多项式理想的Gröbner基初等导论

吕家凤　李会师　著

科学出版社

多项式理想的 Gröbner 基初等导论

吕家凤　李会师　著

科学出版社

北京

内 容 简 介

本书深入浅出地引入多项式理想的 Gröbner 基理论，给出 Gröbner 基(特别是 Gröbner 基的消元原理)在多元多项式方程(组)的求解、多项式理想结构性质、仿射代数结构性质、代数几何、域的代数扩张、整数优化以及图论等方面的一些基本应用，着力于引导读者认识多项式理想的 Gröbner 基理论在代数结构+序结构+算法这个交叉领域平台上得以成功发展和有效应用的数学原理.

本书可作为数学与应用数学专业高年级本科生的选修课教材、研究生教材、计算代数讲习班(或讨论班)使用的选讲材料，也可作为数学与其他科学领域的科研工作者学习 Gröbner 基理论的入门参考书.

图书在版编目(CIP)数据

多项式理想的 Gröbner 基初等导论/吕家凤，李会师著. —北京：科学出版社，2018. 3

ISBN 978-7-03-056949-3

Ⅰ. ①多… Ⅱ. ①吕… ②李… Ⅲ. ①基(数学)–研究 Ⅳ. ① O15

中国版本图书馆 CIP 数据核字(2018) 第 049730 号

责任编辑：王丽平 / 责任校对：邹慧卿
责任印制：张 伟 / 封面设计：陈 敬

科 学 出 版 社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京建宏印刷有限公司 印刷
科学出版社发行 各地新华书店经销

*

2018 年 3 月第 一 版 开本：720 × 1000 B5
2018 年 3 月第一次印刷 印张：10
字数：200 000

定价：78.00 元

(如有印装质量问题，我社负责调换)

前　言

Polynomials and power series,
May they forever rule the world.

— Shreeram S. Abhyankar

设 K 是一个域 (例如 $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$), $K[\mathbb{x}] = K[x_1, \cdots, x_n]$ 是 K 上 n 个未定元 (也称变元) 的多项式环 (也称多项式代数, 参看 2.1 节关于 K-代数的介绍), I 是 $K[\mathbb{x}]$ 的一个理想. 由于 $K[\mathbb{x}]$ 是一个 Noetherian 环 (参看推论 1.5.5), 其每个理想都是有限生成的, 可设 I 是由 s 个多项式 $f_1, \cdots, f_s$ 生成的, 即 $I = \langle f_1, \cdots, f_s \rangle$. 多元多项式环 $K[\mathbb{x}]$ 中理想的构造性 Gröbner 基理论源于 20 世纪 60 年代奥地利数学家 Bruno Buchberger 关于在 $\dim_K K[\mathbb{x}]/I < \infty$ 时如何构造 K-代数 $K[\mathbb{x}]/I$ 的一个 K-基的博士学位论文:

[Bu1] Buchberger B. Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal[D]. PhD thesis. University of Innsbruck, 1965.

而构造 $K[\mathbb{x}]/I$ 的一个 K-基的核心问题是如何由给定的 I 的生成元集 $F = \{f_1, \cdots, f_s\}$ 出发, 通过“基于理想结构性质构造可行算法”的途径有效地求解“理想成员问题”, 即如何有效地检验 $K[\mathbb{x}]$ 中一个多项式 f 是否属于理想 I. Buchberger 的杰出贡献就是在对理想 $I = \langle F \rangle$ 的结构性质深刻认识的基础上, 由 F 出发通过构造 S-多项式和使用多元多项式的除法算法有效地计算出 I 的一个“能解决理想成员问题”的生成元集 $\mathcal{G}$, 从而有效地计算出 $K[\mathbb{x}]/I$ 的一个 K-基. 为纪念其导师 W. Gröbner (20 世纪优秀的代数几何学家) 对该论题的选择和对论文的精心指导所做的不可磨灭的贡献, Buchberger 将自己通过有效算法构造出的这个“能解决理想成员问题”的生成元集 $\mathcal{G}$ 称为“理想 I 的 Gröbner 基”, 他所创造的构造性算法就是如今计算机代数领域著名的 **Buchberger 算法**. 如已有文献 (和本书的内容) 所表明的那样, Buchberger 所开创的构造性 Gröbner 基理论的强大威力在于它可有效地应用于几乎一切与多项式方程组、多项式理想 I 以及剩余类环 (也称剩余类代数) $K[\mathbb{x}]/I$ 有关的数学求解问题. 然而, 也正如历史文献所显示的那样, Gröbner 基理论真正的普及应用和更深入的发展开始于 20 世纪 80 年代计算机科学与技术, 特别是计算机符号演算语言和技术的发展与普及之时. 反映这一里程碑的标志性文献是

[Bu2] Buchberger B. Gröbner bases: An algorithmic method in polynomial ideal theory[A]//Bose N K. Multidimensional Systems Theory. Dordrecht: Reidel, 1985: 184-232.

现如今, 随着 Buchberger 算法在越来越多的计算机代数系统中的成功实施 (参看 1.7 节最后所列出的软件系统), Gröbner 基理论不但在非线性代数方程组的符号求解、各种交换代数结构性质的算法实现, 以及计算代数几何等方面有着非常广泛而深入的有效应用, 而且在多元多项式插值、优化理论 (如整数规划和非线性规划)、代数编码理论、密码学、图论与网络安全、机器人自动化设计 (计算几何)、控制论、统计学、分子生物学等领域也有越来越广泛的有效应用.

