数学机械化丛书

消去法及其应用

王东明 著

科学出版社
www.sciencep.com

内 容 简 介

本书系统介绍多项式系统零点分解的消去算法. 这些算法能将任意多元多项式系统分解为三角系统、正则系统、简单系统、具有投影特性的三角系统和不可约三角系统. 各种三角型系统理论上性质殊异，计算上难易匪同，应用上则各有所长. 书中还简述基于结式和格罗布讷基的消去算法，讨论代数簇的等维与不可约分解以及多项式理想的准素分解，并介绍符号消去法的若干应用，包括代数方程求解、几何定理求证、多项式因子分解和微分系统的定性分析.

本书可供有关科研和工程技术人员参考，也可作为高等院校数学和计算机科学系高年级学生及研究生的教学参考书.

图书在版编目(CIP)数据

消去法及其应用/王东明著. —北京：科学出版社，2002.8
(数学机械化丛书/吴文俊主编)
ISBN 7-03-010560-5

Ⅰ. 消… Ⅱ. 王… Ⅲ. 消去法 Ⅳ. O241.6

中国版本图书馆 CIP 数据核字(2002)第 050262 号

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
源海印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2002 年 8 月第 一 版 开本：B5(720×1000)
2002 年 8 月第一次印刷 印张：20 1/4
印数：1—2 000 字数：350 000

定价：48.00 元

(如有印装质量问题，我社负责调换(新欣))

目　录

第一章　多项式运算与零点

我们首先介绍一些有关多元多项式的基本概念、运算和性质，它们在以后各章中将会用到. 大部分结果的证明见诸于标准代数教科书，因而被略去. 如果参考文献没有给出，建议读者查阅 [71, 72] 和 [41].

1.1 多　项　式

设 $\mathcal{R}$ 为一环，$x_1, x_2, \cdots, x_n$ 为 n 个不属于 $\mathcal{R}$ 的不同符号，称之为 *未定元*, *未知数* 或 *变元*. 我们常将 $x_1, x_2, \cdots, x_i$ 或 $(x_1, x_2, \cdots, x_i)$ 写成 $\boldsymbol{x}_i$, 且命 $\boldsymbol{x} = \boldsymbol{x}_n$. 对于 n 个非负整数 $i_1, i_2, \cdots, i_n$, 我们可作形式幂积

$$\mu = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

并称其为 *项*.

又设 a 为 $\mathcal{R}$ 中的元素，即 $a \in \mathcal{R}$. 称形如

$$\alpha = a\mu = a x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

的表达式为 *单项式*. 我们有时将它写成 $\alpha = a\boldsymbol{x}^{\boldsymbol{i}}$, 其中

$$\boldsymbol{x} = (x_1, \cdots, x_n), \quad \boldsymbol{i} = (i_1, \cdots, i_n).$$

上面的 a 称为 α 的 *系数*. 若 $a \neq 0$, 则说单项式 α 是 *非零的*.

对于 n 元组 $\boldsymbol{i} = (i_1, \cdots, i_n)$, 它的第 l 个分量 i_l 用 $\mathrm{op}(l, \boldsymbol{i})$ 来记. 任意两个由非负整数构成的 n 元组 $\boldsymbol{i}$ 与 $\boldsymbol{j}$ 称为 *不同的*, 如果存在 l $(1 \leq l \leq n)$ 使 $\mathrm{op}(l, \boldsymbol{i}) \neq \mathrm{op}(l, \boldsymbol{j})$. 两个项 $\boldsymbol{x}^{\boldsymbol{i}}$ 与 $\boldsymbol{x}^{\boldsymbol{j}}$ 称为 *不同的*, 如果 $\boldsymbol{i}$ 和 $\boldsymbol{j}$ 不同. 设 $a_1, \cdots, a_t \in \mathcal{R}$, 且 $\boldsymbol{i}_1, \cdots, \boldsymbol{i}_t$ 为 t 个互不相同、由非负整数构成的 n 元组. 我们称有限和

$$P = \sum_{l=1}^{t} a_l \boldsymbol{x}^{\boldsymbol{i}_l} \tag{1.1.1}$$

是系数 $a_1, \cdots, a_t$ 在 $\mathcal{R}$ 中未定元为 $\boldsymbol{x}$ 的 *多项式*. 如果 P 中的所有单项式都为 0, 即 $a_1 = \cdots = a_t = 0$, 那么多项式 P 为 0. 由于单项式 0 可以任意加到一个多项式上或从中抹去，我们假定任意非零多项式 P 中的所有单项式都不

此为试读，需要完整PDF请访问：www.ertongbook.com

为零，即 $a_1 \neq 0, \cdots, a_t \neq 0$，并称 t 为 P 的**项数**. 若 $P \in \mathcal{R}$，则称 P 为**常数**. 今设 $\boldsymbol{x}^{\boldsymbol{i}}$ 为项. 如果存在 $a \in \mathcal{R}$ 且 $a \neq 0$ 使得单项式 $a\boldsymbol{x}^{\boldsymbol{i}}$ 在 P 中出现，则称 a 为 P 关于 $\boldsymbol{x}^{\boldsymbol{i}}$ 的**系数**，并用 $\mathrm{coef}(P, \boldsymbol{x}^{\boldsymbol{i}})$ 来表示. 否则，$\mathrm{coef}(P, \boldsymbol{x}^{\boldsymbol{i}})$ 定义为 0.

