现代数学基础

22 多项式代数

■ 王东明 牟晨琪 李晓亮
杨 静 金 萌 黄艳丽 编著

高等教育出版社
HIGHER EDUCATION PRESS

现代数学基础

22 多项式代数

DUOXIANGSHI DAISHU

■ 王东明 牟晨琪 李晓亮
杨 静 金 萌 黄艳丽 编著

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

图书在版编目（CIP）数据

多项式代数 / 王东明等编著. —北京：高等教育出版社，2011.5
ISBN 978-7-04-031698-8
Ⅰ. ①多… Ⅱ. ①王… Ⅲ. ①多项式－高等代数－高等学校－教材 Ⅳ. ①O15

中国版本图书馆 CIP 数据核字（2011）第064240号

策划编辑 李 鹏 责任编辑 李 鹏 封面设计 张 楠 责任印制 朱学忠

出版发行	高等教育出版社	咨询电话	400-810-0598
社 址	北京市西城区德外大街4号	网 址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印 刷	涿州市京南印刷厂	网上订购	http://www.landraco.com
开 本	787×1092 1/16		http://www.landraco.com.cn
印 张	23.75	版 次	2011年5月第1版
字 数	480 000	印 次	2011年5月第1次印刷
购书热线	010-58581118	定 价	59.00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

物 料 号 31698-00

内容简介

多项式代数是研究多项式和多项式系统所定义的代数与几何对象的结构、性质、特征、表示及计算的非线性代数. 本书系统介绍多项式代数的基本概念、核心理论、主要算法及若干应用. 全书共分六章, 前两章介绍与多项式相关的概念和运算、多项式系统的消元理论以及代数方程组的求解方法. 以此为基础, 第三章探讨交换代数与代数几何中的构造性理论和各种计算问题; 第四章介绍由实系数多项式等式和不等式所构成的半代数系统的求解方法及相关理论; 第五章简述判定高次方程根式可解性的伽罗瓦理论; 第六章讨论多项式代数在五个领域中的应用.

本书可作为高等院校数学和计算机科学系高年级本科生及研究生的教材或教学参考书, 也可供有关科研人员参考.

前　言

多项式是简单初等的数学表达式. 多项式方程和方程组的求解是基本的数学问题, 见之于科学和工程的各个领域. 多项式生成的理想、多项式方程组定义的代数簇以及由多项式等式和不等式构成的半代数系统都是代数学与几何学的研究对象. 本书介绍的多项式代数主要研究由多项式和多项式系统所定义或导出的代数与几何对象的结构、性质、特征、表示、相互关系及有关计算问题. 多项式代数是一种简单的非线性代数, 可以用来描述和处理各种非线性科学问题. 本书 2.1 节将对多项式代数及其与其他学科的关联作一个概述.

多项式代数的经典内容见诸于近世代数、交换代数和代数几何, 其重点在于建立存在性理论和方法, 而非对具体代数与几何对象进行构造性研究. 后者需要涉及大量复杂的多项式运算, 常常会超出传统的纸上推演的可行范围. 多项式代数的研究向构造性和算法化转变始于上个世纪 60 年代. 从那时起, 符号与代数计算的方法和软件快速发展, 在计算机上进行大规模多项式运算变得现实可行. 随之多项式代数的各种有效算法相继出现.

笔者曾在北京航空航天大学主持一个代数讨论班, 带领研究生们系统学习与多项式和多项式系统有关的各种符号与代数计算方法. 当时我们希望能有一本讨论班用书, 但在查阅有关教材和专著之后并未选到一本合适的. 于是笔者提议, 大家分头研读、报告已有论著中的精彩章节, 再按照我们的思路和理解, 以求解多项式系统为主线, 将其部分内容重新整理成书. 这一提议得到了讨论班成员的积极响应. 2007 年秋季, 我们便开始酝酿这本《多项式代数》的写作. 三年多来, 从书的结构和选材到具体结果的陈述和每个符号的使用, 我们进行了无数次的讨论. 在这过程中, 我们使用了传统的和最现代的交流与通信方式, 我们学到了很多, 也获得了很多理解和支持. 呈现在读者面前的这本书的背后是笔者与合作者们共同度过的工作学习、探讨交流的美好时光. 尽管作了不少努力, 我们深知这本尝试之作中一定还有许多缺点和错误. 我们殷切期待读者的批评和指正, 并希望将来在本书有机会再版或重印时对书中的错误和不妥之处予以修订. 如果本书对读者的教学和科研能有所裨益, 那将是笔者最大的欣慰.