【注】 在 Buchberger 之前也有数学家提出类似于 Gröbner 基的概念. 关于这一点, 读者可参看文献 [WK], [Eis].

本书基于李会师 2007—2014 年在海南大学为数学系一年级研究生讲授“计算代数”课程形成的英文讲义第一部分“Gröbner Bases of Polynomial Ideals and Applications” 和 2012 年在浙江师范大学吕家凤组织的暑期讲习班“Summer Mini-course on Gröbner Bases”上使用的英文讲稿, 其目的是向读者提供一个关于多项式理想的 Gröbner 基理论及其应用的初等导论. 因此, 本书可作为数学与应用数学专业高年级本科生的选修课教材、研究生教材、计算代数讲习班 (或讨论班) 使用的选讲材料, 也可作为数学与其他科学领域的科研工作者学习 Gröbner 基理论的入门参考书.

在参照许多关于 Gröbner 基及其应用的优秀的综合性长篇论著和教材 (如本书列出的参考文献) 的基础上, 本书作为 Gröbner 基及其应用的一个初等导论, 着力于引导读者认识多元多项式理想的 Gröbner 基理论在

代数结构 + 序结构 + 算法

这个交叉领域平台上得以成功发展和有效应用的数学原理, 其内容构成的主线为:

- 单项式 + 单项式序 $\Rightarrow$ 多项式的有序结构性质;
- 单项式理想的结构性质 $\Rightarrow$ Dickson 引理;
- 单项式的除法 + 多项式的有序结构性质 $\Rightarrow$ 用一组多项式 $S = \{f_1, \cdots, f_s\}$ 对一个多项式 f 做除法的除法算法 **Algorithm-DIV**(f/S);
- 单项式序下单项式理想 $\langle \mathbf{LM}(I) \rangle$ + Dickson 引理 $\Rightarrow$ 理想 I 的 Gröbner 基的存在性;
- S-多项式的构造 + **Algorithm-DIV**(f/S) $\Rightarrow$ 判定 Gröbner 基的 Buchberger 定理;
- Buchberger 定理蕴涵的算法原理 $\Rightarrow$ 检验和计算 Gröbner 基的 Buchberger

算法**Algorithm-GB**;

• 消元序结构 + Gröbner 基 ⇒ 消元定理;

• Gröbner 基 + 消元理想 ⇒ 对多项式理想结构、K-代数结构、代数几何 (含多元多项式方程组的符号求解), 以及其他领域的各种应用.

除了力求文字叙述与数学证明简明易懂, 我们尽量使本书的内容具有自包含性, 例如, 2.1 节提供了第 2 章所需的交换 K-代数基本知识, 3.1 节提供了第 3 章所需的代数几何基本知识, 第 5 章给出了 3.1 节中 Hilbert(弱、强) 零点定理的详细证明, 给出和证明了与 3.3 节密切相关的延伸学习内容 —— 消元理想的零点扩张原理, 并提供了 2.4 节和 4.3 节要用到的分式环的构造; 另外, 对某些节中的知识难点, 本书在适当的地方以【注】的形式予以强调和进一步阐述, 每节后面配备了一定数量与本节内容密切相关的练习题 (读者可在本书列出的参考文献中, 特别是 [AL] 中找到更多类似的例题和练习题). 因此, 读者只需要具备大学本科“高等代数”和“近世代数”基础知识, 以及最基本的一点算法结构知识, 就可以阅读和理解本书的所有内容, 而有兴趣的读者也可从本书后面列出的参考文献中找到更多延伸学习多项式理想的 Gröbner 基理论的资料.

本书的出版得到浙江省重点高校建设项目浙江师范大学数学学科经费的资助. 作者衷心感谢浙江师范大学数理与信息工程学院对此工作的大力支持.

此外, 吕家凤得到国家自然科学基金 (11571316) 和浙江省自然科学基金 (LY16A010003) 的资助, 在此表示感谢.

吕家凤　李会师

2016 年 12 月 1 日

一些常规约定

$\mathbb{N}$ 表示非负整数集合.
$\mathbb{Z}$ 表示整数集合.
$\mathbb{Q}$ 表示有理数集合.
$\mathbb{R}$ 表示实数集合.
$\mathbb{C}$ 表示复数集合.
K 表示任意一个域, $K^* = K - \{0\}$.
$|S|$ 表示一个给定集合 S 的基数.
所有环 R 均为有单位元 1 的结合环.
$\langle S \rangle$ 表示 环 R 的一个非空子集 S 生成的 (双边) 理想.
K-span$W$ 表示 K-向量空间 V 的一个非空子集 W 生成的子空间.