设 P 为一非零多项式，如 (1.1.1) 所示，而 x_k 为任一变元. 我们将 P 关于 x_k 的**次数**记为

$$\deg(P, x_k) \triangleq \max_{1 \leq l \leq t} \mathrm{op}(k, \boldsymbol{i}_l).$$

上式中 $\triangleq$ 读作“定义为”. 为方便起见，我们又定义 $\deg(0, x_k) = -1$. P 的**全次数**由下式来定义：

$$\mathrm{tdeg}(P) \triangleq \max_{1 \leq l \leq t} \sum_{k=1}^{n} \mathrm{op}(k, \boldsymbol{i}_l).$$

所有项都具有相同全次数的多项式称为是**齐次的**.

例 1.1.1　下面是一个 $x_1, \cdots, x_4$ 的整系数多项式：

$$F_1 = x_4^2 + x_1 x_4^2 - x_2 x_4 - x_1 x_2 x_4 + x_1 x_2 + 3\, x_2.$$

不难看出

$$\begin{aligned} &\mathrm{coef}(F_1, x_1 x_2 x_4) = -1, \quad \mathrm{coef}(F_1, x_2 x_4^3) = 0, \\ &\deg(F_1, x_2) = 1, \quad \deg(F_1, x_4) = 2, \\ &\mathrm{tdeg}(F_1) = 3, \end{aligned}$$

且 F_1 不是齐次的.

设

$$Q = \sum_{l=1}^{s} b_l \boldsymbol{x}^{\boldsymbol{j}_l}$$

为任一其他多项式. 定义 P 与 Q 的**和**为

$$P + Q \triangleq \sum_{l=1}^{r} c_l \boldsymbol{x}^{\boldsymbol{k}_l},$$

其中 $\boldsymbol{k}_1, \cdots, \boldsymbol{k}_r$ 是 $\boldsymbol{i}_1, \cdots, \boldsymbol{i}_t, \boldsymbol{j}_1, \cdots, \boldsymbol{j}_s$ 中所有互不相同的 n 元组，

$$c_l = \mathrm{coef}(P, \boldsymbol{x}^{\boldsymbol{k}_l}) + \mathrm{coef}(Q, \boldsymbol{x}^{\boldsymbol{k}_l}), \quad l = 1, \cdots, r.$$

构造 n 元组

$$\boldsymbol{k}_{\boldsymbol{i}_u\boldsymbol{j}_v} = (\mathrm{op}(1,\boldsymbol{i}_u)+\mathrm{op}(1,\boldsymbol{j}_v),\cdots,\mathrm{op}(n,\boldsymbol{i}_u)+\mathrm{op}(n,\boldsymbol{j}_v)),$$
$$u=1,\cdots,t;\ v=1,\cdots,s,$$

并令 $\boldsymbol{k}_1,\cdots,\boldsymbol{k}_r$ 为它们中所有互不相同者. 定义 P 与 Q 的积为

$$PQ \triangleq \sum_{l=1}^{r} c_l \boldsymbol{x}^{\boldsymbol{k}_l},$$

其中

$$c_l = \sum_{\boldsymbol{k}_{\boldsymbol{i}_u\boldsymbol{j}_v}=\boldsymbol{k}_l} a_u b_v,\quad l=1,\cdots,r.$$

定理 1.1.1 在上面所定义的加法与乘法之下，所有系数在 $\mathcal{R}$ 中变元为 $\boldsymbol{x}$ 的多项式构成一环.

将系数在 $\mathcal{R}$ 中 n 个变元 $x_1,\cdots,x_n$ 的多项式构成的环记为 $\mathcal{R}[x_1,\cdots,x_n]$，或简记为 $\mathcal{R}[\boldsymbol{x}]$. 它也称为由 $\mathcal{R}$ 通过添加 $\boldsymbol{x}$ 导出的多项式环. 如果 $\mathcal{R}$ 是交换环，那么 $\mathcal{R}[\boldsymbol{x}]$ 也是. 特别在 $\mathcal{R}$ 为整数环 $\mathbb{Z}$ 时，$\mathcal{R}[\boldsymbol{x}]$ 成为整系数多项式环.

定理 1.1.2 如果 $\mathcal{R}$ 是一整环，那么 $\mathcal{R}[\boldsymbol{x}]$ 也是.

记住 n 总表示变元 $\boldsymbol{x}$ 的个数. 我们说多项式是一元的，二元的或多元的依据 $n=1$, $n=2$ 或 $n\geq 2$. 相应地，多项式环 $\mathcal{R}[\boldsymbol{x}]$ 亦被称为一元的，二元的或多元的，视 n 为 1, 2 或 ≥ 2 而定. 由 $\mathcal{R}$ 通过添加未定元 $\boldsymbol{x}$ 而导出的多元多项式环 $\mathcal{R}[\boldsymbol{x}]$ 也可视为由 $\mathcal{R}$ 通过依次添加未定元 $x_1,x_2,\cdots,x_n$ 而导出的环 $\mathcal{R}[x_1][x_2]\cdots[x_n]$.

