Gröbner基与环上线性递归阵列

Gröbner Bases and Linear Recurring Arrays over Rings

陆佩忠

高等教育出版社
HIGHER EDUCATION PRESS

Gröbner 基与环上线性递归阵列

Gröbner Bases and Linear Recurring Arrays over Rings

陆佩忠

高等教育出版社
HIGHER EDUCATION PRESS

内容提要

本书用交换代数、同调代数和 Gröbner 基建立交换环(特别是 QP 环)上的线性递归阵列的理论,并将该理论应用到纠错编码、信号分析和密码分析等相关的信息技术领域中.本书给出多项式理想 I 的阵列零化模 $\mathrm{Zer}_M(I)$ 与 $\mathrm{Hom}_R(R[X]/I,R)$ 之间的基本对偶定理,从而构造出 $\mathrm{Zer}_M(I)$ 的生成元集.由此进一步确定函子 Zer_M 与函子 $\mathrm{Ann}_{R[X]}$ 构成互逆的 Galois 对应的充分必要条件,从而得到了 QF 环 R 上多项式环 $R[X]$ 中任意理想的阵列模形式的零点定理.该定理的形式和功效都类似于 Hilbert Nullstellensatz 定理,因而该定理在 LRA 理论研究中是基本的和紧要的.本书给出 I 恰是域 F 上的一个 LRA 的特征理想的简明的判别公式,并将该公式逐步推广到 QF 环上.从而解决了 Nechaev 提出的公开难题,并揭示了 QF 环上高维循环码的结构.本书还论述了 Gröbner 基在代数编码,特别是循环码和代数几何的译码等领域内的重要应用,并由此清晰地揭示了有限 LRS 的齐次特征理想的极小 Gröbner 基中的每个元素与 Berlekamp-Massey 的序列综合算法中的每一步之间的精密联系,还揭示了环上高维循环码的循环模结构.

图书在版编目(CIP)数据

Gröbner基与环上线性递归阵列/陆佩忠.—北京:
高等教育出版社,2002.10

ISBN 7-04-011250-7

Ⅰ.G... Ⅱ.陆... Ⅲ.密码-理论-研究生-教材
Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2002)第 057428 号

Gröbner 基与环上线性递归阵列
陆佩忠

出版发行	高等教育出版社	购书热线	010-64054588
社　　址	北京市东城区沙滩后街 55 号	免费咨询	800-810-0598
邮政编码	100009	网　　址	http://www.hep.edu.cn
传　　真	010-64014048		http://www.hep.com.cn
经　　销	新华书店北京发行所		
印　　刷	北京中科印刷有限公司		
开　　本	787×960　1/16		
印　　张	14.75	版　　次	2002 年 10 月第 1 版
字　　数	270 000	印　　次	2002 年 10 月第 1 次印刷
插　　页	1	定　　价	23.80 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换.

作 者 简 介

陆佩忠，男，1961 年 3 月出生于上海。1982 年 7 月毕业于解放军信息工程大学应用数学系，获学士学位，并于 1987 年 7 月在该校获得硕士学位。1995 年 9 月进入中国科学院系统科学研究所攻读博士学位，师从刘木兰研究员。1998 年 7 月获得理学博士学位。现任复旦大学计算机科学与工程系教授，博士导师。主要研究方向为算法代数、代数编码、信息安全和图像处理。目前已在国内外杂志及国际会议上发表论文 40 余篇。曾先后两次获得“全军科技进步二等奖”，获首届“中国科学院刘永龄奖金”、“中国科学院院长奖学金优秀奖”和“全国首届优秀博士论文奖”等奖励。

通信地址：上海复旦大学计算机科学与工程系（邮政编码：200433）

电　　话：021-65642830(O)

E-mail：pzlu@fudan.edu.cn

导 师 简 介

刘木兰，女，1941 年 10 月出生于北京。1964 年毕业于中国科技大学数学系。自 1964 年至今先后在中国科学院数学研究所和系统科学研究所工作，历任助理研究员、副研究员和研究员。1993 年被国务院学位委员会批准为博士导师。1998 年被聘为中国科学院数学与系统科学研究院创新基地研究员。

