21st CENTURY
规划教材
面向21世纪高等院校计算机系列规划教材
COMPUTER COURSES FOR UNDERGRADUATE EDUCATION

计算机代数基础

——代数与符号计算的基本原理

张树功　雷　娜　刘停战　编

科学出版社
北京

内 容 简 介

随着计算机技术的飞速发展,计算机代数系统已经被广泛地应用于科研、教学以及工程技术,其中比较有名的有 Maple, Mathematica 等. 本书主要介绍这些系统中基本问题的数学原理和基本算法,即计算机代数的基本知识.

本书是为数学、计算数学和计算机科学专业的高年级本科生和低年级研究生编写的教材,也可供相关专业的学生、教师以及科技工作者参考.

图书在版编目(CIP)数据

计算机代数基础:代数与符号计算的基本原理/张树功等编.—北京:科学出版社,2005

(面向 21 世纪高等院校计算机系列规划教材)

ISBN 7-03-015325-1

Ⅰ.计… Ⅱ.张… Ⅲ.电子计算机-数值计算 Ⅳ.TP301.6

中国版本图书馆 CIP 数据核字(2005)第 028854 号

责任编辑:李 娜 丁 波/责任校对:刘彦妮

责任印制:吕春珉/封面设计:三函设计

科学出版社发行 各地新华书店经销

*

2005 年 5 月第 一 版 开本:787×1092 1/16

2005 年 5 月第四次印刷 印张:14 1/2

印数:1—3 000 字数:340 000

定价:19.00 元

(如有印装质量问题,我社负责调换〈新欣〉)

销售部电话:010-62136131 编辑部电话:010-62138978-8004 (HI02)

前　言

在人类生活、经济建设和科技发展过程中，“计算”始终都扮演着非常重要的角色．在对自然界和人类社会各种事物发展规律的研究中，当从定性分析过渡到定量分析时，就必然涉及计算．例如每天的天气预报，就是根据当前的气温、气压数据按某种方法和程序计算出明、后天的天气甚至以后更长时间的各种气象指标；至于人造飞船上天、原子能的开发和利用以及各种矿藏的勘探与开采等高科技活动就更离不开计算。因此，计算能力的强弱直接制约着一个国家的经济和科技发展速度．

人类的计算能力与计算工具密切相关，早期的计算主要是靠人的大脑再加上一些简单的计算工具来完成，计算效率低，可靠性也很差．电子计算机的出现大大地提高了人类的计算能力，从而也促进了科学技术的迅猛发展．最初的电子计算机多用于一般规模的数值计算，因此计算机的出现也催生了计算数学——研究在计算机上实现数值计算的理论与算法的数学分支．

实际上，对科学与工程技术以及数学研究本身的发展需要而言，不仅需要数值计算，还需要公式推导、表达式的化简、函数的微分及积分、精确地解各种方程等计算．这种计算的特点是对一些符号按确定的规则进行的演算，并且计算过程都是精确的，人们称这种计算为符号计算、公式推演或者代数计算．这种计算的需求在实践中是大量存在的，例如，1847 年法国天文学家 Delaunay 花了 10 年的时间推导出了月球的轨道公式，又花了另外 10 年来检查他的结果，并于 1867 年将其公布于世．其结果是非数值的，主要部分都是以公式的形式给出，全部结果长达 128 页之多．另一个有名的例子是 19 世纪海王星的发现．人们发现天王星的实际运行轨道与当时的理论不符，猜想它可能受到其他未知行星的干扰．经过计算，当然包含大量的公式推导，并在计算结果的指导下进行观测，终于发现了海王星．

这些计算的特点都是将计算对象代数化，然后利用代数中的理论及算法进行计算．人们把这种研究可代数化的数学对象的计算理论与方法的学科，或者说符号计算与代数计算的学科称为计算机代数，或者数学机械化．简而言之，计算机代数是计算机科学与数学交叉融合的产物，是符号、代数算法的设计、分析、实现和应用的学科．作为代数算法，它有简单的形式界定（formal specification），有建立在相应数学理论基础之上的正确性证明和渐进时间界限的估计（即所谓计算的复杂性）．而且代数对象可在计算机的内存中准确地表现出来，因而代数计算可以精确地进行；因为计算是精确的，所以可用的代数算法都必定在有限步内完成运算．

由于代数算法都是建立在数学基础之上的，所以代数及代数几何的发展为代数计算提供了广泛的数学理论基础，同时代数计算的研究也促进了代数理论，特别是构造性代数及代数几何理论的发展．近年来产生了计算交换代数与计算代数几何等新的研究领域，或者可以说是更为一般的数学机械化的新的研究领域．

如果我们把计算数学理解为研究在计算机上进行计算的数学理论与算法的学科分支，那么以往的计算数学主要研究数值算法的设计、分析、实现和应用及相应的数学理论，而计算机代数则研究符号计算的相关理论，是计算数学发展的新阶段．与数值计算相比，代数计算要求计算机有高速度与大存储量，所以它与计算机技术发展的联系更为密切．计算机代数作为新的计算工具，在理论物理、高能物理、天体力学、化学化工、机械学、机器人设计以及计算机的各种应用领域都有广泛的应用，同时也成为数学教学与数学研究的重要工具．

在实际应用中，符号计算、公式推演或者说代数计算的问题很多，而且门类繁杂，在理论基础方面几乎涉及数学的各个分支，在应用方面涉及各个行业领域．然而由于计算机的计算速度、存储空间限制等诸多原因，这类计算的自动化过程进展十分缓慢，直到 1953 年，Kahrimanian 与 Nolan 才分别在他们的论文中给出第一个计算形式微分的计算机程序，其后这类计算的自动化进程一直徘徊不前．随着计算机技术的迅速发展，高性能计算机的普及，以及科技工程等实际问题对符号计算的迫切需要，人们开始重视这类计算的理论与算法的研究．经过近 30 年的发展，符号计算的研究与应用才算真正得到长足的进步．

计算机代数是从 20 世纪 60 年代中期发展起来的，与此同时，一些学术机构和团体也相继成立．比较有名的如 ACM（the association for computing machinary）的 SIGSAM (special interest group on symbolic and algebraic manipulation)，该团体还出版了季刊“SIGSAM Bulletin”；此外还有欧洲的 SAME（symbolic and algebraic manipulation in Europe），日本与前苏联也成立了相应的研究机构；我国也在中国科学院建立了数学机械化中心，简称 MMRC．世界各国对符号计算的研究都非常重视，相继设立了一些大型的研究项目，如原欧共体（现称欧盟）的 POSSO 计划及其后继 FRISCO，我国“八五”期间的攀登计划项目“机器证明及其应用”，“九五”期间的 973 项目“数学机械化与自动推理平台”等．这些项目在理论与应用方面，例如几何定理证明与发现、代数方程、微分方程求解、实多项式系统问题以及诸多计算机应用领域都取得了丰硕的成果．

国际上有关计算机代数的学术交流活动也十分活跃，比如定期举行的综合性系列国际学术会议有 ISSAC（international symposium on symbolic and algebraic computation），ASCM（asian symposium on computer mathematics），此外还有许多其他比较专门的系列国际会议，在互联网上用 Symbolic，Algebraic，Geometric，Computation 等关键词搜索，就可以获得相应的信息，这里不再赘述．

计算机代数方向已出版了专门的国际学术刊物“Journal of Symbolic Computation”，此外，“SIAM Journal on Computer”，“ACM Transactions on Mathematical Software”也刊登了这方面的论文；Springer 的丛书“Lecture Notes in Computer Science”中陆续出版了不少计算机代数的专集；自 20 世纪 90 年代起，已陆续出版了计算交换代数、计算代数几何、算法代数等方面的专著．

与数值计算不同，代数算法的研究与计算机代数的软件系统的研制几乎是同时的．随着理论研究的深入，一些多层次、多用途的计算机代数软件，例如比较早期的

μ-Math（Derive），Reduce，后起之秀 Mathematica，Maple，我国自行开发的 MMP 以及比较专业的 CoCoA 等，也相继开发出来．有些计算机代数软件还允许用户定义抽象的代数结构（例如环和代数），并对其元素进行操作，具有这一功能的软件有 Axiom 等．

经 30 余年的发展，许多计算机代数系统已投入使用，这些系统的功能日益强大，效率不断提高．这些代数系统的主要功能如下。

1）提供一基本命令集，可使机器做许多复杂的计算，包括数值的和符号的计算．这个特点使得代数系统具有可用性．

2）提供一种能定义高层命令或扩展原始命令的程序语言，使得系统具有可开发性．

现有的代数系统可处理的问题如下．

1）数的计算，包括整数、有理数、实数和复数的计算，且既可进行浮点计算又可进行精确计算．

2）多项式、有理式的各种计算．

3）矩阵的计算，且其元素可为符号的．

4）数学分析中微分、积分、级数和微分方程等计算．

5）其他各种代数问题的计算．

利用这些计算机代数系统，已经基本上可以解决实际中出现的绝大部分问题。当然对某些问题其效能还不是很高，尚有待于进一步的研究和完善．

这些软件已经发挥了很大的作用，例如，美国西雅图波音科学研究实验室为利用 Delaunay 的结果推导人造卫星的运行轨道，使用计算机代数系统重新推导，结果发现了 3 处错误．又如，人们利用计算机代数系统验算了早期的不定积分表，发现错误高达 1/5～1/4．在数学教育中，已经可以使用计算机证明与发现几何定理．

由于计算机代数在科学研究与工程技术中越来越广泛的应用，每个科研工作者，包括数学、计算数学、计算机科学以及其他领域的研究人员，必须掌握计算机代数的基本知识与熟练使用相关的计算机代数软件．为适应形势发展的需要，我们从 1992 年开始为吉林大学计算专业的研究生和本科生开设计算机代数课程，并在 1997 年由吉林大学出版社出版了计算机代数教材，讲述计算机代数的基本原理与算法．经过几年的教学实践，发现原书有很多错误与疏漏之处，实感确有修订之必要，在吉林大学教材科和科学出版社的支持下，我们进行了修订工作．本次修订主要是修正原书的错误，补充疏漏和一些不完善的地方．考虑到作为计算机代数的入门教材，不宜过多地引入新的内容，因此本次修订未对结构做调整．

在学习计算机代数的过程中，对计算数学、抽象代数以及交换代数等有关基本知识有一些必要的了解是大有裨益的．考虑到一般学生可能没有学过抽象代数，我们在第 1 章及附录中介绍了必要的抽象代数与交换代数的基本内容．此外，因为计算机代数中有些算法理论涉及比较深刻的专门知识，我们感到要想做到教材内容的自包含是比较困难的，在有些情况下不得不放弃某些算法所依据的理论而仅仅描述算法本身．虽然计算机代数所包含的内容十分广泛，但由于篇幅所限，本书仅仅选取了与多项式问题紧密相关的那些内容的基本部分．

张树功对第 1～6 章及附录 A 进行修订；附录 B 由雷娜和刘停战编写．

冯果忱教授一直对本书的编写给予了关心和鼓励，在此表示感谢．

本书是作者在计算机代数教学方面的一个尝试，由于作者水平有限，不可避免地存在这样或那样的错误和不足，殷切希望各位专家和同行们提出宝贵意见和建议．

目　　录

第 2 章　多项式代数

本书的内容基本上都是围绕着计算机代数中多项式问题展开讨论的，因此我们首先应该对有关多项式的各种问题，如多项式的表示、运算性质等有必要的了解．在本章我们先介绍多项式代数的基本内容，然后对当前计算机代数领域中最流行的两种基本研究工具，或者说是研究方法——Groebner 基方法与吴方法——进行简要的介绍．

2.1　一元多项式环

2.1.1　基本概念与结果

设 $\boldsymbol{R}$ 为一交换环，x 为一未定元，用 $\boldsymbol{R}[x]$ 表示 $\boldsymbol{R}$ 上的一元多项式全体，即 $\boldsymbol{R}[x]$ 中元素都具有形式

$$\sum_{i=0}^{m} a_i x^i ,$$

其中 $a_i \in \boldsymbol{R}$，m 为非负整数．对于给定的多项式

$$A = \sum_{i=0}^{m} a_i x^i ,$$

其次数定义为非零系数的下标最大者，记作 $\deg(A)$．

每个非零多项式都可以写成**规范形式**

$$A = \sum_{i=0}^{m} a_i x^i ,\ a_m \neq 0 .$$

如果一个多项式的所有系数都是零，则称其为**零多项式**，且记之为 0．零多项式不定义次数．如果一多项式的次数为 0，则称该多项式为**常数多项式**．若一多项式 A 的次数为 $\deg(A) = n$，A 中的乘幂 x^n 的系数为 a_n，则称 $a_n x^n$ 为 A 的**领式**，记为 $\mathrm{lm}(A) = a_n x^n$．a_n 称为 A 的**领项系数**，记作 $\mathrm{lc}(A) = a_n$．x^n 称为 A 的**领项**，记为 $\mathrm{lt}(A) = x^n$．如果对一多项式 A，有 $\mathrm{lc}(A) = 1$，则称 A 为**首一的**．交换环 $\boldsymbol{R}$ 中的加法运算和乘法运算可以自然地扩展为 $\boldsymbol{R}[x]$ 上的加法和乘法，如下所示．

若 $A = \sum_{i=0}^{m} a_i x^i$，$B = \sum_{i=0}^{n} b_i x^i$，则多项式加法定义为

$$C(x) = A(x) + B(x) = \sum_{i=0}^{\max(m,\,n)} c_i x^i ,$$

其中 $c_i = a_i + b_i$，$i = 0, 1, \cdots, \max(m, n)$．当式中的 i 大于 m 或 n 时，相应的 a_i 或 b_i 取为 0．类似地，多项式的乘法则定义为

$$D(x) = A(x)B(x) = \sum_{k=0}^{m+n} d_k x^k ,$$

其中 $d_k = \sum_{i+j=k} a_i b_j$．关于 $\boldsymbol{R}[x]$ 的代数结构，有如下定理．

定理 2.1.1 1）若 $\boldsymbol{R}$ 为交换环，则 $\boldsymbol{R}[x]$ 亦为交换环，且以零多项式与常数多项式 1 为加法与乘法单位元.

2）若 $\boldsymbol{D}$ 为整环，则 $\boldsymbol{D}[x]$ 亦为整环，其可逆元恰为 $\boldsymbol{D}$ 中的可逆元.

3）若 $\boldsymbol{D}$ 为唯一分解整环，则 $\boldsymbol{D}[x]$ 也是唯一分解整环，其不可约元就是那些相对于 $\boldsymbol{D}$ 不能分解的多项式.

4）如果 $\boldsymbol{D}$ 是 Euclid 整环，则 $\boldsymbol{D}[x]$ 为唯一分解整环，但未必是 Euclid 整环.

5）若 $\boldsymbol{K}$ 是一域，则在赋值

$$v(A)=\deg(A)$$

之下，$\boldsymbol{K}[x]$ 是一 Euclid 整环.

整环上非零多项式的次数函数关于多项式运算有下列关系.

1）$\deg(A+B)\leqslant \max\{\deg(A),\deg(B)\}$.

2）$\deg(AB)=\deg(A)+\deg(B)$.

2.1.2 域上的一元多项式环

设 $\boldsymbol{K}$ 为一域，则由定理 2.1.1，$\boldsymbol{K}[x]$ 是 Euclid 整环.对于任意给定的多项式 A，$B\in \boldsymbol{K}[x]$，$B\neq 0$，存在多项式 Q，R，使得

$$A=QB+R, \tag{2.1.1}$$

其中 $\deg(R)<\deg(B)$，或 $R=0$，式(2.1.1)也称为 **带余除法或** Euclid **除法**. Q 称为 A 除以 B 的**商**，记作 $Q=\mathrm{quo}(A,B)$，R 称为 A 除以 B 的**余式**，记作 $R=\mathrm{rem}(A,B)$.

如果在带余除法中余式 $R=0$，则称 B **整除** A，记作 $B\mid A$.

命题 2.1.1 带余除法中的 Q 和 R 是唯一的.

证明 设有 R_1，Q_1 以及 R_2，Q_2，使得

$$A=Q_iB+R_i,\ R_i=0 \text{ 或 } \deg(R_i)<\deg(B),\ i=1,2.$$

两式相减则有

$$(Q_1-Q_2)B=R_2-R_1.$$

我们断言上式中 Q_1-Q_2 与 R_2-R_1 都是零多项式.不然计算次数得

$$\deg(Q_1-Q_2)+\deg(B)=\deg(R_2-R_1).$$

因为 $\deg(R_i)<\deg(B)$，$i=1,2$，且次数函数是非负的，于是

$$\begin{aligned}\deg(B)&>\max\{\deg(R_1),\deg(R_2)\}\\&\geqslant\deg(R_2-R_1)\\&=\deg(Q_1-Q_2)+\deg(B)\\&\geqslant\deg(B).\end{aligned}$$

这个矛盾说明只能有 $Q_1=Q_2$，$R_1=R_2$，即带余除法的商和余式都是唯一的.

当给定多项式

$$A(x)=\sum_{i=0}^{n}a_ix^i,\ B(x)=\sum_{i=0}^{m}b_ix^i,\ a_n\neq 0,\ b_m\neq 0,$$

则 A 除以 B 的商 Q 与余式 R 可用下列算法求得.

算法 2.1.1 带余除法：

```
Input A=∑_{i=0}^{n} a_i x^i, B=∑_{i=0}^{m} b_i x^i;
Output Q, R such that A=QB+R;
    if n<m then return Q=0, R=A;
    else R:=A;
        Q:=0;
        N:=deg(R)-m;
        while N≥0 do
            R:=R-lc(R)/lc(B)x^N B;
            Q:=Q+lc(R)/lc(B)x^N;
            N:=deg(R)-m;
        return Q, R;
```

例 2.1.1 设 $A=3x^3+x^2+x+5$，$B=5x^2-3x+1$，求 quo(A，B)，rem(A，B).

因为 deg(A)$=3>$ deg(B)$=2$，按照算法 2.1.1 有

$$R_1=A-\frac{3}{5}xB=\frac{14}{5}x^2+\frac{2}{5}x+5,$$

$$Q_1=0+\frac{3}{5}x=\frac{3}{5}x,$$

$$R_2=R_1-\frac{14}{25}x^0B=\frac{52}{25}x+\frac{111}{25},$$

$$Q_2=Q_1+\frac{14}{25}=\frac{3}{5}x+\frac{14}{25},$$

即有

$$A=QB+R,$$

其中 $Q=\frac{3}{5}x+\frac{14}{25}$，$R=\frac{52}{25}x+\frac{111}{25}$.

我们知道，当 $\boldsymbol{K}$ 为域时，$\boldsymbol{K}[x]$是 Euclid 整环，但对一般的整环 $\boldsymbol{D}$，哪怕是 Euclid 整环，$\boldsymbol{D}[x]$也未必是 Euclid 整环.

例 2.1.2 整数环 Z Z$[x]$ 却不是 Euclid 整环. 取例 2.1.1 中的 A，B，如果我们试图求 $Q=q_1x+q_0$，$R=r_1x+r_0\in$Z$[x]$，使得

$$3x^3+x^2+x+5=(5x^2-3x+1)(q_1x+q_0)+(r_1x+r_0).$$

则可导出

$$\begin{cases}3=5q_1,\\ 1=5q_0-3q_1,\\ 1=q_1-3q_0+r_1,\\ 5=q_0+r_0.\end{cases}$$

显然上方程组并没有整数解. 本例说明 Z$[x]$不是 Euclid 整环.而且本例也表明，要想进行多项式的除法，系数的运算必须在域里进行.

例 2.1.3 在域 $\boldsymbol{K}$ 上的多项式整环 $\boldsymbol{K}[x]$ 中，多项式 x 没有乘法逆. 因为如果它有乘法逆，比如说 $Q(x)$，则有

$$xQ(x)=1.$$

取次数则有

$$\deg(x)+\deg(Q)=1+\deg(Q)=\deg(1)=0.$$

由此得 $\deg(Q)=-1$，这是不可能的. 故 x 没有乘法逆.

设 $A\in\boldsymbol{K}[x]$ 为非零多项式，则 $\mathrm{lc}(A)\neq 0$，令 $n(A)=A/\mathrm{lc}(A)$，则 $n(A)$ 是首一多项式. 我们称其为 A 的**正规部分**.

设 A，$B\in\boldsymbol{K}[x]$，C，$D\in\boldsymbol{K}[x]$ 均为 A，B 的最大公因子，则 C，D 可以相差域 $\boldsymbol{K}$ 中的一个常数倍. 但是如果我们取其正规部分，则最大公因子是唯一的.

若 D 为 A，B 的最大公因子，由定理 1.1.3，存在 W，$V\in\boldsymbol{K}[x]$ 使得

$$WA+VB=D, \tag{2.1.2}$$

上述方程称为多项式 Diophantos 方程. 我们感兴趣的是，对于哪些多项式 $C\in\boldsymbol{K}[x]$，存在 W，$V\in\boldsymbol{K}[x]$，使得

$$WA+VB=C \tag{2.1.3}$$

成立. 这种方程求解问题在后面的许多算法中要遇到. 显然若上述方程有解，则必有 $D\mid C$.

定理 2.1.2 设 $\boldsymbol{K}$ 为域，A，$B\in\boldsymbol{K}[x]$ 为给定的非零多项式，$D=\gcd(A,B)\in\boldsymbol{K}[x]$，则对任何满足 $D\mid C$ 的多项式 $C\in\boldsymbol{K}[x]$，存在唯一的 W，$V\in\boldsymbol{K}[x]$，使得

$$WA+VB=C, \tag{2.1.4}$$

且

$$\deg(W)<\deg(B)-\deg(D). \tag{2.1.5}$$

此外，如果还有 $\deg(C)<\deg(A)+\deg(B)-\deg(D)$，则

$$\deg(V)<\deg(A)-\deg(D). \tag{2.1.6}$$

证明 因为 $D=\gcd(A,B)$，则存在 $\widetilde{W}$，$\widetilde{V}\in\boldsymbol{K}[x]$ 使得

$$\widetilde{W}A+B\widetilde{V}=D.$$

因为 $D\mid C$，记 $U=\mathrm{quo}(C,D)$，则有

$$\widetilde{W}UA+\widetilde{V}UB=C. \tag{2.1.7}$$

将 $\widetilde{W}U$ 除以 B 关于 D 的余因子 B/D，得

$$\widetilde{W}U=QB/D+R, \tag{2.1.8}$$

其中 $\deg(R)<\deg(B/D)=\deg(B)-\deg(D)$. 将式(2.1.8)代入式(2.1.7)得

$$RA+(\widetilde{V}U+QA/D)B=C, \tag{2.1.9}$$

于是 $W=R$，$V=\widetilde{V}U+QA/D$ 为所求.

下面证其唯一性. 设有 W_i，V_i，$i=1,2$，满足

$$W_iA+V_iB=C,$$

且

$$\deg(W_i)<\deg(B)-\deg(D). \tag{2.1.10}$$

两式相减得

$$(W_1-W_2)A=-(V_1-V_2)B, \tag{2.1.11}$$

记 $B_1 = B/D$，$A_1 = A/D$，则 A_1，B_1 互素，于是

$$B_1 \mid (W_1 - W_2).$$

但是 $\deg(B_1) = \deg(B) - \deg(D)$，再注意式 (2.1.10) 可知必有 $W_1 - W_2 = 0$，于是由式 (2.1.11) 又得 $V_1 - V_2 = 0$.

现在假设 C 还满足 $\deg(C) < \deg(A) + \deg(B) - \deg(D)$，我们来证式 (2.1.6) 成立. 将式 (2.1.4) 写成

$$V = (C - WA)/B,$$

则有

$$\deg(V) = \deg(C - WA) - \deg(B). \tag{2.1.12}$$

如果 $\deg(C) \geqslant \deg(WA)$，则由式 (2.1.12) 及假设知

$$\begin{aligned}\deg(V) &\leqslant \deg(C) - \deg(B)\\ &< \deg(A) - \deg(D).\end{aligned}$$

如果 $\deg(C) < \deg(WA)$，则由式 (2.1.12) 及式 (2.1.5)知

$$\begin{aligned}\deg(V) &\leqslant \deg(WA) - \deg(B)\\ &= \deg(W) + \deg(A) - \deg(B)\\ &< \deg(A) - \deg(D).\end{aligned}$$

以上定理说明，如果 $D \mid C$，则 Diophantos 方程肯定有解，且可以要求 $\deg(W) < \deg(B/D)$ 或者 $\deg(V) < \deg(A/D)$ 之一成立；如果进一步要求 $\deg(C) < \deg(\mathrm{lcm}(A, B))$，则 $\deg(W) < \deg(B/D)$ 与 $\deg(V) < \deg(A/D)$ 同时成立.

前面的定理讨论的 Diophantos 方程是两项的，我们自然要问，对多项的情形是否也有类似结果. 这个问题和孙子剩余定理有关，我们先来看简单情形. 设 a_1，a_2，$\cdots$，a_n 是 $\boldsymbol{K}$ 中两两互异的点，考虑这些点上的 Lagrange 插值问题，则可得 n 个插值基函数

$$L_i(x) = \prod_{j \neq i} \frac{x - a_j}{a_i - a_j},\ i = 1, \cdots, n.$$

由计算数学中的结论可知：次数小于 n 的多项式 A 在 n 个互异点上的插值都是精确的，而且对任一多项式 B，其插值多项式为 A 当且仅当 $B(a_i) = A(a_i)$. 上面的话可以转述成：若 $A \in \boldsymbol{K}[x]$ 且 $\deg(A) < n$，则有

$$A(x) = A(a_1)L_1(x) + \cdots + A(a_n)L_n(x). \tag{2.1.13}$$

式(2.1.13) 可以看成是 Diophantos 方程的推广. 对于每个次数小于 n 的多项式 A，由式 (2.1.13) 可知其唯一地对应着一组数 $\{A(a_1), \cdots, A(a_n)\}$，而每个 $A(a_i)$ 又可表示成

$$A(a_i) = \mathrm{rem}(A, x - a_i),$$

或者写成

$$A \equiv A(a_i) \bmod (x - a_i).$$

对于任意给定的多项式 $B \in \boldsymbol{K}[x]$，如果 B 关于函数 $F = \prod_{i=1}^{n}(x - a_i)$ 的余式 $R_B = A$，则

$$\begin{aligned}B(a_k) &= \mathrm{quo}(B, F)F(a_k) + R_B(a_k)\\ &= R_B(a_k) = A(a_k).\end{aligned}$$

即

$$B \equiv A(a_k) \bmod (x - a_k),\ k = 1, \cdots, n. \tag{2.1.14}$$

反之，如果某一多项式 B 满足 (2.1.14)，且 $R = \mathrm{rem}(B, F)$，则

$$R(a_k) = B(a_k) = A(a_k),\ k = 1, \cdots, n.$$

因为 R，A 的次数都小于 n，故必有 $R = A$．这个事实用代数的语言叙述出来就是：对于任意给定的多项式 B，$B \equiv A \bmod F$ 当且仅当 $B \equiv A(a_k) \bmod (x - a_k)$，$k = 1, \cdots, n$．

这个结果更一般的形式如下。

定理 2.1.3(孙子剩余定理的多项式形式) 设 A_1，A_2，$\cdots$，A_n 为两两互素的多项式，$\{B_1, B_2, \cdots, B_n\}$ 为给定的多项式组，则存在一多项式 A，使对任意的多项式 B，B 满足

$$B \equiv A \bmod \prod_{i=1}^{n} A_i, \tag{2.1.15}$$

当且仅当

$$B \equiv B_i \bmod A_i,\ i = 1, \cdots, n. \tag{2.1.16}$$

证明 先构造多项式 A．记 $L_i = \prod_{j \neq i} A_j$，则因 A_i 两两互素可知 L_i，A_i 互素．由定理 2.1.2 知，存在 W_i，V_i 使得

$$1 = W_i L_i + V_i A_i,$$

$$\deg(W_i) < \deg(A_i),\ \deg(V_i) < \deg(L_i). \tag{2.1.17}$$

对式 (2.1.17)，关于 A_i 取同余得

$$W_i L_i \equiv 1 \bmod A_i. \tag{2.1.18}$$

而显然有 $W_i L_i \equiv 0 \bmod A_j$，$i \neq j$．取 $A = \sum_{i=1}^{n} B_i W_i L_i$，则易见有

$$A \equiv B_i \bmod A_i,\ i = 1, \cdots, n. \tag{2.1.19}$$

先证必要性．若有 B 使得式 (2.1.15) 成立，则 $B - A$ 可被 $\prod_{i=1}^{n} A_i$ 整除，当然也可被 A_i 整除，亦即 $B \equiv A \bmod A_i$ 成立．结合式 (2.1.19) 则得式 (2.1.16)．

再证充分性．反之，设式(2.1.16) 成立，则由式 (2.1.19) 可知 $B \equiv A \bmod A_i$，$i = 1, \cdots, n$．亦即 $B - A$ 可被 A_i 整除，但 A_i 是两两互素的，故 $B - A$ 可被 $\prod_{i=1}^{n} A_i$ 整除，即式 (2.1.15) 成立．

若 A_1，A_2，$\cdots$，A_n 为两两互素的给定多项式，B_1，$\cdots$，B_n 为另一组给定多项式，我们来求一个次数不超过 $\deg(\prod_{i=1}^{n} A_i)$ 的多项式 B，使得 $B \equiv B_i \bmod A_i$，$i = 1, \cdots, n$．由孙子剩余定理的证明，易见 B 可取为

$$B = \sum_{i=1}^{n} B_i W_i L_i, \tag{2.1.20}$$

但是这样构造的多项式未必满足次数的要求，类似于式 (2.1.17) 的处理，令 $C_i = \mathrm{rem}(B_i W_i, A_i)$，则 $\deg(C_i) < \deg(A_i)$，于是可取

$$B=\sum_{i=1}^{n}C_iL_i\,. \tag{2.1.21}$$

再注意到 L_i 的定义，则有 $\deg(B)<\deg\left(\prod\limits_j A_j\right)$.

