigcup_{i=1}^{N}I_{\lambda_i}=I_{\lambda_0}$,即$I=I_{\lambda_0}$,理想链$\{I_\lambda\}_{\lambda\in\Lambda}$在$\lambda_0$处达到稳定. 确切地说,即对任何$\lambda'\in\Lambda$,如果$I_{\lambda'}\supseteq I_{\lambda_0}$,则$I_{\lambda'}=I_{\lambda_0}$,(1)成立.

定义 1.1.5(诺特么半群)　交换么半群M称为**诺特的**(Noetherian),如果M满足定理1.1.1中的任何一个等价条件.

命题1.1.1　设$\mathbb{N}$是非负整数集合,n是一给定的正整数,则例1.1.2给出的交换么半群$\mathbb{N}^n$是诺特的.

证明　对n施归纳法来证明命题. 设$n=1$,和I是$\mathbb{N}$中的任意给定的一个理想. 由于$\mathbb{N}$是良序集,因此$\mathbb{N}$中任一非空集合都有最小元. 设a_1是集合I中的最小元,则$I=\langle a_1\rangle=\{a_1+a\mid a\in\mathbb{N}\}$,命题成立.

设$n>1$和命题对$\mathbb{N}^{n-1}$成立. 下面证明命题对$\mathbb{N}^n$成立. 首先注意,对于任何$v=(a_1,a_2,\cdots,a_n)\in\mathbb{N}^n$,令$v^{(0)}=(a_2,\cdots,a_n)\in\mathbb{N}^{n-1}$,则$v$可表示$v=(a_1,v^{(0)})$. 设$\{v_m\}_{m\in\mathbb{N}}$是$\mathbb{N}^n$中任意给定的一个序列,其中$v_m=(a_{m1},a_{m2},\cdots,a_{mn})=(a_{m1},v_m^{(0)})$,$v_m^{(0)}=(a_{m2},\cdots,a_{mn})$. 考虑序列$\{v_m\}_{m\in\mathbb{N}}$中的每个$n$维向量元的第一分量构成的$\mathbb{N}$中的序列$\{a_{m1}\}_{m\in\mathbb{N}}$,根据对$n=1$情形的证明和定理1.1.1,存在$a_{m_1 1}$,使得$I(\{a_{m_1 1}\})=I(\{a_{m1}\}_{m\in\mathbb{N}})$. 对于序列$\{v_m\}_{m>m_1}$,考虑它的每个$n$维向量元的第一分量构成的序列,它有最小元$a_{m_2 1}$,并且$a_{m_2 1}=a_{m_1 1}+b_1$. 将此过程继续下去,可由开始的序列$\{v_m\}_{m\in\mathbb{N}}$中抽出子序列

$$\{v_{m_1},v_{m_2},\cdots\},$$