1979—1981 年在美国哥伦比亚大学作访问学者，之后作为访问教授，曾先后访问过美国 Pennsylvania 州立大学、荷兰 Eindhoven 理工大学、挪威 Oslo 大学、意大利 Catania 大学、德国 Bielefeld 大学、日本 Electro-Communication 大学以及香港大学和澳门大学等。

研究工作领域涉及矩阵几何、代数 K-理论、密码学、计算机代数和信息安全。现在的主要研究方向是信息安全的数学理论和计算机代数。在国内外重要学术刊物上，包括 Journal of Pure and Applied Algebra、IEEE on IT、Journal of Symbolic Computation、Discrete Mathematics 以及《中国科学》、《数学学报》等刊物上，发表学术论文近 70 篇，出版专著 3 本。曾获“中国科学院科技进步一等奖”和“中国科学院优秀研究生导师奖”。

前　言

本书的材料主要是以作者的博士论文为基础，并选取了作者近十年来在代数编码领域内所取得的一系列成果，同时也参考了近年来国际上学术界产生的与本书的研究课题相近的一些重要有趣的成果.

本书用交换代数、同调代数和 Gröbner 基建立 Galois 环、QF 环和一般交换环上的线性递归阵列理论，并将该理论应用到信息科学中的几个关键问题的研究中去，特别是解决信号处理、密码、代数几何译码和系统控制论等多领域交叉学科中的一系列问题.

本书共分十二章. 第一章是线性递归阵列理论的研究状况综述. 第二章介绍了在本书中需要使用的一些交换代数与计算代数基础知识，其中包括 Noether 环、Hilbert 基定理、Noether 正规化引理、Hilbert 零点定理、局部化方法、理想的准素分解和 Gröbner 基理论等. 第三章给出域上线性递归阵列特征理想的公式刻画，并给出零维理想的根理想的计算算法. 第四章讨论 Artin 局部主理想环上的多项式理想的 Gröbner 基的标准型，并由此给出理想的准素分解的算法和根理想的计算算法. 第五章解决 Nechaev 问题，即给出了 Artin 局部主理想环上的线性递归序列的特征理想的公式刻画. 第六章给出 Gröbner 基的一个局部性质，并用局部化方法刻画了惟一析因整环上线性递归序列的特征理想. 第七章讨论一般有单位元的交换环 R 上多项式理想 I 的零化阵列模 $\mathrm{Zer}_n(I)$ 与 $\mathrm{Hom}_R(R[X]/I, R)$ 的基本对偶同构关系，并由此给出 $\mathrm{Zer}_n(I)$ 的生成元的构造方法和阵列的广义迹表示. 第八章论述序列的综合算法，用齐次关键方程刻画序列综合问题，并揭示序列的齐次特征理想的极小 Gröbner 基中的每个元素与 Belerkamp-Massey 算法中的每一步之间的精确联系. 第九章介绍代数编码的基本概念和性质. 第十章论述 Gröbner 基在循环码的译码和代数几何码的译码中的应用. 第十一章建立 QF 环上阵列与多项式理想之间的零点定理. 该定理的形式和功效都类似于 Hilbert Nullstellensatz 定理，因而该定理在线性递归阵列理论的研究中是基本的和紧要的. 我们还给出 QF 环上多项式理想恰是一个线性递归阵列

的特征理想的判别公式.第十二章论述环上循环码的结构,并用阵列零点定理和阵列特征理想的判别公式揭示出高维循环码的循环模结构.

本书能基本反映代数编码领域的学术新趋向.因此,本书可作为高等学校数学系、计算机系、通信与电子工程系等专业高年级本科生的教材或参考书,也可供信息工程领域内科研人员作为继续教育的参考书.

衷心感谢导师刘木兰教授将我引入环上线性递归阵列理论的研究领域.在研究过程中,她以深刻的洞察力,渊博的学识和诲人不倦的精神对我进行悉心的指导,特别是她严谨的治学作风,言传身教,将使我终身受益和难忘.