王东明

2010 年 12 月

致　谢

本书的写作得到了北京航空航天大学“计算机数学”专项、数学与系统科学学院、数学、信息与行为教育部重点实验室、软件开发环境国家重点实验室、法国国家科学研究中心和巴黎 Pierre 与 Marie Curie 大学的支持. Hoon Hong, Daniel Lazard, Annick Valibouze, Kazuhiro Yokoyama, Philippe Aubry 和 Guénaël Renault 教授对本书的部分选材提供了有益的建议. 林东岱、王明生研究员和梁野、陈肖宇、牛薇、赵婷、蒋磊同学帮助阅读了书稿的部分章节. 王丽萍、李鹏编辑为本书的出版付出了诸多努力.

符 号 表

$\sim$	相似
$\cong$	同构
$\vee, \wedge, \neg, \rightarrow, \leftrightarrow$	逻辑“或”、“且”、“非”、“蕴涵”、“等价”
$\exists, \forall$	量词“存在”、“任意”
$(\exists_k x)\Phi$	存在 k 个 x 使得 Φ 为真
$<_{\text{grevlex}}$	分次逆字典序
$<_{\text{grlex}}$	分次字典序
$<_{\text{lex}}$	字典序
$<_{\text{rlex}}$	逆字典序
$\xrightarrow[\mu]{P}, \xrightarrow{P}, \xrightarrow{\mathcal{P}}, \xrightarrow[*]{\mathcal{P}}$	约化
$\sum \mathcal{K}^2$	域 $\mathcal{K}$ 中元素的平方和
$\mathfrak{a}+\mathfrak{b}, \mathfrak{a}\mathfrak{b}$	理想 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的和、积
$\mathfrak{a}:\mathfrak{b}$	理想 $\mathfrak{a}$ 关于 $\mathfrak{b}$ 的商
$\mathfrak{a}:H^\infty$	理想 $\mathfrak{a}$ 关于 H 的饱和
$\mathfrak{a}_l$	理想 $\mathfrak{a}$ 的第 l 个消去理想
$\sqrt{\mathfrak{a}}$	理想 $\mathfrak{a}$ 的根
$\mathfrak{a}^e, \mathfrak{a}^c$	理想 $\mathfrak{a}$ 的扩张、限制
${}^a\text{HF}_{\mathfrak{a}}(s)$	理想 $\mathfrak{a}$ 的仿射 Hilbert 函数
$\text{Aut}(\mathcal{K})$	域 $\mathcal{K}$ 上全体自同构的集合
BP	标准半代数系统的边界多项式
$\mathbb{C}$	复数域
$\mathcal{C}_n$	n 维实空间 $\mathbb{R}^n$ 的柱形代数分解
char	域的特征
cls	多项式的类
coef	多项式关于某项的系数
cont	多项式关于某个变元的容度
CP	标准半代数系统的临界多项式
$\text{csgn}, \text{csgn}_0$	多项式集合的柱形符号条件树
csgn_i	柱形符号条件树的 i 阶子树
deg	多项式关于某个变元的次数
det	方阵的行列式