定理 1.1.3 多项式环 $\mathcal{R}[x_1]\cdots[x_n]$, $\mathcal{R}[x_{q_1}]\cdots[x_{q_n}]$ 与 $\mathcal{R}[\boldsymbol{x}]$ 是同构的，这里 $q_1\cdots q_n$ 为 $1\cdots n$ 的任一置换.

因此，一个多元多项式 $P\in\mathcal{R}[\boldsymbol{x}]$ 也可理解为关于某一固定变元，譬如 x_n，系数在 $\mathcal{R}[x_1,\cdots,x_{n-1}]$ 中的一元多项式. 换句话说，可视 P 为 $\mathcal{R}[\boldsymbol{x}_{n-1}][x_n]$ 中的元素.

多项式组是由 $\mathcal{R}[\boldsymbol{x}]$ 中有限多个非零多项式所构成的集合. 说到多项式系统，我们是指一对多项式组 $[\mathbb{P},\mathbb{Q}]$. 作为一般性的约定，在本书中我们用大写字母如 P,Q,F 表示多项式、宽体字母如 $\mathbb{P},\mathbb{Q},\mathbb{T}$ 表示多项式组，哥特体字

母如 $\mathfrak{P},\mathfrak{T},\mathfrak{S}$ 表示多项式系统，希腊字母如 Ψ 表示由多项式系统构成的集合或序列.

以下，我们将未定元排成固定的次序：

$$x_1 \prec \cdots \prec x_n.$$

定义 1.1.1　对于任意两个不同的项 $\boldsymbol{x}^{\boldsymbol{i}}$ 与 $\boldsymbol{x}^{\boldsymbol{j}}$，其中

$$\boldsymbol{i} = (i_1, \cdots, i_n), \quad \boldsymbol{j} = (j_1, \cdots, j_n),$$

我们说 $\boldsymbol{x}^{\boldsymbol{i}}$ 排在 $\boldsymbol{x}^{\boldsymbol{j}}$ 之前 或 $\boldsymbol{x}^{\boldsymbol{j}}$ 排在 $\boldsymbol{x}^{\boldsymbol{i}}$ 之后，记作

$$\boldsymbol{x}^{\boldsymbol{i}} \prec \boldsymbol{x}^{\boldsymbol{j}} \quad 或 \quad \boldsymbol{x}^{\boldsymbol{j}} \succ \boldsymbol{x}^{\boldsymbol{i}},$$

如果存在 k $(1 \leq k \leq n)$，使得

$$i_k < j_k, \quad 且 \quad i_l = j_l \ 对 \ k < l \leq n \ 成立.$$

在 "$\prec$" 之下，所有关于 $\boldsymbol{x}$ 的项以及 $\mathcal{R}[\boldsymbol{x}]$ 中任一非零多项式的单项式都可排列成序. 我们称 "$\prec$" 为项或单项式的 *纯字典序*.

事实上，$\mathcal{R}[\boldsymbol{x}]$ 中任意非零多项式都可以写成 (1.1.1) 的形式，其中

$$a_1 \neq 0, \cdots, a_t \neq 0, \quad a_i \in \mathcal{R},$$
$$\boldsymbol{x}^{\boldsymbol{i}_1} \succ \cdots \succ \boldsymbol{x}^{\boldsymbol{i}_t}.$$

这时，我们称 $\boldsymbol{x}^{\boldsymbol{i}_1}$ 为 P 的 *导项*，$a_1\boldsymbol{x}^{\boldsymbol{i}_1}$ 为 P 的 *导项式*，a_1 为 P 的 *导系数*，分别记为 $\mathrm{lt}(P)$, $\mathrm{lm}(P)$ 与 $\mathrm{lc}(P)$. 在 $P \notin \mathcal{K}$ 时，我们称使得

$$\deg(P, x_p) > 0 \ 或者等价地 \ \deg(\boldsymbol{x}^{\boldsymbol{i}_1}, x_p) > 0$$

成立的最大下标 p 为 P 的 *类*，x_p 为 P 的 *导元*，$\deg(P, x_p)$ 为 P 的 *导次数*，分别记作 $\mathrm{cls}(P)$, $\mathrm{lv}(P)$ 和 $\mathrm{ldeg}(P)$. 用符号表示，我们有

$$\mathrm{lv}(P) = x_{\mathrm{cls}(P)}, \quad \mathrm{ldeg}(P) = \deg(P, \mathrm{lv}(P)).$$

对任意 $P \in \mathcal{K}$ 但 $P \neq 0$，我们将 P 的 *类*，*导元* 与 *导次数* 分别定义为 0, x_0 与 0，这里 x_0 为一新变元，其序排在 x_1 之前 (即 $x_0 \prec x_1$).