作 者

2002 年 3 月

目　录

第1章
线性递归阵列理论的研究概况

本章要点

环上的阵列的理论极有应用前景.然而,该理论现有的结果还不多.线性递归阵列的理论研究的重要方向应该由一维序列向高维阵列延伸,由有限域向一般的交换环(特别是有零因子的环)扩展,由零维理想向一般高维理想深入.由此而产生了大量富有挑战性的问题.要解决这些问题就必须探索新方法、新工具.笔者的工作表明,交换代数中的局部化方法、同调代数方法和 Gröbner 基理论这三大工具,在研究环上阵列问题中,将起到主导作用.而这些工具在传统的线性递归序列研究中很少使用.

1.1 背景和历史

线性递归序列(简称 LRS)的研究历史可以追溯到中世纪的 Fibonacci 序列.在几个世纪中,各个不同时期的著名数学家都先后研究过 LRS.正如 A. V. Mikhavev 和 A. A. Nechaev(1996)最近在一篇综述文章(参考文献[99])中指出的那样,D. Bernulli、L. Euler、E. Lucas、Chebyshev、Markov 等奠定了序列理论的基础.进入本世纪后,F. S. Macaulay(1916)(参考文献[93])、E. Dickson(1919)(参考文献[17])、M. Ward(1938)(参考文献[134][135])和 M. Hall(1938)(参考文献[35])等把域上序列和代数理想对应起来研究,得到更系统和深刻的结果.在 20 世纪 30 年代,M. Ward(参考文献[134])和 M. Hall(参考文献[35])开始研究剩余类环 Z_m 上的 LRS 序列.D. H. Lehmer(参考文献[63])

(1934)运用 LRS 生成伪随机数,为 LRS 开辟了新的应用领域.由于通信和计算机发展的强有力的推动,LRS 的研究进入了蓬勃发展的成长期.在通信中,利用 LRS,解决抗电磁干扰,解决同步问题,解决相位模糊问题,等等.移位寄存器序列在电子、通信等领域是基础性的理论.S. W. Golomb(参考文献[33])(1955)研究了序列的伪随机性.Golomb(1967)(参考文献[34])系统地研究了移位寄存器序列,其中,线性递归序列是重要的内容,在 20 世纪末和进入 21 世纪后,伪随机序列在通信和信息科学等领域中的应用范围更加广阔.在 CDMA 个人移动通信中,由于巧妙而深刻地使用了伪随机序列和相应的复合序列,使得话音、图像等多媒体信息能够在信号强度极其微弱的信道上实现高速、高容量的传输,使得普通大众能够随时随地与任何人建立方便的联系.

LRS 在密码学中有更大的用武之地.在保密通信中,减少连"0"码(或连"1"码)以保证位定时恢复的质量,改善帧同步和自适应均衡等子系统的性能,这是数字基带信号传输中一个十分基本而重要的问题.为此,将二进制数字源信息先作"随机化"处理,即扰码技术.最常用的扰码器实际上是一个 m 序列伪随机码发生器.通过多个 m 序列的非线性组合实现流密码体制的设计(参考文献[121]),这样不但工程上容易实现,而且可以较好地控制线性复杂性.有关研究可以参见参考文献[77][80].m 序列就是极大周期的 LRS 序列.m 序列有优美的代数组合性质和相关性质,因而被巧妙地应用于测距测向、雷达、声纳、GPS 定位系统等领域.

与 LRS 比较而言,线性递归阵列(简称 LRA)的研究历史开始于近代.近年来,LRA 的理论在通信和图像加密等方面的应用得到数学、计算机和通信等领域内的研究人员的重视.Nomura 等(1972)(参考文献[107])和 McWilliams 及 Sloane(1976)(参考文献[98])研究了有限域上极大周期的线性递归 m - 阵列或伪随机阵列,这样的阵列所对应的特征理想是极大理想.Sakata(1978)(参考文献[122])较系统地研究了有限域上 LRA 的一般理论,即多项式理想 I 所对应的零化阵列模 $\mathrm{Zer}_M(I)$ 的代数性质.尤其是研究了双周期阵列的性质.