dim	理想的维数
$\dim_{\mathcal{K}}$	$\mathcal{K}$ 线性空间的维数
disc	多项式的判别式
dismat	多项式关于另一多项式的判别矩阵
DP	标准半代数系统的判别多项式
dpol	矩阵的行列式多项式
$\mathrm{ev}_{\boldsymbol{a}}$	多元多项式在 $\boldsymbol{a}$ 处的赋值同态
ev_{x_i-a}	多元多项式在 $x_i = a$ 处的赋值同态
$\overline{\mathcal{F}}$	域 $\mathcal{F}$ 的代数闭包
$F \mid G$	F 整除 G
$\mathcal{F}[S], \mathcal{F}(S)$	由域 $\mathcal{F}$ 和集合 S 生成的环、域
$\mathfrak{F}(S)$	S 的不动域
$\mathcal{G}'$	$\mathcal{G}$ 的换位子群
$[G]$	G 在对应商空间中的像
$\mathrm{Gal}(F)$	多项式 F 在 $\mathbb{Q}$ 上的 Galois 群
$\mathrm{Gal}(\mathcal{K}/\mathcal{F})$	域扩张 $\mathcal{K}/\mathcal{F}$ 的 Galois 群
gcd	两个或多个多项式的最大公因子
GDL	多项式关于另一多项式的广义判别式序列
$H_{\boldsymbol{u}}$	变元集 $\boldsymbol{u}$ 的标空间
hc, hm, ht	多项式关于给定项序的首项系数、首单项式、首项
$\mathrm{ht}(\mathfrak{a})$	非零理想 $\mathfrak{a}$ 的首项集合
i	$\sqrt{-1}$
$\mathfrak{I}(Z)$	仿射空间的子集 Z 的对应理想
$\mathrm{im}(\pi)$	映射 π 的像
ini	多项式的初式, 三角列中多项式的初式构成的集合
$J_{\mathcal{T}}$	多项式集合 $\mathcal{T}$ 中所有初式的乘积
$\mathcal{K}^*$	域 $\mathcal{K}$ 的乘法群
$\mathcal{K}_F$	多项式 F 的分裂域
$(\mathcal{K}, \leqslant)$	由 $\leqslant$ 确定的序域
$[\mathcal{K} : \mathcal{F}]$	扩域 $\mathcal{K}$ 在基域 $\mathcal{F}$ 上的次数
$\mathcal{K}/\mathcal{F}$	域扩张
ker	同态映射的核
ldeg	多项式的导次数
lv	多项式的导元, 一组多项式的导元构成的集合
$\mathrm{lc}(F, x_k)$	多项式 F 关于变元 x_k 的导系数

$\mathfrak{M}$	多项式中所有单项式构成的集合
$\boldsymbol{M}^T$	矩阵 $\boldsymbol{M}$ 的转置
$\min(\mathcal{F}, \alpha)$	代数元 α 在 $\mathcal{F}$ 上的极小多项式
nform	范式
num	一元多项式在给定区间上的实根数 (重根按重数计算)
num_+	使给定多项式为正的一元多项式的实根数目
num_-	使给定多项式为负的一元多项式的实根数目
Ω_F	$\mathbb{Q}$ 上多项式 F 在 $\overline{\mathbb{Q}}$ 中的所有根构成的集合
$\mathcal{P}_{\leqslant s}$	多项式集 $\mathcal{P}$ 中全次数小于或等于 s 的多项式构成的集合
$\mathsf{pop}(\cdot)$	从 $\cdot$ 中选取一个元素, 然后删除
pp	多项式关于某个变元的本原部分
pquo	多项式对另一多项式关于某个变元的伪商
prem	多项式对另一多项式关于某个变元的伪余式, 多项式对三角列的伪余式, 一组多项式对三角列的伪余式构成的集合
proj	多项式集合的投影算子
$\text{Proj}_{\boldsymbol{x}_i} Z$	零点集 Z 到 $\boldsymbol{x}_i$ 的投影
p-sat	对三角列伪余式为零的所有多项式构成的集合
$\mathbb{Q}$	有理数域
quo	多项式关于另一多项式的商
$\mathcal{R}$	环
$\mathscr{R}$	经典多元结式
$\mathbb{R}$	实数域
$\overline{\mathbb{R}}$	$\mathbb{R} \cup \{-\infty, +\infty\}$
$\mathbb{R}_{\geqslant 0}$	非负实数的全体
$\mathbb{R}_{\text{alg}}$	有理数域上的全体实代数数
$\mathcal{R}[\boldsymbol{x}]$	$\mathcal{R}$ 上关于变元 $\boldsymbol{x}$ 的多项式环
$\mathbb{Q}^{(d)}[x_1, \ldots, x_n]$	$\mathbb{Q}[x_1, \ldots, x_n]$ 中关于每个 x_i 的次数都小于 d 的多项式的全体
rank	多元多项式的秩
rem	多项式关于另一多项式的余式
res	两个多项式关于某个变元的 Sylvester 结式
Res	两个多项式关于某个变元的结式
RZ	三角列、三角系统的所有正则零点构成的集合
$\lvert S\rvert, \#S$	S 中元素的个数
$\mathcal{S}_n$	n 次对称群
S_{sp}	柱形代数分解的样本