设 P 为一多项式，其类 $\mathrm{cls}(P) = p > 0$. 那么可视 P 为 x_p 的一元多项式. 对任一其他多项式 $Q \in \mathcal{R}[\boldsymbol{x}]$，如果 $\deg(Q, x_p) < \mathrm{ldeg}(P)$，则称 Q 对 P 是 *约化的*. P 关于 x_p 的导系数 $\mathrm{lc}(P, x_p)$ 称为 P 的 *初式*，记作 $\mathrm{ini}(P)$，它是 $x_1, \cdots, x_{p-1}$ 的多项式. 定义任意 $P \in \mathcal{K}$ 的 *初式* 为其本身. 对任意多项式组 $\mathbb{P}$，我们定义

$$\mathrm{ini}(\mathbb{P}) \triangleq \{\mathrm{ini}(P) \colon \ P \in \mathbb{P}\}.$$

例 1.1.2 按照变元序 $x_1 \prec \cdots \prec x_4$, 例 1.1.1 中的多项式 F_1 可重写为

$$\begin{aligned} F_1 &= x_1x_4^2 + x_4^2 - x_1x_2x_4 - x_2x_4 + x_1x_2 + 3\,x_2 \\ &= (x_1+1)\,x_4^2 + (-x_1x_2 - x_2)\,x_4 + x_1x_2 + 3\,x_2. \end{aligned}$$

由此可见

$$\begin{aligned} &\mathrm{lc}(F_1) = 1, \\ &\mathrm{lt}(F_1) = \mathrm{lt}(F_1) = x_1x_4^2, \\ &\mathrm{cls}(F_1) = 4, \quad \mathrm{lv}(F_1) = x_4, \\ &\mathrm{ldeg}(F_1) = 2, \quad \mathrm{ini}(F_1) = x_1 + 1. \end{aligned}$$

多项式

$$F_2 = x_1x_4 + x_3 - x_1x_2$$

对 F_1 是约化的, 但 F_1 对 F_2 不是约化的.

1.2 最大公因子、伪除与多项式余式序列

以下将 $\mathcal{R}$ 限定为 **唯一析因整环**, 即带有单位元的交换环. 这时, 对 $\mathcal{R}$ 中的任意非零元素 a 和 b 都有 $ab \neq 0$, 并且每个 $a \in \mathcal{R}$ 或为 "可逆元" 或有如下形式的 "唯一" 表示:

$$a = up_1 \cdots p_t, \quad t \geq 1,$$

式中 $p_1, \cdots, p_t$ 为 **"素数"**, u 为一可逆元. 每个域都是唯一析因整环, 其中每个非零元素都是可逆元, 但无素数. 若 $\mathcal{R}$ 被假定为唯一析因整环, 那么根据定理 1.1.2 $\mathcal{R}[\boldsymbol{x}]$ 也是唯一析因整环.

设 F 与 G 为 $\mathcal{R}[\boldsymbol{x}]$ 中的多项式, 且 $G \neq 0$. 我们说 G **整除** F 或 F **能被** G **除尽**, 记作 $G \mid F$, 如果存在商多项式 $Q \in \mathcal{R}[\boldsymbol{x}]$ 使 $F = QG$. 这时, 称 G **为** F **的因子**, F **为** G **的倍数**.

定义 1.2.1 设 $P_1, \cdots, P_s$ 为 $\mathcal{R}[\boldsymbol{x}]$ 中不全为 0 的多项式. 如果多项式 $G \in \mathcal{R}[\boldsymbol{x}]$ 整除所有 $P_1, \cdots, P_s$ 并且 $P_1, \cdots, P_s$ 的每个公因子都整除 G, 则称 G 为 $P_1, \cdots, P_s$ **的最大公因子**.

如果 $P_1, \cdots, P_s$ 都整除某一多项式 $L \in \mathcal{R}[\boldsymbol{x}]$ 且 L 整除 $P_1, \cdots, P_s$ 的每个公倍数, 则称 L 为 $P_1, \cdots, P_s$ **的最小公倍数**.

该定义中的多项式 G 是不唯一的：对任意可逆元 a, aG 也是最大公因子. 但根据唯一析因整环的性质，任意两个最大公因子只相差一个可逆元因子. 所以，可将 $P_1,\cdots,P_s$ 的所有最大公因子看作是恒同的. 对最小公倍数也是如此. 令 $\mathbb{P}=\{P_1,\cdots,P_s\}$.

$$\gcd(\mathbb{P})=\gcd(P_1,\cdots,P_s)\quad 与\quad \operatorname{lcm}(\mathbb{P})=\operatorname{lcm}(P_1,\cdots,P_s)$$

分别表示 $P_1,\cdots,P_s$ 的最大公因子与最小公倍数.

例 1.2.1　考虑多项式

$$G_1=3x_4^2-3x_2x_4+6x_1x_4-3x_3x_4+3x_2x_3-6x_1x_3,$$
$$G_2=6x_4^2+15x_1x_2x_4-6x_3x_4-15x_1x_2x_3.$$

可以验证 $3x_3-3x_4$ 整除 G_1 与 G_2. 实际上，x_4-x_3 (乘上任一常数) 是 G_1 和 G_2 在 $\mathbb{Q}[x_1,\cdots,x_4]$ 中的最大公因子，这里 $\mathbb{Q}$ 表示有理数域.