LRA 在代数编码中有重要的应用.笔者(1992[78],1993[79],[80],[82])将 LRA 的综合应用于代数几何码的译码.冯贵良(G. L,Feng,1994[27])将多条 LRS 序列的综合算法巧妙地应用于代数几何码的译码,使其纠错能力达到理论码限,得到编码学界的高度评价.LRA 在离散时间系统理论、自动控制论等领域也有广泛的使用(参考文献[138],[139],[140]).例如,对行为(behavior)的精确建模(参考文献[50]).在数字信号处理研究领域中,一个重要的课题是要研究高维线性非移变系统(参考文献[113]),它化为研究线性递归阵列(LRA)与常系数差分方程的解空间之间的对应关系.因而,研究 LRA 与求解常系数偏微分方程也有一定的参考价值.

Sakata 在有限阵列的综合等方面做了很好的工作.他给出了求给定有限阵列的极小递归关系的 BMS 算法(参考文献[124],1989;参考文献[125],1991).他还把他的算法推广到对 $Z/(m)$环上的 LRA 的综合.此算法已经应用于代数几何码的快速译码.Cerlienco 等(1991,参考文献[13])也研究了零维理想与阵列的代数联系,最近,Mulan Liu、L. Hu 和 D. Lin 等对有限域上的 LRA 做了大量的研究(参考文献[65],[66],[67],[68],[69]).特别是 Mulan Liu 和 Lei Hu 在参考文献[68]和[69]中开始利用 Gröbner 基理论研究 LRA 阵列的结构性质,取得了本质性的进展.Mulan Liu、Lei Hu(参考文献[68])给出了阵列的迹表示,而且这种迹表示突破了对特征理想 I 无重根的条件限制.从而为深入研究阵列的代数性质和组合性质提供了有力的工具.

到目前为止,有关 LRA 的研究基本上都是在特征理想 I 是 $R[X]$的**零维**理想的条件下进行的.惟一例外的是 Macaulay(1916)(参考文献[93])的部分结果适合 R 是**域**且 I 是 $R[X]$的一般的理想的情形.这是值得特别提出的工作.他实际上研究了域上线性递归阵列与代数理想的紧密联系.尽管他的工作完成在 Noether 建立代数理想理论之前,但是 M. S. Macaulay 的工作是极有深度的,包含了丰富的创新性,即使到了现在仍不失其魅力(参考文献[93]).F. S. Macaulay 是基于纯理论上的需求而研究 LRA 的,由于对环 R 上的 LRA 的研究,导致了 Cohn-Macaulay 环的概念的诞生,而 Cohn-Macaulay 环是环论、代数几何等领域的重要研究对象.

需要指出,**零维理想所对应的零化阵列模与一般高维理想所对应的零化阵列模之间存在本质性的差异**.这种情形类似于代数几何中的代数簇.零维理想对应的代数簇是有限个点,而一维理想对应的代数簇是代数曲线.其中的差异是很大的.当 $R=F$ 是域,I 是一维或高维理想时,研究 I 所对应的 LRA 阵列模 $\mathrm{Zer}_M(I)$的有关性质的难度远远大于 I 是零维理想时的情形.虽然 Macaulay[93]的部分结果的提法是针对一般的理想 I,但他给出的证明只适合 I 是零维理想时的情形.实际上,Macaulay 的两个针对一般理想的重要定理中,他只证明了零维理想时的情形,其中一个定理(参考文献[93],§60,p69)在一般情形下也是正确的,对此,我们要给出完整的证明,且进一步推广到一般 QF 环上.而 Macaulay 的另一个定理(参考文献[93],§82,p91)在一般情况下是错的.尽管如此,Macaulay 提出的一些独特的方法(如 dialytic 方法)是很值得人们注意的.实际上,在本书中要论述一些新结果.在得到这些新结果的研究过程中,受益于 Macaulay 的启发,有关情况本书还要进一步论述.总而言之,当 I 是高维理想时,对 $\mathrm{Zer}_M(I)$的研究基本上还是一个空白,而本书要论述笔者和同事在这方面取得的一系列有本质性进展的成果,特别是建立了刻画理想与有限生成线性递归阵列 $R[X]$-模之间对应关系的强零点定理.