$\mathrm{S}(F,G)$	F 和 G 的 S 多项式
sat	正则列的饱和理想
sgn	符号函数, 序列的符号序列, 多项式集在某点处的符号表
$\mathrm{span}_{\mathcal{K}}(F_1,\ldots,F_m)$	由 $F_1,\ldots,F_m$ 张成的 $\mathcal{K}$ 线性空间
sres_j	两个多项式关于某变元的第 j 个子结式
Syl	两个多项式关于某变元的 Sylvester 矩阵
$\mathfrak{T}$	关于一组变元的所有项构成的集合, 多项式的所有项构成的集合, 属于给定理想的所有项构成的集合
$\mathcal{T}_{i-1}$	三角列 $\mathcal{T}$ 中的前 $i-1$ 个多项式构成的三角列
$\mathcal{T}_{x_i}$	多项式集合 $\mathcal{T}$ 中以 x_i 为导元的多项式构成的集合
$\mathcal{T}_{<x_i}$	多项式集合 $\mathcal{T}$ 中导元小于 x_i 的多项式构成的集合
$[\mathcal{T},\mathcal{U}]$	多项式系统
tail	多项式的尾式
$\mathrm{tail}^{(i)}$	多项式的 i 阶尾式
tdeg	多项式的全次数
Trem	Tarski 余式
V	多项式集合的仿射代数簇
Van	Vandermonde 矩阵
var	符号序列的变号数, 序列的变号数, 一元多项式序列在某点处的变号数, 多项式序列在某个区间上的变号数
$\boldsymbol{x}$	$x_1,\ldots,x_n$
$\langle \boldsymbol{x}^{\boldsymbol{\alpha}} : \boldsymbol{\alpha}\in S\rangle$	项理想
χ_d	$\mathbb{Q}[x_1,\ldots,x_n]$ 到 $\mathbb{Q}[x]$ 的映射
$\mathbb{Z}$	整数环
$\mathbb{Z}_p$	模 p 的剩余类环
$\overline{Z}$	仿射空间中点集 Z 的 Zariski 闭包
$Z(S)$	区域 S 上的柱形
$\mathsf{Z}_{\tilde{\mathcal{K}}}$	$\tilde{\mathcal{K}}^n$ 中的代数簇或拟代数簇
$\mathsf{Z}(\mathcal{P}/\mathcal{Q})$	多项式系统 $[\mathcal{P},\mathcal{Q}]$ 的零点集

郑 重 声 明

目　录

第一章　多项式——概念及基本运算

多项式方程和方程组的求解是代数学中的基本问题, 有着广泛而深入的应用. 本章介绍多项式的基础知识, 主要给出建立本书中各种理论和方法所需要的基本结论, 以及在后面各章中要用到的概念和性质. 更详细的讨论参见标准的代数教科书.

1.1 多项式基础

本节主要介绍与多项式有关的基本概念、运算及性质, 它们在以后的章节中将会经常用到.