设 F 为 $\mathcal{R}[\boldsymbol{x}]$ 中的多项式，而 x_k 为一固定变元. 作为 x_k 的多项式，F 可以写成

$$F=F_0x_k^m+F_1x_k^{m-1}+\cdots+F_m,$$
$$F_i\in\mathcal{R}[x_1,\cdots,x_{k-1},x_{k+1},\cdots,x_n],$$

这里 $m=\deg(F,x_k)$. 上式中，F_{m-i} 称为 F 关于 x_k^i 的系数，记作 $\operatorname{coef}(F,x_k^i)$. 特别 F_0 是 F 关于 x_k 的导系数，记作 $\operatorname{lc}(F,x_k)$. 于是

$$\operatorname{lc}(F,x_k)=\operatorname{coef}(F,x_k^{\deg(F,x_k)}).$$

多项式 $F-F_0x_k^m$ 称为 F 关于 x_k 的尾式，记作 $\operatorname{red}(F,x_k)$. 在 $x_k=\operatorname{lv}(F)$ 时，x_k 将从 $\operatorname{red}(F,x_k)$ 中略去. 用符号来表示，我们有

$$\operatorname{lc}(F,x_k)\triangleq F_0,$$
$$\operatorname{red}(F,x_k)\triangleq F_1x_k^{m-1}+\cdots+F_m,$$
$$\operatorname{red}(F)\triangleq\operatorname{red}(F,\operatorname{lv}(F)).$$

$F_0,\cdots,F_m$ 的最大公因子 —— 视作 $\mathcal{R}[x_1,\cdots,x_{k-1},x_{k+1},\cdots,x_n]$ 中的多项式 —— 称为 F 关于 x_k 的容度，记为 $\operatorname{cont}(F,x_k)$. 如果 $\operatorname{cont}(F,x_k)$ 是 $\mathcal{R}$ 中的可逆元，则说 F 关于 x_k 是本原的. 对任意非零多项式 F, 称 $F/\operatorname{cont}(F,x_k)$ 为 F 关于 x_k 的本原部分，记作 $\operatorname{pp}(F,x_k)$; 于是 F 可以写成

$$F=\operatorname{cont}(F,x_k)\cdot\operatorname{pp}(F,x_k).$$

引理 1.2.1 (高斯引理) 唯一析因整环上本原多项式的积仍是本原的.

设 $F \neq 0$ 且 $m = \deg(F, x_k)$ 如上, 而 G 为任一其他多项式, 它关于 x_k 的次数为 l. 视为 x_k 的多项式, 用 F 对 G 作伪除, 我们有如下伪除算法. 命 $R = G$; 重复下面的过程直至 $r = \deg(R, x_k) < m$:

$$R \leftarrow F_0 R - R_0 x_k^{r-m} F,$$

其中 $R_0 = \mathrm{lc}(R, x_k)$. 由于 r 在每个循环中都严格下降, 该程序必定终止. 最后得到两个 $\mathcal{R}[\boldsymbol{x}]$ 中的多项式 Q 与 R 满足下列关系:

$$I^q G = QF + R, \tag{1.2.1}$$

这里

$$I = \mathrm{lc}(F, x_k), \quad q = \max(l - m + 1, 0),$$
$$\deg(R, x_k) < m, \quad \deg(Q, x_k) = \max(l - m, -1).$$

在 $m = 0$ 时, $R = 0$, 而 $Q = F^l G$.

我们称表达式 (1.2.1) 为伪余公式; Q 为 G 对 F 关于 x_k 的伪商, R 为 G 对 F 关于 x_k 的伪余式, 分别记为 $\mathrm{pquo}(G, F, x_k)$ 与 $\mathrm{prem}(G, F, x_k)$. 实际上, (1.2.1) 式中的多项式 Q 和 R 由 F 与 G 唯一确定. 现将这一事实叙述如下供以后使用.

命题 1.2.2 设多项式 F, G, I, Q, R 及整数 q 如上. 如果 Q' 与 R' 为 $\mathcal{R}[\boldsymbol{x}]$ 中的多项式, 使得

$$I^q G = Q'F + R',$$

则 $Q' = Q$, 且 $R' = R$.

证 见 [41] 中 402 和 407 页. □

通过用 F 对 G (关于 x_k) 作伪除获得 Q 与 R 的过程称为伪约化. 它是本书中许多算法的基础, 因而将在以后各章中担任关键角色. 由于这一原因, 我们将计算伪余式的过程表述成如下形式的算法.

算法 prem: $R \leftarrow \mathrm{prem}(G, F, x)$. 任给多项式 $G, F \in \mathcal{R}[\boldsymbol{x}]$ 及变元 $x \in \{\boldsymbol{x}\}$, 本算法计算 G 对 F 关于 x 的伪余式 R.

P1. 命 $R \leftarrow G$, $r \leftarrow \deg(R, x)$, $H \leftarrow F$, $h \leftarrow \deg(H, x)$, $d \leftarrow r - h + 1$.

此为试读,需要完整PDF请访问: www.ertongbook.com

P2. 若 $h \le r$, 则命 $L \leftarrow \mathrm{lc}(H,x)$, $H \leftarrow \mathrm{red}(H,x)$; 否则命 $L \leftarrow 1$.

P3. 重复下列步骤直至[①] $r < h$ 或 $R = 0$:

P3.1. 计算 $T \leftarrow x^{r-h}\mathrm{lc}(R,x)H$.

P3.2. 命 $R \leftarrow \mathrm{red}(R,x)$.