LRA 的理论研究不但历史悠久，而且充满活力，研究领域不断扩展，方法不断创新，应用前景日益广阔. 现在，就笔者对 LRA 的最新研究进展作扼要的论述.

1.2 基本概念和符号

在本书中 R 始终表示一个 Noether 交换环，$\mathbb{N}$ 是正整数集. $R[X]=R[x_1,x_2,\cdots,x_n]$是 R 上 n 个未定元的多项式环，$R[x]$是 R 上单变元多项式环. 设 M 是$R[X]$－模. I 是$R[X]$的理想，S 是 M 的子集. 定义

$$\mathrm{Zer}_M(I)=\{a\in M\mid r\cdot a=0,r\in I\} \tag{1}$$

$$\mathrm{Ann}_{R[X]}(S)=\{r\in R[X]\mid r\cdot s=0,s\in S\} \tag{2}$$

显然，$\mathrm{Zer}_M(I)$是 M 的子模，$\mathrm{Ann}_{R[X]}(S)$是 $R[X]$的理想.

环 R 上的一个 n－维阵列，α 是指一个无穷矩阵 $\alpha=(a_i)_{i\in\mathbb{N}^n}$，$a_i\in R$. 设 $s=(s_1,s_2,\cdots,s_n)\in\mathbb{N}^n$，一个作用于阵列 α 上的 s－移位算子定义为 $X^s\alpha$，使得

$$X^s\alpha=(b_i)_{i\in\mathbb{N}^n}$$

其中，$b_i=a_{i+s}$，$i\in\mathbb{N}^n$. 对任意 $f(X)=\sum_i f_iX^i\in R[X]$，$f_i\in R$，定义

$$f(X)\cdot\alpha=\sum_i f_i(X^i\alpha)$$

其中，$X^i\alpha$ 是指 i－移位算子 X^i 作用在 α 上.

设 M 是 R 上全体 n－维阵列构成的集合，即

$$M=\{\alpha=(a_i)_{i\in\mathbb{N}^n}\mid a_i\in R,i\in\mathbb{N}^n\} \tag{3}$$

显然式(3)中定义的集合 M 是一个$R[X]$－模. 称一个阵列 $\alpha\in M$ 是一个线性递归阵列(简记 LRA)，如果存在 $R[X]$中的非零多项式 $0\neq f(X)=\sum_i f_iX^i$，$f_i\in R$，使得

$$f(X)\cdot\alpha=0$$

当 I 是 $R[X]$的理想，S 是 M 的子集，在上下文明确时，简记 $\mathrm{Zer}(I)=\mathrm{Zer}_M(I)$，$\mathrm{Ann}(S)=\mathrm{Ann}_{R[X]}(S)$.

称 $R[X]$的理想 I 是零维的，如果 $R[X]/I$ 是一个有限生成R－模. 因此，I 是零维理想当且仅当 I 中包含 n 个首一单变元多项式 $f_1(x_1),f_2(x_2),\cdots,f_n(x_n)$. 零维理想在参考文献[99][101]中称之为首一(monic)理想. 交换环 R 可称为 Quasi-Frobenius(简记 QF)环，如果对 R 中的每一个理想 I，均满足如下性质

$$\mathrm{Ann}_R(\mathrm{Ann}_R(I))=I$$

常见的 QF 环的例子有：域，Artin 局部主理想环，Galois 环，特别是剩余类环 $Z/(m)$.

下面重点介绍 LRA 理论研究领域中所面临的一些重要课题和最新研究概况.

1.3 阵列形式的零点定理

1.3.1 从多项式到阵列

设 R 是一个 QF 环，I 是 $R[X]$的任意一个理想. 下述 3 个问题是非常重要的. 在此借鉴代数几何中 Hilbert Nullstellensatz 定理的含义，把它们总称为阵列形式的零点问题.

问题 A(弱零点问题)：若 I 是 $R[X]$的理想，且 $I\neq R[X]$，则是否存在一个非全零阵列 $\mu\in M$，使得 $\mu\in \mathrm{Zer}_M(I)$?