上述问题实际上是一个广义的多项式插值问题.

在孙子剩余定理中，要求 A_i 两两互素的目的是为了保证存在 W_i，使得式 (2.1.18) 成立，这样对任何 B_i，都有

$$B_iW_iL_i\equiv\begin{cases}B_i \bmod A_i\,,\\ 0 \bmod A_j\,,\ j\neq i\,.\end{cases}$$

当 A_i 不是两两互素时，只要能求得 $\overline{W}_i$ 使其满足

$$\overline{W}_iL_i\equiv\begin{cases}B_i \bmod A_i\,,\\ 0 \bmod A_j\,,\ j\neq i\,,\end{cases}$$

取 $B=\sum\limits_{i=1}^{n}\overline{W}_iL_i$，则仍有 $B\equiv B_i \bmod A_i$ 成立.

2.1.3 环上的一元多项式环

2.1.2 节我们讨论了域上的一元多项式环，这样的环是 Euclid 整环.而在 Euclid 整环上是可以进行带余除法运算的，这使得我们能够容易地处理一些给定的问题. 但是有时很多研究对象不是 Euclid 整环，比如说整数环上的一元多项式环. 又如对某一多元多项式，当把它看成某一个未定元的多项式时，它的系数是其他未定元的多项式，这种观点下的多元多项式全体就是一个环上的多项式环. 基于问题的需要，我们必须讨论环上的多项式环. 设 $\boldsymbol{D}$ 为一整环，由定理 2.1.1，$\boldsymbol{D}[x]$ 仍为一整环. 有时为了使 $\boldsymbol{D}[x]$ 成为 UFD，我们也要求 $\boldsymbol{D}$ 为 UFD. 下面我们来研究这种环上的多项式及其运算. 先来看一个例子.

例 2.1.4 设 A，$B\in\mathrm{Z}[x]$，其中

$$A(x)=48x^3-84x^2+42x-36\,,$$
$$B(x)=-4x^3-10x^2+44x-30\,.$$

它们可分解为

$$A(x)=2\times3\times(2x-3)(4x^2-x+2)\,,$$
$$B(x)=(-1)\times2\times(2x-3)(x-1)(x+5)\,.$$

于是

$$\gcd(A\,,\ B)=2(2x-3)=4x-6\,.$$

但是在 $\mathrm{Q}[x]$ 中考虑问题时，A，B 的最大公因子则为

$$\gcd(A\,,\ B)=x-\frac{3}{2}\,.$$

造成这个差别的原因是：在域 Q
数的公因子；而在 Z

对 $A\in\boldsymbol{D}[x]$，如果 $\mathrm{lc}(A)$ 为 $\boldsymbol{D}$ 中规范元，则称 A 为规范多项式，可取规范多项式为 $\boldsymbol{D}[x]$ 中的规范元.对一般 $A\in\boldsymbol{D}[x]$，易见 $u(\mathrm{lc}(A))^{-1}A$ 为规范多项式，为方便计，

简记 $u(\mathrm{lc}(A))$ 为 $u(A)$.

定义 2.1.1 设 $\boldsymbol{D}$ 为 UFD，$A=\sum_{i=0}^{k} a_i x^i \in \boldsymbol{D}[x]$. A 的**容度**(content)，记作 $\mathrm{cont}(A)$，定义为 $\mathrm{cont}(A)=\gcd(a_0,\cdots,a_k)$. 若 $\mathrm{cont}(A)=1$，且 $\mathrm{lc}(A)$ 为规范元，则称 A 是**本原的**(primitive). A 的**本原部分**(primitive part)记作 $\mathrm{pp}(A)$，定义为 $\mathrm{pp}(A)=u(A)^{-1}A/\mathrm{cont}(A)$. 为方便计，定义 $\mathrm{cont}(0)=\mathrm{pp}(0)=0$.

定理 2.1.4(Gauss 引理) 设 $\boldsymbol{D}$ 为 UFD，A，$B\in\boldsymbol{D}[x]$，则

$$\begin{aligned}\mathrm{cont}(AB)&=\mathrm{cont}(A)\mathrm{cont}(B),\\ \mathrm{pp}(AB)&=\mathrm{pp}(A)\mathrm{pp}(B).\end{aligned}\tag{2.1.22}$$

证明 先证若 $\mathrm{cont}(A)=\mathrm{cont}(B)=1$，则 $\mathrm{cont}(AB)=1$. 不然，则应有不可约元 d 整除 $\mathrm{cont}(AB)$. 又设 $A=a_n x^n+\cdots+a_0$，$B=b_m x^m+\cdots+b_0$，且有 $r\leqslant n$，$s\leqslant m$，使得

$$d\mid a_0,\cdots,d\mid a_{r-1},d\nmid a_r,\ d\mid b_0,\cdots,d\mid b_{s-1},d\nmid b_s.$$

考虑 AB 的 $r+s$ 次项系数，则有

$$c_{r+s}=\cdots+a_{r-1}b_{s+1}+a_r b_s+a_{r+1}b_{s-1}+a_{r+2}b_{s-2}+\cdots$$

由 $d\mid b_{s-1},\cdots,d\mid b_0$ 及 $d\mid c_{r+s}$ 可推知 $d\mid a_r b_s$. 因为 d 是不可约元，必有 $d\mid a_r$ 或 $d\mid b_s$，矛盾.

对一般情形，可将 AB 表示成

$$AB=u(A)u(B)\mathrm{cont}(A)\mathrm{cont}(B)\mathrm{pp}(A)\mathrm{pp}(B),$$

由前段证明知 $\mathrm{pp}(A)\mathrm{pp}(B)$ 是本原的，从而 $\mathrm{cont}(AB)=\mathrm{cont}(A)\mathrm{cont}(B)$，再由本原部分的定义即知 $\mathrm{pp}(AB)=\mathrm{pp}(A)\mathrm{pp}(B)$.

推论 2.1.1 设 $\boldsymbol{D}$ 为 UFD，A，$B\in\boldsymbol{D}[x]$，则

$$\begin{aligned}\mathrm{cont}(\gcd(A,B))&=\gcd(\mathrm{cont}(A),\mathrm{cont}(B)),\\ \mathrm{pp}(\gcd(A,B))&=\gcd(\mathrm{pp}(A),\mathrm{pp}(B)).\end{aligned}\tag{2.1.23}$$

证明 设 $D=\gcd(A,B)$，$A=DB_1$，$B=DB_2$，由定理 2.1.4

$$\mathrm{cont}(A)=\mathrm{cont}(D)\mathrm{cont}(B_1),$$

$$\mathrm{cont}(B)=\mathrm{cont}(D)\mathrm{cont}(B_2).$$

令 $\widetilde{d}=\gcd(\mathrm{cont}(A),\mathrm{cont}(B))$，于是 $\mathrm{cont}(D)\mid\widetilde{d}$. 另一方面，若有 $\bar{d}$ 使得 $\widetilde{d}=\mathrm{cont}(D)\bar{d}$，则 $\bar{d}$ 同时整除 $\mathrm{cont}(B_1)$ 和 $\mathrm{cont}(B_2)$，从而

$$\bar{d}D\mid A,\ \bar{d}D\mid B,$$

故 $\bar{d}D\mid D$，说明 $\bar{d}$ 为可逆元，但 $\widetilde{d}$ 为规范元，故必 $\widetilde{d}=\mathrm{cont}(D)$. 类似地，可证另一结果.

定理 2.1.4 与推论 2.1.1 无非是说本原多项式的乘积与最大公因子仍为本原的. 这些结果无论对一元问题还是对多元问题都十分重要.

例 2.1.5 对例 2.1.4 中的多项式

$$A(x)=48x^3-84x^2+42x-36,$$

$$B(x)=-4x^3-10x^2+44x-30,$$

有

$$\mathrm{cont}(A)=6,$$

$$\begin{aligned}\mathrm{pp}(A)&=8x^3-14x^2+7x-6\\&=(2x-3)(4x^2-x+2);\\\mathrm{cont}(B)&=2,\\\mathrm{pp}(B)&=2x^3+5x^2-22x+15\\&=(2x-3)(x-1)(x+5).\end{aligned}$$

容易看出,有

$$\gcd(A,B)=\gcd(\mathrm{cont}(A),\mathrm{cont}(B))\gcd(\mathrm{pp}(A),\mathrm{pp}(B)).$$

因为我们这里讨论的环不是 Euclid 整环,而带余除法在非 Euclid 整环内不能进行,可是很多问题又需要进行除法计算,这就要求我们将除法推广,下面介绍的伪除就是这样一种运算.我们还是先来看一个具体的例子,这对问题的理解是有帮助的.

例 2.1.6 设

$$\begin{aligned}A(x)&=3x^3+x^2+x+5,\\B(x)&=5x^2-3x+1.\end{aligned}$$

它们在 $\mathbf{Q}[x]$ 中的带余除法为

$$3x^3+x^2+x+5=\left(\frac{3}{5}x+\frac{14}{25}\right)(5x^2-3x+1)+\left(\frac{52}{25}x+\frac{111}{25}\right).$$

如果在等式两端都乘以 5^2,则两端都变成整系数多项式.如果在 $\mathbf{Z}[x]$ 中考虑问题,则除法不能进行.但考虑 $5A$ 除以 B,计算一步则有

$$\begin{aligned}5A&=3xB+(14x^2+2x+25)\\&\triangleq 3xB+R_1.\end{aligned}$$

又 $\mathrm{lc}(R_1)$ 不能被 $\mathrm{lc}(B)$ 整除,再考虑 $5R_1$ 除以 B,计算一步得

$$\begin{aligned}5R_1&=14B+(52x+111)\\&\triangleq 14B+R_2.\end{aligned}$$

注意 R_2 的次数已经小于 B 的次数,于是

$$\begin{aligned}5^2A&=5(3xB+R_1)\\&=15xB+14B+R_2\\&=(15x+14)B+R_2.\end{aligned}$$

现在我们来考虑一般情形.设 $A(x)=\sum\limits_{i=0}^{m}a_ix^i$,$B(x)=\sum\limits_{i=0}^{n}b_ix^i\in\boldsymbol{D}[x]$,$m\geqslant n$ 且 $b_n\neq 0$.令

$$\begin{aligned}R_1(x)&=b_nA(x)-a_mx^{m-n}B(x)\\&=(b_na_{m-1}-a_mb_{n-1})x^{m-1}+\cdots\end{aligned}\tag{2.1.24}$$

则显然 $R_1\in\boldsymbol{D}[x]$.记 $R_1(x)=\sum\limits_{i=0}^{m-1}r_i^{(1)}x^i$,再令

$$\begin{aligned}R_2(x)&=b_nR_1(x)-r_{m-1}^{(1)}x^{m-n-1}B(x)\\&=(b_nr_{m-2}^{(1)}-r_{m-1}^{(1)}b_{n-1})x^{m-2}+\cdots\end{aligned}\tag{2.1.25}$$

可见仍然有 $R_2\in\boldsymbol{D}[x]$.这样继续下去,记 $R_k(x)=\sum\limits_{i=0}^{m-k}r_i^{(k)}x^i$,在进行 $m-n$ 步以

后,得

$$R_{m-n}(x)= b_nR_{m-n-1}(x)-r_{n+1}^{(m-n-1)}xB(x)$$
$$=(b_nr_n^{(m-n-1)}-r_{n+1}^{(m-n-1)}b_{n-1})x^n+\cdots \tag{2.1.26}$$
$$R_{m-n+1}(x)= b_nR_{m-n}(x)-r_n^{(m-n)}B(x)$$
$$=(b_nr_{n-1}^{(m-n)}-r_n^{(m-n)}b_{n-1})x^{n-1}+\cdots \tag{2.1.26$'$}$$

将第一式乘以 b_n^{m-n},第二式乘以 b_n^{m-n-1},……,第 $m-n$ 式乘以 $b_n^{m-n-(m-n-1)}=b_n$,最后一式乘以 $b_n^0=1$. 再将所有的式子相加并消去相同的项,得

$$R_{m-n+1}=b_n^{m-n+1}A-B\Big(\sum_{i=0}^{m-n}b_n{}^{m-n-i}r_{m-i}^{(i)}x^{m-n-i}\Big). \tag{2.1.27}$$

由前述推导可知,若记 $R=R_{m-n+1}$, $Q=\sum_{i=0}^{m-n}b_n{}^{m-n-i}r_{m-i}^{(i)}x^{m-n-i}$,则有以下定理.

定理 2.1.5 设 A, $B\in \boldsymbol{D}[x]$, $\deg(A)\geqslant\deg(B)$ 且 $\mathrm{lc}(B)=b\neq 0$,则存在 Q, $R\in\boldsymbol{D}[x]$ 满足 $\deg(R)<\deg(B)$ 或 $R=0$,使得

$$b^lA=QB+R, \tag{2.1.28}$$

其中 $l=\deg(A)-\deg(B)+1$.

上述定理中所叙述的这种性质称为**伪除**(pseudo-division)性质. 我们称定理中的 Q 为 A 除以 B 的**伪商**,记作 $Q=\mathrm{pquo}(A,B)$. 称定理中的 R 为 A 除以 B 的**伪余**,记作 $R=\mathrm{prem}(A,B)$.

分析定理证明可知,式(2.1.28)中的 l 有时可以取得小于 $(\deg(A)-\deg(B)+1)$,这是因为在证明中我们始终假定 $b_nr_{m-k-1}^{(k)}-r_{m-k}^{(k)}b_{n-1}\neq 0$. 倘若这些系数有等于 0 的,则整个计算步数就会减少,因此最终 b_n 的方次也可以降低,当然相应的伪商和伪余也会随之变化. 在这种意义上说,伪商和伪余是不唯一的. 但是对使式 (2.1.28) 成立的最小的 l 来说,伪商和伪余是唯一的. 因为倘若有 Q_1, Q_2, R_1, R_2,使式(2.1.28)成立,则两式相减得 $(Q_1-Q_2)B=R_2-R_1$,比较两端的次数就会得到 $Q_1=Q_2$, $R_2=R_1$.

有了上述的伪除概念,我们就可以讨论 $\boldsymbol{D}[x]$ 中的最大公因子的计算问题了.

定理 2.1.6 设 $\boldsymbol{D}$ 为 UFD. A, $B\in\boldsymbol{D}[x]$ 为本原多项式,且 $\deg(A)\geqslant\deg(B)$, $\mathrm{lc}(B)=b\neq 0$. 又设 Q, R 为定理 2.1.5 所述的伪商和伪余,则有

$$\gcd(A,B)=\gcd(B,\mathrm{pp}(R)). \tag{2.1.29}$$

证明 由伪除性质有

$$b^lA=QB+R.$$

容易证得

$$\gcd(b^lA,B)=\gcd(B,R). \tag{2.1.30}$$

由 Gauss 引理

$$\gcd(b^lA,B)=\gcd(b^l,1)\gcd(A,B)$$
$$=\gcd(A,B). \tag{2.1.31}$$

这里我们利用了 A, B 为本原多项式的假设. 再由 Gauss 引理又有

$$\gcd(B,R)=\gcd(1,\mathrm{cont}(R))\gcd(B,\mathrm{pp}(R))$$
$$=\gcd(B,\mathrm{pp}(R)). \tag{2.1.32}$$

综合式 (2.1.30)~式 (2.1.32) 即得定理结论.

根据上述定理的结论,对给定的本原多项式 A, B, $\deg(A)\geqslant\deg(B)$,为求其最大公因子,可构造如下的**伪余多项式序列**

$$R_0=A,\ R_1=B,$$

$$R_k=\mathrm{pp}(\mathrm{prem}(R_{k-2},R_{k-1})),\ k=2,3,\cdots$$

注意到序列 $\deg(R_1)>\deg(R_2)>\cdots>\deg(R_k)>\cdots$,故序列 R_0, R_1,…, R_k,… 必终止于某 R_l,于是由定理 2.1.6 可知,有 $R_l=\gcd(A,B)$.

例 2.1.7 设

$$A(x)=48x^3-84x^2+42x-36,$$

$$B(x)=-4x^3-10x^2+44x-30.$$

令 $R_0=\mathrm{pp}(A)=8x^3-14x^2+7x-6$, $R_1=\mathrm{pp}(B)=2x^3+5x^2-22x+15$,其余计算结果为

$$R_2=34x^2-95x+66,$$

$$R_3=2x-3,$$

$$R_4=0.$$

最终得

$$\begin{aligned}\gcd(A,B)&=\gcd(\mathrm{cont}(A),\mathrm{cont}(B))\gcd(\mathrm{pp}(A),\mathrm{pp}(B))\\&=2(2x-3)\\&=4x-6.\end{aligned}$$

对于具体的多项式环 $\mathbf{Z}[x]$,会不会存在这样的问题:给定多项式 A, $B\in\mathbf{Z}[x]$,它们在 $\mathbf{Z}[x]$ 与 $\mathbf{Q}[x]$ 上有不同次数的最大公因子?这种担心是不必要的.下面就来说明这个问题.设 A, B 在 $\mathbf{Q}[x]$ 的最大公因子为 D,则有 A_1, $B_1\in\mathbf{Q}[x]$ 使得

$$A=DA_1,\ B=DB_1.$$

去分母得

$$d_1A=\overline{D}\overline{A}_1,\ d_2B=\overline{D}\overline{B}_1.$$

由 Gauss 引理知

$$\mathrm{pp}(A)=\mathrm{pp}(\overline{D})\mathrm{pp}(\overline{A}_1),$$

$$\mathrm{pp}(B)=\mathrm{pp}(\overline{D})\mathrm{pp}(\overline{B}_1).$$

即 $\mathrm{pp}(\overline{D})$ 是 $\mathrm{pp}(A)$, $\mathrm{pp}(B)$ 的因子,因为 $\mathrm{pp}(\overline{D})$ 的次数和 D 的次数相同,且若 $\widetilde{D}$ 为 A, B 在 $\mathbf{Z}[x]$ 上的最大公因子,则 $\mathrm{pp}(\overline{D})\mid\widetilde{D}$,故可知 D 的次数不超过 $\widetilde{D}$ 的次数.反之,易见 $\widetilde{D}$ 在 $\mathbf{Q}[x]$ 上整除 D,即 $\widetilde{D}$ 的次数又不超过 D 的次数,从而二者相等.并且由上面的推导可以看出, $\widetilde{D}$ 和 D 实际只相差一 Q

综上所述,有如下定理.

定理 2.1.7 多项式 A, B 在 $\mathbf{Z}[x]$ 中有非平凡公因子当且仅当它们在 $\mathbf{Q}[x]$ 中有非平凡的公因子.

2.2 多元多项式环

2.2.1 基本概念与结果

在符号计算中，人们最感兴趣并且实际问题涉及最多的多项式环是整数环、有理数域以及有限域上的多元多项式环，因此设计多元多项式问题的有效算法是符号计算的中心课题之一．在讨论各种算法之前，先对多元多项式环的基本概念以及基本结果有一些了解是十分必要的．

设 $\boldsymbol{R}$ 为一交换环，x_1，x_2，$\cdots$，x_n 为 n 个未定元．有如下形式的有限和

$$A(x_1,\cdots,x_n)=\sum_{i_1,i_2,\cdots,i_n} a_{i_1,i_2,\cdots,i_n} x_1^{i_1} x_2^{i_2}\cdots x_n^{i_n}, \tag{2.2.1}$$

其中 $a_{i_1,i_2,\cdots,i_n}\in \boldsymbol{R}$，称为 $\boldsymbol{R}$ 上的 n **元多项式**，其中每个和项称为一个**单项式**．特别地，如果每个 $a_{i_1,i_2,\cdots,i_n}$ 都等于 0，则称其为零多项式；而 $\boldsymbol{R}$ 上的每个元都是一个常数多项式．$\boldsymbol{R}$ 上的所有 n 元多项式全体记为 $\boldsymbol{R}[x_1,\cdots,x_n]$，或者简记作 $\boldsymbol{R}[X]$，其中 $X=(x_1,\cdots,x_n)$．

因为每个**单项** $x_1^{i_1} x_2^{i_2}\cdots x_n^{i_n}$ 都唯一地对应一个 n 元有序非负整数组 $i=(i_1,i_2,\cdots,i_n)$，因此我们可以简单地记其为

$$X^i = x_1^{i_1} x_2^{i_2}\cdots x_n^{i_n}, \tag{2.2.2}$$

并称 $i=(i_1,i_2,\cdots,i_n)$ 为单项 X^i 的**多重次数**，简记为 $\mathrm{md}(X^i)=i$．因此式 (2.2.1) 可以简记为

$$A(X)=\sum_i a_i X^i \tag{2.2.3}$$

对单项 X^i，记 $\deg(X^i)=|i|=\sum_{j=1}^{n} i_j$，称为 X^i 的**全次数**．而对多项式 $A(X)=\sum_i a_i X^i$，则定义其全次数为

$$\deg(A)=\max\{\deg(X^i)\mid a_i\neq 0\}.$$

对于 $A\in R[X]$，当视其为某未定元 x_r 的一元多项式时，其关于 x_r 的次数记为 $\deg_{x_r}(A)$ 或 $\deg(A,x_r)$．

关于 $\boldsymbol{R}[X]$，在适当定义多项式的加法和乘法后，有下列基本结果．

定理 2.2.1 1）如果 $\boldsymbol{R}$ 为交换环，则 $\boldsymbol{R}[X]$ 仍为交换环．$\boldsymbol{R}[X]$ 中的零元就是零多项式 0，而单位元即为常数多项式 1．

2）如果 $\boldsymbol{D}$ 为整环，则 $\boldsymbol{D}[X]$ 仍为整环，且其可逆元为 $\boldsymbol{D}$ 中作为常数多项式的那些可逆元．

3）如果 $\boldsymbol{D}$ 是 UFD，则 $\boldsymbol{D}[X]$ 也为 UFD．

4）如果 $\boldsymbol{D}$ 为 Euclid 整环，则 $\boldsymbol{D}[X]$ 为 UFD，但不是 Euclid 整环．

5）如果 $\boldsymbol{K}$ 是域，则 $\boldsymbol{K}[X]$ 是 UFD，且当未定元的个数大于 1 时不再是 Euclid 整环．

2.2.2 单项序与多项式的约化

对于一元多项式情形，我们可以将多项式的项按未定元的方次由大到小排列，再利

用带余除法就可以研究和计算一元多项式的问题了. 对多元情形, 也应该对所有的单项排出一个次序,并将除法的定义推广.

现在考虑所有单项的集合

$$\boldsymbol{T}=\{X^{\boldsymbol{i}}=x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\mid \boldsymbol{i}=(i_1,i_2,\cdots,i_n)\in \boldsymbol{N}^n\},$$

其中 $\boldsymbol{N}^n$ 是所有分量为非负整数的 n 元组的集合.

定义 2.2.1 集合 $\boldsymbol{T}$ 上的一个全序 $<_T$ 称为一个**容许的单项序**, 如果

1) 对所有 $t\in \boldsymbol{T}$, 成立 $1<_T t$.

2) 如果 $s,t\in \boldsymbol{T}$ 且 $s<_T t$, 则对任意 $u\in \boldsymbol{T}$, $su<_T tu$ 成立.

单项序还有另外一种等价定义:

1) $<_T$ 是 $\boldsymbol{T}$ 上的全序.

2) 如果 $s,t\in \boldsymbol{T}$ 且 $s<_T t$, 则对任意 $u\in \boldsymbol{T}$, $su<_T tu$ 成立.

3)每个非空子集都有极小元.

条件 3)称为良序性质. 上述定义中的条件 3)还可等价地叙述为:

3)′每个严格下降的单项序列都是有限终止的.

一般地, 给定 $\boldsymbol{T}$ 上一单项序, 因为单项与 n 元组是一一对应的,从而也诱导了 $\boldsymbol{N}^n$ 上的一个序, 以后我们也用 $i<T^j$ 来表示 $X^i<_T X^j$.

满足上述条件的单项序有很多, 但最常用的有如下三种.

定义 2.2.2 $<_l$ 称为 $\boldsymbol{T}$ 上的(纯)**字典序**, 如果

$$X^{\boldsymbol{i}}<_l X^{\boldsymbol{j}}$$

当且仅当

$$(j_1-i_1,\cdots,j_n-i_n)$$

的左数第一个非零元为正.

容易验证上面定义的 $<_l$ 确实满足定义 2.2.1 的两个条件, 所以它是一单项序. 注意,在上述定义中已蕴含了

$$x_n<_l x_{n-1}<_l\cdots<_l x_1.$$

例 2.2.1 对三个未定元 $x>y>z$ 的情形, 单项按字典序由小到大的排列次序为

$$1<_l z<_l z^2<_l\cdots<_l y<_l yz<_l yz^2<_l\cdots$$
$$<_l y^2<_l y^2z<_l\cdots<_l x<_l xz<_l\cdots<_l xy<_l\cdots$$

定义 2.2.3 $<_t$ 称为 $\boldsymbol{T}$ 上的**全幂序**或称**分次字典序**, 如果

$$X^{\boldsymbol{i}}<_t X^{\boldsymbol{j}},$$

当且仅当

$$(|\boldsymbol{j}|-|\boldsymbol{i}|,j_1-i_1,\cdots,j_n-i_n)$$

的左数第一个非零元为正.

定义 2.2.4 $<_r$ 称为 $\boldsymbol{T}$ 上的**分次反字典序**, 如果

$$X^{\boldsymbol{i}}<_r X^{\boldsymbol{j}},$$

当且仅当

$$(j_1-i_1,\cdots,j_n-i_n,|\boldsymbol{i}|-|\boldsymbol{j}|)$$

的右数第一个非零元为负.

例 2.2.2 对三个未定元 $x > y > z$ 的情形，单项按分次反字典序由小到大的排列次序为

$$1 <_r z <_r y <_r x <_r z^2 <_r yz <_r xz <_r y^2 <_r xy$$
$$<_r x^2 <_r z^3 <_r yz^2 <_r xz^2 <_r y^2 z <_r xyz <_r \cdots$$

如果规定 $z <_t y <_t x$，再将 3 个未定元的单项按分次字典序由小到大排列，则有

$$1 <_t z <_t y <_t x <_t z^2 <_t yz <_t y^2 <_t xz$$
$$<_t xy <_t x^2 <_t z^3 <_t yz^2 <_r y^2 z <_t xyz <_t \cdots$$

一般情况下，当不至于产生混淆时，我们常略去序 $<_r$ 的下标，而简记作 $<$.

定义 2.2.5 多项式 $P \in \boldsymbol{D}[X]$（相对于单项序 $<$）的**领式**是 P 中出现的单项式（按序 $<$）的最大者，记作 $\mathrm{lm}(P)$. 而领式中出现的幂积称为 P 的**领项**，记作 $\mathrm{lt}(P)$. 领项的多重次数记作 $\mathrm{md}(P)$. 领项的系数记作 $\mathrm{lc}(P)$.

显然对任何多项式 P 总成立 $\mathrm{lm}(P) = \mathrm{lc}(P)\mathrm{lt}(P)$. 以后我们总假定多项式都是按其单项式的次序由大到小递降排列的.