P3.3. 计算 $R \leftarrow LR - T$, 且命 $r \leftarrow \deg(R,x)$, $d \leftarrow d-1$.

P4. 输出 $R \leftarrow L^d R$.

在 $x_k = \mathrm{lv}(F)$ 时, 变元 x_k 将从 $\mathrm{prem}(G,F,x_k)$ 中略去. 对任一多项式组 $\mathbb{Q}$, $\mathrm{prem}(\mathbb{Q},F)$ 表示 $\{\mathrm{prem}(Q,F)\colon\ Q \in \mathbb{Q}\}$. 下面给出用作演示伪除过程的简单例子和较复杂的计算例子.

例 1.2.2　考虑多项式

$$F = xy^2 + 1, \quad G = 2y^3 - y^2 + x^2 y.$$

关于 y, 相应的 R 和 Q 可如下计算:

$$\begin{array}{rrr}
 & 2xy - x & = Q \\
xy^2+1 & \overline{)\ 2y^3 - y^2 + x^2 y} & G \\
 & 2xy^3 - xy^2 + x^3 y & xG \\
 & \underline{-(2xy^3 + 2y)} & -2yF \\
 & -xy^2 + x^3 y - 2y & \bar{R} \\
 & -x^2 y^2 + x^4 y - 2xy & x\bar{R} \\
 & \underline{-(-x^2 y^2 - x)} & xF \\
 & x^4 y - 2xy + x & = R.
\end{array}$$

由此即得

$$x^2 G = (2xy - x)F + x^4 y - 2xy + x. \tag{1.2.2}$$

可将公式 (1.2.1) 中的整数 q 定得尽可能小, 只要伪除过程不给 Q 和 R 引进分式即可. 对 prem 的某些应用, 步骤 P4 中的乘式 L^d 可被略去. 在 (1.2.2) 中, 也可取 $q = 1$ 代替 2 使其简化为

$$xG = (2y - 1)F + x^3 y - 2y + 1.$$

① 一旦条件 "$r < h$ 或 $R = 0$" 满足便停止执行.

在实际计算时，选取最小的 q 对控制伪余式的扩大乃至关重要. 而且，可以通过用 $I_1^{q_1}\cdots I_e^{q_e}$ 替代 I^q 对公式 (1.2.1) 加以修正，这里 $I_1,\cdots,I_e$ 是 I 的所有互异不可约因子 (关于不可约的定义，参见 1.4 节)，并取最小的 $q_1,\cdots,q_e$ 使相应的伪余公式仍然成立. 对于这一修正，R 的确定需要附加计算，因而在每步中占用更多的时间. 然而，修正后的伪除法可以避免一些多余的因子而使后面的计算受益.

例 1.2.3 考虑例 1.1.1, 1.1.2 与 1.2.1 中给出的多项式 F_1,F_2,G_1,G_2. 用 F_2 对 F_1 关于 x_4 作伪除可得下面的伪余公式:

$$x_1^2F_1=QF_2+R,$$

其中

$$\begin{aligned}Q&=x_1^2x_4+x_1x_4-x_1x_3-x_3,\\ R&=\operatorname{prem}(F_1,F_2)=x_1x_3^2+x_3^2-x_1^2x_2x_3-x_1x_2x_3+x_1^3x_2+3\,x_1^2x_2.\end{aligned}$$

也可以验证

$$\begin{aligned}G_3&=\operatorname{prem}(G_1,G_2,x_4)\\ &=-45\,x_1x_2x_4-18\,x_2x_4+36\,x_1x_4+45\,x_1x_2x_3+18\,x_2x_3-36\,x_1x_3,\\ G_3'&=\operatorname{prem}(F_1,G_2,x_4)\\ &=6\,x_1x_3x_4+6\,x_3x_4-15\,x_1^2x_2x_4-21\,x_1x_2x_4-6\,x_2x_4+15\,x_1^2x_2x_3\\ &\quad+15\,x_1x_2x_3+6\,x_1x_2+18\,x_2,\end{aligned}$$

以及

$$\begin{aligned}&\operatorname{cont}(F_1,x_4)=1,\\ &\operatorname{cont}(G_1,x_4)=\operatorname{cont}(G_2,x_4)=\operatorname{cont}(G_3',x_4)=3,\\ &\operatorname{cont}(G_3,x_4)=45\,x_1x_2+18\,x_2-36\,x_1,\\ &\operatorname{pp}(G_3,x_4)=x_3-x_4.\end{aligned}$$

两个多项式 $F,G\in\mathcal{R}[x]$ 称为 相似的，记作 $F\backsim G$，如果存在 $a,b\in\mathcal{R}$，$ab\neq0$，使得 $aF=bG$.

将多项式 G 和 F 更名为 P_1 和 P_2，并假定 $\deg(P_1,x_k)\geq\deg(P_2,x_k)$. 作多项式序列

$$P_1,P_2,P_3,\cdots,P_r$$

使得

$$P_i\backsim\operatorname{prem}(P_{i-2},P_{i-1},x_k),\quad i=3,\cdots,r$$

且

$$\operatorname{prem}(P_{r-1}, P_r, x_k) = 0.$$

这样的序列称为 G 和 F 关于 x_k 的 *多项式余式序列*.