目　　录

前言
一些常规约定
第 1 章　多项式理想的 Gröbner 基……1
1.1　问题的引入……1
1.2　单项式序……8
1.3　单项式理想……12
1.4　除法算法……15
1.5　Gröbner 基……19
1.6　Buchberger 定理……22
1.7　Buchberger 算法……28
1.8　极小与约化 Gröbner 基……33
1.9　消元序下的 Gröbner 基与消元定理……38
第 2 章　对仿射 K-代数的初等应用……45
2.1　交换 K-代数与代数同态映射简介……45
2.2　对多项式理想几个结构性质的应用……48
2.3　求解多项式理想 $I \cap J$ 的生成元集……52
2.4　对仿射 K-代数几个结构性质的应用……54
2.5　对仿射 K-代数同态映射的应用……63
2.6　对仿射 K-代数中 K-代数元的一个应用……70
第 3 章　在代数几何中的初等应用……73
3.1　初等代数几何的一些基本元素简介……73
3.2　求解 $\mathcal{V}(I) \neq \varnothing$? $\mathcal{V}(I)$ 有限? $f \in \sqrt{I}$?……79
3.3　求解 $\pi(V)$ 的 Zariski 闭包 $\mathcal{V}(\mathcal{I}(\pi(V)))$……84
3.4　对多项式映射 $\mathcal{V}(I) \xrightarrow{\alpha} \mathcal{V}(J)$ 的应用……87
第 4 章　Gröbner 基的更多应用简介……92
4.1　对域的有限代数扩张的一个应用……92
4.2　在整数优化中的应用举例……100
4.3　在图论中的应用举例……111
第 5 章　附录……120
5.1　Hilbert 零点定理的证明……120

5.2　消元理想的零点扩张原理 ····· 128
5.3　分式环的构造 ····· 139
参考文献 ····· 146
索引 ····· 147

第 1 章　多项式理想的 Gröbner 基

在本章中, 基于单项式序结构、单项式理想结构以及多元多项式的 (带余) 除法算法, 我们系统地引入 Buchberger 所创立的域 K 上 n-元多项式环 $K[x_1, \cdots, x_n]$ 中理想的构造性 Gröbner 基理论, 其中着重论述:

- 多项式理想的 Gröbner 基产生的代数结构基础;
- 判别和计算 Gröbner 基的 Buchberger 定理和 Buchberger 算法形成的数学原理, 并由此导出计算极小 Gröbner 基和约化 Gröbner 基的算法;
- 在消元序下 Gröbner 基的计算过程中所蕴涵的消元定理, 以及应用消元序下的 Gröbner 基求解多项式方程组的消元原理.

1.1　问题的引入

先回顾一下有关多元多项式环的基本结构要素. 令 $K[\mathbb{x}] = K[x_1, \cdots, x_n]$ 为域 K 上 n 个未定元的多元多项式环. 则熟知的事实是:

- $K[\mathbb{x}]$ 是一个唯一分解整环 (UFD).
- $K[\mathbb{x}]$ 是 K 上一个向量空间 (所以 $K[\mathbb{x}]$ 也是一个 K-代数, 参看 2.1 节关于 K-代数的介绍).
- 令 $\mathbb{N}^n = \{\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \mid \alpha_j \in \mathbb{N}\}$. 则 $K[\mathbb{x}]$ 的标准 K-基为

$$\mathcal{B} = \{x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid \alpha \in \mathbb{N}^n\}.$$

因此, $\dim_K K[\mathbb{x}] = \infty$.

- $\mathcal{B}$ 对于 $K[\mathbb{x}]$ 的乘法来说做成一个有单位元的半群 (monoid) (即 $1 \in \mathcal{B}$, 对于任意 $x^\alpha, x^\beta \in \mathcal{B}$ 有 $x^\alpha \cdot x^\beta = x^{\alpha+\beta} \in \mathcal{B}$, 而乘法满足结合律), 且有半群同构 $(\mathcal{B}, \cdot) \cong (\mathbb{N}^n, +)$.

$K[\mathbb{x}]$ 的标准 K-基 $\mathcal{B}$ 中的元素通常称为**单项式** (monomial). 一个单项式 $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ 的全次数 $\deg(x^\alpha)$ 定义为

$$\deg(x^\alpha) = \alpha_1 + \alpha_2 + \cdots + \alpha_n.$$

若 $f = \sum_{i=1}^m \lambda_i x^{\alpha(i)} \in K[\mathbb{x}]$, 其中 $\lambda_i \in K^*$, $\alpha(i) = (\alpha_{i1}, \cdots, \alpha_{in}) \in \mathbb{N}^n$, 那么 f 的**全次数** (total degree) $\deg(f)$ 定义为

$$\deg(f) = \max\left\{ \deg(x^{\alpha(i)}) \;\middle|\; i = 1, \cdots, m \right\}.$$

现在, 令 $\mathbb{A}^n(K)=\{P=(a_1,\cdots,a_n)\mid a_i\in K,\ 1\leqslant i\leqslant n\}$ 为域 K 上 n-**维仿射空间**. 对于 $F=\{f_1,\cdots,f_s\}\subset K[\mathbb{x}]$, 考察由 F 定义的方程组:

$$\text{(I)}\qquad \begin{cases} f_1=0,\\ \quad\vdots\\ f_s=0, \end{cases}$$

并记方程组 (I) 的解集 (或等价地, F 的零点集) 为

$$\mathcal{V}(F)=\{P\in\mathbb{A}^n(K)\mid f_i(P)=0,\ f_i\in F\}.$$

问题

当方程组 (I) **不是线性方程组**时,

(1) 如何验证方程组 (I) 有解, 或等价地, 何时 $\mathcal{V}(F)\neq\varnothing$?