对多项式的加法和乘法，有

$$\mathrm{lt}(PQ) = \mathrm{lt}(P) \cdot \mathrm{lt}(Q),$$
$$\mathrm{lt}(P + Q) \leqslant \max\{\mathrm{lt}(P), \mathrm{lt}(Q)\}.$$

例 2.2.3 下列多项式是按 $x > y > z$ 的分次字典序递降排列的.

$$P = 2xy^2z^2 - 2xyz^3 + x^2y^2 - 2x^2yz + x^2z^2$$
$$+ x^2y - xy - yz + z^2 + 5,$$

且有

$$\mathrm{lm}(P) = 2xy^2z^2, \mathrm{lt}(P) = xy^2z^2, \mathrm{lc}(P) = 2.$$

但是如果按字典序排列，则有

$$P = x^2y^2 - x^2yz + x^2y + x^2z^2 + 2xy^2z^2$$
$$- 3xyz^3 - xy + yz + z^2 + 5.$$

相应的领项、领式及领项系数分别为

$$\mathrm{lm}(P) = \mathrm{lt}(P) = x^2y^2, \mathrm{lc}(P) = 1.$$

对域上的一元多项式环情形，因其为 Euclid 整环，我们可以用 Euclid 除法来计算最大公因子以及其他问题. 但对多元多项式环的情形，它不再是 Euclid 整环，无法定义 Euclid 除法. 因此我们需要引进一种与一元情形的除法求余运算有相同作用的运算，即多项式的约化. 下面我们讨论多项式的约化问题，并假定考虑的是域 $\boldsymbol{K}$ 上的多项式.

定义 2.2.6 设 $P, Q \in \boldsymbol{K}[X]$，如果 P 中有某个单项可被 $\mathrm{lt}(Q)$ 整除，P 称为（相对于某固定单项序 $<$）是**模 Q 可约的**.

如果 P 模 Q 可约，且 P 可以表示成 $P = at + R$，其中 a 为非零常数，$t \in T$，$R \in \boldsymbol{K}[X]$ 为某一多项式，又 $\dfrac{t}{\mathrm{lt}(Q)} = u \in \boldsymbol{K}[X]$，记

$$\overline{P} = P - \frac{a}{\mathrm{lc}(Q)}uQ, \tag{2.2.4}$$

则称 P **模 Q 约化到** $\overline{P}$，记作

$$P \longrightarrow_Q \overline{P}. \tag{2.2.5}$$

如果 $Q \in \boldsymbol{G}=\{Q_1,\cdots,Q_m\}$，我们也称 P **模** $\boldsymbol{G}$ **可约**，并记之为

$$P \longrightarrow_{G} \bar{P}. \tag{2.2.6}$$

如果在 $\boldsymbol{G}$ 中不存在多项式 Q_i 使得 P 模 Q_i 可约，则称 P **模** $\boldsymbol{G}$ **不可约**或 P 相对于 $\boldsymbol{G}$ **是约化的**. 我们约定 0 **相对于任何多项式或多项式组总是不可约的**.

例 2.2.4 对多项式

$$P=6x^4+13x^3-6x+1,\ Q=3x^2+5x-1.$$

如果约化 P 的领项，则有

$$P \longrightarrow_{Q} P-2x^2Q=3x^3+2x^2-6x+1.$$

注意，$3x^3+2x^2-6x+1$ 仍然是模 Q 可约的. 事实上，P 可以模 Q 约化到 0，这是因为 $Q \mid P$. 在一元情形，约化等价于多项式的除法求余.

例 2.2.5 考虑多项式

$$P=-xz^2+2y^2z,$$
$$Q=7y^2+yz-4,$$
$$R=2yz-3x+1.$$

在分次字典序（$x>y>z$）下，它们都已表示成依单项递降排列的形式. P 的项 $2y^2z$ 既可以被 lt(Q) 整除，也可以被 lt(R) 整除. 先用 Q 约化得

$$P \longrightarrow_{Q} P-\frac{2}{7}zQ=-xz^2-\frac{2}{7}yz^2+\frac{8}{7}z,$$

此时，$\bar{P}=-xz^2-\frac{2}{7}yz^2+\frac{8}{7}z$ 模 Q 不可约但模 R 可约，且

$$\bar{P} \longrightarrow_{R} \bar{P}+\frac{1}{7}zR=-xz^2-\frac{6}{7}xz+\frac{9}{7}z.$$

最后这个多项式既不是模 Q 可约的也不是模 R 可约的.

倘若我们一开始不用 Q 而用 R 去约化，则有

$$P \longrightarrow_{R} P-yR=-xz^2+3xy-y.$$

$-xz^2+3xy-y$ 模 Q，R 都不是可约的. 由此例可以看出，对于给定的一多项式 P 与一多项式组 $\boldsymbol{G}=\{Q_1,\cdots,Q_m\}$，$P$ 模 $\boldsymbol{G}$ 约化的结果是不唯一的，它依赖于约化的次序. 但是对上例而言，不管约化的次序如何，最终总可得一多项式，它相对于 $\boldsymbol{G}=\{Q,R\}$ 是不可约的. 事实上，这是约化的一个重要性质.

命题 2.2.1 设 $\boldsymbol{G}$ 为给定的多项式组，P 为任意一多项式，如果相对于某单项序 $<$ 有

$$P \longrightarrow_{G} Q,$$

则有 lt(P) $\geqslant$ lt(Q).

证明 按照约化的定义，存在 $G \in \boldsymbol{G}$ 与 P 的某项 at 以及 u，使得 $t=\mathrm{lt}(G)u$，且

$$Q=P-\frac{a}{\mathrm{lc}(G)}uG.$$

记 $P=\mathrm{lc}(P)\mathrm{lt}(P)+at+\bar{P}$，$G=\mathrm{lc}(G)\mathrm{lt}(G)+(G-\mathrm{lm}(G))$，则有 lt($P$) $>$ lt($\bar{P}$)，lt(G) $>$ lt($G-\mathrm{lm}(G)$).

当 lt(P) $=t$ 时，因

$$Q = \bar{P} - \frac{a}{\mathrm{lc}(G)} u(G - \mathrm{lm}(G)),$$

故 $\mathrm{lt}(Q) \leqslant \max\{\mathrm{lt}(\bar{P}), \mathrm{lt}(u(G - \mathrm{lm}(G)))\} < t = \mathrm{lt}(P)$. 当 $\mathrm{lt}(P) > t$ 时,因

$$\mathrm{lt}(u(G - \mathrm{lm}(G))) < u\mathrm{lt}(G) = t$$

$$Q = \mathrm{lc}(P)\mathrm{lt}(P) + \bar{P} - \frac{a}{\mathrm{lc}(G)} u(G - \mathrm{lm}(G)),$$

从而 $\mathrm{lt}(Q) = \mathrm{lt}(P)$.

对固定的单项序 $<$,我们在多项式之间定义一偏序.

对于任意两个多项式

$$P_1 = \sum_{i=1}^{k} a_i t_i^{(1)}, \quad P_2 = \sum_{i=1}^{l} b_i t_i^{(2)},$$

我们称 P_1 小于 P_2,记作 $P_1 < P_2$,如果它们满足下列条件之一:

1) 存在 $s \leqslant \min\{k, l\}$,使得 $t_i^{(1)} = t_i^{(2)}$, $i = 1, \cdots, s-1$, $t_s^{(1)} < t_s^{(2)}$.

2) $l > k$,且对任意 $i = 1, \cdots, k$, $t_i^{(1)} = t_i^{(2)}$.

否则,称 P_1, P_2 是**不可比较的**.

引理 2.2.1 任何严格单调下降的多项式序列都是有限的.

证明 设

$$P_0 > P_1 > \cdots > P_k > \cdots$$

是严格单调下降的多项式序列,且每个多项式的项都是按序由大到小排列的. 记每个 P_k 的第 j 项为 $t_j^{(k)}$, $k = 0, 1, \cdots$

考虑集合 $\{P_k\}$ 的每个多项式的第 1 项构成的单项序列,则其为单调不增的序列

$$t_1^{(1)} \geqslant t_1^{(2)} \geqslant \cdots \geqslant t_1^{(k)} \geqslant \cdots$$

由单项序定义的条件 3),存在正整数 N_1,使得当 $k > N_1$ 时,有 $t_1^{(k)} = t_1^{(N_1)}$.

如果仍有 P_k,使得 $P_k < P_{N_1}$,再考虑多项式序列 $\{P_k\}_{k > N_1}$,则由多项式偏序的定义,每个 P_k 都存在第 2 项 $t_2^{(k)}$, $k = N_1 + 1, \cdots$ 于是又得一单调不增的单项序列

$$t_2^{(N_1+1)} \geqslant t_2^{(N_1+2)} \geqslant \cdots \geqslant t_2^{(k)} \geqslant \cdots$$

再由单项序定义的条件 3),存在正整数 $N_2 > N_1$,使得当 $k > N_2$ 时, $t_2^{(k)} = t_2^{(N_2)}$.

如此下去,则或者在某一步已得 $\{P_k\}$ 的有限性;或者得一严格下降的单项序列

$$t_1^{(N_1)} > t_2^{(N_2)} > \cdots > t_k^{(N_k)} > \cdots$$

再由单项序定义的条件 3),知该序列是有限的,即有 $t_s^{(N_s)}$,使得

$$t_1^{(N_1)} > t_2^{(N_2)} > \cdots > t_k^{(N_k)} > \cdots > t_s^{(N_s)}.$$

此时 $\{P_k\}$ 必终止于 P_{N_s},不然,若还有 $k > N_s$ 使得 $P_k < P_{N_s}$,则由序列 $t_1^{(N_1)}$, $t_2^{(N_2)}, \cdots$, $t_k^{(N_k)}, \cdots$ 的构造方法知,该序列又含有某多项式 $P_{N_{s+1}}$ ($N_{s+1} > N_s$) 的某项 $t_{s+1}^{(N_{s+1})}$,使得 $t_s^{(N_s)} > t_{s+1}^{(N_{s+1})}$,这与序列 $t_1^{(N_1)}$, $t_2^{(N_2)}, \cdots, t_k^{(N_k)}, \cdots$ 终止于 $t_s^{(N_s)}$ 矛盾,故序列 $\{P_k\}$ 必终止于 P_{N_s}.

定理 2.2.2 对于给定的多项式集合 $\boldsymbol{G}$ 与固定的单项序 $<$,任何 P_0 的模 $\boldsymbol{G}$ 约化序列

$$P_0 \longrightarrow_{\boldsymbol{G}} P_1 \longrightarrow_{\boldsymbol{G}} P_2 \longrightarrow_{\boldsymbol{G}} \cdots$$

都是有限的,且 P_0 可以在有限步内约化为一模 $\boldsymbol{G}$ 不可约的多项式.

证明 先证在约化序列中,P_k 是严格单调下降多项式序列.若 P_k 模 $\boldsymbol{G}$ 约化到 P_{k+1},则有 $Q \in \boldsymbol{G}$ 以及 P_k 的某项 ct 使得 $t = \mathrm{lt}(Q)u$ 且

$$P_{k+1} = P_k - \frac{c}{\mathrm{lc}(Q)} uQ, \tag{2.2.7}$$

不妨设

$$P_k = R_1 + ct + R_2,$$

其中 R_1 的任何一项都严格大于 t,R_2 的任何一项都严格小于 t.同理,将 Q 表示成

$$Q = \mathrm{lc}(Q)\mathrm{lt}(Q) + S,$$

则因 $t = \mathrm{lt}(Q)u$,对 S 的任何项 $s \in T$,都有 $su < t$.由式 (2.2.7)有

$$P_{k+1} = R_1 + R_2 - \frac{c}{\mathrm{lc}(Q)} uS.$$

若 $R_2 - \frac{c}{\mathrm{lc}(Q)} uS \neq 0$,则 $\mathrm{lt}(R_2 - \frac{c}{\mathrm{lc}(Q)} uS) < t$;若 $R_2 - \frac{c}{\mathrm{lc}(Q)} uS = 0$,则 $P_{k+1} = R_1$,再由多项式的偏序的定义知,$P_k > P_{k+1}$,从而引理 2.2.2 保证约化序列是有限的.

如果在上述约化过程中,当 P_k 模 $\boldsymbol{G}$ 可约时,继续约化其到 P_{k+1},则可得一约化序列,设该序列终止于 P_l,此时 P_l 必为模 $\boldsymbol{G}$ 不可约的,不然 P_l 又可模 $\boldsymbol{G}$ 约化到 P_{l+1},这与序列终止于 P_l 矛盾,故 P_0 可以在有限步内约化为模 $\boldsymbol{G}$ 不可约多项式.

如果存在一约化序列

$$P \xrightarrow{}_{G} P_2 \xrightarrow{}_{G} P_m = Q,$$

记 $P \xrightarrow{*}_{G} Q$.如果 Q 还是不可约的,则记 $P \xrightarrow{}_{G} Q$,并记之为 $Q = \mathrm{Reduce}(P, \boldsymbol{G})$.

例 2.2.6 采用分次反字典序,考虑多项式组 $\boldsymbol{G} = \{P_1, P_2, P_3\}$,其中

$$P_1 = x^3yz - xz^2,$$

$$P_2 = xy^2z - xyz,$$

$$P_3 = x^2y^2 - z^2.$$

又设

$$Q = x^2y^2z - z^3,\ R = -x^2y^2z + x^2yz.$$

则

$$Q \xrightarrow{}_{P_3} x^2y^2z - z^3 - z(x^2y^2 - z^2) = 0.$$

同理有 $R \xrightarrow{}_{P_2} 0$.但 $Q + R = x^2yz - z^3$ 却不再是模 $\boldsymbol{G}$ 可约的.

命题 2.2.2 设 $P \in \boldsymbol{K}[X]$,$\boldsymbol{G} = \{G_1, G_2, \cdots, G_s\} \subset \boldsymbol{K}[X]$,且 $P \xrightarrow{*}_{G} Q$,则存在多项式 H_j,使得

$$P = \sum_{j=1}^{s} H_jG_j + Q,$$

且 $\mathrm{lt}(Q) \leqslant \mathrm{lt}(P)$,$\mathrm{md}(H_jG_j) \leqslant \mathrm{md}(P)$.

证明 留作练习.

2.3 Groebner 基

2.3.1 Groebner 基的定义与基本性质

设 $\boldsymbol{I}\subset \boldsymbol{K}[X]$ 为一多项式集合，如果其满足下述性质，则称为一理想(见附录 A)．

1) $0\in \boldsymbol{I}$．

2)若 $A,B\in \boldsymbol{I}$，则 $A+B\in \boldsymbol{I}$．

3)若 $A\in \boldsymbol{I}$，则对任何 $B\in \boldsymbol{K}[X]$，$AB\in \boldsymbol{I}$．

称 $\boldsymbol{G}\subset \boldsymbol{K}[X]$ 为 $\boldsymbol{I}$ 的一组**生成元**，如果 $\boldsymbol{G}=\{G_1,G_2,\cdots,G_m\}$，且对任意 $A\in \boldsymbol{I}$ 都可表示成 $A=\sum_{i=1}^{m}B_iG_i$，其中 $B_i\in \boldsymbol{K}[X]$．我们也称 $\boldsymbol{G}$ 为 $\boldsymbol{I}$ 的一个**理想基**，记作 $\boldsymbol{I}=\langle \boldsymbol{G}\rangle$．易知理想基不是唯一的．

设 $\boldsymbol{K}$ 为域，考虑一元多项式环 $\boldsymbol{K}[x]$ 上的理想 $\boldsymbol{I}$．由于 $\boldsymbol{I}$ 中的多项式的次数构成非负整数全体的一个子集，故其有极小元，即 $\boldsymbol{I}$ 中次数极小的多项式是存在的．设 $A\in \boldsymbol{I}$ 为一次数极小的多项式，则对任何 $B\in \boldsymbol{I}$，由带余除法，有 $Q,R\in \boldsymbol{K}[x]$，使得

$$B=QA+R,\ \deg(R)<\deg(A).$$

如果 $R\neq 0$，则有 $R=B-QA\in \boldsymbol{I}$，这与 A 的定义矛盾，故必有 $R=0$．上述分析说明，$\boldsymbol{I}=<A>$，即 A 是 $\boldsymbol{I}$ 的理想基，$\boldsymbol{I}$ 中的任何多项式除以 A 的余式为 0，或者说可以被 A 约化到 0，具有这种性质的理想基称为 Groebner 基，是符号计算中一种强有力的工具．

Groebner 基的概念是 B. Buchberger 于 1965 年在其博士论文中提出来的，为纪念其导师 W. Groebner 而将这种特殊的理想基命名为 Groebner 基．下面我们来介绍有关 Groebner 基的一些基本内容．

定义 2.3.1 理想基 $\boldsymbol{G}\subset \boldsymbol{K}[X]$ 称为(关于某固定单项序 $<$ 的) Groebner **基**，如果

$$P\in\langle \boldsymbol{G}\rangle \text{ 当且仅当 } P\xrightarrow[G]{*}0. \tag{2.3.1}$$

由上述定义可以看出，给定理想 $\boldsymbol{I}\subset \boldsymbol{K}[X]$ 的 Groebner 基 $\boldsymbol{G}$ 与任意一多项式 $P\in \boldsymbol{K}[X]$，则可判断是否有 $P\in \boldsymbol{I}$，即所谓理想成员问题是可以计算地判别的．下面研究 Groebner 基的性质．

命题 2.3.1 理想基 $\boldsymbol{G}$ 为理想 $\boldsymbol{I}$ 的 Groebner 基的充分必要条件是：对任何 $P\in \boldsymbol{I}$，存在 $G_j\in \boldsymbol{G}$，使得 $\mathrm{lt}(G_j)\mid \mathrm{lt}(P)$．

证明 必要性．设 $\boldsymbol{G}$ 为 Groebner 基，则对任何 $P\in \boldsymbol{I}$，有

$$P\xrightarrow[G]{*}0.$$

我们断言，若 $\mathrm{lt}(P)\neq 0$，则其必被 $\boldsymbol{G}$ 中某多项式 G_j 的领项整除．不然设有有限约化过程

$$P\xrightarrow[G]{}P_1\xrightarrow[G]{}P_2\xrightarrow[G]{}\cdots\xrightarrow[G]{}P_k\xrightarrow[G]{}\cdots\xrightarrow[G]{}0,$$

但 $\mathrm{lt}(P)$ 不被 $\boldsymbol{G}$ 中任何多项式的领项整除，则由命题 2.2.1 的证明可知，有 $\mathrm{lt}(P)=\mathrm{lt}(P_1)=\cdots=\mathrm{lt}(P_k)=\cdots=\mathrm{lt}(0)=0$，这与 $\mathrm{lt}(P)\neq 0$ 矛盾．

充分性．设对任意的 $P\in \boldsymbol{I}$，存在 $G_j\in \boldsymbol{G}$ 及单项 u 使得 $\mathrm{lt}(P)=\mathrm{lt}(G_j)u$．令

$$P_1=P-\frac{\mathrm{lc}(P)}{\mathrm{lc}(G_j)}uG_j,$$

则由命题 2.2.1，$\mathrm{lt}(P_1)<\mathrm{lt}(P)$. 注意 $P_1\in \boldsymbol{I}$，重复上述过程，再由引理 2.2.1，可知 P 可在有限步内约化为 0.

设 $S\subset N^n$ 为一(有限或无穷)子集，则

$$I=<X^{\alpha}\mid \alpha\in S>=\{\text{有限和}\sum{}_{\alpha}C_{\alpha}X^{\alpha},C_{\alpha}\in \boldsymbol{K}[X]\}$$

为一理想，称之为**单项理想**.

单项理想的一个性质是：如果 $t\in T$ 且 $t\in I=<X^{\alpha}\mid \alpha\in S>$，则存在 $\alpha_0\in S$，使得 $X^{\alpha_0}\mid t$. 这是因为 $t\in I=<X^{\alpha}\mid \alpha\in S>$ 意味着存在有限和 $\sum{}_{\alpha}C_{\alpha}X^{\alpha},C_{\alpha}\in \boldsymbol{K}[X]$ 使得 $t=\sum{}_{\alpha}C_{\alpha}X^{\alpha}$. 将右端展开，则展开式的每一项都含有形如 $X^{\alpha},\alpha\in S$ 的因子；又左端为单项，故右端的项除一项外其他项必相互消去，即有 $a_{\alpha_0}\in \boldsymbol{K},X^{\alpha_0},\alpha_0\in S$ 与 $u\in T$，使得 $t=a_{\alpha_0}uX^{\alpha_0}$，这说明 X^{α_0} 整除 t.

定义如下的单项理想

$$\langle \mathrm{lt}(\boldsymbol{I})\rangle=\langle \mathrm{lt}(P)\mid P\in \boldsymbol{I}\rangle,$$
$$\langle \mathrm{lt}(\boldsymbol{G})\rangle=\langle \mathrm{lt}(G)\mid G\in \boldsymbol{G}\rangle,$$

则命题 2.3.1 可以等价地叙述为如下.

命题 2.3.1′ 理想基 $\boldsymbol{G}$ 为理想 $\boldsymbol{I}$ 的 Groebner 基的充分必要条件是

$$\langle \mathrm{lt}(\boldsymbol{I})\rangle=\langle \mathrm{lt}(\boldsymbol{G})\rangle. \tag{2.3.2}$$

例 2.3.1 对于例 2.2.6 中的 P_1，P_2，P_3 与 Q，R，则

$$\boldsymbol{G}=\{P_1,P_2,P_3,x^2yz-z^3,xz^3-xz^2,yz^3-z^3,xyz^2-xz^2,x^2z^2-z^2,z^5-z^4\}$$

是关于分次反字典序的 Groebner 基. 我们已知 $Q\xrightarrow{G}0$，$R\xrightarrow{G}0$. 计算可知，也有 $Q+R\xrightarrow{G}0$.

定义 2.3.2 对固定的单项序，任何两个多项式 $P,Q\in \boldsymbol{K}[X]$ 的 S-多项式定义为

$$\mathrm{Spoly}(P,Q)=lcm(lt(\mathrm{P}),lt(\mathrm{Q}))\left(\frac{\mathrm{P}}{lm(\mathrm{P})}-\frac{\mathrm{Q}}{lm(\mathrm{Q})}\right). \tag{2.3.3}$$

例 2.3.2 对于分次反字典序，多项式

$$P=3x^2y-y^3-4,\ Q=xy^3+x^2-9$$

的 S-多项式为

$$\begin{aligned}\mathrm{Spoly}(P,Q)&=(x^2y^3)\left(\frac{P}{3x^2y}-\frac{Q}{xy^3}\right)\\&=\frac{1}{3}y^2(3x^2y-y^3-4)-x(xy^3+x^2-9)\\&=-\frac{1}{3}y^5-x^3-\frac{4}{3}y^2+9x.\end{aligned}$$

引理 2.3.1 设有和式 $\sum_{i=1}^{r}c_iX^{\alpha(i)}G_i$，其中 c_i 为常数，$X^{\alpha(i)}$ 为单项，G_i 为多项式，且对任意 i，$\alpha(i)+\mathrm{md}(G_i)=\delta\in \boldsymbol{N}^n$. 如果

$$\mathrm{md}\left(\sum_{i=1}^{r}c_iX^{\alpha(i)}G_i\right)<\delta, \tag{2.3.4}$$

则存在常数 $c_{j,j+1}$，使得

$$\sum_{i=1}^{r} c_i X^{\alpha(i)} G_i = \sum_{j=1}^{r-1} c_{j,j+1} X^{\delta-\gamma_{j,j+1}} \mathrm{Spoly}(G_j, G_{j+1}), \tag{2.3.5}$$

其中 $X^{\gamma_{j,j+1}} = \mathrm{lcm}(\mathrm{lt}(G_j), \mathrm{lt}(G_{j+1}))$. 此外对每个 j，有

$$\mathrm{md}(X^{\delta-\gamma_{j,j+1}} \mathrm{Spoly}(G_j, G_{j+1})) < \delta. \tag{2.3.6}$$

证明 令 $d_i = \mathrm{lc}(G_i)$，则 $\mathrm{lc}(c_i X^{\alpha(i)} G_i) = c_i d_i$. 由式 (2.3.4)，$\sum_{i=1}^{r} c_i d_i = 0$.

定义 $P_i = X^{\alpha(i)} G_i / d_i$，则 P_i 是首一的. 于是

$$\begin{aligned}\sum_{i=1}^{r} c_i X^{\alpha(i)} G_i &= \sum_{i=1}^{r} c_i d_i P_i \\ &= c_1 d_1 (P_1 - P_2) \\ &\quad + (c_1 d_1 + c_2 d_2)(P_2 - P_3) + \cdots \\ &\quad + (c_1 d_1 + \cdots + c_{r-1} d_{r-1})(P_{r-1} - P_r) \\ &\quad + (c_1 d_1 + \cdots + c_r d_r) P_r .\end{aligned}$$

注意最后一项等于 0. 现在设 $\mathrm{lm}(G_i) = d_i X^{\beta(i)}$，则有 $\alpha(i) + \beta(i) = \delta$，由此可推出 $X^{\gamma_{jk}} \mid X^{\delta}$，且有

$$\begin{aligned}X^{\delta-\gamma_{jk}} \mathrm{Spoly}(G_j, G_k) &= X^{\delta-\gamma_{jk}} \left(\frac{X^{\gamma_{jk}}}{\mathrm{lm}(G_j)} G_j - \frac{X^{\gamma_{jk}}}{\mathrm{lm}(G_k)} G_k \right) \\ &= \frac{X^{\delta}}{d_j X^{\beta(j)}} G_j - \frac{X^{\delta}}{d_k X^{\beta(k)}} G_k \\ &= \frac{X^{\alpha(j)}}{d_j} G_j - \frac{X^{\alpha(k)}}{d_k} G_k \\ &= P_j - P_k .\end{aligned}$$

定义 $c_{j,j+1} = c_1 d_1 + \cdots + c_j d_j$，$j = 1, \cdots, r-1$，则有

$$\sum_{i=1}^{r} c_i X^{\alpha(i)} G_i = \sum_{j=1}^{r-1} c_{j,j+1} X^{\delta-\gamma_{j,j+1}} \mathrm{Spoly}(G_j, G_{j+1}).$$

注意 P_i 是首一的，且 $\mathrm{md}(P_i) = \delta$，故 $\mathrm{md}(P_j - P_{j+1}) < \delta$. 由此得 $\mathrm{md}(X^{\delta-\gamma_{j,j+1}} \mathrm{Spoly}(G_j, G_{j+1})) < \delta$.

定理 2.3.1 理想基 $\boldsymbol{G}$ 是 Groebner 基的充分必要条件是对任何 $P, Q \in \boldsymbol{G}$，$\mathrm{Spoly}(P, Q) \xrightarrow[G]{*} 0$.

证明 必要性是显然的，只需证明充分性. 而按定义，又只需证对任何 $P \in \langle \boldsymbol{G} \rangle$，存在 $G_j \in \boldsymbol{G}$，使得 $\mathrm{lt}(G_j) \mid \mathrm{lt}(P)$.

因为 $P \in \langle \boldsymbol{G} \rangle$，故 P 有表示

$$P = \sum_i H_i G_i , \tag{2.3.7}$$

且 $\mathrm{md}(P) \leqslant \max\{\mathrm{md}(H_i G_i)\} = \delta$. 因这种表示可能不唯一，对每种表示存在一个相应的 δ. 因单项序是良序，每个非空子集有极小元，故这样的 δ 有极小元，假定所取的表示所对应的 δ 是极小的. 我们将证明 $\mathrm{md}(P) = \delta$，因为一旦如此，则有 $H_j G_j$ 使得 $\mathrm{md}(P) = \mathrm{md}(H_j G_j)$，即 $\mathrm{lt}(G_j) \mid \mathrm{lt}(P)$，从而完成证明.