1.1.1 多项式环与项序

设 $\mathcal{R}$ 为带单位元的交换环, $x_1, \ldots, x_n$ 为 $\mathcal{R}$ 上的未定元.

定义 1.1.1　称形式幂积 $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ $(\alpha_i \geqslant 0)$ 为关于 $x_1, \ldots, x_n$ 的 *项* (term), 简记为 $\boldsymbol{x}^{\boldsymbol{\alpha}}$, 其中 $\boldsymbol{x}$ 和 $\boldsymbol{\alpha}$ 分别表示向量 $(x_1, \ldots, x_n)$ 和 $(\alpha_1, \ldots, \alpha_n)$. 又称 α_i 为 $\boldsymbol{x}^{\boldsymbol{\alpha}}$ 关于变元 x_i 的 *次数* (degree), 记为 $\deg(\boldsymbol{x}^{\boldsymbol{\alpha}}, x_i)$, 而 $\alpha_1 + \cdots + \alpha_n$ 为 $\boldsymbol{x}^{\boldsymbol{\alpha}}$ 的 *全次数* (total degree), 记为 $\mathrm{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}})$. 关于变元 $x_1, \ldots, x_n$ 的所有项组成的集合记为 $\mathfrak{T}(\boldsymbol{x})$.

定义 1.1.2　称有限和

$$F = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}} \ \ (c_{\alpha} \in \mathcal{R})$$

为 $\mathcal{R}$ 上关于 $x_1, \ldots, x_n$ 的 *多项式* (polynomial), 而 $c_{\boldsymbol{\alpha}}$ 为 F 关于项 $\boldsymbol{x}^{\boldsymbol{\alpha}}$ 的 *系数* (coefficient), 记为 $\mathrm{coef}(F, \boldsymbol{x}^{\boldsymbol{\alpha}})$. 若 $c_{\boldsymbol{\alpha}} \neq 0$, 则称 $\boldsymbol{x}^{\boldsymbol{\alpha}}$ 为 F 的项, 并称 $c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$ 为 F 的 *单项式* (monomial). F 的所有项和所有单项式组成的集合分别记为 $\mathfrak{T}(F)$ 和 $\mathfrak{M}(F)$. 若 $F \neq 0$, 我们称

$$\deg(F, x_i) := \max\{\deg(\boldsymbol{x}^{\boldsymbol{\alpha}}, x_i) : \mathrm{coef}(F, \boldsymbol{x}^{\boldsymbol{\alpha}}) \neq 0\}$$

为 F 关于变元 x_i 的 *次数* (degree);

$$\mathrm{tdeg}(F) := \max\{\mathrm{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) : \mathrm{coef}(F, \boldsymbol{x}^{\boldsymbol{\alpha}}) \neq 0\}$$

为 F 的 *全次数* (total degree). 规定 $\deg(0, x_i) := -1$, $\mathrm{tdeg}(0, x_i) := -1$.

定义 1.1.3　设 $F = \sum_{\mu \in \mu(F)} c_\mu \cdot \mu \in \mathcal{K}[\boldsymbol{x}]$ 为多项式, 其中 $\mu(F)$ 表示 F 中项的全体, c_μ 为 F 关于项 μ 的系数. 若存在固定整数 i, 对任意 $\mu \in \mu(F)$ 都有 $\mathrm{tdeg}(\mu) = i$, 则称 F 为 i 次 *齐次多项式* (homogeneous polynomial).

对于 $\mathcal{R}$ 上关于 $x_1, \ldots, x_n$ 的任意多项式 $F = \sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$, $G = \sum_{\boldsymbol{\alpha}} b_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$, 定义加法和乘法如下.

$$F + G := \sum_{\boldsymbol{\alpha}} (a_{\boldsymbol{\alpha}} + b_{\boldsymbol{\alpha}}) \boldsymbol{x}^{\boldsymbol{\alpha}}, \quad F \cdot G := \sum_{\boldsymbol{\gamma}} c_{\boldsymbol{\gamma}} \boldsymbol{x}^{\boldsymbol{\gamma}},$$

其中 $c_{\boldsymbol{\gamma}} = \sum_{\boldsymbol{\alpha}+\boldsymbol{\beta}=\boldsymbol{\gamma}} a_{\boldsymbol{\alpha}} b_{\boldsymbol{\beta}}$.