(2) 若知道 $\mathcal{V}(F)\neq\varnothing$, 如何检验 $\mathcal{V}(F)$ 是有限集还是无限集?

(3) 若知道 $\mathcal{V}(F)\neq\varnothing$, 能否给出方程组 (I) 符号求解公式 (类似于线性方程组的基础解系)?

代数几何理论上的求解途径(见第 3 章)

给定任一非空子集 $F\subset K[\mathbb{x}]$, 考虑理想 $I=\langle F\rangle$. 那么可直接验证

$$\mathcal{V}(F)=\mathcal{V}(I)=\mathcal{V}(S),$$

其中 S 为 I 的**任何一个生成元集**. 这种将寻求方程组 (I) 的解的离散问题与多项式理想的整体代数结构联系起来的思想正是**代数几何的灵魂**所在. 因为若进一步令

$$\sqrt{I}=\{f\in K[\mathbb{x}]\mid \text{存在某个正整数 } m \text{ 使得 } f^m\in I\},$$
$$\mathcal{I}(\mathcal{V}(I))=\{f\in K[\mathbb{x}]\mid f(P)=0,\ \forall P\in\mathcal{V}(I)\},$$

那么直接验证可知 $\sqrt{I}$ 与 $\mathcal{I}(\mathcal{V}(I))$ 都是 $K[\mathbb{x}]$ 的理想且有 $\sqrt{I}\subseteq\mathcal{I}(\mathcal{V}(I))$. 而代数几何的核心定理, 即著名的 Hilbert 零点定理 (Hilbert's nullstellensatz), 告诉我们当 K 为代数闭域时有

$$\sqrt{I}=\mathcal{I}(\mathcal{V}(I))\quad\text{(Hilbert 强零点定理)}.$$

由此便可得到

$$\mathcal{V}(F)=\varnothing\Leftrightarrow 1\in I\quad\text{(Hilbert 弱零点定理)},$$

即 F 确定的方程组 (I) 的解的存在性问题可转换为一个理想成员问题. 进一步地应用线性代数方法和 Hilbert 零点定理可得

$$\mathcal{V}(F)\text{ 有限}\Leftrightarrow\ \dim_K K[\mathbb{x}]/I<\infty,$$

即在解的存在性确定的前提下, 解集 $\mathcal{V}(F)$ 的有限或无限的问题可转换为确定 K-代数 $K[\mathbb{x}]/I$ 作为 K-向量空间的维数问题, 或等价地, 可转换为确定 K-向量空间 $K[\mathbb{x}]/I$ 的一个 K-基的问题. 因为每个域 K 包含在一个代数闭域中 (即 K 的代数闭包存在), 这就**从理论上回答了**前面的问题 (1) 和 (2).

关于前面的问题 (3), 注意到理想 I 中的元素对于 $K[\mathbb{x}]$ 的**加 (减) 法、乘法、数乘**是封闭的, 即 $\forall f, g \in I$, $h \in K[\mathbb{x}]$, $\lambda \in K$, 有

$$\lambda f,\ f \pm g,\ fg,\ hf \in I.$$

因此, **直觉 + 解线性方程组的经验**给我们的启示是:

• 有可能使用代数运算来"折腾" (即化简) I 的生成元集 F, 以期得到 I 的一个"好的"生成元集 S, 而由 S 出发则有可能解决问题 (3).

例 1.1.1 熟知的线性方程组的求解是 Hilbert 弱零点定理的最好例证和解决我们上面的问题 (3) 的最好诱因. 若 f_i 都是一次多项式, 则由线性方程组的初等变换得到的等价方程组是一个梯形方程组. 这就给出 I 一个"好生成元集" S, 即若 S 含有一个非零常数 λ (从而 $1 = \lambda\lambda^{-1} \in I$), 则方程组无解; 若 S 不含非零常数, 那么方程组有解且由 S 可得方程组的符号求解公式 (基础解系 + 特解).

例 1.1.2 在 $\mathbb{C}[x, y]$ 中令 $I = \langle f_1 = xy^2 + x - y + 1, f_2 = xy - x - 1\rangle$. 则 $I = \langle f_2, f_3 = xy + x + 1\rangle$ (注意到 $f_1 = yf_2 + f_3$). 于是 $\mathcal{V}(f_1, f_2) = \mathcal{V}(f_2, f_3) \neq \varnothing$ 且有限.

例 1.1.3 在 $\mathbb{C}[x, y, z]$ 中令 $I = \langle F\rangle$, 其中

$$F = \{f_1 = x^2 + y + z - 1, f_2 = x + y^2 + z - 1, f_3 = x + y + z^2 - 1\}.$$

注意到可置 $f_1 \in \mathbb{C}[y, z][x]$, $f_2 \in \mathbb{C}[x, z][y]$, $f_3 \in \mathbb{C}[x, y][z]$. 这样, 用首项系数为 1 的 f_1, f_2, f_3 相继对 $f \in \mathbb{C}[x, y, z]$ 做除法可知, 作为 $\mathbb{C}$-向量空间

$$\mathbb{C}[x, y, z]/I = \mathbb{C}\text{-span}\{\overline{1}, \overline{x}, \overline{y}, \overline{z}, \overline{xy}, \overline{xz}, \overline{yz}, \overline{xyz}\},$$

有 $\dim_{\mathbb{C}}\mathbb{C}[x, y, z]/I \leqslant 8$. 由此进一步可证 $\mathcal{V}(F)$ 有限.