用反证法. 设 $\mathrm{md}(P)<\delta$, 将式 (2.3.7) 改写成

$$\begin{aligned}P&=\sum_{\mathrm{md}(H_iG_i)=\delta}H_iG_i+\sum_{\mathrm{md}(H_iG_i)<\delta}H_iG_i\\&=\sum_{\mathrm{md}(H_iG_i)=\delta}\mathrm{lm}(H_i)G_i+\sum_{\mathrm{md}(H_iG_i)=\delta}(H_i-\mathrm{lm}(H_i))G_i\\&\quad+\sum_{\mathrm{md}(H_iG_i)<\delta}H_iG_i.\end{aligned}$$

因为第二、第三个和式的领项的多重次数都小于 δ, 又 $\mathrm{md}(P)<\delta$, 故必有

$$\mathrm{md}\Big(\sum_{\mathrm{md}(H_iG_i)=\delta}\mathrm{lm}(H_iG_i)\Big)<\delta.$$

由引理 2.3.1, 在对 G_i 重新排序后, 存在常数 $c_{j,j+1}$, 使得

$$\sum_{\mathrm{md}(H_iG_i)=\delta}\mathrm{lm}(H_i)G_i=\sum_j c_{j,j+1}X^{\delta-\gamma_{j,j+1}}\mathrm{Spoly}(G_j,\ G_{j+1}),$$

且有 $\mathrm{md}(X^{\delta-\gamma_{j,j+1}}\mathrm{Spoly}(G_j,\ G_{j+1}))<\delta$. 由假设知, 每个 $\mathrm{Spoly}(G_j,\ G_{j+1})$ 都可以被约化为 0, 由命题 2.2.2 知, $\mathrm{Spoly}(G_j,\ G_{j+1})$ 可表示成

$$\mathrm{Spoly}(G_j,\ G_{j+1})=\sum_k H_{j,k}G_k.$$

且有 $\mathrm{md}(H_{j,k}G_i)\leqslant\mathrm{md}(\mathrm{Spoly}(G_j,\ G_{j+1}))$. 于是

$$\begin{aligned}\sum_{\mathrm{md}(H_iG_i)=\delta}\mathrm{lm}(H_i)G_i&=\sum_j c_{j,j+1}X^{\delta-\gamma_{j,j+1}}\mathrm{Spoly}(G_j,G_{j+1})\\&=\sum_j c_{j,j+1}X^{\delta-\gamma_{j,j+1}}\Big(\sum_k H_{j,k}G_k\Big)\\&=\sum_k\Big(\sum_j(c_{j,j+1}X^{\delta-\gamma_{j,j+1}}H_{j,k})\Big)G_k,\end{aligned}$$

且

$$\begin{aligned}&\mathrm{md}(X^{\delta-\gamma_{j,j+1}}H_{j,k}G_k)\\<&\mathrm{md}(X^{\delta-\gamma_{j,j+1}})+\mathrm{md}(\mathrm{Spoly}(G_j,G_{j+1}))\\=&\mathrm{md}(X^{\delta-\gamma_{j,j+1}}\mathrm{Spoly}(G_j,G_{j+1}))\\<&\delta.\end{aligned}$$

这表明存在 P 的表示

$$\begin{aligned}P=&\sum_k\sum_j(c_{j,j+1}X^{\delta-\gamma_{j,j+1}}H_{j,k})G_k\\&+\sum_{\mathrm{md}(H_iG_i)=\delta}(H_i-\mathrm{lm}(H_i))G_i+\sum_{\mathrm{md}(H_iG_i)<\delta}H_iG_i.\end{aligned}$$

此时右端的每个和式中的项都满足 $\mathrm{md}(HG_i)<\delta$, 这与 δ 的定义矛盾, 从而必有 $\mathrm{md}(P)=\delta$.

推论 2.3.1 如果 $\boldsymbol{G}$ 为 Groebner 基, $P\in\boldsymbol{K}[X]$, 则 $\mathrm{Reduce}(P,\ \boldsymbol{G})$ 是唯一的.

证明 设 $R=\mathrm{Reduce}(P,\ \boldsymbol{G})$. 若另有 R' 使得 $R'=\mathrm{Reduce}(P,\ \boldsymbol{G})$, 则 $R'-R\in\langle\boldsymbol{G}\rangle$. 若 $R-R'\neq 0$, 则 $R'-R$ 的某项可被 $\boldsymbol{G}$ 中某多项式 G 的领项整除, 但是该项必为 R 或 R' 的某项, 这说明 R 或 R' 关于 $\boldsymbol{G}$ 不是约化的, 与 R, R' 的定义矛盾, 故必有 $R=R'$.

推论 2.3.1 说明, 若 G 为 Groebner 基, 则 $R=\mathrm{Reduce}(P,\ \boldsymbol{G})$ 与约化次序无关.

2.3.2 Buchberger 算法

假设 $I \subset K[X]$ 为一多项式理想，$S \subset I$ 为给定的理想基，一个自然的问题就是如何由 S 出发构造 I 的 Groebner 基 G.

定理 2.3.1 表明，一个理想基 S 为 Groebner 基当且仅当 S 中的任何两个多项式的 S-多项式可以模 S 约化为 0. 该定理一方面告诉我们如何判断一个理想基是否为 Groebner 基，另一方面也提示我们怎样由一个理想基构造 Groebner 基. 当给定一理想基 S 以后，任意取两个多项式 P，$Q \in S$，然后模 S 约化 $\mathrm{Spoly}(P, Q)$，当 $R = \mathrm{Reduce}(\mathrm{Spoly}(P, Q), S) \neq 0$ 时，令 $S_1 = S \cup \{R\}$，则显然 S_1 仍为 I 的理想基，且有

$$\mathrm{Spoly}(P, Q) \xrightarrow{*}_{s_1} 0.$$

再对 S_1 重复上述过程，又可得一新多项式组 S_2. 继续下去，则可得到一多项式集合序列 S，S_1，…，S_k，… 这种算法就是所谓的 Buchberger 算法. 需要证明的是：① 这个序列是有限的；② 最后得到的多项式集合，比如说，S_l，即为 Groebner 基.

先来看一个例子.

例 2.3.3 设 $S = \{G_1, G_2, G_3\}$，其中

$$G_1 = x^2 + yz - 2,$$

$$G_2 = y^2 + xz - 3,$$

$$G_3 = xy + z^2 + 5.$$

依照分次反字典序，先取 G_1，G_2 计算，得

$$\begin{aligned}\mathrm{Spoly}(G_1, G_2) &= x^2(x^2 + yz - 2) - z^2(y^2 + xz - 3)\\ &= -x^3z + y^3z + 3x^2 - 2y^2\\ &\xrightarrow{*}_{G_1} y^3z + xyz^2 + 3x^2 - 2y^2 - 2xz\\ &\xrightarrow{*}_{G_2} 3x^2 - 2y^2 - 2xz + 3yz\\ &\xrightarrow{*}_{G_1} -2y^2 - 2xz + 6\\ &\xrightarrow{*}_{G_2} 0.\end{aligned}$$

再取 G_1，G_3 计算，得

$$\begin{aligned}\mathrm{Spoly}(G_1, G_3) &= y^2z - xz^2 + 5x - 2y\\ &\xrightarrow{*}_{G_2} -2xz^2 + 5x - 2y + 3z.\end{aligned}$$

令 $G_4 = -2xz^2 + 5x - 2y + 3z$，$S_1 = S \cup \{G_4\}$，继续计算：

$$\mathrm{Spoly}(G_2, G_3) \xrightarrow{*}_{G_1} G_5 = -2yz^2 - 3x + 5y + 2z,$$

$$S_2 = S_1 \cup \{G_5\},$$

$$\mathrm{Spoly}(G_1, G_4) \xrightarrow{*}_{s_1} 0,$$

$$\mathrm{Spoly}(G_2, G_4) \xrightarrow{*}_{s_1} 0,$$

$$\mathrm{Spoly}(G_3, G_4) \xrightarrow{*}_{s_1} G_6,$$

$$G_6 = -2z^4 - 2xz - 3yz + 15z^2 - 19.$$

再令 $\boldsymbol{S}_3 = \boldsymbol{S}_2 \cup \{G_6\}$，经计算可知，对 $\boldsymbol{S}_3$ 中任何两个多项式，其 S-多项式都可模 $\boldsymbol{S}_3$ 约化为 0，因此 $\boldsymbol{S}_3$ 为 Groebner 基.

算法 2.3.1 Buchberger 算法.

```
Input S={G1,G2,…,Gk};
Output Groebner basis G such that ⟨G⟩=⟨S⟩;
    G:=S;
    B:={(i, j) | 1≤i<j≤k};
    while B≠∅ do
          Select(i, j)∈B;
          B:=B−{(i, j)};
          H=Reduce(Spoly(Gi, Gj), G);
          if H≠0 then;
            G:=G∪{H};
            k:=k+1;
            B:=B∪{(i, k) |1≤i<k};
```

定理 2.3.2 算法 2.3.1 是正确的.

证明 1)终止性. 记初始的多项式集合为 $\boldsymbol{G}_0$. 一般地，若在算法进入 while 之前的多项式集合为 $\boldsymbol{G}_k$，则在每次循环之后所得的多项式集合记为 $\boldsymbol{G}_{k+1}$. 考虑理想链 $\boldsymbol{I}_k = \langle \mathrm{lt}(G) \mid G \in \boldsymbol{G}_k \rangle$. 因 $\boldsymbol{G}_{k+1}$ 是由 $\boldsymbol{G}_k$ 加入多项式 H 而得，而 H 关于 $\boldsymbol{G}_k$ 是约化的，故必有 $\mathrm{lt}(H) \notin \boldsymbol{I}_k$，即有

$$\boldsymbol{I}_0 \subsetneq \boldsymbol{I}_1 \subsetneq \cdots \subsetneq \boldsymbol{I}_k \subsetneq \cdots.$$

由理想的升链条件，即任何单调不减的理想链只能由有限个理想组成(见附录 A)，必存在 N，使得当 $k \geqslant N$ 时

$$\boldsymbol{I}_k = \boldsymbol{I}_N.$$

成立. 于是在 $k > N$ 以后不再向指标集 B 加入新的指标对，但是 B 是有限集，因此在有限步内 B 变为空集. 算法终止.

2)正确性. 设算法终止时的多项式集合为 $\boldsymbol{G}$，则对任意一对 G_i，$G_j \in \boldsymbol{G}$，由算法可知有

$$\mathrm{Reduce}(\mathrm{Spoly}(G_i, G_j), \boldsymbol{G}) = 0.$$

再由定理 2.3.1，即知 $\boldsymbol{G}$ 为 Groebner 基.

事实上，在 Buchberger 算法中，并非每对多项式的 S-多项式都需要约化，利用下面的结果，可以找出那些 S-多项式必定可以约化为零的多项式对. 在算法中去掉这些多项式对的约化，则可大大提高计算效能.

定理 2.3.3(Buchberger 算法的第一判别准则) 设 $\boldsymbol{F}$ 为有限多项式集合，P，$Q \in \boldsymbol{F}$ 且 $\mathrm{lt}(P)\mathrm{lt}(Q) = \mathrm{lcm}(\mathrm{lt}(P), \mathrm{lt}(Q))$，即 $\mathrm{lt}(P)$，$\mathrm{lt}(Q)$ 互素，则

$$\mathrm{Spoly}(P, Q) \xrightarrow{}_{F} 0.$$

证明 留作练习.

为了介绍 Buchberger 算法的的第二判别准则，需要引进一个定义.

定义 2.3.3 设 $\boldsymbol{F} \subset \boldsymbol{K}[X]$ 为一多项式的有限集合，$P \in \boldsymbol{K}[X]$，$t \in \boldsymbol{T}$，如果

$$P=\sum_{i=1}^{k} m_i G_i\,, \tag{2.3.8}$$

其中 m_i 为非零单项式，$G_i \in \boldsymbol{F}$ 未必两两互异，且

$$\max\{\mathrm{lt}(m_i G_i) \mid 1 \leqslant i \leqslant k\} \leqslant t\,, \tag{2.3.9}$$

则称其为 P 关于 $\boldsymbol{F}$ 的一个 t- **表示**. 如果 $t=\mathrm{lt}(P)$，则称 P 关于 $\boldsymbol{F}$ 有一**标准表示**.

下面先来介绍 Groebner 基的一些重要性质.

定理 2.3.4 设 $\boldsymbol{G}$ 为有限多项式集合且 $0 \notin \boldsymbol{G}$，则 $\boldsymbol{G}$ 为 Groebner 基当且仅当每个 $0 \neq P \in \langle \boldsymbol{G} \rangle$ 关于 $\boldsymbol{G}$ 有一标准表示.

证明 留作练习.

定理 2.3.5 设 $\boldsymbol{G}$ 为有限多项式集合且 $0 \notin \boldsymbol{G}$，如果对所有的多项式对 G_1，$G_2 \in \boldsymbol{G}$，$\mathrm{Spoly}(G_1, G_2)$ 或者为零或者对某 $t < \mathrm{lcm}(\mathrm{lt}(G_1), \mathrm{lt}(G_2))$，它关于 $\boldsymbol{G}$ 有一 t- 表示，则 $\boldsymbol{G}$ 为一 Groebner 基.

证明 我们来证每个 $0 \neq P \in \langle \boldsymbol{G} \rangle$ 关于 $\boldsymbol{G}$ 有一标准表示，再由定理 2.3.4，即可知本定理成立.

设 $0 \neq P \in \langle \boldsymbol{G} \rangle$ 关于 $\boldsymbol{G}$ 有一表示

$$P=\sum_{i=1}^{k} m_i G_i\,, \tag{2.3.9}'$$

其中 $m_i = a_i t_i$ 为非零单项式，$G_i \in \boldsymbol{G}$ 未必两两互异. 设

$$s = \max\{\mathrm{lt}(m_i G_i) \mid 1 \leqslant i \leqslant k\}$$

为所有这样的表示中的最小者，需要证明 $s = \mathrm{lt}(P)$.

如果 $s > \mathrm{lt}(P)$，我们将用归纳法证明存在 P 关于 $\boldsymbol{G}$ 的一 s'- 表示，而 $s > s'$，这将与 s 的极小性相矛盾.

对式 $(2.3.9)'$ 中使得 $\mathrm{lt}(m_i G_i) = s$ 的指标 i 的个数 l 做归纳法. 当 $l=1$ 时，显然结论正确. 设 $l=2$，不失一般性，假设 $\mathrm{lt}(m_1 G_1) = \mathrm{lt}(m_2 G_2) = s$. 这意味着

$$s = t_1 \mathrm{lt}(G_1) = t_2 \mathrm{lt}(G_2)\,,$$

因而 $\mathrm{lcm}(\mathrm{lt}(G_1), \mathrm{lt}(G_2)) \mid s$. 设 $s = u \cdot \mathrm{lcm}(\mathrm{lt}(G_1), \mathrm{lt}(G_2))$，因为式 $(2.3.9)'$ 右端的最高项必须消去，故有

$$\mathrm{lm}(m_1 G_1) = -\mathrm{lm}(m_2 G_2)\,,$$

从而

$$a_1 \mathrm{lc}(G_1) = -a_2 \mathrm{lc}(G_2)\,.$$

令 $a = a_1 \mathrm{lc}(G_1) = -a_2 \mathrm{lc}(G_2)$，不难证明

$$m_1 G_1 + m_2 G_2 = au\,\mathrm{Spoly}(G_1, G_2)\,. \tag{2.3.10}$$

由假设，$\mathrm{Spoly}(G_1, G_2) = 0$ 或者对某 $t < \mathrm{lcm}(\mathrm{lt}(G_1), \mathrm{lt}(G_2))$ 有 t- 表示

$$\mathrm{Spoly}(G_1, G_2) = \sum_{i=1}^{k'} m_i' G_i'\,,\ G_i' \in \boldsymbol{G}\,. \tag{2.3.11}$$

将式 (2.3.10) 代入式 $(2.3.9)'$ 得

$$P = \sum_{i=3}^{k} m_i G_i + au \sum_{i=1}^{k'} m_i' G_i'\,, \tag{2.3.12}$$

由 s 的定义有

$$\max\{\mathrm{lt}(m_iG_i)\mid 3\leqslant i\leqslant k\}<s,$$
$$\max\{\mathrm{lt}(um_i'G_i')\mid 1\leqslant i\leqslant k'\}=ut<u\mathrm{lcm}(G_1,G_2)=s,$$

这说明式 (2.3.12) 为 P 的一个 s'- 表示，且有 $s'<s$.

现在假设结论对 $l-1>2$ 成立，则当 $\mathrm{lt}(m_iG_i)=s$ 的指标 i 的个数为 l 时，不妨假定仍有 $\mathrm{lt}(m_1G_1)=\mathrm{lt}(m_2G_2)=s$，则

$$\begin{aligned}P&=\sum_{i=1}^{k}m_iG_i\\&=m_1G_1-\frac{\mathrm{lc}(m_1G_1)}{\mathrm{lc}(m_2G_2)}m_2G_2+\left(\frac{\mathrm{lc}(m_1G_1)}{\mathrm{lc}(m_2G_2)}+1\right)m_2G_2+\sum_{i=3}^{k}m_iG_i.\end{aligned}\tag{2.3.13}$$

前两项中的 s 显然被消掉，由引理 2.3.1 以及 $l=2$ 情形的证明，前两项可以表示为 $\sum_i m_i'G_i'$，$\mathrm{lt}(m_i'G_i')<s$ 的形式. 因此式 (2.3.13) 中使得 $\mathrm{lt}(m_iG_i)=s$ 的指标 i 的个数为 $l-1$，由归纳假定，存在 P 的关于 $\boldsymbol{G}$ 的一 s'- 表示，而 $s>s'$.

定理 2.3.6(Buchberger 算法第二判别准则) 设 $\boldsymbol{F}$ 为有限多项式集合，G_1，G_2，$P\in\boldsymbol{K}[X]$ 使得下列条件成立

1) $\mathrm{lt}(P)\mid\mathrm{lcm}(\mathrm{lt}(G_1),\mathrm{lt}(G_2))$.

2) 对 $i=1,2$，$\mathrm{Spoly}(G_i,P)$ 关于 $\boldsymbol{F}$ 有 t_i- 表示，并且 $t_i<\mathrm{lcm}(\mathrm{lt}(G_i),\mathrm{lt}(P))$.

则对某 $t<\mathrm{lcm}(\mathrm{lt}(G_1),\mathrm{lt}(G_2))$，多项式 $\mathrm{Spoly}(G_1,G_2)$ 关于 $\boldsymbol{F}$ 有 t- 表示.

证明 留作练习.

利用 Buchberger 算法的两个判别准则，可以将算法 2.3.1 加以改进，请读者自己完成这个工作.

2.3.3 Groebner 基的应用

在符号计算领域，特别是在多项式代数的理论研究与计算中，Groebner 基方法扮演着十分重要的角色，而且它在诸多理论研究与实际问题中也都起着重要作用. 我们这里仅举几个简单的例子.

1. 商环中的计算

对给定的多项式理想 $\boldsymbol{I}\subset\boldsymbol{K}[X]$，可以定义 $\boldsymbol{K}[X]$ 上的等价关系 $\sim$ 如下：对任何 A，$B\in\boldsymbol{K}[X]$，$A\sim B$ 当且仅当 $A-B\in\boldsymbol{I}$，此时我们也称 A 与 B 是模 $\boldsymbol{I}$ 同余的，记作 $A\equiv B \bmod \boldsymbol{I}$. $\boldsymbol{K}[X]$ 中这种等价类全体构成的集合在定义恰当的运算后可得一交换环，称为 $\boldsymbol{K}[X]$ 对 $\boldsymbol{I}$ 的商环(见附录 A)，记作 $\boldsymbol{K}[X]/\boldsymbol{I}$. 我们期望能够实现商环中的各种计算，而 Groebner 基恰好就是一种有效的工具.

对于全体单项的集合 $\boldsymbol{T}$，利用 Groebner 基可以将其分为两部分，一部分是 Groebner 基中多项式的领项的倍式全体 $\{t\in\boldsymbol{T}\mid$ 存在 $P\in\boldsymbol{G}$，使得 $\mathrm{lt}(P)\mid t\}$，另一部分是它关于 $\boldsymbol{T}$ 的补集 $\boldsymbol{N}=\boldsymbol{T}-\{t\mid$ 存在 $P\in\boldsymbol{G}$ 使得 $\mathrm{lt}(P)\mid t\}$. 对于任何 $P\in\boldsymbol{K}[X]$，若记 $R=\mathrm{Reduce}(P,\boldsymbol{G})$，则易见有

$$R=\sum_{u\in\boldsymbol{N}}c_uu,$$

且若记 $[P]$ 为 P 的模 $\boldsymbol{I}$ 同余类，则有 $R \in [P]$. 因此有可能用 Span$\{\boldsymbol{N}\}$ 中的运算来表示商环中的运算.

定理 2.3.7 设 $\boldsymbol{I} \subset \boldsymbol{K}[X]$ 为多项式理想，$\boldsymbol{G} \subset \boldsymbol{I}$ 为 $\boldsymbol{I}$ 的关于某个单项序的 Groebner 基，定义

$$\boldsymbol{U} = \{[u] \mid u \in \boldsymbol{N}\},$$

其中 $[u]$ 表示 u 的模 $\boldsymbol{I}$ 的同余类，则 $\boldsymbol{U}$ 是商环 $\boldsymbol{K}[X]/\boldsymbol{I}$ 的一组向量空间基.

证明 只需证明 $\boldsymbol{U}$ 中元是线性无关的，且任何 $[P] \in \boldsymbol{K}[X]/\boldsymbol{I}$ 都可由 $\boldsymbol{U}$ 中元线性表示. 对于任何 $P \in \boldsymbol{K}[X]$，由推论 2.3.1 知，存在唯一的 R，使得 $R = \text{Reduce}(P, \boldsymbol{G})$，$R \in \text{Span}\{\boldsymbol{N}\}$ 且 $[P] = [R]$. 由此可知商环中任何元素都可以表示成 $\boldsymbol{U}$ 中元素的线性组合. 其次，如果在 $\boldsymbol{U}$ 中有线性关系

$$a_1[u_1] + \cdots + a_m[u_m] = 0,$$

其中 $a_i \in \boldsymbol{K}$，$u_i \in \boldsymbol{N}$，$i = 1, \cdots, m$，则有 $P = a_1 u_1 + \cdots + a_m u_m \in \boldsymbol{I}$. 倘若存在 $a_i \neq 0$，则 P 必可模 $\boldsymbol{G}$ 约化为 0. 由此推得存在某 u_i 可被 $\boldsymbol{G}$ 中某多项式的领项整除，这与 u_i 的定义矛盾，故必 $a_i = 0$，$i = 1, \cdots, m$，即 $\boldsymbol{N}$ 中元是线性无关的.

定理 2.3.7 表明，商环 $\boldsymbol{K}[X]/\boldsymbol{I}$ 与 Span$\{\boldsymbol{N}\}$ 作为向量空间是同构的，因此商环中 $[P]$，$[Q]$ 的加减法可以用 $R = \text{Reduce}(P, \boldsymbol{G})$，$S = \text{Reduce}(Q, \boldsymbol{G})$ 的加减法来表示，这是因为仍然有 $R + S \in \text{Span}\{\boldsymbol{N}\}$. 但是 $[P][Q]$ 却不能再用 RS 来表示，因为未必有 $RS \in \text{Span}\{\boldsymbol{N}\}$.

例 2.3.4 对例 2.3.3 中计算所得的 Groebner 基

$$\begin{aligned}\boldsymbol{G} = \{&x^2 + yz - 2,\ y^3 + xz - 3,\ xy + z^2 - 5,\\ &-2xz^2 + 5x - 2y + 3z,\ -2yz - 3x + 5y + 2z,\\ &-2z^4 - 2xz - 3yz + 15z^2 - 19\},\end{aligned}$$

商环 $\mathbb{Q}[x, y, z]/\langle \boldsymbol{G} \rangle$ 的向量空间基为

$$\begin{aligned}\boldsymbol{U} = \{&[1], [x], [y], [z],\\ &[xz], [yz], [z^2], [z^3]\}.\end{aligned}$$

虽然 xz，$yz \in \text{Span}\{\boldsymbol{N}\}$，但是 $xyz^2 \notin \text{Span}\{\boldsymbol{N}\}$. 因此要计算 $[xz][yz]$，还需要计算

$$\text{Reduce}(xyz^2, \boldsymbol{G}) = xz + \frac{3}{2}yz - \frac{5}{2}z^2 + \frac{19}{2},$$

从而

$$[xz][yz] = [xz] + \frac{3}{2}[yz] - \frac{5}{2}[z^2] + \frac{19}{2}[1].$$

一般说来，对于给定的理想，相应的商环未必是一域. 但是当商环是有限维向量空间时，利用 Groebner 基可以判断商环中某一元素是否可逆，并在其可逆时求得其逆元素.

例 2.3.5 考虑例 2.3.4 中的 $[x]$，如果其可逆，则其逆元也必为商环中的元，设其逆元为

$$[Q] = a_0[1] + a_1[x] + a_2[y] + a_3[z] + a_4[xz] + a_5[yz] + a_6[z^2] + a_7[z^3],$$

则其应满足 $[x][Q] = [1]$. 由此可得

$$P = x(a_0 + a_1 x + a_2 y + a_3 z + a_4 xz$$

$$+a_5yz+a_6z^2+a_7z^3)-1\in\langle \boldsymbol{G}\rangle .$$

约化得

$$\begin{aligned}\mathrm{Reduce}(P,\boldsymbol{G})=&(-1+2a_1+5a_2)+(a_0+3/2\,a_4+5/2\,a_6)x\\&+(-5/2\,a_4-a_6)y+(a_4+5a_5+3/2\,a_6)z\\&+(-a_1-a_7)yz+(a_3+5/2\,a_7)xz\\&+(-a_2+3/2\,a_7)z^2-a_5z^3.\end{aligned}$$

因为 $P\in\langle \boldsymbol{G}\rangle$，故必 $\mathrm{Reduce}(P,\boldsymbol{G})=0$. 由此推得所有系数为 0，于是得一关于 $a_0,\cdots,a_7$ 的线性方程组，解之得

$$a_0=a_4=a_5=a_6=0,\ a_1=-\frac{2}{11},\ a_2=\frac{3}{11},\ a_3=-\frac{5}{11},\ a_7=\frac{2}{11}.$$

最终有

$$[x]^{-1}=\frac{2}{11}[z^3]-\frac{2}{11}[x]+\frac{3}{11}[y]-\frac{5}{11}[z].$$

2. 多项式方程组求解

设

$$P_i(x_1,\cdots,x_n)=0,\ i=1,\cdots,m,$$

为域 $\boldsymbol{K}$ 上的多项式方程组，要求解这样一方程组，自然应该解决以下几个问题：该方程组是否有解，有多少解，怎样求解. 考虑由该方程组的多项式生成的理想 $\langle P_1,\cdots,P_m\rangle\subset\boldsymbol{K}[X]$，计算其关于某单项序的 Groebner 基 $\boldsymbol{G}$，那么以上几个问题都可以通过 $\boldsymbol{G}$ 来解决.

在解决所提问题之前，先来介绍一个有关域的概念. 设 $\boldsymbol{K}$ 为一域，以 $\boldsymbol{K}$ 中元为系数的多项式的根称为 $\boldsymbol{K}$ 上的代数元. 如果 $\boldsymbol{K}$ 上的任何代数元均属于 $\boldsymbol{K}$，则称 $\boldsymbol{K}$ 为代数封闭域，简称代数闭域. 设 $\boldsymbol{K}$，$\boldsymbol{L}$ 为域，且 $\boldsymbol{K}\subset\boldsymbol{L}$，如果 $\boldsymbol{L}$ 中的元都是 $\boldsymbol{K}$ 上的代数元，且 $\boldsymbol{L}$ 是代数封闭的，则称 $\boldsymbol{L}$ 为 $\boldsymbol{K}$ 的代数闭包.

定理 2.3.8 设 $\boldsymbol{K}$ 为代数闭域，$\{P_1,\cdots,P_m\}\subset\boldsymbol{K}[X]$，$\boldsymbol{G}$ 为 $\langle P_1,\cdots,P_m\rangle$（关于任何单项序）的 Groebner 基，则方程组 $P_i=0$，$i=1,\cdots,m$，在 $\boldsymbol{K}$ 中有解当且仅当 $1\notin\boldsymbol{G}$.

证明 由 Hilbert 零点定理（见附录 A），$P_i=0$，$i=1,\cdots,m$，在 $\boldsymbol{K}$ 中无解当且仅当 $1\in\langle P_1,\cdots,P_m\rangle$. 而由 Groebner 基的定义，$1\in\langle P_1,\cdots,P_m\rangle$ 当且仅当 $1\in\boldsymbol{G}$. 因此方程组有解当且仅当 $1\notin\boldsymbol{G}$.

定理 2.3.8 解决了解的存在性问题，只要求出相应的 Groebner 基，便可以由其是否包含 1 而断定解的存在性. 下面的定理解决了解的有限性问题.