问题 B(零点问题)：下述恒等式是否成立?

$$I=\mathrm{Ann}_{R[X]}(\mathrm{Zer}_M(I)) \tag{4}$$

当 R 是**域**，I 是**零维**理想时，在 §3 中(命题 3.2)，利用公式(6)，不难证明公式(4)，即解决了问题 B，从而也就容易导出问题 A 的解决. 但要特别强调的是，在原问题中，理想 I 是**任意**理想. 应该指出，**欲把 I 是零维理想时，其对应的阵列模 $\mathrm{Zer}_M(I)$的有关性质推广到 I 是非零维理想时的情形，将会遇到很多困难**.

F. S. Macaulay 在他的不朽名著([93]，§57～§93)中着力研究逆系(Inverse Systems)问题. 逆系问题与问题 A、B 是密切相关的. Macaulay 由此而独创的概念、思想和方法在交换代数的研究史上占有重要地位. 该书中的许多问题仍是当今深受重视的研究课题(Macaulay(1916)(参考文献[120]，xv，xvi，xxiv). 在证明式(4)时，Macaulay 采用了 dialytic arrays 方法. 然而，据本书稍后章节中有关内容的分析，笔者认为 Macaulay 的 dialytic arrays 方法只适合于理想 I 是零维时的情形. D. G. Northcott(1974)(参考文献[108])给出了公式(4)的完全证明. Northcott 是知道 Macaulay 公式的，但他没有解释为什么还要给出新的证明，Northcott 的证明需用到代数扩域、代数封闭域和局部化等性质，依赖于 R 是域的条件，故他的方法难以推广到 R 是 QF 环时的情形.

阵列形式零点问题是本书研究的重点之一. 本书还要考虑如下更深刻的问题.

问题 C(强零点问题)：设 R 是 QF 环，给定一个多项式理想 $I\subset R[X]$. 是否存在一个由有限个 LRA 阵列生成的 $R[X]$－子模 $M\subset M$，使得 $I=\mathrm{Ann}_{R[X]}(M)$?

当 $R=F$ 是域时，问题C是多维线性系统理论中的一个重要研究课题.这个问题实质上是问能否用有限个行为(behavior)数据确定整个系统.这也是系统识别理论中的一个核心问题，所以深受系统论、控制论等领域有关研究人员的重视.J. C. Willems(1986)(参考文献[138],[139],[140])对这个问题有系统的研究，但离解决问题还差很远.C. Heij(1992)(参考文献[38])得到了一些进展，但也未解决此问题.这个问题直到最近才由 S. Zampieri(1997)(参考文献[142])对 $\mathbb{F}[X]=\mathbb{F}[x_1,x_2]$ 时给出了肯定的解答.

对于问题C，如果只要求 M 是 $R[X]$ - 模时，则答案是肯定的.实际上 Macaulay 就给出了解答.然而，笔者发现 Macaulay(参考文献[93]，§82，p91)有个论断：

对 $R[X]$ 的任意理想 I，$\mathrm{Zer}_M(I)$ 一定是有限生成 $R[X]$ - 模.

如果利用 Macaulay 的这个论断，再利用 Macaulay 的另一个定理：

$$I=\mathrm{Ann}_{R[X]}(\mathrm{Zer}_M(I))$$

则问题C似乎可以轻松地解决.然而，经过细致地分析，我们发现 Macaulay 的这个论断是不对的，他给出的证明只有当 I 是零维理想时才通得过.那么，要使 Macaulay 的论断成立，是否一定要加上 I 是零维理想这个条件？这不是一个简单的问题.然而，本书将解决这个问题.

关于零点问题，我们得到如下结果.

定理A(弱零点定理)：设 R 是QF环，I 是 $R[X]$ 的任意一个理想.则 $\mathrm{Zer}(I)\neq 0$ 当且仅当 $I\neq R[X]$.

定理B(零点定理)：设 R 是QF环，I 是 $R[X]$ 的任意一个理想.则

$$I=\mathrm{Ann}_{R[X]}(\mathrm{Zer}_M(I))$$

定理C(强零点定理)：设 R 是QF环，I 是 $R[X]$ 的任意一个理想.则存在一个有限生成的 M 的 $R[X]$ - 子模 M，使得 $I=\mathrm{Ann}_{R[X]}(M)$.