容易知道, 在非线性的情况下, 上面各例中的方法不能作为解决问题 (1)—(3) 的一般有效方法. 事实上, 在 Buchberger 的博士学位论文之前, 没有人给出系统地解决以下问题的有效算法途径.

问题

一般地, 对于任意给定的有限集 $F = \{f_1, \cdots, f_m\} \subset K[\mathbb{x}]$,

• 能否算法地实现 Hilbert 弱零点定理, 即算法地判别是否有 $1 \in I = \langle F\rangle$?

• 在 $1 \notin I$ 时能否算法地判别 $\mathcal{V}(F)$ 是有限还是无限?

• 在 $\mathcal{V}(F)$ 有限时能否算法地确定 K-代数 $K[\mathbb{x}]/I$ 的一个 K-基并由此确定其乘法运算表?

• 在 $\mathcal{V}(F)\neq\varnothing$ 时, 能否在理想 $I=\langle F\rangle$ 中算法地实现"消元", 即能否算法地将 F 化简为 I 的一个新的生成元集 S, 使得 S 确定的方程组是一个方便求解的"梯形"方程组?

具有划时代意义的事情是, Buchberger 在他 1965 年的博士学位论文中创立的多项式理想的 Gröbner 基理论告诉我们, 在 $K[\mathbb{x}]$ 的标准 K-基 $\mathcal{B}$ 上一个**单项式序** $\prec$ 下, 由理想 $I=\langle F\rangle$ 的生成元集 F 出发可算法地计算出 I 的一个新的生成元集 $\mathcal{G}=\{g_1,\cdots,g_t\}$, 称为 I 的一个 Gröbner 基, 而因为 $\langle F\rangle=I=\langle\mathcal{G}\rangle$, 由 $\mathcal{G}$ 中多项式的具体"长相"便可同时读出以上四个问题的答案, 即

(1) $\mathcal{V}(F)=\varnothing\Leftrightarrow 1\in I=\langle F\rangle\Leftrightarrow\exists\,\lambda\in K^*,\ g_i\in\mathcal{G}$ 使得 $\lambda=g_i$ (见定理 3.2.1);

(2) 若 $\mathcal{V}(F)\neq\varnothing$, 则 $\mathcal{V}(F)$ 有限 $\Leftrightarrow$ 对每个 $i=1,\cdots,n,\ \exists\ g_{i_j}\in\mathcal{G}$, 正整数 m_i 使得其首项单项式 $\mathbf{LM}(g_{i_j})=x_i^{m_i}$ (见定理 3.2.2);

(3) 若 $\mathcal{V}(F)\neq\varnothing$ 且有限, 则 $K[\mathbb{x}]/I$ 具有 K-基

$$\overline{x}^{\alpha}=\{\overline{x}_1^{\alpha_1}\cdots\overline{x}_n^{\alpha_n}\mid 0\leqslant\alpha_i\leqslant m_{i_j}-1,\ 1\leqslant i\leqslant n\},$$

其乘法表通过对单项式的乘积取模 $\mathcal{G}$ 的余式即可建立 (见命题 2.4.1 及随后论述);

(4) 若 $\mathcal{V}(F)$ 有限, 或者 $\mathcal{V}(F)$ 为无限集而 $\prec$ 是一个"完全型消元序", 则 $\mathcal{G}$ 确定的方程组是一个与 F 确定的方程组等价的方便求解的"梯形"方程组, 也就是说, 在两种情况下计算出的 $\mathcal{G}$ 的过程具有通常解线性方程组意义下的"消元功能" (见定理 1.9.3 后小结及推论 3.2.3).

为了自然地进入 Gröbner 基理论, 以下我们先来回顾以上问题在一元多项式环中是如何进行算法求解的.

一元多项式环中以上问题的算法求解

令 $K[x]$ 为域 K 上未定元 x 的一元多项式环, 即

$$K[x]=\left\{f(x)=\sum_{i=0}^{n}\lambda_i x^i\ \middle|\ \lambda_i\in K,\ n\in\mathbb{N}\right\}.$$

则熟知的事实是:

• 作为 K 上的向量空间, $\dim_K K[x]=\infty$, $K[x]$ 的标准 K-基是 $\mathcal{B}=\{x^k\mid k\in\mathbb{N}\}$, 即 $K[x]$ 中所有关于 x 的单项式 (包括 $1=x^0$) 的集合. 对于 $x^k\in\mathcal{B}$, 定义 x^k 的次数为 k, 记为 $\deg(x^k)=k$. 对于 $K[x]$ 中**非零多项式** $f(x)=\lambda_n x^n+\lambda_{n-1}x^{n-1}+\cdots+\lambda_0$, 若 $\lambda_n\neq 0$, 则 $f(x)$ 的次数定义为 $\deg f(x)=n=\deg(x^n)$.