定理 2.3.9 设 $\boldsymbol{K}$ 为代数闭域，$\boldsymbol{G}$ 为 $\langle P_1,\cdots,P_m\rangle\subset\boldsymbol{K}[X]$（关于任何单项序）的 Groebner 基，则方程组 $P_i=0$，$i=1,\cdots,m$，在 $\boldsymbol{K}$ 中仅有有限多解当且仅当对每个 $j=1,\cdots,n$，存在正整数 m_j 及 $G_j\in\boldsymbol{G}$ 使得 $\mathrm{lt}(G_j)=x_j^{m_j}$.

证明 设方程组 $P_i=0$，$i=1,\cdots,m$，在 $\boldsymbol{K}$ 中仅有有限多个解 $\{a_1,\cdots,a_r\}\subset\boldsymbol{K}$，记 $a_k^{(j)}$ 为 a_k 的第 j 个分量，则

$$F=(x_j-a_1^{(j)})(x_j-a_2^{(j)})\cdots(x_j-a_r^{(j)})$$

在 $\{a_1,\cdots,a_r\}$ 上取 0 值，由 Hilbert 零点定理，存在正整数 m 使得 $F^m\in\langle P_1,\cdots,P_m\rangle$. 由 Groebner 基的定义，存在 $G_j\in\boldsymbol{G}$ 使得 $\mathrm{lt}(G_j)\mid\mathrm{lt}(F^m)$. 但是 F 为仅含 x_j 的多项式，故有 m_j，使得 $\mathrm{lt}(G_j)=x_j^{m_j}$.

反之，若有 $G_j\in\boldsymbol{G}$ 及 m_j，使得 $\mathrm{lt}(G_j)=x_j^{m_j}$，则 $\boldsymbol{N}=\boldsymbol{T}-\{t\mid t\in\langle\mathrm{lt}(\boldsymbol{G})\rangle\}\subset\{x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\mid i_1<m_1,\cdots,i_n<m_n\}$. 因后者是有限集，故 $\boldsymbol{N}$ 也为有限集. 由定理 2.3.7，商环是有限维的向量空间. 于是对任何 $j=1,\cdots,n$，存在 d_j 使得$[1],[x_j],[x_j^2],\cdots,[x_j^{d_j}]$是线性相关的. 即有

$$Q_j=a_0+a_1x_j+a_2x_j^2+\cdots+a_{d_j}x_j^{d_j}\in\langle P_1,\cdots,P_m\rangle.$$

但是每个 $Q_j=0$ 的解的个数是有限的，故方程组 $P_i=0$，$i=1,\cdots,m$，的解的个数有限.

例 2.3.6 在例 2.3.3 中我们给出了一组多项式

$$G_1=x^2+yz-2,$$
$$G_2=y^2+xz-3,$$
$$G_3=xy+z^2-5.$$

例 2.3.3 中计算了 $\langle G_1,G_2,G_3\rangle$ 的 Groebner 基

$$\begin{aligned}\boldsymbol{G}=\{&x^2+yz-2,y^2+xz-3,xy+z^2-5,\\&-2xz^2+3x-2y+3z,2yz^2+3x+5y+2z,\\&-2z^4-2xz-3yz+15z^2-19\}.\end{aligned}$$

其中 x^2，y^2 以及 z^4 都出现在某些多项式的领项当中，所以方程组

$$x^2+yz-2=0,$$
$$y^2+xz-3=0,$$
$$xy+z^2-5=0,$$

仅有有限多个解.

需要注意的是，定理 2.3.9 所叙述的“仅有有限多个解”是指在代数闭域中有限. 当系数域不是代数闭域时，结论未必正确. 例如取 $P=x^2+y^2\in\mathbb{Q}[X]$，则 $P=0$ 在 $\mathbb{Q}$ 只有一解 $(0,0)$. 注意 P 本身就是 $\langle P\rangle$ 的 Groebner 基，无论取哪种单项序，领项只能取 x^2 或 y^2 之中的一个. 实际上在复数域 $\mathbb{C}$ $P=0$ 有无穷多解.

以下假定方程组仅有有限多解，我们来讨论其求解方法. 设给定 $\boldsymbol{K}[X]$ 中的一方程组

$$P_1(X)=0,\ P_2(X)=0,\cdots,P_m(X)=0.$$

选取字典序(假定未定元之间的排列为 $x_1>x_2>\cdots>x_n$)计算理想 $<P_1,\cdots,P_m>$ 的 Groebner 基 $\boldsymbol{G}=\{G_1,G_2,\cdots,G_r\}$. 由定理 2.3.12，在对 $\boldsymbol{G}$ 中的多项式适当排序后，存在 $G_i\in\boldsymbol{G}$ 与 m_i 使得 $\mathrm{lt}(G_i)=x_i^{m_i}$，$i=1,\cdots,n$. 由此可推知必有 $n\leqslant r$. 因为所用的序是字典序，$\mathrm{lt}(G_n)=x_n^{m_n}$，$G_n$ 的其他项也必仅含 x_n，也就是说，G_n 是 x_n 的一元多项式. 同理分析可知，G_{n-1} 仅含未定元 x_{n-1}，x_n. 类推下去，可知 $\boldsymbol{G}$ 包含了如下的多项式组.

$$G_1 = G_1(x_1, x_2, \cdots, x_n),$$
$$G_2 = G_2(x_2, \cdots, x_n),$$
$$\cdots\cdots$$
$$G_{n-1} = G_{n-1}(x_{n-1}, x_n),$$
$$G_n = G_n(x_n).$$

由最后一个方程 $G_n = 0$ 解出一组 x_n 的解 $\{a_{n1}, \cdots, a_{nl}\}$，再将每个 $a_{ni}, i = 1, \cdots, l$，代入 G_{n-1} 以及其他 $\boldsymbol{G}$ 中仅包含 x_{n-1}，x_n 的多项式 $G_j(x_{n-1}, x_n), \cdots$ 可得一组含 x_{n-1} 的方程组 $G_{n-1}(x_{n-1}, a_i) = 0$，$G_j(x_{n-1}, a_{ni}) = 0, \cdots$ 这仍然是一个一元多项式方程组，解之又可得一组对应 x_{n-1} 的解．继续下去即可求得原方程组的全部解．

例 2.3.7 对例 2.3.3 中的多项式

$$G_1 = x^2 + yz - 2 = 0,$$
$$G_2 = y^2 + xz - 3 = 0,$$
$$G_3 = xy + z^2 - 5 = 0.$$

我们已知它仅有有限多个解．计算 $< G_1, G_2, G_3 >$ 的字典序下的 Groebner 基，得

$$\boldsymbol{G} = \left\{ x - \frac{88}{361}z^7 + \frac{872}{361}z^5 - \frac{2690}{361}z^3 + \frac{125}{19}z, \right.$$
$$y + \frac{8}{361}z^7 + \frac{52}{361}z^5 - \frac{740}{361}z^3 + \frac{75}{19}z,$$
$$\left. z^8 - \frac{25}{2}z^6 + \frac{219}{4}z^4 - 95z^2 + \frac{361}{8} \right\}.$$

从第三个多项式方程

$$z^8 - \frac{25}{2}z^6 + \frac{219}{4}z^4 - 95z^2 + \frac{361}{8} = 0$$

可以解出 8 个根，代入前两个方程即可得全部解．

2.3.4 多项式的理想-adic 表示

本节我们讨论多项式的理想-adic 表示．这种表示在符号计算的许多算法中要用到．设 $A \in \boldsymbol{K}[X]$ 为给定的多项式，$\boldsymbol{I} \subset \boldsymbol{K}[X]$ 为多项式理想．我们期望将 A 表示为

$$A = A^{(0)} + A^{(1)} + \cdots + A^{(m)}$$

的形式，其中 m 为充分大的正整数，且 $A^{(i)} \in \boldsymbol{I}^i$，$i = 0, \cdots, m$，$\boldsymbol{I}^i$ 表示理想的乘幂(见附录 A)．多项式的这种表示称为 $\boldsymbol{I}$-adic **表示**．我们感兴趣的是 $\boldsymbol{I} = \langle x_2 - a_2, \cdots, x_n - a_n \rangle$ 的情形．容易看出，在 A 的 $\boldsymbol{I}$-adic 表示中成立

$$A = A^{(0)} + \cdots + A^{(i-1)} \bmod \boldsymbol{I}^i, \quad i = 1, \cdots, m+1.$$

因此只要知道了 $\boldsymbol{I}^i$ 的 Groebner 基 $\boldsymbol{G}^{(i)}$，$A^{(i)}$ 就可以递推地确定出来

$$A^{(i)} = \text{Reduce}(A - (A^{(0)} + \cdots + A^{(i-1)}), \boldsymbol{G}^{(i+1)}).$$

所以我们只要求出 $\boldsymbol{G}^{(i)}$ 即可．

当 $i = 1$ 时，容易验证 $\boldsymbol{G}^{(1)} = \{x_2 - a_2, \cdots, x_n - a_n\}$．

当 $i = 2$ 时，按照理想的乘幂的定义，$(x_k - a_k)(x_l - a_l) \in \boldsymbol{I}^2$，$2 \leqslant k \leqslant l \leqslant n$．并且可以证明，它们确实构成 $\boldsymbol{I}^2$ 的理想基，且为 Groebner 基．换言之，

$$\boldsymbol{G}^{(2)}=\{(x_k-a_k)(x_l-a_l),2\leqslant k\leqslant l\leqslant n\}.$$

容易看出，$\boldsymbol{G}^{(2)}$ 中的多项式与齐 2 次 $n-1$ 元单项式是一一对应的. 应用组合数学的知识可知，在 $\boldsymbol{G}^{(2)}$ 中计有 $\binom{n-2+2}{n-2}$ 个多项式. 一般地，对于 $\boldsymbol{I}^i$，仿 $i=2$ 的情形可得

$$\boldsymbol{G}^{(i)}=\{(x_{k_1}-a_{k_1})(x_{k_2}-a_{k_2})\cdots(x_{k_i}-a_{k_i}),2\leqslant k_1\leqslant k_2\leqslant\cdots\leqslant k_i\leqslant n\}.$$

此时 $\boldsymbol{G}^{(i)}$ 中的多项式是与齐 i 次 $n-1$ 元单项式一一对应的，计有 $\binom{n-2+i}{n-2}$ 个. 为了书写方便，对应每个 $\boldsymbol{G}^{(i)}$，定义 $n-1$ 重指标集

$$\boldsymbol{J}^{(i)}=\{(j_2,j_3,\cdots,j_n)\mid 0\leqslant j_k\leqslant i,\ j_2+\cdots+j_n=i\},$$

则 $\boldsymbol{G}^{(i)}$ 可以表示成

$$\boldsymbol{G}^{(i)}=\{G_S^{(i)}\mid S\in\boldsymbol{J}^{(i)}\},$$

其中 $G_S^{(i)}=(x_2-a_2)^{j_2}\cdots(x_n-a_n)^{j_n}$，$S=(j_2,\cdots,j_n)\in\boldsymbol{J}^{(i)}$.

利用前面定义的记号，可将每个 $A\in\boldsymbol{K}[X]$ 表示为

$$A=\sum_{i=0}^{d}\sum_{S\in J^{(i)}}A_S^{(i)}(x_1)G_S^{(i)}(x_2,\cdots,x_n)$$

其中 $d=\deg(A)$.

例 2.3.8 对于多项式

$$A=x^2y^4z-xy^9z^2+xyz^3+2x-y^6z^4-2y^5z,$$

取 $\boldsymbol{K}=Z_5$，$\boldsymbol{I}=\langle y-1,z-1\rangle$，则有

$$\boldsymbol{G}^{(1)}=\{y-1,z-1\},$$

$$\boldsymbol{G}^{(2)}=\{(y-1)^2,(y-1)(z-1),(z-1)^2\},$$

……

而相应的系数 $A_S^{(i)}(x)$ 为

$$A_{(0,0)}^{(0)}=x^2+2x+2,\quad A_{(1,0)}^{(1)}=-(x-1)^2,$$

$$A_{(0,1)}^{(1)}=x^2+x-1,\quad A_{(2,0)}^{(2)}=x^2-x,$$

$$A_{(1,1)}^{(2)}=-(x^2-1),\quad A_{(0,2)}^{(2)}=2x-1,$$

$$A_{(3,0)}^{(3)}=-(x^2-x),\quad A_{(2,1)}^{(3)}=x^2-2x,$$

$$A_{(1,2)}^{(3)}=-(x+1),\quad A_{(0,3)}^{(3)}=x+1,$$

…… ……

$$A_{(10,0)}^{(10)}=0,\quad A_{(9,1)}^{(10)}=-2x,$$

$$A_{(8,2)}^{(10)}=x,\quad A_{(6,4)}^{(10)}=-1,$$

$$A_{(9,2)}^{(11)}=-x.$$

在上标大于等于 10 的系数中，没有写出来的都是 0.

2.4 吴 方 法

吴方法，又称特征列方法，是吴文俊于 20 世纪 70 年代提出的处理多项式代数问题

的一种方法．与 Groebner 基方法不同之处在于，它完全采用零点集的观点来处理问题，因此在定理证明、多项式方程组求解以及其他许多方面较 Groebner 基方法更有效．现在吴方法在数学理论研究、理论物理、机器人制造等诸多领域都得到了广泛的应用．限于篇幅，我们这里不可能对其做详细的介绍，只给出一些基本概念以及解多项式方程组与定理证明的简单例子．

2.4.1 升列、基列与特征列

设 $\boldsymbol{K}$ 为特征为 0 的域．$\boldsymbol{K}[x_1,\cdots,x_n]$ 为多项式环．此后我们总假定所用的单项序为字典序，且未定元的序为 $x_1 < x_2 < \cdots < x_n$．这一点和我们以前定义的字典序实质上是一样的，只不过未定元的次序交换一下而已．

对于给定的单项式 $at = ax_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \in \boldsymbol{K}[x_1,\cdots,x_n]$，在 t 的多重次数中，如果最后一个不为零的是 i_p，则称 t 的**类**(class)为 p，并记作 $\mathrm{cl}(t) = p$．非零常数的类定义为 0．

如果一个单项式的类为 p，这个单项必定含未定元 x_p，且必定不含 $x_{p+1},\cdots,x_n$．例如，$x_1 x_2 x_3$ 与 x_3^2 的类都是 3．

对任何 $F \in \boldsymbol{K}[x_1,\cdots,x_n]$，可以按单项由大到小的次序排列，将其表示为

$$F = a_1 t_1 + a_2 t_2 + \cdots + a_s t_s,$$

其中 $a_i \in \boldsymbol{K}$ 为常数，$t_i \in \boldsymbol{K}[x_1,\cdots,x_n]$ 为单项．F 的领项的类称为 F **的类**，记作 $\mathrm{cl}(F)$．同理，当 $\mathrm{cl}(F) = p$ 时，F 必定不含未定元 $x_{p+1},\cdots,x_n$．

设 F 为一非零多项式，$\mathrm{cl}(F) = p$，且 F 的领项关于 x_p 的次数为 m，则 F 可表示为

$$F = C_0 x_p^m + C_1 x_p^{m-1} + \cdots + C_m,$$

其中 $C_0 \neq 0$，C_i，$0 \leqslant i \leqslant m$，是仅含未定元 $x_1,\cdots,x_{p-1}$ 的多项式．C_0 称为 F 的**初式**．如果 C_0 的领项为 $\overline{C}_0$，则 F 的领项显然为 $\overline{C}_0 x_p^m$．

设有两个多项式 F，G，考虑未定元 x_p，如果 $\deg_{x_p}(F) < \deg_{x_p}(G)$，则称 F **相对于** x_p **的级别**比 G 低．如果在这二者中，每个相对于 x_p 的级别都不比另一个低，则称二者相对于 x_p 具有相同的级别．注意这个概念与两个多项式的类没有关系．

对于两个非零多项式 F 和 G，如果下列两条件之一成立：

1) $\mathrm{cl}(F) < \mathrm{cl}(G)$．

2) $\mathrm{cl}(F) = \mathrm{cl}(G) = p > 0$，但 $\deg_{x_p}(F) < \deg_{x_p}(G)$．

我们称 F 的**级别**比 G 低(或者称 G 的级别比 F 高)，记作

$$F \prec G \text{ 或 } G \succ F.$$

如果在 F 和 G 中，每一个都不比另一个级别低，则称它们具有相同的级别，记作 $F \sim G$．注意在上述定义中，如果条件 1) 或 2) 之一成立，则必有 $\mathrm{lt}(F) < \mathrm{lt}(G)$(关于 $x_1 < \cdots < x_n$ 的字典序)；反之不然，例如对 $F = x_1 x_2^2 x_3$ 与 $G = x_1^2 x_3$，二者具有相同的级别，但 $x_1 x_2^2 x_3 > x_1^2 x_3$．

设 F 是一个多项式，$\mathrm{cl}(F) = p > 0$．对任何一个相对于 x_p 比 F 级别低的多项式 G 都称为**相对于** F **是约化的**，记为 $G\ \mathrm{red}/F$．

显然任何比 F 级别低的多项式都是相对于 F 约化的，特别地，F 的初式的类小于 F

的类，所以它相对于 F 是约化的，即一个多项式的初式相对于自己来说总是约化的．一般说来，相对于 F 约化的多项式未必比 F 的级别低．例如，对 $F=x_1x_2^2+x_1^2$，$G=x_1+x_2+x_3$，则有 G red$/F$，但是 $\mathrm{cl}(G)=3>\mathrm{cl}(F)=2$．此外，$G$ 相对于 x_p 比 F 的级别低并不意味着 G red$/F$．G red$/F$ 明确要求 $\mathrm{cl}(F)=p>0$，而 G 相对于 x_p 比 F 的级别低时，$\mathrm{cl}(F)$ 可以大于 p．

前面已经提到过，如果一多项式 F 的类 $\mathrm{cl}(F)=p$，则 F 可表示为

$$F=f_0x_p^m+f_1x_p^{m-1}+\cdots+f_m,$$

其中 $f_0\neq0$，$f_i\in\boldsymbol{K}[x_1,\cdots,x_{p-1}]$，$0\leqslant i\leqslant m$．对任何多项式 G，如果它相对于 F 不是约化的，那么它总可以写成

$$G=g_0x_p^M+g_1x_p^{M-1}+\cdots+g_M,$$

其中 $g_0\neq0$，$g_i\in\boldsymbol{K}[x_1,\cdots,x_{p-1},x_{p+1},\cdots,x_n]$，$0\leqslant i\leqslant M$，且 $M\geqslant m$．

视 F，G 为 $\boldsymbol{K}[x_1,\cdots,x_{p-1},x_{p+1},\cdots,x_n][x_p]$ 上的多项式，利用伪除概念，则有非负整数 s 使得

$$f_0^sG=QF+R.\tag{2.4.1}$$

容易看出，当 $R\neq0$ 时，必有 $\deg_{x_p}(R)<\deg_{x_p}(F)$，即有 R red$/F$．如果已经有 G red$/F$，取 $s=0$，$Q=0$，$R=G$，则 F 和 G 也可写成式 (2.4.1) 的形式，即对给定的 F 与任意的 G，总有 s，Q，R 存在，使得式 (2.4.1) 成立．因此我们称多项式 R 为 G 相对于 F 的(**伪**)**余式**，这种由 G 求得余式 R 的过程称为 G **相对于** F **的约化**．

下面考虑有限多个多项式组成的序列

$$\boldsymbol{A}:A_1,A_2,\cdots,A_r,$$

如果下列两条件之一成立：

1) $r=1$，$A_1\neq0$．

2) $r>1$，$0<\mathrm{cl}(A_1)<\mathrm{cl}(A_2)<\cdots<\mathrm{cl}(A_r)$，且对任意 $j>i$，A_j red$/A_i$．

我们称 $\boldsymbol{A}$ 为一个**升列**(ascending set)．

因为未定元的个数为 n，多项式的类只有 $n+1$ 类．在上述定义中，无论哪一种情形成立，总有 $r\leqslant n$．

例如，多项式列

$$A_1=-x_1^8-4x_1^6+8x_1^4+32x_1^2-16,$$

$$A_2=(4x_1)x_2+x_1^4-4,$$

$$A_3=-2x_3+x_1^2,$$

就是一个升列．

一个升列称为**矛盾列**，如果 $r=1$，$A_1\neq0$，但 $\mathrm{cl}(A_1)=0$．即一个非零常数构成的升列是矛盾列．当把升列看成多项式方程组时，矛盾列总是没有解的．

设 $\boldsymbol{A}$ 为一升列，G 为一多项式．如果 G 相对于升列 $\boldsymbol{A}$ 中每个多项式都是约化的，则称 G **相对于升列** $\boldsymbol{A}$ **是约化的**．

设另有升列

$$\boldsymbol{B}:B_1,B_2,\cdots,B_s,$$

如果下列两条件之一成立：

1) 存在 $j \leqslant \min(r, s)$，使得

$$A_1 \sim B_1, \cdots, A_{j-1} \sim B_{j-1}, \text{但 } A_j \succ B_j.$$

2) $s \succ r$ 且 $A_1 \sim B_1, \cdots, A_r \sim B_r$.

我们称 $\boldsymbol{A}$ 比 $\boldsymbol{B}$ 的**级别**高，或者说 $\boldsymbol{B}$ 比 $\boldsymbol{A}$ 的级别低，记为

$$\boldsymbol{A} \succ \boldsymbol{B} \text{ 或 } \boldsymbol{B} \prec \boldsymbol{A}.$$

如果 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 中每个都不比另一个级别低，则称二者有相同的级别，记作 $\boldsymbol{A} \sim \boldsymbol{B}$. 此时必有

$$r = s, A_1 \sim B_1, \cdots, A_r \sim B_r.$$

容易看出，级别在全体升列集合上定义了一个偏序，因此对任何升列集可以引进极小升列的概念. 下面的定理在整个吴特征列理论中起着非常重要的作用.

定理 2.4.1（Ritt 引理） 设

$$\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_q, \cdots$$

为一不增的升列组成的序列，即对任何 q，有 $\boldsymbol{A}_{q+1} \prec \boldsymbol{A}_q$ 或 $\boldsymbol{A}_{q+1} \sim \boldsymbol{A}_q$ 成立，则存在指标 q'，使得对任意 $q \succ q'$ 恒有 $\boldsymbol{A}_q \sim \boldsymbol{A}_{q'}$，即 $\boldsymbol{A}_{q'}$ 为上述序列中级别最低的升列.

证明 我们用 r_q 表示 $\boldsymbol{A}_q$ 中多项式中的数目，A_q 表示 $\boldsymbol{A}_q$ 的第一个多项式，则

$$A_1, A_2, \cdots, A_q, \cdots$$

是一个不增的多项式序列，即对任意 q，或有 $A_{q+1} \prec A_q$ 或 $A_{q+1} \sim A_q$. 因此或有 $\mathrm{cl}(A_{q+1}) < \mathrm{cl}(A_q)$ 或 $\mathrm{cl}(A_{q+1}) = \mathrm{cl}(A_q) = p > 0$，但是 $\deg_{x_p}(A_{q+1}) < \deg_{x_p}(A_q)$. 由于类和次数都是非负整数，存在 q_1 使得当 $q \geqslant q_1$ 时，所有的 A_q 具有相同的级别. 再考虑 $q \geqslant q_1$ 时的 $\boldsymbol{A}_q$ 中的第二个多项式 $A_q^{(1)}$

$$A_q^{(1)}, A_{q+1}^{(1)}, \cdots, A_q^{(1)}, \cdots$$

类似前面的分析，可知存在 q_2，使得当 $q \geqslant q_2$ 时 $A_q^{(1)} \sim A_{q_2}^{(1)}$. 注意在每个升列中多项式的个数不超过 n 个，所以上述过程可在 n 步内找到一 q'，使得当 $q \geqslant q'$ 时，$r_q = r_{q'}$ 且 $\boldsymbol{A}_q \sim \boldsymbol{A}_{q'}$.

由定理 2.4.1，可推出：

推论 2.4.1 若由升列组成的序列严格下降，则该序列必定只由有限个升列构成.

现在我们来定义升列集合上的极小元.

设 $\boldsymbol{PS}$ 为有限多个非零多项式组成的多项式集合. 一个升列 $\boldsymbol{A}$ 称为**属于** $\boldsymbol{PS}$ 是指 $\boldsymbol{A}$ 的每个多项式都属于 $\boldsymbol{PS}$. 因为单个多项式本身也构成一个升列，所以属于 $\boldsymbol{PS}$ 的升列集是非空的. 于是属于 $\boldsymbol{PS}$ 的升列集上的级别是一个偏序. 由定理 2.4.1，按此偏序每个升列的不增序列都有一极小元，该极小元自然属于 $\boldsymbol{PS}$. 我们称这种极小元为 $\boldsymbol{PS}$ 的一个**基本列**(basic set).

下面的定理不但指出了基本列的存在性，而且也给出了基本列的构造方法.

定理 2.4.2 设 $\boldsymbol{PS}$ 为非零多项式构成的有限集，则 $\boldsymbol{PS}$ 必有一基本列，而且存在一种方法使得这样的基本列能在有限步内构造出来.

证明 因为 $\boldsymbol{PS}$ 有限，其基本列的存在是显然的. 我们只需将其构造出来.

首先从 $\boldsymbol{PS}_1 = \boldsymbol{PS}$ 中选一级别最低的多项式 A_1，这是能够办到的. 如果 $\mathrm{cl}(A_1) = 0$，则 A_1 已经是一基本列. 假设 $\mathrm{cl}(A_1) > 0$，检查 $\boldsymbol{PS}_1 - \{A_1\}$ 中的多项式相对于 A_1 是否都

是未约化的，若是，则 PS 中不可能再有比 $\{A_1\}$ 级别低的升列，因此 A_1 就是 PS 的基本列．否则令 PS_2 为 PS_1 中相对于 A_1 已约化的多项式全体．由 A_1 的选取，PS_2 中的多项式的级别都高于 A_1 的级别．再注意到 PS_2 中的多项式相对于 A_1 都是约化的，PS_2 中多项式的类一定大于 $\mathrm{cl}(A_1)$．

再在 PS_2 中选取一级别最低的多项式 A_2．如果 $PS_2-\{A_2\}$ 中关于 A_2 都是未约化的，则 PS 中不可能再有比 $\{A_1, A_2\}$ 级别低的升列，故 $\{A_1, A_2\}$ 即为 PS 的基本列．否则再构造 PS_3，从而得 A_3．注意按照构造方法，A_1，A_2，A_3，… 的类是严格增加的，但是多项式的类只有 n 个，所以这种列必定在有限步内终止．又由构造方法知，该列中后面的多项式相对于前面的多项式都是约化的，因此我们得到的多项式列是一升列，且由构造原则知其为 PS 的基本列．

定理 2.4.3 设 PS 为非零多项式构成的有限集

$$\boldsymbol{A}: A_1, A_2, \cdots, A_r$$

是 PS 的一基本列，$\mathrm{cl}(A_1)>0$．设 B 为一非零多项式，且 B red/A_i，$i=1,\cdots,r$，则 $PS'=PS\cup\{B\}$ 有一比 $\boldsymbol{A}$ 级别低的基本列．

证明 如果 $\mathrm{cl}(B)=0$，则 B 本身即为 PS' 的基本列，且其级别比 $\boldsymbol{A}$ 低．如果 $\mathrm{cl}(B)=p>0$，且存在 s，$1\leqslant s\leqslant r$，使得 $\mathrm{cl}(A_{s-1})<p\leqslant\mathrm{cl}(A_s)$，因为 B red/A_i，$i=1,\cdots,r$，则或 $p=\mathrm{cl}(A_s)$，$\deg_{x_p}(B)<\deg_{x_p}(A_s)$，或者 $p<\mathrm{cl}(A_s)$，在这两种情况下都有 $B\prec A_s$，于是

$$A_1, A_2, \cdots, A_{s-1}, B \tag{2.4.2}$$

是 PS' 的一升列，且级别低于 $\boldsymbol{A}$．又 PS' 的基本列的级别必不高于式(2.4.2)，当然该基本列的级别低于 $\boldsymbol{A}$．

如果 $\mathrm{cl}(B)>\mathrm{cl}(A_r)$，$A_1,\cdots,A_r,B$ 的级别也小于 $\boldsymbol{A}$ 的级别，当然 PS' 的基本列的级别低于 $\boldsymbol{A}$ 的级别．

设

$$\boldsymbol{A}: A_1, A_2, \cdots, A_r$$

为一给定的升列，$\mathrm{cl}(A_i)=p_i$，$p_1<p_2<\cdots<p_r$．I_i 为 A_i 的初式．设 B 为一多项式，如果对 $\boldsymbol{A}$ 中的每个 A_i 都有 B red/A_i，则称 B **相对于 $\boldsymbol{A}$ 是约化的**．

如果 B 相对于 $\boldsymbol{A}$ 不是约化的，依次对 A_r，A_{r-1}，…，A_1 求余式

$$\begin{aligned}
I_r^{s_r}B &= Q_rA_r+R_r,\ R_r\ \mathrm{red}/A_r,\\
I_{r-1}^{s_{r-1}}R_r &= Q_{r-1}A_{r-1}+R_{r-1},\ R_{r-1}\ \mathrm{red}/A_{r-1},\\
&\cdots\cdots\\
I_1^{s_1}R_2 &= Q_1A_1+R_1,\ R_1\ \mathrm{red}/A_1.
\end{aligned}\tag{2.4.3}$$

最后所得的 R_1 相对所有 A_i 都是约化的，即相对 $\boldsymbol{A}$ 是约化的．我们称 R_1 为 B **对 $\boldsymbol{A}$ 的余式**．

利用式 (2.4.3) 可推知，存在 Q_i' 使得

$$I_1^{s_1}I_2^{s_2}\cdots I_r^{s_r}B=\sum_{i=1}^{r}Q_i'A_i+R_1. \tag{2.4.4}$$

该式称为**余式公式**．

下面假设 PS 为一非零多项式构成的集合，我们来讨论其所谓特征列的构造.