按上述定义的加法和乘法, $\mathcal{R}$ 上关于 $x_1, \ldots, x_n$ 的所有多项式组成的集合构成带单位元的交换环, 称为 $\mathcal{R}$ 上关于 $x_1, \ldots, x_n$ 的 *多项式环* (polynomial ring), 记为 $\mathcal{R}[x_1, \ldots, x_n]$ 或 $\mathcal{R}[\boldsymbol{x}]$. 当 $n = 1$ 时, $\mathcal{R}[\boldsymbol{x}]$ 称为 *一元多项式环* (univariate polynomial ring); 当 $n > 1$ 时, $\mathcal{R}[\boldsymbol{x}]$ 称为 *多元多项式环* (multivariate polynomial ring).

全体多项式组成的集合 $\mathcal{R}[\boldsymbol{x}]$ 上除了存在自然的代数结构 (环结构) 之外, 还能赋予序结构. $\mathcal{R}[\boldsymbol{x}]$ 上序的存在性是多项式环的一个重要性质, 正因为有了序, 很多相关算法的终止性才能得到保证. 下面给出多项式环上项序的概念.

定义 1.1.4　集合 $\mathfrak{T}(\boldsymbol{x})$ 上的全序关系 $<$ 称为 *项序* (term ordering), 如果下列条件满足:

(a) 对任意 $\mu_1, \mu_2, \mu \in \mathfrak{T}(\boldsymbol{x})$, 若 $\mu_1 < \mu_2$, 则 $\mu\mu_1 < \mu\mu_2$;
(b) $<$ 为良序, 即 $\mathfrak{T}(\boldsymbol{x})$ 中任意非空子集关于 $<$ 都有最小元.

除非另有说明, 我们默认变元序为 $x_1 < \cdots < x_n$. 下面介绍 $\mathcal{R}[\boldsymbol{x}]$ 上几种常见的全序关系. 设 $\boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $\boldsymbol{x}^{\boldsymbol{\beta}} = x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathfrak{T}(\boldsymbol{x})$, 定义

(1) *字典序* (lexicographical order): $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\mathrm{lex}} \boldsymbol{x}^{\boldsymbol{\beta}}$, 如果存在 i $(1 \leqslant i \leqslant n)$ 使得

$$\alpha_j = \beta_j \ \ (i+1 \leqslant j \leqslant n) \ \text{且} \ \alpha_i < \beta_i;$$

(2) *逆字典序* (reverse lexicographical order): $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\mathrm{rlex}} \boldsymbol{x}^{\boldsymbol{\beta}}$, 如果存在 i $(1 \leqslant i \leqslant n)$ 使得

$$\alpha_j = \beta_j \ \ (1 \leqslant j \leqslant i-1) \ \text{且} \ \alpha_i > \beta_i;$$

(3) *分次字典序* (graded lexicographical order): $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\mathrm{grlex}} \boldsymbol{x}^{\boldsymbol{\beta}}$, 如果

$$\mathrm{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) < \mathrm{tdeg}(\boldsymbol{x}^{\boldsymbol{\beta}}), \ \text{或者} \ \mathrm{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \mathrm{tdeg}(\boldsymbol{x}^{\boldsymbol{\beta}}) \ \text{且} \ \boldsymbol{x}^{\boldsymbol{\alpha}} <_{\mathrm{lex}} \boldsymbol{x}^{\boldsymbol{\beta}};$$