• 若 $\deg f(x)=n>0$, 则方程 $f(x)=0$ 在 K 中最多有 n 个解 (若 K 是代数闭的, 则有且仅有 n 个解).

• 带余除法算法: 对于 $f(x), g(x) \in K[x]$, 若 $g(x) \neq 0$, 则存在唯一的 $q(x), r(x) \in K[x]$ 使得

$$(*) \qquad f(x) = q(x)g(x) + r(x), \text{ 其中 } r(x) = 0 \text{ 或 } \deg r(x) < \deg g(x).$$

上面表达式中的 $q(x)$, $r(x)$ 分别称为用 $g(x)$ 对 $f(x)$ 做除法所得的**商**和**余式**. 若 $r(x) = 0$, 则称 $g(x)$ **整除** $f(x)$, 记为 $g(x)|f(x)$.

应用 $K[x]$ 中多项式的带余除法算法即可得到:

(1) $K[x]$ 是 PID (主理想整环), 从而 $K[x]$ 是 UFD.

(2) 理想成员问题的解决: 设 $I = \langle g(x) \rangle$ 是 $K[x]$ 中由非零多项式 $g(x)$ 生成的理想. 若 $f(x) \in K[x]$, 则 $f(x) \in I \Leftrightarrow g(x)|f(x)$.

(3) $\dim_K K[x]/I = m$, 其中 $m = \deg g(x)$, $\{\overline{1}, \overline{x}, \overline{x}^2, \cdots, \overline{x}^{m-1}\}$ 是 $K[x]/I$ 的一个 K-基, $K[x]/I$ 关于此基的加法与乘法法则为

$$\sum_{i=0}^{m-1} \lambda_i \overline{x}^i + \sum_{i=0}^{m-1} \mu_i \overline{x}^i = \sum_{i=0}^{m-1} (\lambda_i + \mu_i) \overline{x}^i,$$

$$\left(\sum_{i=0}^{m-1} \lambda_i \overline{x}^i \right) \left(\sum_{i=0}^{m-1} \mu_i \overline{x}^i \right) = r(\overline{x}),$$

其中 $r(x)$ 为 $\left(\sum_{i=0}^{m-1} \lambda_i x^i \right) \left(\sum_{i=0}^{m-1} \mu_i x^i \right)$ 在用 $g(x)$ 做除法后所得余式. 换言之, $K[x]/I$ 的乘法表可以按照法则 $\overline{x}^i \overline{x}^j = r(\overline{x})$ 得到, 其中 $0 \leqslant i, j \leqslant m-1$, $r(x)$ 为 $x^i x^j$ 在用 $g(x)$ 做除法后所得余式.

(4) 最大公因子与最小公倍元: 对于非零 $f(x)$, $g(x) \in K[x]$, $\gcd(f(x), g(x))$ 可通过辗转除法算法得到. 于是 $\operatorname{lcm}(f(x), g(x))$ 可根据性质

$$f(x) \cdot g(x) = \gcd(f(x), g(x)) \cdot \operatorname{lcm}(f(x), g(x))$$

得到, 从而可得

$$\langle \gcd(f(x), g(x)) \rangle = \langle f(x), g(x) \rangle,$$
$$\langle \operatorname{lcm}(f(x), g(x)) \rangle = \langle f(x) \rangle \cap \langle g(x) \rangle.$$

对于任意给定的有限多个多项式 $f_1(x), f_2(x), \cdots, f_s(x)$, 其最大公因子和最小公倍元有类似的性质并可算法地计算. 特别地, 若

$$\gcd(f_1(x), f_2(x), \cdots, f_s(x)) = d(x),$$

则方程组

$$\begin{cases} f_1(x) = 0, \\ f_2(x) = 0, \\ \quad \vdots \\ f_s(x) = 0 \end{cases}$$

等价于方程 $d(x)=0$.

我们看到, 在上面的 (1)—(4) 中, 一元多项式的带余除法是一个**决定性的角色**. 所以自然的问题是:

• 注意到 $n\geqslant 2$ 时多元多项式环 $K[\mathbb{x}]=K[x_1,\cdots,x_n]$ 是 UFD 而不是 PID, 那么能否在 $K[\mathbb{x}]$ 中构建类似于一元多项式环中的带余除法算法呢?

因为**假如**这样一个除法算法在 $K[\mathbb{x}]$ 中成立, 那么对于 $K[\mathbb{x}]$ 中一个理想 I 来说, **至少 I 的理想成员问题有可能得到解决**: 当 $I=\langle g\rangle$ 是由多项式 g 生成的主理想时, I 的理想成员问题可像在一元多项式环中那样通过用 g 做除法来解决. 进一步地, 当 $t\geqslant 2$ 且 $I=\langle g_1,\cdots,g_t\rangle$ 不是主理想时, 注意到每个 $h\in I$ 可被表示为 $h=\sum_{i=1}^{t}f_ig_i$, 其中 $f_i\in K[\mathbb{x}]$, 而每个 f_ig_i 是 g_i 的一个倍元 (即 g_i 整除 f_ig_i), 形式上这就给我们一种 "h 可被 $\{g_1,\cdots,g_t\}$ 整除" 的感觉. 所以, 对于 $f\in K[\mathbb{x}]$, **可以设想**用 I 的生成元集 $\{g_1,\cdots,g_t\}$ 中元素逐次对余式做除法便有可能可判别是否有 $f\in I$.