为了解决上述问题，本书采用了同调代数中一些基本方法和 Matlis 理论，该理论通过不可约内射模，建立了 Artin 模范畴与 Noether 模范畴之间的对应关系.Hilbert Nullstellensatz 定理在代数几何等领域中是非常基本和重要的定理.在计算机代数、Gröbner 基理论、几何定理的自动证明等近代蓬勃发展起来的理论中，其基本原理很大程度上要依赖于 Hilbert Nullstellensatz 定理.本书要建立代数理想与线性递归阵列之间的对应关系.类似于代数簇与理想的对应关系的 Hilbert Nullstellensatz 定理，也要建立理想 I 与其零化阵列模 $\mathrm{Zer}_M(I)$ 之间的零点定理，这是一项紧要的工作.经过我们层层推进，建立了弱形式零点定理、零点定理和强形式零点定理.正如要证明 Hilbert Nullstellensatz 定理需要域的代数扩张、代数封闭域和整扩张等概念，建立理想与阵列零点定理也强烈地需要模的内

射扩张、模的内射闭包和同态的提升等概念和技巧.

1.3.2 从阵列到多项式

下面要考虑零点定理逆问题.

设 $M\subset M$ 是任意一个由有限个 R 上的 LRA 生成的 M 的 $R[X]$ - 子模.

问题 D:对上述有限生成 $R[X]$ - 模 M,是否存在 $R[X]$ 的一个理想 I,使得 $M=\mathrm{Zer}_M(I)$?

当 R 是一个域时,又是 Macaulay(参考文献[93],§63,p71)给出了肯定的回答.他是用 dialytic 方法证明了这个"定理".然而,我们认为,Macaulay 的这个证明也只能在 M 是有限生成 R - 模时才能通过.实际上,对一般的有限生成 $R[X]$ - 模 M,Macaulay 对问题 E 的解答肯定是错了.本书将证明:

定理 D:设 R 是一个 QF 环,M 是 M 的有限生成 $R[X]$ - 子模,则 M 是 $R[X]$ 的某理想的零化阵列模.(即存在 $R[X]$ 的理想 I 使得 $M=\mathrm{Zer}_M(I)$),当且仅当 M 是有限生成 R - 模.)

定理 E:设 R 是一个有限域,$M=\langle A_1,A_2,\cdots,A_k\rangle$ 是 M 的有限生成 $R[X]$ - 子模,其中 $A_i\in M$.则存在 $R[X]$ 的理想 I 使得 $M=\mathrm{Zer}_M(I)$ 当且仅当每个 LRS 阵列 A_i 最终周期的(即:不计初始的有限项外是周期的).

值得注意的是,每个 A_i 周期性质成了观察 M 能否完全构成一个线性递归伪随机阵列系统的判别条件.这是一个有趣的现象,也许在密码分析中有一定的理论指导意义.

1.4 零化阵列模的结构与 Nechaev 问题

问题 E:给定一个多项式理想 $I\subset R[X]$,给出 I 恰是某个 LRA 阵列的特征理想的判别准则,即给出充要条件,使得存在一个 LRA $A\in M$,满足 $I=\mathrm{Ann}_{R[X]}(A)$.

问题 E 是强零点定理的精细化.当 $n=1$ 且 R 是一个域时,则问题 E 是平凡的.因为,$R[x]$ 是一个主理想整环,$R[x]$ 的任意一个理想 I 由一个首一的多项式生成,即 $I=\langle g(x)\rangle$,其中 $g(x)\in R[x]$.故 $R[X]$ 每个理想都恰是一个 LRS 的特征理想.

当 $n=1$ 且 R 是一个惟一因子分解整环(简记为 UFD)时,问题就不像在域上时那么简单.当 R 为 Potential 整环时,即要求 R 和 $R[[x]]$ 都是 UFD 时,Fitzpatrick 和 Norton(1995)(参考文献[28])证明 $R[x]$ 中的理想 I 恰是一个 LRS 的特征理想的充分必要条件是 I 是由一个首一多项式生成的主理想.在本