对给定的 $PS_1 = PS$，由定理 2.4.3，存在 PS_1 的基本列 BS_1. 将所有 $PS_1 - BS_1$ 中的多项式对基本列 BS_1 求余式，则得一余式的集合 RS_1. 若 $RS_1 \neq \varnothing$，令 $PS_2 = PS_1 \cup RS_1$，再找出 PS_2 的一基本列 BS_2. 注意，PS_2 是由 PS_1 添加所有对 BS_1 的余式而得的，所以 BS_2 的级别比 BS_1 低. 再将 $PS_2 - BS_2$ 中的多项式对 BS_2 求余式，并记该余式集合为 RS_2. 如果 $RS_2 \neq \varnothing$，令 $PS_3 = PS_2 \cup RS_2$，并求其基本列 BS_3，此时有

$$BS_1 \succ BS_2 \succ BS_3 \succ \cdots.$$

由推论 2.4.1，这个基本列构成的序列是有限的，因而必在某一步，比如说 m，使得 $RS_m = \varnothing$. 此时我们称相应的基本列 BS_m 为 PS 的**特征列**(characteristic set)，并记之为 CS.

例 2.4.1 求给定的多项式组

$$P_1 = -x_2^2 + x_1 x_2 + 1,$$
$$P_2 = -2x_3 + x_1^2,$$
$$P_3 = -x_3^2 + x_1 x_2 - 1$$

的特征列.

首先求 $PS_1 = \{P_1, P_2, P_3\}$ 的基本列 BS_1. 按照定理 2.4.3 的方法，因为 $\mathrm{cl}(P_1) = 2$，$\mathrm{cl}(P_2) = \mathrm{cl}(P_3) = 3$，故 PS_1 中级别最低的多项式为 P_1. 又在 $PS_1 - \{P_1\} = \{P_2, P_3\}$ 中，P_2，P_3 相对于 P_1 都是约化的，故下一个多项式应在 $\{P_2, P_3\}$ 中选取. 在 $\{P_2, P_3\}$ 中，P_2 的级别最低，故应该选 P_2. 因剩下的 P_3 相对于 P_2 是未约化的. 于是 P_1，P_2 构成 PS_1 的基本列. 接下来计算 RS_1. 因 $PS_1 - BS_1 \neq \{P_3\}$，RS_1 为 P_3 相对于 BS_1 的余式组成. 为计算 P_3 相对于 BS_1 的余式，先计算其对 P_2 的余式得

$$I_2^{s_2} P_3 = Q_2 P_2 + R_2.$$

其中 $I_2 = -2$，$s_2 = 2$，$Q_2 = 2x_3 + x_1^2$，$R_2 = 4(x_1 x_2 - 1) - x_1^4$. 因为 $\mathrm{cl}(R_2) = \mathrm{cl}(P_1) = 2$，且 $\deg_{x_2}(R_2) = 1 < \deg_{x_2}(P_1) = 2$，$R_2$ 相对于 P_1 是约化的，故 R_2 相对于 P_1 的余式为其本身，于是 $RS_1 = \{R_2\} \neq \varnothing$.

记 $P_4 = R_2$，令 $PS_2 = PS_1 \cup RS_1 = \{P_1, P_2, P_3, P_4\}$. 再找基本列 $BS_2 = \{P_4, P_2\}$. 将 P_1 对 BS_2 求余式，得

$$I_4^2 I_2^0 P_1 = Q'_2 P_4 + 0 P_2 + R'_2,$$

其中 $I_4 = 4x_1$，$R'_2 = -x_1^8 + 4x_1^6 - 8x_1^4 + 32x_1^2 - 16$. 而 P_3 相对于 BS_2 的余式为 0，于是 $RS_2 = \{R'_2\} \neq \varnothing$. 再令 $P_5 = R'_2$，$PS_3 = \{P_1, P_2, P_3, P_4, P_5\}$，求得其基本列为

$$BS_3 = \{P_5, P_4, P_2\}.$$

经过计算可知，P_1，P_3 相对于 BS_3 的余式都是 0，故最后得 PS 的特征列 $CS = BS_3 = \{P_5, P_4, P_2\}$，其中

$$C_1 = P_5 = -x_1^8 + 4x_1^6 - 8x_1^4 + 32x_1^2 - 16,$$
$$C_2 = P_4 = (4x_1)x_2 - x_1^4 - 4,$$
$$C_3 = P_2 = -2x_3 + x_1^2.$$

对于上例，特征列中第一个多项式仅含未定元 x_1，第二个仅含 x_1，x_2，第三个含 x_1，

x_2，x_3. 所以我们又称这种多项式列为**三角列**. 对于给定的多项式组 $\boldsymbol{PS}$，用上述方法求得它的特征列 $\boldsymbol{CS}$ 的过程与线性方程组的 Gauss 消元法有同样的效果，故吴特征列方法又称为吴消元法.

2.4.2 多项式方程组求解

在线性方程组中，我们总是首先利用 Gauss 消去法将给定的方程组化为三角形，该三角形方程组与原方程组有相同的解；然后再回代求解这个三角形方程组，以得到原方程组的解. 对于多项式方程组的求解，也可以采取同样的思想方法. 分析前面特征列的构造过程，恰好是将原方程组化为三角形方程组的过程. 将该过程写成下列形式：

$$\begin{array}{llll} \boldsymbol{PS}_1 = \boldsymbol{PS} & \boldsymbol{PS}_2 = \boldsymbol{PS}_1 \cup \boldsymbol{RS}_1 & \cdots & \boldsymbol{PS}_m = \boldsymbol{PS}_{m-1} \cup \boldsymbol{RS}_{m-1} \\ \boldsymbol{BS}_1 & \boldsymbol{BS}_2 & \cdots & \boldsymbol{BS}_m = \boldsymbol{CS} \\ \boldsymbol{RS}_1 & \boldsymbol{RS}_2 & \cdots & \boldsymbol{RS}_m = \varnothing . \end{array}$$

分析上述过程，其中每个 $\boldsymbol{BS}_i$ 都是一个三角列，如果对某个 i，$\boldsymbol{BS}_i$ 与原方程组有相同的解集合，当然可以求解该三角列，以得到解. 但是一般情况下未必有此结论，不过对最后所得的特征列，这个结论是正确的. 下面我们来证明这一点. 首先引进记号

$$\mathrm{zero}(\boldsymbol{PS}) = \{ a \in \boldsymbol{K}^n \mid \text{对任何 } P \in \boldsymbol{PS}, \text{成立 } P(a) = 0 \}.$$

引理 2.4.1 在特征列的构造中，以下等式成立：

$$\mathrm{zero}(\boldsymbol{PS}_1) = \mathrm{zero}(\boldsymbol{PS}_2) = \cdots = \mathrm{zero}(\boldsymbol{PS}_m).$$

证明 只需证明

$$\mathrm{zero}(\boldsymbol{PS}_1) = \mathrm{zero}(\boldsymbol{PS}_2)$$

即可，其他情形证明是同样的.

首先由定义得

$$\boldsymbol{PS}_1 \subset \boldsymbol{PS}_2,$$

由此可得

$$\mathrm{zero}(\boldsymbol{PS}_1) \supset \mathrm{zero}(\boldsymbol{PS}_2).$$

为证反包含关系，注意到 $\boldsymbol{PS}_2$ 的定义，只要证明对任何 $R \in \boldsymbol{RS}_1$ 与 $a \in \mathrm{zero}(\boldsymbol{PS}_1)$，$R(a) = 0$ 即可.

由 $\boldsymbol{RS}_1$ 的定义，对任何 $R \in \boldsymbol{RS}_1$，存在 $P \in \boldsymbol{PS}_1$，使得

$$I_r^{s} \cdots I_1^{s_1} P = Q'_r A_r + \cdots + Q'_1 A_1 + R, \tag{2.4.5}$$

其中 $A_1, \cdots, A_r$ 为 $\boldsymbol{PS}_1$ 的基本列，$I_1, \cdots, I_r$ 分别为 $A_1, \cdots, A_r$ 的初式. 于是对任何 $a \in \mathrm{zero}(\boldsymbol{PS}_1)$，因 $P, A_1, \cdots, A_r \in \boldsymbol{PS}_1$，有

$$P(a) = A_1(a) = \cdots = A_r(a) = 0.$$

再由式 (2.4.5)，即知 $R(a) = 0$.

对 $\boldsymbol{PS}_m$，因为其基本列 $\boldsymbol{BS}_m$ 为特征列 $\boldsymbol{CS}$，所以 $\boldsymbol{PS}_m$ 中的所有多项式相对于 $\boldsymbol{CS}$ 的余式都是 0. 设特征列为

$$\boldsymbol{CS}: A_1, \cdots, A_r,$$

A_i 的初式为 I_i，并记 $J = I_1 \cdots I_r$，则有

定理 2.4.4

$$\text{zero}(\boldsymbol{PS})=\text{zero}(\boldsymbol{CS}/J)+\text{zero}(\boldsymbol{PS},I_1)+\cdots+\text{zero}(\boldsymbol{PS},I_r),$$

其中，$\text{zero}(\boldsymbol{CS}/J)=\text{zero}(\boldsymbol{CS})-\text{zero}(J)$，“+”表示求并集.

证明 对任何 $P\in\boldsymbol{PS}_m$，由特征列的定义，存在整数 $s_1,\cdots,s_r$ 及多项式 $Q'_1,\cdots,Q'_r$，使得

$$I_r^{s_r}\cdots I_1^{s_1}P=Q'_rA_r+\cdots+Q'_1A_1. \tag{2.4.6}$$

由此容易证得

$$\text{zero}(\boldsymbol{PS}_m)=\text{zero}(\boldsymbol{CS}/J)+\text{zero}(\boldsymbol{PS}_m,I_1)+\cdots+\text{zero}(\boldsymbol{PS}_m,I_r).$$

再由引理 2.4.1 及 $\text{zero}(\boldsymbol{PS}_m,I_i)=\text{zero}(\boldsymbol{PS},I_i)$，即可证明本定理.

当 $\boldsymbol{CS}$ 为矛盾列时，$\text{zero}(\boldsymbol{CS})=\varnothing$. 因为 $\boldsymbol{CS}\subset\boldsymbol{PS}_m$，$\text{zero}(\boldsymbol{CS})\supset\text{zero}(\boldsymbol{PS}_m)=\text{zero}(\boldsymbol{PS})$，即 $\text{zero}(\boldsymbol{PS})=\varnothing$.

应用上述定理，可将多项式组 $\boldsymbol{PS}$ 的求解问题转化成若干个简单方程组的求解问题. 将 $(\boldsymbol{PS},I_i)$ 视为新的方程组，再求其特征列 $\boldsymbol{CS}'$. 注意 I_i 为 A_i 的初式，它相对于 $\boldsymbol{CS}$ 必定为约化的(练习). 于是由定理 2.4.4，$\boldsymbol{CS}'$ 的级别低于 $\boldsymbol{CS}$ 的级别. 利用这一点可以证明以下定理.

定理 2.4.5 设 $\boldsymbol{PS}$ 为给定的多项式集合，则存在一系列特征列 $\boldsymbol{CS}_l$，$l=1,2\cdots$，使得

$$\text{zero}(\boldsymbol{PS})=\bigcup_l\text{zero}(\boldsymbol{CS}_l/J_l),$$

其中 J_l 为特征列 $\boldsymbol{CS}_l$ 中多项式的初式之积.

证明 将定理 2.4.4 中的 $\boldsymbol{PS}$ 记为 $\boldsymbol{PS}^{(0)}$，特征列记为 $\boldsymbol{CS}^{(0)}$，$(\boldsymbol{PS},I_i)$ 记为 $\boldsymbol{PS}_i^{(1)}$，$i=1,\cdots,r$. 应用定理 2.4.6，又得特征列 $\boldsymbol{CS}_i^{(1)}$ 与 $\boldsymbol{CS}_i^{(1)}$ 的初式与 $\boldsymbol{PS}_i^{(1)}$ 组合而成的新多项式组 $\boldsymbol{PS}_{i_j}^{(2)}$，$j=1,\cdots,r_i$. 将 $\boldsymbol{CS}_i^{(1)}$ 那些矛盾列去掉(将剩下的个数仍记为 r). 对 $\boldsymbol{PS}_{i_j}^{(1)}$，$j=1,\cdots,r_i$，$i=1,\cdots,r$，再用定理 2.4.4 可得特征列组的序列

$$\boldsymbol{CS}_{i_j}^{(2)},\ j=1,\cdots,r_i,\ i=1,\cdots,r,$$

且有

$$\boldsymbol{CS}^{(0)}\succ\boldsymbol{CS}_i^{(1)}\succ\boldsymbol{CS}_{i_j}^{(2)}.$$

去掉特征列中的矛盾列，再对 $\boldsymbol{PS}_{i_j}^{(2)}$ 与 $\boldsymbol{CS}_{i_j}^{(2)}$ 中多项式的初式组成的多项式组利用定理 2.4.4，又可得一组升列与一组多项式组. 继续下去，可得一列严格下降的升列序列. 由推论 2.4.1，这种严格降的升列序列是有限的，所以这种做法必在有限步内停止. 做法停止处的特征列必为矛盾列，因为不然则可继续做下去. 已知以矛盾列为特征列的多项式组的零点集是空集，反复应用有限次定理 2.4.4 即得本定理.

例 2.4.2 求解多项式方程组

$$P_1=-x_2^2+x_1x_2+1=0,$$
$$P_2=-2x_3+x_1{}^2=0,$$
$$P_3=-x_3^2+x_1x_2-1=0.$$

我们在例 2.4.1 中已经求得该多项式组的特征列

$$C_1 = -x_1^8 - 4x_1^6 + 8x_1^4 + 32x_1^2 - 16,$$

$$C_2 = (4x_1)x_2 + x_1^4 - 4,$$

$$C_3 = -2x_3 + x_1^2.$$

显然,各多项式的初式分别为

$$I_1 = -1,\ I_2 = 4x_1,\ I_3 = -2.$$

由定理 2.4.4 有

$$\text{zero}(\boldsymbol{PS}) = \text{zero}(\boldsymbol{CS}/J) + \text{zero}(\boldsymbol{PS}, I_1) + \text{zero}(\boldsymbol{PS}, I_2) + \text{zero}(\boldsymbol{PS}, I_3).$$

容易看出,对 $i = 1, 3$, $\{P_1, P_2, P_3, I_i\}$ 的特征列为矛盾列. 又 $J = I_1 I_2 I_3 = 8x_1 = 0$ 的解 $x_1 = 0$ 不是特征列的零点,即 $\text{zero}(\boldsymbol{CS}/J) = \text{zero}(\boldsymbol{CS})$. 又可算出 $(\boldsymbol{PS}, I_2)$ 的特征列亦为矛盾列. 于是

$$\text{zero}(P_1, P_2, P_3) = \text{zero}(C_1, C_2, C_3).$$

求解 $C_1 = 0$,可得 8 个根 x_{1i}, $i = 1, \cdots, 8$. 注意,所有这些根都是非零的,分别代入 $C_2 = 0$, $C_3 = 0$,又可解得

$$x_{2i} = (4 - x_{1i}^4)/(4x_{1i}),$$

$$x_{3i} = x_{1i}^2/2,\ i = 1, \cdots, 8.$$

2.4.3 定理机械化证明

假设 $\boldsymbol{K}$ 为域. 一个几何定理在引进适当的坐标系后,就像在解析几何中所做的那样,其假设条件与结论可以用它们点的坐标之间的数量关系来描述. 在初等几何中,这些关系一般都是多项式的. 这个过程称为几何定理的**代数化**. 因此定理的假设条件可用一组多项式 $\boldsymbol{HS} \subset \boldsymbol{K}[x_1, \cdots, x_n]$ 来表示. 而相应的结论也可用一多项式 $G = 0$ 来描述. 因此有

定义 2.4.1 一个定理定义为 $\boldsymbol{T} = \{\boldsymbol{HS}, G\}$,其中 $\boldsymbol{HS}$ 为**假设**, G 为**结论**.

定理 2.4.6 设 $\boldsymbol{HS}$ 为一定理的假设, G 为结论.

$$\boldsymbol{CS}: A_1, \cdots, A_r$$

为 $\boldsymbol{HS}$ 的特征列, $J = I_1 \cdots I_r$ 为 A_i 的初式之积,则在非退化条件 $J \neq 0$ 之下,当 G 相对于 $\boldsymbol{CS}$ 的余式为 0 时,结论 $G = 0$ 可由 $A_i = 0$, $i = 1, \cdots, r$ 推出.

证明 将 G 对特征列求余,则有

$$I_1^{s_1} \cdots I_r^{s_r} G = Q_1 A_1 + \cdots + Q_r A_r + R.$$

如果余式 $R = 0$,则对任何使得假设条件成立且又满足非退化条件的点 $\boldsymbol{a} \in \text{zero}(\boldsymbol{CS}/J)$,显然有

$$G(\boldsymbol{a}) = 0.$$

这表示结论成立.

为了简单起见,只给出了上面特殊情况的定理. 实际上尚有很多情形需要讨论. 比如:

1) 当余式不为零时结论是否成立.

2) 在退化条件 $J = 0$ 时结论是否成立.

这里不再作介绍，有兴趣的读者请参阅吴文俊编著的《几何定理机器证明的基本原理》(科学出版社，1984)．

例 2.4.3 Desargues 定理的证明．

假设 平面上任意两条直线 l_1，l_2 交于点 O．在 l_1 上任取两点 A_1，A_2，在 l_2 上任取一点 B_1，过 A_2 做直线平行于 A_1B_1，设其交 l_2 于 B_2．在平面上任取一点 C_1，过 A_2，B_2 分别做直线平行于 A_1C_1，B_1C_1，两直线交于 C_2(图 2.4.1)．

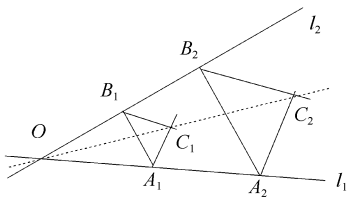

图 2.4.1

结论 O，C_1，C_2 三点共线．

证明 首先将问题代数化．取坐标：$O(0,0)$，$A_1(u_1,0)$，$A_2(u_2,0)$，$B_1(0,u_3)$，$C_1(u_4,u_5)$，$B_2(0,x_1)$，$C_2(x_2,x_3)$．注意这里各点坐标的写法．对那些任取的点，其坐标都用 u_i 表示，而对那些非任取的点，其坐标都用 x_i 表示．利用这些坐标，假设条件可以写成

$$H_1 = u_1x_1 - u_2u_3 = 0, \quad (A_1B_1 \parallel A_2B_2)$$
$$H_2 = u_4(x_3 - x_1) - x_2(u_5 - u_3) = 0, \quad (B_1C_1 \parallel B_2C_2)$$
$$H_3 = (u_4 - u_1)x_3 - u_5(x_2 - u_2) = 0. \quad (A_1C_1 \parallel A_2C_2)$$

而结论可以写成

$$G = u_4x_3 - u_5x_2 = 0.$$

为应用定理 2.4.6，先求 ***HS*** 的(相对于 $u_1 < \cdots < u_5 < x_1 < \cdots < x_3$ 的字典序的)特征列 ***CS***

$$C_1 = I_1x_1 - u_2u_3,$$
$$C_2 = I_2x_2 + (u_4 - u_1)u_4x_1 + u_2u_4u_5,$$
$$C_3 = I_3x_3 - (u_5 - u_3)x_2 - u_4x_1.$$

其中 $I_1 = u_1$，$I_2 = u_1u_3 - u_1u_5 - u_3u_4$，$I_3 = u_4$．

计算 G 对 ***CS*** 的余式可知其为零．由定理 2.4.6 知，在非退化条件 $J = I_1I_2I_3 \neq 0$ 的情况下，Desargues 定理成立．

下面分析退化条件 $J = I_1I_2I_3 = 0$．

若 $I_1 = u_1 = 0$，表示点 A_1 取在 O 点．这时点 B_2 无定义，定理无意义．

在 $I_3 = u_4 = 0$ 时，定理仍然成立．如图 2.4.2 所示，这时点 C_1 落在 l_2 上，可以看出 C_2 此时也在 l_2 上．而 l_2 上的点的第一个坐标都是零，即有 $x_2 = 0$，由此可知 $G = -u_5x_2 = 0$．

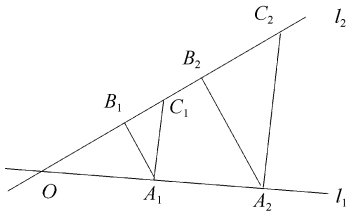

图 2.4.2

当 $I_2 = u_1 u_3 - u_1 u_5 - u_3 u_4 = 0$ 时，如图 2.4.3 所示，点 $C_1(u_4, u_5)$ 在直线 $A_1 B_1$ 上，C_2 无确定的定义，定理不成立.

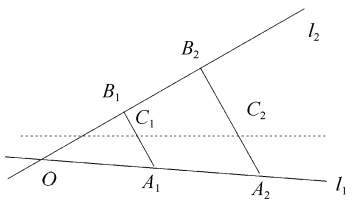

图 2.4.3

在几何问题中，无论是欧氏几何还是非欧氏几何，利用吴方法不但能够证明定理，还可以发现新定理与未知关系，限于篇幅，我们这里不再介绍.

练　习

1. 设 D 为 UFD，A，$B \in \boldsymbol{D}[X]$. 若存在 $b \in \boldsymbol{D}$，Q，$R \in \boldsymbol{D}[X]$，整数 l，使得

$$b^l A = QB + R,$$

证明 $\gcd(b^l A, B) = \gcd(B, R)$.

2. 设对某固定的 m，定义 n 元单项式全体 T 上的一个序 $<_m$ 如下：

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} <_m x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n},$$

当且仅当或者存在 l，$1 \leqslant l \leqslant n$，使 $i_l < j_l$ 且 $i_k = j_k$，$1 \leqslant k \leqslant l$，或者 $i_k = j_k$，$1 \leqslant k \leqslant m$ 且 $x_{m+1}^{i_{m+1}} \cdots x_n^{i_n} <_t x_{m+1}^{j_{m+1}} \cdots x_n^{j_n}$，其中 $<_t$ 表示分次字典序. 证明 $<_m$ 是一个容许的单项序.

3. 若 P，R 为多项式，$\boldsymbol{G}$ 为多项式集合. 证明若 $P \xrightarrow[G]{*} R \neq 0$，令 $\boldsymbol{G}' = \boldsymbol{G} \cup \{R\}$，则 $P \xrightarrow[G']{} 0$.

4. 设 P，Q，$R \in \boldsymbol{K}[X]$ 而 $\boldsymbol{S} \subset \boldsymbol{K}[X]$. 如果 $P - Q \xrightarrow[s]{} R$，则存在 $\overline{P}$，$\overline{Q}$，使得

$$P \xrightarrow[s]{} \overline{P},\ Q \xrightarrow[s]{} \overline{Q} \text{ 且 } R = \overline{P} - \overline{Q}.$$

5. 假设 P，$Q \in \boldsymbol{K}[X]$，使得对某 $\boldsymbol{S} \subset \boldsymbol{K}[X]$ 成立 $P - Q \xrightarrow[s]{} 0$，则存在 $R \in \boldsymbol{K}[X]$，使得 $P \xrightarrow[s]{*} R$，$Q \xrightarrow[s]{*} R$.

6. 假设 P_1，$P_2 \in \boldsymbol{K}[X]$ 与 $\boldsymbol{S} \subset \boldsymbol{K}[X]$，使得 $P_1 \xrightarrow[s]{} P_2$，则对任何 $R \in \boldsymbol{K}[X]$ 存

在多项式 Q，使得 $P_1 + R \xrightarrow{*}_s Q$，$P_2 + R \xrightarrow{*}_s Q$.

7. 试举一例：一个多项式理想的理想基 $\boldsymbol{G}$ 是多种容许单项序下的 Groebner 基.

8. 证明定理 2.3.4.

9. 证明定理 2.3.5.

10. 证明定理 2.3.7.

11. 利用定理 2.3.4 与 2.3.7 改进 Buchberger 算法.

12. 判断是否有 $A = xz^4 - xyz^3 \in \langle P_1, P_2, P_3 \rangle$，其中

$$P_1 = x^3yz - xz^2,\ P_2 = xy^2z - xyz,\ P_3 = x^2y^2 - z^2.$$

若有，则求 A_1，A_2，A_3，使得

$$A = A_1P_1 + A_2P_2 + A_3P_3.$$

13. 设 $I = < x_2 - a_2, \cdots, x_n - a_n >$，证明在多项式 A 的 $\boldsymbol{I}$- *adic* 表示中，若 $S = (j_2, \cdots, j_n) \in \boldsymbol{J}^{(i)}$，则有

$$A_S^{(i)}(x_1) = \frac{1}{j_2! \cdots j_n!} \frac{\partial^{j_2} \cdots \partial^{j_n}}{\partial x_2^{j_2} \cdots \partial x_n^{j_n}} A(x_1, a_2, \cdots, a_n).$$

14. 设 $\boldsymbol{CS}$：$A_1, A_2, \cdots, A_r$ 为特征列，I_i 为 A_i 的初式，证明它相对于 $\boldsymbol{CS}$ 必定为约化的.

第 3 章　多项式最大公因子的计算

多项式最大公因子的计算是计算机代数中最基本的问题之一. 在符号计算中，很多问题要涉及到最大公因子的计算. 例如为使运算效率更高，在有理分式的表示中我们常常希望分子与分母互素，这样对给定的原始数据，就要求我们去掉其最大公因子. 又如在因式分解或积分等许多计算中也都以最大公因子计算作为子算法. 因此设计最大公因子计算的有效算法，对提高符号计算的效率十分有意义.

3.1　多项式的余式序列与结式

3.1.1　多项式余式序列

我们先来考虑一元多项式的最大公因子问题. 整数最大公因子计算的方法在多项式情形中仍然成立. 因为在计算机代数中，所有的计算都是精确的，故只需讨论有理系数的多项式. 而有理系数的多项式问题与整系数多项式问题可以相互转化，因此我们只需讨论整系数多项式问题即可.

设 $\boldsymbol{K}$ 为域，则 $\boldsymbol{K}[x]$ 为 Euclid 整环. 对任何 $A, B \in \boldsymbol{K}[x], B \neq 0$，由带余除法，存在唯一的 $Q, R \in \boldsymbol{K}[x]$，使得

$$A = QB + R, \tag{3.1.1}$$

其中 $\deg(R) < \deg(B)$ 或 $R = 0$. 这里我们要讨论的是如何利用这个结果来计算给定的 A，B 的最大公因子. 对上式中的 A，B，Q，R，为了方便地描述它们之间的关系，仍记余式与商为

$$R = \mathrm{rem}(A, B),\ Q = \mathrm{quo}(A, B). \tag{3.1.2}$$

对多项式的最大公因子计算问题，Euclid 方法仍然有效.

算法 3.1.1　Euclid 算法：

```
Input A, B;
Output U=gcd(A, B);
    R:=B;
    U:=A;
    V:=B;
    while R≠ 0 do
        R:= rem(U, V);
        U:= V;
        V:=R;
```

命题 3.1.1　Euclid 算法是有限终止的，且当算法终止时，$U = \gcd(A, B)$.

此命题的证明留作练习.