为了在后面对上面的问题给出肯定的回答, 我们先仔细考察一下一元多项式环中带余除法算法能够有效施行的条件保障.

一元多项式环中带余除法算法能够有效施行的条件保障

为了方便起见, 对于一元多项式环 $K[x]$ 中任意非零多项式

$$f(x)=\lambda x^n+\text{ 低次项, 其中 }\lambda\in K^*=K-\{0\},$$

我们用 $\mathbf{LC}(f(x))$ 表示 $f(x)$ 的**首项系数**, 即 $\mathbf{LC}(f(x))=\lambda$, $\mathbf{LM}(f(x))$ 表示 $f(x)$ 的**首项单项式**, 即 $\mathbf{LM}(f(x))=x^n$, $\mathbf{LT}(f(x))$ 表示 $f(x)$ 的**首项**, 即 $\mathbf{LT}(f(x))=\lambda x^n$.

取定非零多项式 $g(x)$, $f_0(x)\in K[x]$, 那么用 $g(x)$ 对 $f_0(x)$ 做带余除法的算法可表述如下:

INPUT $g(x)$, $f_0(x)$

OUTPUT $q(x)$, $r(x)\in K[x]$ with $r(x)=0$ or $\deg r(x)<\deg g(x)$,

　　such that $f_0(x)=q(x)g(x)+r(x)$

INITIALIZATION $f(x):=f_0(x)$, $q(x):=0$, $r(x):=0$

BEGIN

LOOP

　IF $\deg f(x)=n\geqslant m=\deg g(x)$ THEN

　$q(x):=q(x)+\dfrac{\mathbf{LC}(f(x))}{\mathbf{LC}(g(x))}x^{n-m}$

　$f(x):=f(x)-\dfrac{\mathbf{LC}(f(x))}{\mathbf{LC}(g(x))}x^{n-m}g(x)$

ELSE
$r(x) := r(x) + f(x)$
END
END
END

注意到 $K[x]$ 的 K-基, 或等价地, 所有单项式的集合 $\mathcal{B} = \{x^k \mid k \in \mathbb{N}\}$ 中单项式的除法特别简单, 即 $x^m | x^n \Leftrightarrow x^n = x^{n-m} \cdot x^m \Leftrightarrow m \leqslant n$. 我们看到, 在 K 中非零元素 (对于乘法来说) 可逆这个基本条件下, 一元多项式除法算法的**本质**是用 $\mathbf{LT}(g(x))$ 通过单项式的除法**消去** $\mathbf{LT}(f(x))$, 即若 $\deg(f(x)) = n \geqslant m = \deg(g(x))$, 那么 $\mathbf{LM}(g(x))|\mathbf{LM}(f(x))$, 从而 $\mathbf{LT}(f(x)) = \mathbf{LC}(f(x))x^n = \dfrac{\mathbf{LC}(f(x))}{\mathbf{LC}(g(x))}x^{n-m}\mathbf{LT}(g(x))$. 算法之所以能顺利地在有限步终止是因为:

(1) $K[x]$ 的 K-基 $\mathcal{B} = \{x^k \mid k \in \mathbb{N}\}$ 上有一个**由次数诱导出的**自然序关系 $\prec$: $x^m \prec x^n \Leftrightarrow m \leqslant n$, 而这个序关系显然是 $\mathcal{B}$ 上一个良序关系 (即 $\prec$ 是 $\mathcal{B}$ 上一个全序关系且 $\mathcal{B}$ 的每个非空子集 S 对于 $\prec$ 来说都有一个"最小元" $x^\gamma \in S$, 即 $x^\gamma \prec x^\alpha$, $\forall x^\alpha \in S$).

(2) 在 $\prec$ 下每个非零多项式 $f(x)$ 有唯一的首项 $\mathbf{LT}(f(x))$ (尽管我们通常使用 $f(x)$ 的次数 $\deg f(x)$ 来确定该首项).

(3) 单项式的乘法是保序的: $x^n \prec x^m \Rightarrow x^d x^n \prec x^d x^m$, $\forall x^d \in \mathcal{B}$; 单项式的除法与 $\prec$ 是相容的, 即 $x^m | x^n \Leftrightarrow x^m \prec x^n$.

(4) 上面的 (3) 保证了在每一次施行除法算法时能成功地**消去** $\mathbf{LT}(f(x))$, 从而所得到的新的 $f(x) := f(x) - \dfrac{\mathbf{LC}(f(x))}{\mathbf{LC}(g(x))}x^{n-m}g(x)$ 的首项单项式 $\mathbf{LM}(f(x))$ 在 $\prec$ 下是严格递减的.

(5) $\prec$ 的良序性保证了算法能在有限步终止 (尽管我们通常使用 $\deg f(x) < \infty$ 这个事实).