(4) 分次逆字典序 (graded reverse lexicographical order): $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\text{grevlex}} \boldsymbol{x}^{\boldsymbol{\beta}}$, 如果

$$\text{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) < \text{tdeg}(\boldsymbol{x}^{\boldsymbol{\beta}}), \text{ 或者 } \text{tdeg}(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \text{tdeg}(\boldsymbol{x}^{\boldsymbol{\beta}}) \text{ 且 } \boldsymbol{x}^{\boldsymbol{\alpha}} <_{\text{rlex}} \boldsymbol{x}^{\boldsymbol{\beta}}.$$

引理 1.1.5 设 $<$ 为 $\mathfrak{T}(\boldsymbol{x})$ 上的全序关系, 则 $<$ 为良序当且仅当 $\mathfrak{T}(\boldsymbol{x})$ 中任意严格递减序列都终止.

证 假定 $<$ 不是良序, 则存在子集 $\mathcal{T} \subseteq \mathfrak{T}(\boldsymbol{x})$, 该子集没有最小元. 现取 $T_1 \in \mathcal{T}$. 因为 T_1 不是最小元, 所以存在 $T_2 \in \mathcal{T}$ 使得 $T_1 > T_2$, 且 T_2 也不是最小元. 于是又存在 $T_3 \in \mathcal{T}$ 使得 $T_2 > T_3$, 且 T_3 不是最小元. 如此下去, 我们可以得到无限严格递减序列 $T_1 > T_2 > T_3 > \cdots$.

反之, 若存在无限严格递减序列 $T_1 > T_2 > \cdots$, 则令 $\mathcal{T} = \{T_1, T_2, \ldots\}$. 这时 $\mathcal{T}$ 没有最小元, 从而 $<$ 不是良序. □

上述引理常常用来证明多项式算法的终止性.

定理 1.1.6 全序关系 $<_{\text{lex}}, <_{\text{grlex}}$ 和 $<_{\text{grevlex}}$ 均为项序.

证 我们只证明 $<_{\text{lex}}$ 为项序, 而将 $<_{\text{grlex}}$ 和 $<_{\text{grevlex}}$ 为项序的证明留作习题.

设 $\boldsymbol{x}^{\boldsymbol{\alpha}} <_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\beta}}$, 即存在 i $(1 \leqslant i \leqslant n)$ 使得

$$\alpha_j = \beta_j \ (i+1 \leqslant j \leqslant n) \text{ 且 } \alpha_i < \beta_i.$$

因此

$$\alpha_j + \gamma_j = \beta_j + \gamma_j \ (i+1 \leqslant j \leqslant n) \text{ 且 } \alpha_i + \gamma_i < \beta_i + \gamma_i,$$

从而 $\boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{x}^{\boldsymbol{\gamma}} <_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\beta}}\boldsymbol{x}^{\boldsymbol{\gamma}}$.

下面利用反证法证明 $<_{\text{lex}}$ 为良序. 假设 $<_{\text{lex}}$ 不是良序, 根据引理 1.1.5, $\mathfrak{T}(\boldsymbol{x})$ 中存在无限严格递减序列

$$\boldsymbol{x}^{\boldsymbol{\alpha}_1} >_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\alpha}_2} >_{\text{lex}} \boldsymbol{x}^{\boldsymbol{\alpha}_3} >_{\text{lex}} \cdots. \tag{1.1}$$

根据字典序的定义, $\boldsymbol{x}^{\boldsymbol{\alpha}_i}$ 关于 x_n 的次数形成了非负整数集 $\mathbb{Z}_{\geqslant 0}$ 上的递减序列

$$\boldsymbol{\alpha}_1(n) \geqslant \boldsymbol{\alpha}_2(n) \geqslant \boldsymbol{\alpha}_3(n) \geqslant \cdots, \tag{1.2}$$

这里 $\boldsymbol{\alpha}_i(k)$ 表示向量 $\boldsymbol{\alpha}_i$ 的第 k 个分量. 由于 $\mathbb{Z}_{\geqslant 0}$ 为良序集, 序列 (1.2) 必终止, 即存在正整数 l 使得

$$\boldsymbol{\alpha}_l(n) = \boldsymbol{\alpha}_{l+1}(n) = \boldsymbol{\alpha}_{l+2}(n) = \cdots.$$