例 3.1.1　设

$$A = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5,$$

$$B = 3x^6 + 5x^4 - 4x^2 - 9x + 21,$$

求它们的最大公因子. 按 Euclid 算法，得如下余式序列：

$$-\frac{5}{9}x^4 + \frac{1}{9}x^2 - \frac{1}{3},$$

$$-\frac{117}{25}x^2 - 9x + \frac{441}{25},$$

$$\frac{233150}{19733}x - \frac{102500}{2195},$$

$$-\frac{1288744821}{543589225}.$$

因为余式序列的最后一个是非零常数，故 $\gcd(A, B) = 1$.

有时为了某种需要，要求计算一个多项式模另一多项式的逆，即给定 A，$B \in \boldsymbol{K}[x]$，求多项式 W，使得

$$WA \equiv 1 \bmod B.$$

如果这样的 W 存在，则有 $B \mid (WA - 1)$，即有 V 存在，使得 $WA - 1 = VB$，这说明 A，B 互素. 如果 A，B 互素，由定理 2.1.3 知，这样的 W 是肯定存在的. 至于 W 的计算，可以用第 2 章商环中元素的求逆方法，也可以用扩展 Euclid 方法. 当 A，B 互素时，由定理 2.1.3 知，存在 W，V，使得

$$1 = WA + VB,$$

其中 $\deg(W) < \deg(B)$，$\deg(V) < \deg(A)$. 显然这样的 W 即为 A 模 B 的逆.

算法 3.1.2 扩展 Euclid 算法：

```
Input A, B, deg(B)≤deg(A);
Output C, W, V;
    S: = [1, 0];
    T: = [0, 1];
    while B≠0 do
        R: = rem(A, B);
        Q: = quo(A, B);
        L: = S - QT;
        A: = B;
        B: = R;
        S: = T;
        T: = L;
    return A, S;
```

当 A，B 都是 $\mathbf{Z}[x]$ 上的多项式时，如果它们有非常数的公因子，由 Gauss 引理，该公因子也可取为整系数的. 但是 Euclid 算法必须在域内进行. 如果我们希望只进行环上的计算，直接套用 Euclid 算法是不行的. 为达到这个目的，在 Euclid 算法中，每步用伪除来代替除法，这样每步所得的伪余多项式仍然是整系数的. 自然，当算法终止时，得到的多项式也是整系数的. 对于上例，应用前面所说的算法，则有

$$-15x^4 + 3x^2 - 9,$$

$$15795x^2 + 30375x - 59535,$$

$$1254542875143750\,x-1654608338437500,$$
$$125933387955007431009311419921875 00.$$

但是这样做的后果是系数迅速膨胀，给存储及运算都带来了困难．那么能否找到一种算法，使得系数膨胀的比较缓慢，而运算又保持在整数环内呢？回答是肯定的，对前面所说的方法加以改造就可以达到这样的目的，为此我们先来讨论多项式余式序列．

定义 3.1.1 设 $\boldsymbol{R}$ 为环，A，$B\in\boldsymbol{R}[x]$，$\deg(A)\geqslant\deg(B)$，则 A，B 的**多项式余式序列**是满足下列条件的多项式序列 R_0，R_1，$\cdots$，R_k：

1）$R_0=A$，$R_1=B$．

2）$\alpha_i R_{i-1}=Q_i R_i+\beta_i R_{i+1}$，其中 α_i，$\beta_i\in\boldsymbol{R}$．

3）$\mathrm{prem}(R_{k-1},R_k)=0$．

利用定理 2.1.6 容易证明，如果 A，B 都是本原多项式，则 $\mathrm{pp}(R_k)=\gcd(A,B)$．

在以上定义中，α_i 的选取应该使得满足

$$\alpha_i R_{i-1}=Q_i R_i+R,$$

且 $\deg(R)<\deg(R_i)$ 或 $R=0$ 的 $R_i\in\boldsymbol{R}[x]$ 存在．而 β_i 则应选取为 R 的系数尽可能“大”的公因子．

当 $\boldsymbol{R}$ 为域时，若取 $\alpha_i=\beta_i=1$，则 $\{R_i\}$ 即为 Euclid 方法所得的多项式序列．但是当 $\boldsymbol{R}$ 为环时，就难以再取 $\alpha_i=\beta_i=1$，这时未必存在这样的 $R_i\in\boldsymbol{R}[x]$．

记 $\delta_i=\deg(R_{i-1})-\deg(R_i)$，如果取

$$\begin{aligned}\alpha_i&=(\mathrm{lc}(R_{i-1}))^{\delta_i+1},\\ \beta_i&=\mathrm{cont}(\mathrm{prem}(R_{i-1},R_i)),\end{aligned}\tag{3.1.3}$$

则得第 2 章介绍的伪余序列．这样计算的结果虽然系数膨胀得最慢，但每步要计算一个多项式的容度，计算量较大．如果放宽对系数膨胀的控制，减少计算量，可取

$$\begin{aligned}&\alpha_i=(\mathrm{lc}(R_i))^{\delta_i+1},\ \beta_1=(-1)^{\delta_1+1},\\ &\beta_i=-(\mathrm{lc}(R_{i-1}))\,\psi_i^{\delta_i},\ 2\leqslant i\leqslant k,\ \psi_1=-1,\\ &\psi_i=(-\mathrm{lc}(R_{i-1}))^{\delta_{i-1}}\,\psi_{i-1}^{1-\delta_{i-1}},\ 2\leqslant i\leqslant k.\end{aligned}\tag{3.1.4}$$

所得的多项式序列称为 A，B 的**子结式余式序列**．

例 3.1.2 设

$$A=x^8+x^6-3x^4-3x^3+8x^2+2x-5,$$
$$B=3x^6+5x^4-4x^2-9x+21,$$

用子结式余式序列方法求它们的最大公因子．

取 $R_0=A$，$R_1=B$，按上述公式可算得

$$\delta_1=2,\ \alpha_1=27,\ \beta_1=-1,$$
$$R_2=15x^4-3x^2+9,$$
$$\delta_2=2,\ \psi_2=-9,\ \alpha_2=3375,\ \beta_2=-243,$$
$$R_3=65x^2+125x-245.$$

如此下去，最后得

$$R_4 = 9326x - 12300,$$
$$R_5 = 260708.$$

例 3.1.3　在定义 3.1.1 中，若取

$$\alpha_i = (\mathrm{lc}(R_i))^{\delta_i+1},\ \beta_1 = 1,$$
$$\beta_i = \alpha_{i-1},\ 2 \leqslant i \leqslant k, \tag{3.1.5}$$

则所得的多项式余式序列称为**约化多项式余式序列**.

对于多项式

$$A = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5,$$
$$B = 3x^6 + 5x^4 - 4x^2 - 9x + 21,$$

其约化多项式余式序列为

$$R_2 = -15x^4 + 3x^2 - 9,$$
$$R_3 = 585x^2 + 1125x - 2205,$$
$$R_4 = -18885150x + 24907500,$$
$$R_5 = 527933700.$$

在定义 3.1.1 中，α_i 和 β_i 的不同定义则给出不同的多项式余式序列. 注意对所给的例子，所有的 α_i 的取法都是一样的，实质上它们都是基于对伪余的改造而得到的，既注重对系数膨胀的控制，又注重对计算量的控制. 作为计算最大公因子的算法，子结式余式序列方法是这一类方法中最好的，它的特点是：

1）计算量较小.

2）序列中的每个多项式都是整系数的.

3）系数的(位数)长度增长是线性的.

3.1.2　结式

定义3.1.2　设 $\boldsymbol{R}$ 为交换环，A，$B \in \boldsymbol{R}[x]$，为非零多项式，其中 $A = \sum_{i=0}^{m} a_i x^i$，$B = \sum_{i=0}^{n} b_i x^i$，则 A，B 的 Sylvester **矩阵**定义为 $(m+n)$ 阶方阵：

$$\boldsymbol{M} = \begin{pmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & & \\ & a_m & a_{m-1} & \cdots & a_1 & a_0 & \\ & & \cdots & \cdots & \cdots & \cdots & \\ & & & a_m & a_{m-1} & \cdots & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & & \\ & b_n & b_{n-1} & \cdots & b_1 & b_0 & \\ & & \cdots & \cdots & \cdots & \cdots & \\ & & & b_n & b_{n-1} & \cdots & \cdots & b_0 \end{pmatrix}. \tag{3.1.6}$$

定义 3.1.3　多项式 A，$B \in \boldsymbol{R}[x]$ 的**结式**，记作 $\mathrm{res}(A, B)$，定义为 A，B 的 Sylvester 矩阵的行列式. 对任何 $B \in \boldsymbol{R}[x]$，定义 $\mathrm{res}(0, B) = 0$. 而对非零常数 A，$B \in \boldsymbol{R}$，则定义 $\mathrm{res}(A, B) = 1$. 有时为了强调未定元，也将 A，B 的结式记作 $\mathrm{res}_x(A, B)$.

无论是理论研究还是实际计算，结式对多项式问题都是有力的工具，以后我们将看到这一点.

例 3.1.4 对于多项式

$$A = 3x^4 + 3x^3 + x^2 - x - 2,$$
$$B = x^3 - 3x^2 + x + 5,$$

其结式为

$$\mathrm{res}(A, B) = \det(\boldsymbol{M}) = 0,$$

其 Sylvester 矩阵为

$$\boldsymbol{M} = \begin{pmatrix} 3 & 3 & 1 & -1 & -2 & 0 & 0 \\ 0 & 3 & 3 & 1 & -1 & -2 & 0 \\ 0 & 0 & 3 & 3 & 1 & -1 & -2 \\ 1 & -3 & 1 & 5 & 0 & 0 & 0 \\ 0 & 1 & -3 & 1 & 5 & 0 & 0 \\ 0 & 0 & 1 & -3 & 1 & 5 & 0 \\ 0 & 0 & 0 & 1 & -3 & 1 & 5 \end{pmatrix}.$$

多项式 A，B 的结式可以用来判断 A，B 是否有非平凡的公因子. 后面我们将证明两个多项式有非平凡公因子，当且仅当其结式为 0.

定理 3.1.1 设 A，$B \in \boldsymbol{R}[x]$ 为次数分别为 m，$n > 0$ 的多项式，则存在满足 $\deg(S) < n$，$\deg(T) < m$ 的 S，$T \in \boldsymbol{R}[x]$，使得

$$A(x)S(x) + B(x)T(x) = \mathrm{res}(A, B). \tag{3.1.7}$$

证明 设 A，B 的系数分别为 a_i 与 b_i，构造 $m+n$ 阶线性方程组

$$\begin{cases} a_m x^{m+n-1} + a_{m-1} x^{m+n-2} + \cdots + a_0 x^{n-1} = x^{n-1} A \\ a_m x^{m+n-2} + \cdots + a_1 x^{n-1} + a_0 x^{n-2} = x^{n-2} A \\ \cdots\cdots \quad\quad \cdots \\ a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0 = A \\ b_n x^{m+n-1} + b_{n-1} x^{m+n-2} + \cdots + b_0 x^{m-1} = x^{m-1} B \\ \cdots\cdots \quad\quad \cdots \\ b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0 = B \end{cases}$$

利用矩阵形式，以上方程组可以写成

$$\boldsymbol{M} \begin{pmatrix} x^{m+n-1} \\ \cdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} x^{n-1} A(x) \\ \cdots \\ xB(x) \\ B(x) \end{pmatrix}. \tag{3.1.8}$$

利用 Cramer 法则求解最后一个分量 1，得

$$\det(\boldsymbol{M})=\det\begin{pmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & & x^{n-1}A \\ & a_m & a_{m-1} & \cdots & a_1 & a_0 & \\ & & \cdots & \cdots & \cdots & \cdots & \\ & & & a_m & a_{m-1} & \cdots & a_1 & A \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & & x^{m-1}B \\ & b_n & b_{n-1} & \cdots & b_1 & b_0 & \\ & & \cdots & \cdots & \cdots & \cdots & \\ & & & b_n & b_{n-1} & \cdots & b_1 & B \end{pmatrix}.$$

将上式右端的行列式按最后一列展开即得式(3.1.7).

推论 3.1.1 设 $\boldsymbol{R}$ 为 UFD，A，$B\in\boldsymbol{R}[x]$，A，B 有非平凡公因子，则当且仅当 $\operatorname{res}(A,B)=0$.

证明 假设 A，B 有非平凡公因子，但 $\operatorname{res}(A,B)\neq 0$，则由定理 3.1.1，$A$，$B$ 的任何公因子都将整除结式. 但是结式为常数，这说明 A，B 可能的公因子必是 0 次的，即 A，B 的公因子都是平凡的，矛盾，故必 $\operatorname{res}(A,B)=0$.

反之，假设 $\operatorname{res}(A,B)=0$，则由定理 3.1.1，有多项式 S，T 使得

$$A(x)S(x)=-B(x)T(x).$$

如果 A，B 互素，则由上式可推出 B 整除 S，但是 $\deg(S)<\deg(B)$，这是不可能的. 从而 A，B 有非平凡公因子.

一个有趣的结论是，$Z[x]$ 中的多项式 A，B 的最大公因子可以通过对它们的 Sylvester 矩阵进行行变换得到.

定理 3.1.2 设 A，$B\in Z[x]$，如果只允许使用行变换将 A，B 的 Sylvester 矩阵化为行阶梯形，则最后一个非零行即为 A，B 的(在 Q
量.

证明 如果 A，B 互素，则 $\operatorname{res}(A,B)\neq 0$. 此时 A，B 的 Sylvester 矩阵 $\boldsymbol{M}$ 是非奇异的，经行变换化为行阶梯形后，其最后一个非零行必为最后一行，且该行只有最后一个元素非零. 它对应的多项式为常数，此时 A，B 只有平凡的公因子. 当 $\operatorname{res}(A,B)=0$ 时，A，B 有非平凡公因子. 由定理 2.1.2 知，存在多项式 $S(x)$，$T(x)$ 满足 $\deg(S)<\deg(B)$，$\deg(T)<\deg(A)$，使得

$$\gcd(A,B)=A(x)S(x)+B(x)T(x). \tag{3.1.9}$$

注意，关于 S，T 的次数的限制，式(3.1.9)表明 $\gcd(A,B)$ 的系数向量是 $\boldsymbol{M}$ 的行向量的线性组合. 假设 $\boldsymbol{M}$ 化为阶梯形后最后一个非零行对应的多项式为 D，利用定理 3.1.1 证明中的式 (3.1.8) 可知，有 W，V 使得

$$D(x)=A(x)W(x)+B(x)V(x).$$

因 $\gcd(A,B)\mid D$，D 的系数向量的第一个非零元所在的列数必定不大于 $\gcd(A,B)$ 的系数的第一个非零元所在的列数. 可以断言，这两个系数向量必定只相差一常数倍.

不然，一方面因 $\gcd(A,B)$ 的系数向量是 $\boldsymbol{M}$ 的行向量的线性组合，记 C 为 $\gcd(A,B)$ 的系数向量，则有

$$\operatorname{rank}\begin{pmatrix} M \\ C \end{pmatrix}=\operatorname{rank}(\boldsymbol{M}).$$

另一方面，若 C 的第一个非零元所在的列数大于 D 的第一非零元所在的列数，或者虽然二者第一非零元在同一列，但是二向量不是倍数关系，则由线性代数知识可知

$$\operatorname{rank}\begin{pmatrix} M \\ C \end{pmatrix} > \operatorname{rank}(M).$$

这个矛盾说明，C 和 D 只能相差一常数倍，即 D 亦为 A，B 在 $\mathrm{Q}[x]$ 上的最大公因子.

3.2 模 方 法

利用多项式余式序列求最大公因子仍然需要进行大整数计算，当所给多项式的次数较高时，计算过程中系数的膨胀问题就会更加突出. 为了提高计算效率，避免大整数的计算，就必须寻找另外的方法. 为此考虑多项式环的同态映射

$$\Phi_p : \mathrm{Z}[x] \longrightarrow \mathrm{Z}_p[x],$$
$$\sum_i a_i x^i \longmapsto \sum_i \Phi_p(a_i) x^i,$$

其中 p 为素数，$\Phi_p(a_i)$ 表示 a_i 的模 p 同态像，即 $\Phi_p(a_i) \equiv a_i \bmod p$，$-p/2 < \Phi_p(a_i) < p/2$. 容易验证如此定义的 Φ_p 的确为环同态. 后面我们将记 $\Phi_p(A)$ 为 A_p.

设给定 A，$P \in \mathrm{Z}[x]$. 若 $P \mid A$，则有 Q 使 $A = QP$. 从而其同态像满足

$$A_p = Q_p P_p.$$

上式说明，若 P 为 A，B 的公因子，则 P_p 相应地为 A_p，B_p 的公因子. 因此若 $D = \gcd(A, B)$，且素数 p 使得 D 的系数的绝对值不超过 $p/2$，只要我们能够求出 A_p，B_p 的最大公因子，则有可能成立 $D = D_p = \gcd(A_p, B_p)$，从而求得 $D = \gcd(A, B)$. 而求 A_p，B_p 的公因子时，系数的计算又可控制在绝对值小于 $p/2$ 的范围内. 这种方法称为**模方法**(*modular methods*). 在讨论模方法之前，我们先来看一个例子.

例 3.2.1 设

$$A = x^8 + x^6 - 3x^4 - 3x^3 + x^2 + 2x - 5,$$
$$B = 3x^6 + 5x^4 - 4x^2 - 9x + 21,$$

则 A，B 模 5 的像为

$$A_5 = x^8 + x^6 + 2x^4 + 2x^3 + x^2 + 2x,$$
$$B_5 = -2x^6 + x^2 + x + 1.$$

下面我们计算 A_5，B_5 的公因子，注意计算是模 5 进行的.

$$A_5 = 2(x^2+1)B_5 + 2x^2 - 2,$$
$$R_2 = 2(x^2 - 1);$$
$$B_5 = (-x^4 - x^2 + 2)R_2 + x,$$
$$R_3 = x;$$
$$R_2 = 2xR_3 - 2,$$
$$R_4 = -2.$$

即 $\gcd(A_5, B_5) = 1$. 因此若 P 为 A，B 的公因子，则 P 的同态像 P_5 必整除 $\gcd(A_5,$

$B_5)=1$，由此可知 $P_5=1$. 我们断言，A，B 的任何公因子都必为常数. 不然，设整系数多项式 P 为 A，B 的公因子，则有 Q 使得 $B=PQ$. 不妨设

$$P=\sum_{i=0}^{m}p_i x^i,\quad Q=\sum_{i=0}^{n}q_i x^i,\quad m,\ n\leqslant 6.$$

注意 B 是本原多项式，由 *Gauss* 引理可知，P，Q 也都是本原的. 又由前段分析可知 $P_5=1$，故 $p_i=0 \bmod 5$，$i=1,\cdots,m$. 比较系数可知必有

$$-2\equiv p_0 q_n \bmod 5.$$

由此推得 $n=6$，$m=0$. 这说明 P 为平凡因子，从而 A，B 的最大公因子为 1.

一般说来，若 A，B 的最大公因子为 D，p 为任一素数，则有 $D_p \mid \gcd(A_p, B_p)$，从而 $\deg(D_p)\leqslant \deg(\gcd(A_p, B_p))$. 但一般等式未必成立. 例如，$A=x+3$，$B=x-2$，则 $\gcd(A_5, B_5)=x-2$，但 $D=\gcd(A, B)=1$，即 $\deg(D_5)<\deg(\gcd(A_5, B_5))$.

在用模方法计算时，为通过 $\gcd(A_p, B_p)$ 求得 $D=\gcd(A, B)$，我们总希望成立

$$D=\gcd(A_p, B_p).$$

但是一般使这个等式成立的条件很难分析，为此我们寻求 $D_p=\gcd(A_p, B_p)$ 成立的条件，再要求 $D=D_p$，则得

$$D=D_p=\gcd(A_p, B_p).$$

分析可知，前一个等式要求 p 大于 D 系数的绝对值的 2 倍，而后一个等式则对素数 p 有进一步要求. 因此要想利用模方法求得多项式的最大公因子，素数 p 的恰当选择十分重要. 我们首先来估计多项式因子系数的界.

定理 3.2.1（Landau-Mignotte 不等式）若 Q，$P\in \mathbf{Z}[x]$，$Q=\sum_{i=0}^{q}b_i x^i$ 为 $P=\sum_{i=0}^{p}a_i x^i$ 的因子，则

$$\sum_{i=0}^{q}|b_i|\leqslant 2^q\left|\frac{b_q}{a_p}\right|\sqrt{\sum_{i=0}^{p}a_i^2}.$$

证明 见附录 A.

推论 3.2.1 $A=\sum_{i=0}^{m}a_i x^i$ 与 $B=\sum_{i=0}^{n}b_i x^i$ 的最大公因子的系数不超过

$$2^{\min(m,n)}\gcd(a_m, b_n)\min\left\{\frac{1}{|a_m|}\sqrt{\sum_{i=0}^{m}a_i^2}, \frac{1}{|b_n|}\sqrt{\sum_{i=0}^{n}b_i^2}\right\}.$$

证明 设 A，B 的公因子为 D，则必有 $\deg(D)<\min(m,n)$，从而 $2^{\deg(D)}<2^{\min(m,n)}$. 另一方面，因 D 为 A，B 的因子，$\mathrm{lc}(D)$ 必同时整除 a_m，b_n，从而 $\mathrm{lc}(D)\leqslant\gcd(a_m, b_n)$，再利用 Landau-Mignotte 不等式即得.

推论 3.2.2 $A=\sum_{i=0}^{m}a_i x^i$ 与 $B=\sum_{i=0}^{n}b_i x^i$ 的最大公因子的系数不超过

$$2^{\min(m,n)}\gcd(a_0, b_0)\min\left\{\frac{1}{|a_0|}\sqrt{\sum_{i=0}^{m}a_i^2}, \frac{1}{|b_0|}\sqrt{\sum_{i=0}^{n}b_i^2}\right\}.$$

证明 若 $C=\sum_{i=0}^{l}c_i x^i$ 为 $A=\sum_{i=0}^{m}a_i x^i$ 的因子，则 $\overline{C}=\sum_{i=0}^{l}c_{l-i}x^i$ 为 $\overline{A}=\sum_{i=0}^{m}a_{m-i}x^i$

的因子，反之亦然．对 $\overline{A}$，$\overline{B}$ 应用推论 3.2.1 即得．

以上的一些结论告诉我们，可用于模方法的素数的粗略下界 M，当 $p>2M$ 时，则可保证 $D=D_p$．但并非大于这些下界的素数就可以用于模方法，为保证 $D_p=\gcd(A_p,B_p)$ 成立，素数 p 还必须满足下述条件．

命题 3.2.1 若素数 p 不能整除 $\mathrm{lc}(\gcd(A,B))$，则

$$\deg(\gcd(A_p,B_p))\geqslant\deg(\gcd(A,B)).$$

证明 记 $D=\gcd(A,B)$，则因 $D\mid A$，$D\mid B$，可知 $D_p\mid\gcd(A_p,B_p)$．这说明 $\deg(D_p)\leqslant\deg(\gcd(A_p,B_p))$．但 $p\nmid\mathrm{lc}(D)$，所以

$$\deg(D)=\deg(D_p)\leqslant\deg(\gcd(A_p,B_p)).$$

推论 3.2.3 若素数 p 不同时整除 $\mathrm{lc}(A)$ 与 $\mathrm{lc}(B)$，则

$$\deg(\gcd(A_p,B_p))\geqslant\deg(\gcd(A,B)).$$

证明 p 不同时整除 $\mathrm{lc}(A)$，$\mathrm{lc}(B)$，令 $D=\gcd(A,B)$，则必 $p\nmid\mathrm{lc}(D)$．不然设 $p\mid\mathrm{lc}(D)$，则因 $\mathrm{lc}(D)\mid\mathrm{lc}(A)$，$\mathrm{lc}(D)\mid\mathrm{lc}(B)$，可推出 p 同时整除 $\mathrm{lc}(A)$，$\mathrm{lc}(B)$，矛盾．再由命题 3.2.1 即得本推论．

定理 3.2.2 设 $D=\gcd(A,B)$，若 p 满足推论 3.2.3 的条件，且 $p\nmid\mathrm{res}_x(A/D,B/D)$，则 $\gcd(A_p,B_p)=D_p$．

证明 易见 $\mathrm{res}_x(A/D,B/D)\neq0$．由推论 3.2.3 知，$D_p\neq0$．由定理 3.1.1 知，存在 S,T，使得

$$S(A/D)+T(B/D)=\mathrm{res}_x(A/D,B/D),$$

由此得

$$SA+TB=\mathrm{res}_x(A/D,B/D)D,$$

进而有

$$S_pA_p+T_pB_p=\mathrm{res}_x(A/D,B/D)_pD_p.$$

由此可推出

$$\gcd(A_p,B_p)\mid D_p.$$

但一般总有

$$D_p\mid\gcd(A_p,B_p),$$

故

$$\gcd(A_p,B_p)=D_p.$$

定义 3.2.1 如果 $\gcd(A_p,B_p)=\gcd(A,B)_p$，则称该问题的约化是**良好的**，或 p 是**良约化的**，否则称为**劣约化的**．

定理 3.2.2 说明劣约化的素数 p 是有限的．这是因为可以整除 $\mathrm{res}_x(A/D,B/D)$ 的整数显然是有限的．因此在计算时，如果我们随机地选取素数 p，则几乎可以满测度地取得良约化的素数．

例 3.2.2 设

$$A=3x^6+5x^4-4x^2-9x+21,$$

$$B = x^8 + x^6 - 3x^4 - 3x^3 + x^2 + 2x - 5.$$

则在模 2 运算下有

$$A_2 = x^6 + x^4 + x + 1,$$
$$B_2 = x^8 + x^6 + x^4 + x^3 + x^2 + 1,$$

且

$$A_2 \equiv (x+1)(x^5 + x^4 + 1) \bmod 2,$$
$$B_2 \equiv (x+1)(x^7 + x^6 + x^3 + x + 1) \bmod 2.$$

这说明 $\deg(\gcd(A_2, B_2)) \geqslant 1$. 但我们已知 $\gcd(A, B) = 1$，按照定义 3.2.1，2 是劣约化的. 在以后的素数中，3 整除 A 领项系数，因此有可能是劣约化的，由例 3.2.1 可知，素数 5 是良约化的.

算法 3.2.1 最大公因子的模方法：

```
Input A, B primitive;
Output D;
  M:= Landau-Mignotte-bound(A, B);
  do p:= find-large-prime(2M);
    if deg(A_p) = deg(A) or deg(B_p) = deg(B);
      then D:= modular-gcd(A,B,p);
        if D|A and D|B;
          then return D;
  forever;
```


在算法 3.2.1 中，Landau-Mignotte-bound(A, B) 表示利用 Landau-Mignotte 不等式求得 A，B 的因子的系数的一上界；find-large-prime$(2M)$ 表示随机地选取一个大于 $2M$ 的素数 p；当该素数不同时整除 A 和 B 的领项系数时，modular-gcd(A, B, p) 用模 p 的 Euclid 方法计算 A，B 的最大公因子 D；若 D 整除 A 和 B，则 D 为所求，否则重新选取素数 p 进行计算. 当然上述算法仅仅是说明性的，真正在机器上实现时还需要考虑许多细节问题.

命题 3.2.2 设 A，B 为给定的本原多项式，M 为利用 Landau-Mignotte 不等式求得的 A，B 的因子的系数的一上界，$p > 2M$ 为某一正整数，则当 $\gcd(A_p, B_p)$ 同时整除 A 和 B 时，$\gcd(A_p, B_p) = \gcd(A, B)$；否则 p 是劣约化的.

证明 当 $p > 2M$ 时，易见 $D_p = D$. 若 $\gcd(A_p, B_p)$ 同时整除 A 和 B，则应有 $\gcd(A_p, B_p) \mid D$. 但一般总有 $D = D_p \mid \gcd(A_p, B_p)$，从而 $\gcd(A_p, B_p) = D$. 若 $\gcd(A_p, B_p)$ 不同时整除 A 和 B，则由 $D = D_p \mid \gcd(A_p, B_p)$ 可知，存在 Q，使得

$$\gcd(A_p, B_p) = DQ.$$

如果 Q 为常数，则因 $\gcd(A_p, B_p)$ 可选为本原形式，可知 $Q = 1$，这与 $\gcd(A_p, B_p)$ 不同时整除 A 和 B 矛盾，故 Q 非常数，此时必有 $\deg(Q) > 0$，于是可以推知

$$\deg(D) = \deg(D_p) < \deg(\gcd(A_p, B_p)),$$

这说明 p 是劣的.