上面对一元多项式除法算法的分析对于如何构建多元多项式除法算法最重要的启迪就是:

• 从理论上讲, 域 K 上的多元多项式环 $K[\mathbb{x}] = K[x_1, \cdots, x_n]$ 是一个 UFD, $K[\mathbb{x}]$ 中非零元素的整除性是有意义的. 而从实际操作的层面上讲, 虽然多元单项式的除法法则与一元单项式的除法法则一样, 即

$$\begin{aligned} & x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid x_1^{\beta_1} \cdots x_n^{\beta_n} \\ \Leftrightarrow\ & x_1^{\beta_1} \cdots x_n^{\beta_n} = \left(x_1^{\beta_1 - \alpha_1} \cdots x_n^{\beta_n - \alpha_n}\right) \cdot (x_1^{\alpha_1} \cdots x_n^{\alpha_n}) \\ \Leftrightarrow\ & \alpha_i \leqslant \beta_i, \quad 1 \leqslant i \leqslant n, \end{aligned}$$

但因为用多元多项式的**全次数**去定义 $K[\mathbb{x}]$ 中任一非零多项式的首项显然已不再有效, 所以, 要有一个像一元多项式除法算法那样"通过使用单项式除法有效地消去首项"的多元多项式除法算法, 就必须在 $K[\mathbb{x}]$ 的 K-基 $\mathcal{B}=\{x^{\alpha}=x_1^{\alpha_1}\cdots x_n^{\alpha_n}\mid \alpha=(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n\}$ 上有一个良序关系 $\prec$, 使得在 $\prec$ 下 $K[\mathbb{x}]$ 中每个非零多项式 $f=\sum_i \lambda_i x^{\alpha(i)}$ 有唯一的首项 $\mathbf{LT}(f)$, 单项式的乘法是保序的: $x^{\alpha}\prec x^{\beta}\Rightarrow x^{\gamma}x^{\alpha}\prec x^{\gamma}x^{\beta}$, $\forall x^{\gamma}\in\mathcal{B}$, 且单项式的除法与 $\prec$ 至少是"同向相容"的, 即 $x^{\alpha}|x^{\beta}\Rightarrow x^{\alpha}\prec x^{\beta}$.

1.2　单项式序

令 $K[\mathbb{x}]=K[x_1,\cdots,x_n]$ 为域 K 上的 n-元多项式环, $\mathcal{B}=\{x^{\alpha}=x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}\mid \alpha\in\mathbb{N}^n\}$ 为 K-向量空间 $K[\mathbb{x}]$ 的标准 K-基. 根据 1.1 节中对一元多项式除法算法的分析, 本节引入 $\mathcal{B}$ 上 (或等价地, $K[\mathbb{x}]$ 上) 单项式序的概念.

首先回忆一个集合 A 上一个 (二元) 关系 $\prec$, 如果具有

(a) 自反性: $a\prec a$, $\forall a\in A$;

(b) 反对称性: 若 $a,b\in A$ 且 $a\prec b$, $b\prec a$, 则 $a=b$;

(c) 传递性: 若 $a,b,c\in A$ 且 $a\prec b$, $b\prec c$, 则 $a\prec c$,

那么就称 $\prec$ 为 A 上一个**偏序关系**(partial ordering relation). 若 $\prec$ 是 A 上一个偏序关系且 $\forall a,b\in A$ 有 $a=b$, 或 $a\precneqq b$, 或 $b\precneqq a$, 则称 $\prec$ 是 A 上一个**全序关系**(total ordering relation).

【注】　(i) 注意当 $\prec$ 代表的不是通常数的大小关系 $\leqslant$ 时, 一般集合 A 上偏序关系 $\prec$ 的自反性 $a\prec a$ 指的是"a **与** a **具有关系** $\prec$", 而不可理解为"a 小于 a".

(ii) 上面定义中的记号 $a\precneqq b$ 表示 $a\neq b$ 且 $a\prec b$. 在后面的章节中 (如 1.9 节), 如果需要强调 $a\neq b$ 且 $a\prec b$ 时, 我们将会沿用记号 $a\precneqq b$.

定义 1.2.1　设 $\prec$ 是 $\mathcal{B}$ 上一个偏序关系. 如果 $\prec$ 满足以下三个条件:

(1) $\prec$ 是一个全序关系 (total ordering relation);

(2) $x^{\alpha}\in\mathcal{B}$ 且 $1\neq x^{\alpha}\Rightarrow 1\prec x^{\alpha}$;

(3) $x^{\alpha}\prec x^{\beta}\Rightarrow x^{\gamma}x^{\alpha}\prec x^{\gamma}x^{\beta}$, $\forall x^{\gamma}\in\mathcal{B}$,

则称 $\prec$ 为 $\mathcal{B}$ 上一个**单项式序** (monomial ordering). 有时为了方便起见, 也称 $\mathcal{B}$ 上一个单项式序 $\prec$ 为 $K[\mathbb{x}]$ 上**一个单项式序**.

【注】　我们将在 1.3 节证明 $\mathcal{B}$ 上每个单项式序 $\prec$ 都是 $\mathcal{B}$ 上一个良序关系, 即 $\mathcal{B}$ 的每个非空子集 S 对于 $\prec$ 来说都有一个"最小元" $x^{\gamma}\in S$ (即 $x^{\gamma}\prec x^{\alpha}$, $\forall x^{\alpha}\in S$).

由定义可知一个单项式序 $\prec$ 首先是 $\mathcal{B}$ 上一个全序关系, 所以必有 $1,2,\cdots,n$