从伪余公式及多项式余式序列的构造可以看出

$$\gcd(P_1, P_2), \gcd(P_2, P_3), \cdots, \gcd(P_{r-1}, P_r), P_r$$

之间只相差 $\mathcal{R}[x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n]$ 中的多项式因子. 如果 P_1 和 P_2 关于 x_k 都是本原的, 则

$$\gcd(G, F) = \gcd(P_1, P_2) = \operatorname{pp}(P_r, x_k).$$

另一方面, 容易看出

$$\gcd(G, F) = \gcd(\operatorname{cont}(G, x_k), \operatorname{cont}(F, x_k)) \cdot \gcd(\operatorname{pp}(G, x_k), \operatorname{pp}(F, x_k))$$

对任意多项式 G 和 F 成立. 因而, 构造多项式余式序列为求两个多项式的最大公因子提供了一种手段; 而求多个多项式的最大公因子可以很容易地归结到两个多项式的情形.

例 1.2.4　考虑例 1.2.1 中的多项式. 经算法 prem 计算表明

$$\begin{aligned}
&\operatorname{prem}(G_2, G_3, x_4) = 0,\\
G_4' &= \operatorname{prem}(G_2, G_3', x_4)\\
&= 2430\,x_1^2x_2^2x_3^2 + 3240\,x_1^3x_2^2x_3^2 - 2430\,x_1^2x_2^3x_3 + 864\,x_1x_2x_3^2\\
&\quad - 540\,x_1x_2^3x_3 + 216\,x_1^2x_2x_3^2 + 1350\,x_1^4x_2^2x_3^2 - 216\,x_1^2x_2^2x_3\\
&\quad - 3240\,x_1^3x_2^3x_3 - 1350\,x_1^4x_2^3x_3 + 540\,x_1x_2^2x_3^2 - 864\,x_1x_2^2x_3\\
&\quad + 1296\,x_1x_2^2 + 216\,x_1^2x_2^2 + 6210\,x_1^2x_2^3 + 5940\,x_1^3x_2^3 + 1350\,x_1^4x_2^3\\
&\quad + 1620\,x_1x_2^3 - 648\,x_2^2x_3 + 648\,x_2x_3^2 + 1944\,x_2^2,\\
&\operatorname{prem}(G_3', G_4', x_4) = 0.
\end{aligned}$$

因而 G_1, G_2, G_3 和 F_1, G_2, G_3', G_4' 都是多项式余式序列. 由此得出

$$\begin{aligned}
&\gcd(G_1, G_2) = \operatorname{pp}(G_3, x_4) = x_3 - x_4,\\
&\gcd(F_1, G_2) = \operatorname{pp}(G_4', x_4) = 1.
\end{aligned}$$

定义 1.2.2 环 $\mathcal{R}[x]$ 中的非零多项式序列 $P_1, P_2, \cdots, P_r$ 称为 P_1 和 P_2 关于 x 的 *子结式多项式余式序列*, 这里

$$r \geq 2, \quad d_i = \deg(P_i, x), \quad d_1 \geq d_2, \quad I_i = \mathrm{lc}(P_i, x),$$

如果

$$P_{i+2} = \mathrm{prem}(P_i, P_{i+1}, x)/Q_{i+2}, \quad 1 \leq i \leq r-2,$$
$$\mathrm{prem}(P_{r-1}, P_r, x) = 0,$$

这里

$$Q_3 = (-1)^{d_1-d_2+1}, \quad H_3 = -1,$$
$$Q_i = -I_{i-2} H_i^{d_{i-2}-d_{i-1}},$$
$$H_i = (-I_{i-2})^{d_{i-3}-d_{i-2}} H_{i-1}^{1-d_{i-3}+d_{i-2}}, \quad i = 4, \cdots, r.$$

下一节中, 我们将介绍若干有关 *子结式* 的已知结果. 它们确保上面子结式多项式余式序列的定义是合适的, 即对所有 $i \geq 3$, 只要 $P_1, P_2 \in \mathcal{R}[x]$ 就有 $P_i \in \mathcal{R}[x]$.

1.3 结式与子结式

两个一元多项式 $F, G \in \mathcal{R}[x]$ 的 *结式* 是关于 F 和 G 的系数的一种形式, 该形式为零将为这两个多项式关于 x 有公共零点提供某种条件. 这里 F 和 G 的公共 *零点* $\bar{x}$ 是指 $\mathcal{R}$ 之商域的某一扩域中的数使得 $F(\bar{x}) = G(\bar{x}) = 0$. 它的正式定义将在 1.5 节中给出. 本节的理想参考文献是 [57] 中的第七章.

设 F 和 G 关于 x 的次数分别为 m 和 l, 且 $m \geq l > 0$, 并将 F 与 G 写成

$$\begin{aligned} F &= a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1} x + a_m, \\ G &= b_0 x^l + b_1 x^{l-1} + \cdots + b_{l-1} x + b_l. \end{aligned} \tag{1.3.1}$$

我们构造一个 $m+l$ 阶方阵如下:

$$\mathbf{S} = \begin{pmatrix} a_0 & a_1 & \cdots & a_m & & & \\ & a_0 & a_1 & \cdots & a_m & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_0 & a_1 & \cdots & a_m \\ b_0 & b_1 & \cdots & b_l & & & \\ & b_0 & b_1 & \cdots & b_l & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_0 & b_1 & \cdots & b_l \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} l \\ \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \end{matrix},$$

其中空白处的元素都为 0. 称该方阵为 F 和 G 关于 x 的 *西尔维斯特矩阵*.