考虑 $\boldsymbol{x}^{\boldsymbol{\alpha}_i}$ $(i \geqslant l)$ 关于 x_{n-1} 的次数, 我们得到递减序列

$$\boldsymbol{\alpha}_l(n-1) \geqslant \boldsymbol{\alpha}_{l+1}(n-1) \geqslant \boldsymbol{\alpha}_{l+2}(n-1) \geqslant \cdots.$$

同理可知, 存在 $s \geqslant l$ 使得

$$\boldsymbol{\alpha}_s(n-1) = \boldsymbol{\alpha}_{s+1}(n-1) = \boldsymbol{\alpha}_{s+2}(n-1) = \cdots,$$

$$\boldsymbol{\alpha}_s(n) = \boldsymbol{\alpha}_{s+1}(n) = \boldsymbol{\alpha}_{s+2}(n) = \cdots.$$

以此类推, 考虑其余的变量, 最后得到整数 t, 使得当 $i \geqslant t$ 时, $\boldsymbol{x}^{\boldsymbol{\alpha}_i}$ 关于每个变元的次数均相等, 即 (1.1) 有限, 矛盾. □

这里需要注意, 逆字典序 $<_{\mathrm{rlex}}$ 并不是项序. 例如, 考虑项集 $\mathcal{T} = \{x_1^i : i \in \mathbb{Z}_{\geqslant 0}\}$, 我们可得严格递减序列

$$x_1^0 >_{\mathrm{rlex}} x_1^1 >_{\mathrm{rlex}} x_1^2 >_{\mathrm{rlex}} \cdots.$$

根据引理 1.1.5 可知, $<_{\mathrm{rlex}}$ 不是良序.

我们将优先按项的全次数进行排序的项序称为 **分次序** (graded order). 例如, 分次字典序和分次逆字典序均为分次序.

设 $F \in \mathcal{R}[\boldsymbol{x}]$, 则 F 的单项式关于加法可以任意交换. 但是对特定的项序, F 的单项式可以从大到小排列, 于是多项式的写法就唯一确定了.

例 1.1.7　设变元序为 $x < y < z$. 多项式

$$x^2yz + 2\,x^3yz + 3\,xy^3 + 4\,y^2z^2 \in \mathbb{Z}[x, y, z]$$

可按字典序、分次字典序和分次逆字典序从大到小排列:

- 字典序: $4\,y^2z^2 + 2\,x^3yz + x^2yz + 3\,xy^3$;
- 分次字典序: $2\,x^3yz + 4\,y^2z^2 + x^2yz + 3\,xy^3$;
- 分次逆字典序: $2\,x^3yz + 4\,y^2z^2 + 3\,xy^3 + x^2yz$.

设 $F = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}}\,\boldsymbol{x}^{\boldsymbol{\alpha}}$ 为 $\mathcal{R}[\boldsymbol{x}]$ 中的非零多项式, $<$ 为 $\mathcal{R}[\boldsymbol{x}]$ 上的项序, 称

$$\mathrm{ht}_<(F) := \max\nolimits_<\{\mu : \mu \in \mathfrak{T}(F)\}$$

为 F 关于 $<$ 的 **首项** (head term),

$$\mathrm{hc}_<(F) := \mathrm{coef}(F, \mathrm{ht}_<(F))$$

为 F 关于 $<$ 的 **首项系数** (head coefficient), 而

$$\mathrm{hm}_<(F) := \mathrm{hc}_<(F) \cdot \mathrm{ht}_<(F)$$

为 F 关于 $<$ 的 **首单项式** (head monomial). 在不引起混淆的情况下, 上述记号分别简写为 $\mathrm{ht}(F)$, $\mathrm{hc}(F)$ 和 $\mathrm{hm}(F)$. 若 $\mathrm{hc}(F) = 1$, 则称 F 为 **首一** (monic) 多项式.