定义 1.3.1　称西尔维斯特矩阵 $\mathbf{S}$ 的行列式为 F 和 G 关于 x 的 *西尔维斯特结式*, 记作 $\mathrm{res}(F,G,x)$.

和往常一样, 我们用 $\det(\square)$ 表示方阵 $\square$ 的 *行列式*. 结式 $\mathrm{res}(F,G,x)=\det(\mathbf{S})$ 是齐次的, 它关于 a_i 的次数为 l, 关于 b_i 的次数为 m.

例 1.3.1　考虑 x 的三次多项式

$$F=ax^3+bx^2+cx+d.$$

F 与其导数

$$\frac{dF}{dx}=3\,ax^2+2\,bx+c$$

的结式 R 也称为 F 的 *判别式*. 若 $a\neq 0$, $F=0$ 有重根的充要条件为 $R=0$.

F 和 dF/dx 关于 x 的 5 阶西尔维斯特矩阵 $\mathbf{S}$ 如下:

$$\mathbf{S}=\begin{pmatrix} a & b & c & d & 0\\ 0 & a & b & c & d\\ 3\,a & 2\,b & c & 0 & 0\\ 0 & 3\,a & 2\,b & c & 0\\ 0 & 0 & 3\,a & 2\,b & c \end{pmatrix}.$$

因而 F 和 dF/dx 关于 x 的西尔维斯特结式为

$$\mathrm{res}(F,dF/dx,x)=\det(\mathbf{S})=a\,(27\,a^2d^2-18\,abcd+4\,b^3d+4\,ac^3-b^2c^2).$$

引理 1.3.1　设 F 和 G 如 (1.3.1) 所示, 则存在多项式 $A,B\in\mathcal{R}[x]$, 使得

$$AF+BG=\mathrm{res}(F,G,x),$$

这里 $\deg(A,x)<\deg(G,x)$, $\deg(B,x)<\deg(F,x)$.

这一引理的证明见于 [72] 中第 85 页和 [57] 中 228、229 页. 作为以上引理和定义的推论, 我们有下述定理中的充分性.

定理 1.3.2　设 F 和 G 如 (1.3.1) 所示, 则 $\mathrm{res}(F,G,x)=0$ 当且仅当 F 和 G 关于 x 有公共零点, 或者 $a_0=b_0=0$.

该定理中的必要性也不难证明 (见 [72] 第 83 、84 页). 如果 a_0, b_0 之一不为零, 则 $\mathrm{res}(F,G,x)=0$ 是 F 和 G 有公共零点的充要条件.

现设 $\mathbf{S}_{ij}$ 为通过删除矩阵 $\mathbf{S}$ 中 l 行 F 系数中的最后 j 行, m 行 G 系数中的最后 j 行, 和最后 $2j+1$ 列, 但第 $m+l-i-j$ 列除外, 所得的子矩阵, 这里 $0\le i\le j<l$.

定义 1.3.2 对 $0\le j<l$, 多项式

$$S_j(x)=\sum_{i=0}^{j}\det(\mathbf{S}_{ij})x^i$$

称为 F 和 G 关于 x 的第 j 个 *子结式*. 这里 $\deg(S_j,x)\le j$, 并称 $R_j=\det(\mathbf{S}_{jj})$ 为 F 和 G 关于 x 的第 j 个 *主子结式系数*, 或第 j 个 *结式*.

如果 $m>l+1$, 则将 F 和 G 关于 x 的第 j 个 *子结式* $S_j(x)$ 与 *主子结式系数* R_j 的定义拓广如下:

$$S_l(x)=b_0^{m-l-1}G,\quad R_l=b_0^{m-l};\quad S_j(x)=R_j=0,\ l<j<m-1.$$

如果 $\deg(S_j,x)=r<j$, 则称 S_j 为 *r 次亏损的*; 否则, 称 S_j 为 *正则的*.

容易看出 $S_0=R_0$ 为 F 和 G 关于 x 的 *结式*.

定理 1.3.3 设 F 和 G 为 $\mathcal{R}[x]$ 中的多项式, 且 $m=\deg(F,x)\ge\deg(G,x)=l>0$. 又设 S_j 为 F 和 G 关于 x 的第 j 个子结式, $0\le j<m-1$, 则存在多项式 $A_j,B_j\in\mathcal{R}[x]$, 使得

$$A_jF+B_jG=S_j,$$

这里 $\deg(A_j,x)<l-j$, $\deg(B_j,x)<m-j$.

证 见 [57] 第 255 、256 页. □

定义 1.3.3 设 F 和 G 为 $\mathcal{R}[x]$ 中的多项式, 且 $m=\deg(F,x)\ge\deg(G,x)=l>0$. 令

$$\mu=\begin{cases} m-1 & \text{若 } m>l,\\ l & \text{否则.}\end{cases}$$

此为试读,需要完整PDF请访问: www.ertongbook.com