命题 3.2.2 保证算法 3.2.1 终止时，计算所得结果就是 A 和 B 的最大公因子，而劣约化素数的有限性又可以保证算法是有限步终止的.

利用算法 3.2.1 原则上可以计算多项式的最大公因子，但是利用 Landau-Mignotte 不等式确定的素数 p 有可能很大，如果直接用算法 3.2.1 计算多项式的最大公因子，就难以达到利用较少的数据位数进行计算的目的．我们希望利用孙子剩余定理来改进上述方法，以达到使用尽可能少的数据位数计算的目的，我们称为**改进的模方法**．

改进模方法的基本思想是：假设 p，q 为两个互素的良约化整数，且已经利用某种方法求得 A_p，B_p 与 A_q，B_q 的最大公因子 D_p，D_q，此时应存在 $W^{(i)}$，$V^{(i)}$，$i=p,q$，使得

$$D_p = W^{(p)}A_p + V^{(p)}B_p,$$

$$D_q = W^{(q)}A_q + V^{(q)}B_q,$$

其中 $\deg(D)=\deg(D_p)=\deg(D_q)$，$\deg(W^{(r)})<\deg(B_r)$，$\deg(V^{(r)})<\deg(A_r)$，$r=p,q$．对上面两个等式中的多项式的系数应用孙子定理，设 $\deg(D)=m$，

$$D_p = a_0{}^{(p)}x^m + \cdots + a_{m-1}{}^{(p)}x + a_m{}^{(p)},$$

$$D_q = a_0{}^{(q)}x^m + \cdots + a_{m-1}{}^{(q)}x + a_m{}^{(q)},$$

考虑同余方程

$$a_i{}^{(pq)} \equiv a_i{}^{(p)} \mod p,$$

$$a_i{}^{(pq)} \equiv a_i{}^{(q)} \mod q,\ i=0,1,\cdots,m,$$

则可求得

$$D^{(pq)} = a_0{}^{(pq)}x^m + \cdots + a_{m-1}{}^{(pq)}x + a_m{}^{(pq)}.$$

同理，也应存在 $W^{(pq)}$，$V^{(pq)}$，使得

$$D^{(pq)} = W^{(pq)}A_{pq} + V^{(pq)}B_{pq}.$$

假设 A_{pq}，B_{pq} 的最大公因子为 D_{pq}，则应有 D_{pq} 整除 $D^{(pq)}$，但是 p，q 是良约化的，pq 也应为良约化的，故 $\deg(D)=\deg(D_{pq})=\deg(D^{(pq)})$，从而 D_{pq}，$D^{(pq)}$ 只能相差一常数倍．再注意它们都取本原形式，可知二者相等．这说明仅对 D_p，D_q 应用孙子定理即可求得 A_{pq}，B_{pq} 的最大公因子．

一般地，我们可以先选两个良约化的素数 p，q，分别计算 A，B 的模 p 与模 q 的公因子 $\gcd(A_p,B_p)$ 与 $\gcd(A_q,B_q)$，然后再利用孙子定理求得 A，B 的模 pq 的公因子 $\gcd(A_{pq},B_{pq})$．反复利用这种方法即可求得 A，B 的模任意大的整数的公因子．

事实上，对于给定的 p，q，我们无法知道它们是否为良约化的．但当它们满足推论 3.2.3 条件时，则有 $\deg(D)=\deg(D_p)=\deg(D_q)$，在计算中，若 $\deg(\gcd(A_p,B_p))<\deg(\gcd(A_q,B_q))$，则必有 $\deg(\gcd(A_q,B_q))\neq\deg(D_q)=\deg(D)$，此时 q 必为劣约化的，可放弃 q 重新选择；否则，只好认为 p，q 是良约化的．

算法 3.2.2 改进的最大公因子的模方法：

```
    Input A, B;
    Output D;
        M:=LandauMignotte-bound(A, B);
        Avoid:=gcd(lc(A), lc(B));
    E0: p:=find-prime(Avoid);
        D:=modular-gcd(A, B, p);
    E1: if deg(D)=0 then return 1;
```

```
Known:=p;
Result:=D;
while Known≤2M do
    p:= find-prime(Avoid);
    D:=modular-gcd(A, B, p);
    if deg(D)<deg(Result) then goto E1;
    if deg(D)=deg(Result)
      then Result:=CRT(Result,Known,D,p);
        Known:= Known×p;
if Result|A and Result|B;
    then return Result;
goto E0;
```

在上述算法中，M 仍然是利用 Landau-Mignotte 不等式寻找 A，B 的因子的系数的一个上界；p 为随机选取的不能整除 $Avoid$ 的素数；modular-gcd（A，B，p）表示用 Euclid 方法在模 p 运算下求得的 A，B 的最大公因子．循环体中的 CRT（$Result$，$Known$，D，p）表示对多项式 $Result$（modulo $Known$）和 D（modulo p）利用孙子定理求 A，B 的模（$Known\times p$）的最大公因子 $\gcd(A_{(Known\times p)}, B_{(Known\times p)})$．

在上算法中，有几种情况需要说明：

1）在 E_1 步有一个出口“if deg（D）= 0 then return 1”，这说明对所选定的 p，有 $\deg(\gcd(A_p, B_p))=0$．若 $C=\gcd(A, B)$，由推论 3.2.3 知，$\deg(C)\leqslant\deg(\gcd(A_p, B_p))=0$，从而必有 $C=1$．

2）在循环体 while-do 内有一个出口“if deg（D）≤ deg（$Result$）then goto E_1”，这是因为对满足推论 3.2.3 的任意素数 p，总成立 $\deg(C)=\deg(C_p)\leqslant\deg(\gcd(A_p, B_p))$，因此若 $\deg(\gcd(A_p, B_p))<\deg(\gcd(A_q, B_q))$，则必有 $\deg(\gcd(A_q, B_q))\neq\deg(D_q)=\deg(D)$，说明对应 $Result$ 的前一个素数是劣约化的，故转到步 E_1 重新选素数．

3）如果计算不从以上出口转出，则只好认为所进行的约化都是良好的；当循环体执行结束时，还需要检查所得的结果 $Result$ 是否整除 A，B．如果 $Result=\gcd(A_{Known}, B_{Known})$ 同时整除 A 和 B，则有

$$D_p \mid \gcd(A_{Known}, B_{Known}) \mid D.$$

但 $\deg(D)=\deg(D_p)$，故 D 和 D_p 只相差一常数倍，又二者都是本原的，故必相等．

4）若 $Known>2M$ 且 $Result=\gcd(A_{Known}, B_{Known})$ 不同时整除 A 和 B，则由命题 3.2.2 知，$Known$ 是劣的，则需转到 E_0 步重新选择素数计算．

例 3.2.3 设 A，$B\in Z[x]$，为

$$A = x^4+25x^3+145x^2-171x-360,$$
$$B = x^5+14x^4+15x^3-x^2-14x-15.$$

按上述算法则有

$$M := 446,$$
$$Avoid := \gcd(\mathrm{lc}(A), \mathrm{lc}(B)) = 1.$$

取 $p=5$，模 5 计算得

$$A_5 = x^4-x,\ B_5 = x^5-x^4-x^2+x,$$

$$\gcd(A_5, B_5) = x^4 - x.$$

再模 7 计算得

$$A_7 = x^4 - 3x^3 - 2x^2 - 3x - 3,$$
$$B_7 = x^5 + x^3 - x^2 - 1,$$
$$\gcd(A_7, B_7) = x^2 + 1.$$

因为 $\deg(\gcd(A_7, B_7)) < \deg(\gcd(A_5, B_5))$，5 是劣约化的．放弃模 5 的计算，再选下一个素数 11，模 11 计算得

$$A_{11} = x^4 + 3x^3 + 2x^2 + 5x + 3,$$
$$B_{11} = x^5 + 3x^4 + 4x^3 - x^2 - 3x - 4,$$
$$\gcd(A_{11}, B_{11}) = x^2 + 3x + 4.$$

现在 $\deg(\gcd(A_7, B_7)) = \deg(\gcd(A_{11}, B_{11}))$．设 $\gcd(A_{77}, B_{77}) = x^2 + ax + b$，其中 $-77/2 < a, b < 77/2$．由

$$a \equiv 3 \bmod 11,\ a \equiv 0 \bmod 7,$$
$$b \equiv 4 \bmod 11,\ b \equiv 1 \bmod 7,$$

以及

$$(-3)\times 7 + 2 \times 11 = 1,$$

应用孙子剩余定理可求得

$$a \equiv 0 + (3 - 0) \times (-3) \times 7 \equiv 14 \bmod 77,$$
$$b \equiv 1 + (4 - 1) \times (-3) \times 7 \equiv 15 \bmod 77.$$

即 $D = \gcd(A_{77}, B_{77}) = x^2 + 14x + 15$．经检验，$D \mid A$ 且 $D \mid B$，故 $D = x^2 + 14x + 15$ 为所求．注意，在本例中，因为 $\gcd(A_7, B_7) = 1$，$\gcd(A_{11}, B_{11})$ 的领系数都是 1，故 $\gcd(A_{77}, B_{77})$ 的领系数也直接取为 1．

3.3 多元多项式的最大公因子

3.3.1 Euclid 方法

设 $A, B \in \mathbf{Z}[x_1, \cdots, x_r]$．令 $\boldsymbol{R} = \mathbf{Z}[x_1, \cdots, x_{r-1}]$，则 A，B 可视作系数为 $\boldsymbol{R}$ 中元素的关于未定元 x_r 的一元多项式，即 $A, B \in \boldsymbol{R}[x_r]$．我们称 x_r 为主未定元．此时一元多项式最大公因子计算的许多方法都可以推广到多元情形．利用多项式的本原部分和容度的概念，记 $\mathrm{cont}(A, r)$，$\mathrm{pp}(A, r)$ 为视 A 为 $\boldsymbol{R}[x_r]$ 中元素时 A 的容度和本原部分，$gcd(A, B, x_r)$ 为 A，B 在 $\boldsymbol{R}[x_r]$ 中的公因子，则由 Gauss 引理有

$$\begin{aligned}\gcd(A, B) &= \mathrm{cont}(\gcd(A, B, x_r))\mathrm{pp}(\gcd(A, B, x_r)) \\ &= \gcd(\mathrm{cont}(A, r), \mathrm{cont}(B, r)) \\ &\quad \times \gcd(\mathrm{pp}(A, r), \mathrm{pp}(B, r)).\end{aligned}$$

此时 $\mathrm{pp}(A, r)$，$\mathrm{pp}(B, r)$ 为关于未定元 x_r 的一元多项式，可用已知的方法，譬如说 Euclid 方法，求其最大公因子．而 $\mathrm{cont}(A, r)$，$\mathrm{cont}(B, r)$ 均为 $r-1$ 元多项式．这样我们就把 r 元问题化归为 $r-1$ 元问题，从而可递归地求得多元多项式的最大公因子．

算法 3.3.1 多元多项式最大公因子的 Euclid 递归算法：

```
Procedure gcd(A, B, r)
    A_cont := cont(A, r);
    A_pp := A/A_cont;
    B_cont := cont(B, r);
    B_pp := B/B_cont;
    return pp(Euclid(A_pp, B_pp, r), x_r)×
           gcd(A_cont, B_cont, r−1);
```

算法中 gcd（A，B，r）表示求 r 元问题的最大公因子；Euclid（A_{pp}，B_{pp}，r）表示视 A_{pp}，B_{pp}为 $\boldsymbol{R}[x_r]$上的一元多项式，并用 Euclid 方法求其最大公因子．设求得的公因子为 D，则有 Q_1，$Q_2 \in \boldsymbol{R}[x_r]$，$c_1$，$c_2 \in \boldsymbol{R}$ 使得

$$c_1 A_{pp} = DQ_1,\ c_2 B_{pp} = DQ_2.$$

于是由 Gauss 引理，得

$$A_{pp} = pp(D)pp(Q_1),\ B_{pp} = pp(D)pp(Q_2).$$

即用 Euclid 算法求得最大公因子后，还需取其本原部分．gcd（A_{cont}，B_{cont}，$r-1$）表示求一 $r-1$ 元问题，即已把原问题降维．对于上算法中求 $\boldsymbol{R}[x_r]$中多项式的容度，可用下列子算法求得．

算法 3.3.2 容度的计算：

```
Subprocedure cont(A, r)
    Result := coef(A, x_r, 0);
    i := 1;
    while Result ≠ 1 and i < deg(A, x_r) do
        Result = gcd(Result, coef(A, x_r, i), r−1);
        i := i+1;
    return Result;
```


在上述子算法中，coef（A，x_r，i）表示 A 关于主未定元 x_r 的 i 次项的系数．整个子算法仍需调用计算 $r-1$ 元多项式最大公因子的程序．

例 3.3.1 设 $A(x, y)$，$B(x, y) \in Z[x, y]$，定义为

$$A(x, y) = (y^2 - y - 1)x^2 - (y^2 - 2)x + (y^2 + y + 1),$$
$$B(x, y) = (y^2 - y + 1)x^2 - (y^2 + 2)x + (y^2 + y + 2).$$

视 x 为主未定元，容易看出 cont(A) = cont(B) = 1．即 A，B 都是本原的．用伪除方法求余式序列(把 A，B 看成 x 的一元多项式)得

$$R_2 = (2y^2 - 4y)x + (y^2 + 3y + 3),$$
$$R_3 = -7y^6 + 5y^5 - 16y^4 + 15y^3 - 26y^2 + 15y - 9.$$

最后一个多项式关于 x 是常数，其本原部分为 1，故

$$gcd(A, B) = gcd(cont(A), cont(B))pp(R_3) = 1.$$

由本例可以看出，多元多项式的 Euclid 方法是不实用的．在计算过程中，多项式的系数与非主未定元的次数增长得都很快．

3.3.2 模方法

已知在一元多项式中采用模方法可以控制中间未定元的系数与次数的增长. 那么在多元情形模方法是否也可以应用它并具有同样的效果呢? 回答是肯定的. 下面我们就来讨论这个问题.

设 A, B, $D \in \mathbf{Z}[x_1, x_2, \cdots, x_r]$ 且 $D \mid A$, $D \mid B$, 则有 P, $Q \in \mathbf{Z}[x_1, x_2, \cdots, x_r]$, 使得

$$A = DP, \quad B = DQ.$$

记 $L_a^{(2)} = x_2 - a$, $D_{L_a^{(2)}}$ 为将未定元 x_2 用 a 代换所得的多项式, 其他多项式定义类似, 则有

$$A_{L_a^{(2)}} = D_{L_a^{(2)}} P_{L_a^{(2)}}, \quad B_{L_a^{(2)}} = D_{L_a^{(2)}} Q_{L_a^{(2)}}.$$

这表明 $D_{L_a^{(2)}}$ 仍为 $A_{L_a^{(2)}}$, $B_{L_a^{(2)}}$ 的公因子.

例 3.3.2 设

$$A = (y^2 - y - 1)x^2 - (y^2 - 2)x + (y^2 + y + 1),$$
$$B = (y^2 - y + 1)x^2 - (y^2 + 2)x + (y^2 + y + 2),$$

取 $L_2^{(y)} = y - 2$, 则

$$A_{L_2^{(y)}} = x^2 - 2x + 7, \quad B_{L_2^{(y)}} = 3x^2 - 6x + 8.$$

易算得 $B_{L_2^{(y)}} = 3A_{L_2^{(y)}} - 13$, 即 $B_{L_2^{(y)}}$, $A_{L_2^{(y)}}$ 互素. 设 D 为 A, B 的最大公因子, 由此可推得 $D_{L_2^{(y)}} = 1$. 记 $\mathrm{lc}_x(D)$ 为 D 的关于 x 的一元多项式的领项系数, 则 $\mathrm{lc}_x(D)$ 必同时整除 $\mathrm{lc}_x(A)$, $\mathrm{lc}_x(B)$, 从而 $\mathrm{lc}_x(D) \mid \gcd(\mathrm{lc}_x(A), \mathrm{lc}_x(B))$. 但 $\gcd(\mathrm{lc}_x(A), \mathrm{lc}_x(B)) = \gcd(y^2 - y - 1, y^2 - y + 1) = 1$, 从而 $\mathrm{lc}_x(D) = 1$. 在将 2 赋予 y 以后, D 与 $D_{L_2^{(y)}}$ 关于 x 应具有相同的次数, 由此推得 $D = 1$.

从表面上看, 我们是对多项式的某个未定元赋值, 但实际上是将该多项式除以一个线性多项式求余. 如果 $A \in \mathbf{Z}[x_1, \cdots, x_r]$, $a \in \mathbf{Z}$, 考虑 A 伪除以 $x_r - a$, 则有

$$A = Q(x_r - a) + C,$$

其中 C 关于 x_r 的次数为 0, 或者说 C 不含有未定元 x_r, 在上式两端对 x_r 赋以值 a, 则得

$$A_{L_a^{(r)}} = C_{L_a^{(r)}} = C.$$

如果 $A \in \mathbf{Z}[x_1, \cdots, x_r]$, $P \in \mathbf{Z}[x_r]$, 并且有 $\mathrm{lc}_{x_r}(P) = 1$, $\deg_{x_r}(P) = m$, 则由伪除性质有 Q, $R_P \in \mathbf{Z}[x_1, \cdots, x_r]$, 使得

$$A = QP + R_P, \ \deg_{x_r}(R_P) < m.$$

考虑商环 $\mathbf{Z}[x_1, \cdots, x_r]/\langle P \rangle$, 记 A_P 为 A 在环同态

$$\Phi_P : \mathbf{Z}[x_1, \cdots, x_r] \longrightarrow \mathbf{Z}[x_1, \cdots, x_r]/\langle P \rangle$$

下的同态像, 即

$$A_P = \Phi_P(A),$$

则上述关系又可写成

$$A_P = \Phi_P(A) \equiv A \bmod P.$$

需要注意的是, 当 $\deg_{x_r}(P) = m > \deg_{x_r}(A)$ 时, $A = A_P$. 类似于一元情形, 我们也有

良约化与劣约化的概念.

定义 3.3.1 设 $\boldsymbol{R}$ 为整环，A，$B \in \boldsymbol{R}[y][x]$. $\boldsymbol{R}$ 的元素 a 称为**良约化的**，如果

$$\gcd(A, B)_{L_a^{(y)}} = \gcd(A_{L_a^{(y)}}, B_{L_a^{(y)}}),$$

否则称为**劣约化的**.

和一元情形相类似，我们有下列结果.

命题 3.3.1 设 $\boldsymbol{R}$ 为整环，A，$B \in \boldsymbol{R}[y][x]$，$D = \gcd(A, B)$，则 $\boldsymbol{R}$ 的元素 a 是劣约化的当且仅当 $y - a$ 整除 $\mathrm{res}_x(A/D, B/D)$.

证明 完全类似于一元情形.

命题 3.3.2 若 a 是良约化的，且 $y - a$ 不同时整除 A 与 B 的(关于 x 的)领项系数，则 $\gcd(A, B)$ 与 $\gcd(A_{L_a^{(y)}}, B_{L_a^{(y)}})$ 关于 x 有相同的次数.

证明 因为 $(y-a) \nmid \mathrm{lc}_x(A)$ 并且 $(y-a) \nmid \mathrm{lc}_x(B)$，故 $(y-a) \nmid \mathrm{lc}_x(\gcd(A, B))$. 从而

$$\begin{aligned}\deg_x(\gcd(A, B)) &= \deg_x(\gcd(A, B)_{L_a^{(y)}}) \\ &= \deg_x(\gcd(A_{L_a^{(y)}}, B_{L_a^{(y)}})).\end{aligned}$$

命题 3.3.3 若 D 为 A 的因子，则 D 关于 y 的次数不超过 A 关于 y 的次数.

证明 显然.

有了以上的准备，我们可以讨论算法.

算法的基本思想是递归地把 r 元问题化归为 $r-1$ 元问题. 假定已经能解决 $r-1$ 元问题，我们来讨论 r 元问题的求解.

设 A，$B \in \mathbb{Z}[x_1, \cdots, x_r]$，则存在一个最小正整数 m，使得 $\deg(A, x_{r-1}) \leqslant m$，$\deg(B, x_{r-1}) \leqslant m$. 首先随机地取一整数 v_1，记 $L_1 = x_{r-1} - v_1$，$A_{v_1} = A_{L_1}$，$B_{v_1} = B_{L_1}$，则 A_{v_1}，B_{v_1} 为 $r-1$ 元多项式. 当 $\deg(A_{v_1}, x_r) = \deg(A, x_r)$ 且 $\deg(B_{v_1}, x_r) = \deg(B, x_r)$，即 $x_{r-1} - v_1$ 不整除 A 和 B 的关于 x_r 的最高项系数时，计算 A_{v_1}，B_{v_1} 的最大公因子. 这是一个 $r-1$ 元问题，按假定是可以解决的，将计算结果记为 $\gcd(A_{v_1}, B_{v_1}, r, r-1)$.

再随机地取另一不同的整数 v_2，重复进行上述过程，将所得结果记为 $\gcd(A_{v_2}, B_{v_2}, r, r-1)$. 如果 $\deg_{x_r}(\gcd(A_{v_1}, B_{v_1}, r, r-1)) > \deg_{x_r}(\gcd(A_{v_2}, B_{v_2}, r, r-1))$，说明 v_1 是劣约化的，放弃关于 v_1 的计算，重新选取一整数(不妨仍叫做 v_1)进行计算，直到两者相等，此时我们可以假定约化是良好的.

假设 $\gcd(A_{v_1}, B_{v_1}, r, r-1)$，$\gcd(A_{v_2}, B_{v_2}, r, r-1)$ 中出现的单项集合为 $\{t_1, t_2, \cdots, t_l\} \subset \mathbb{Z}[x_1, \cdots, x_{r-2}, x_r]$，则其可以表示为

$$\gcd(A_{v_1}, B_{v_1}, r, r-1) = a_1 t_1 + a_2 t_2 + \cdots + a_l t_l,$$

$$\gcd(A_{v_2}, B_{v_2}, r, r-1) = b_1 t_1 + b_2 t_2 + \cdots + b_l t_l,$$

其中 $a_i, b_i \in \mathbb{Z}$. 通过解同余方程

$$c_i(x_{r-1}) \equiv a_i, \mod L_1$$

$$c_i(x_{r-1}) \equiv b_i, \mod L_2, \quad i = 1, 2, \cdots, l.$$

则可得 A，B 模 $(x_{r-1}-v_1)(x_{r-1}-v_2)$ 的同态像的最大公因子

$$\gcd(A_{L_1L_2}, B_{L_1L_2}, r, r-1) = c_1(x_{r-1})t_1 + c_1(x_{r-1})t_2 + \cdots + c_l(x_{r-1})t_l .$$

求得 $\gcd(A_{L_1L_2}, B_{L_1L_2}, r, r-1)$ 后，再选异于 v_1，v_2 的整数 v_3，此时 L_1L_2 与 $L_3 = x_{r-1}-v_3$ 是互素的，再利用孙子定理，则可求得 A，B 模 $(x_{r-1}-v_1)(x_{r-1}-v_2)(x_{r-1}-v_3)$ 的同态像的最大公因子 $\gcd(A_{L_1L_2L_3}, B_{L_1L_2L_3}, r, r-1)$.

重复上述过程，可求得 A，B 模 x_{r-1} 的更高次多项式 $L_1L_2\cdots L_s$ 的最大公因子，当 $s \geqslant m$，即多项式 $L_1L_2\cdots L_s$ 的次数高于 m 时，因 A，B 关于 x_{r-1} 的次数不超过 m，故其同态像与其本身相等，我们自然也就求得了 A，B 的最大公因子.

在后面的算法 3.3.3 中，r 表示主未定元的足标，它在整个计算中保持不变；s 表示除主未定元之外的未定元的个数，也是我们将要赋值的未定元的足标；在开始计算时，s 应取作 $r-1$. 当 s 下降到 0 时，我们得到一个一元问题，可用 3.3.1 节的方法解决此问题，此时递归过程结束. 算法中的 random() 表示随机地产生一个整数，当然假定每次产生的整数都不相同；subs (x_s, v, A) 表示将 A 中的未定元 x_s 赋予值 v；在算法结束时，还需判断所得的最大公因子是否为 A，B 的最大公因子. 若不是，还需重新计算.

算法 3.3.3 多元多项式最大公因子的模方法：

```
Proc  gcd(A, B, r, s)
      if s=0 then return gcd-simple(A, B, x_r);
      M:=1+min(deg(A, x_s), deg(B, x_s));
E0:   do v:=random();
        A_v:=subs(x_s, v, A);
        B_v:=subs(x_s, v, B);
        while deg(A_v, x_r)≠deg(A, x_r)
              and deg(B_v, x_r)≠deg(B, x_r);
      D:=gcd(A_v, B_v, r, s-1);
E1:   Known:=x_s-v;
      n:=1; Res:=D;
      while n≤M do
          do v:= random();
            A_v:=subs(x_s, v, A);
            B_v:=subs(x_s, v, B);
            while deg(A_v, x_r)≠deg(A, x_r)
                  and deg(B_v, x_r)≠deg(B, x_r);
          D:=gcd(A_v, B_v, r, s-1);
          if deg(D, x_r)<deg(Res, x_r) then goto E1;
          if deg(D, x_r)= deg(Res, x_r) then
            Res:= CRT(Res, Known, D, x_s-v);
            Known:=Known×(x_s-v);
            n:=n+1;
      if Res|A and Res|B then return Res;
      goto E0;
```

例 3.3.3 设 A，$B\in \mathbf{Z}[x,y,z]$ 的定义为

$$\begin{aligned}A(x,y,z)=&\,9x^5+2x^4yz-189x^3y^3z+117x^3yz^2+3x^3\\&-42x^2y^4z^2+26x^2y^2z^3+18x^2-63xy^3z\\&+39xyz^2+4xyz+6,\\B(x,y,z)=&\,6x^6-126x^4y^3z+78x^4yz^2+x^4y\\&+x^4z+13x^3-21x^2y^4z-21x^2y^3z^2\\&+13x^2y^2z^2+13x^2yz^3-21xy^3z\\&+13xyz^2+2xy+2xz+2.\end{aligned}$$

首先对本例而言，若取 x 作为主未定元，则 A，B 关于 x 的最高项系数都是常数. 因此若选 z 作为第一个赋值未定元，则无论 z 在哪一点赋值，相应的线性式都不会整除最高项系数. 其次要想利用模方法求 A，B 的最大公因子，应估计出最大公因子关于各个非主未定元的次数，这关系到我们在算法中应该使用多少次多项式形式的孙子剩余定理. 因为最大公因子关于某个未定元的次数不会超过 A，B 关于该未定元的次数的最小者，若 $C=\gcd(A,B)$，则有

$$\deg_y(C)\leqslant 4,\ \deg_z(C)\leqslant 3.$$

按照模方法的思想，关于 z，应该取 4 个赋值点(因 $\deg_z(C)\leqslant 3$) z_i，$i=1,\cdots,4$. 然后分别计算 $A(x,y,z_i)$，$B(x,y,z_i)$，$i=1,\cdots,4$，的最大公因子 C_i，$i=1,\cdots,4$. 最后利用孙子剩余定理求出 C. 这样就将问题化归为 4 个二元问题.

为了控制系数的膨胀，对系数我们也采用模方法，即取一系列素数 p_i，$i=1,\cdots,$用关于未定元的模方法求出 A，B 在 $\mathbf{Z}_p[x,y,z]$ 内的最大公因子，再利用整数形式的孙子剩余定理计算 A，B 在 $\mathbf{Z}_{p_1\cdots p_i}[x,y,z]$ 中的最大公因子. 因为事先无法估计出 A，B 的因子的系数的界，我们不能确定应该使用多少次整数形式的孙子剩余定理，只能在每次求得 A，B 在 $\mathbf{Z}_{p_1\cdots p_i}[x,y,z]$ 内的最大公因子后，检验其是否整除 A，B，是则停止，否则继续计算.

按照上述思想，我们首先取 $p_1=11$，求 A，B 在 $\mathbf{Z}_{11}[x,y,z]$ 内的同态像的最大公因子. 此时其同态像为

$$\begin{aligned}A_{11}(x,y,z)=&-2x^5+2x^4yz-2x^3y^3z-4x^3yz^2+3x^3\\&+2x^2y^4z^2+4x^2y^2z^3-4x^2+3xy^3z\\&-5xyz^2+4xyz-5,\\B_{11}(x,y,z)=&-5x^6-5x^4y^3z+x^4yz^2+x^4y\\&+x^4z+2x^3+x^2y^4z+x^2y^3z^2\\&+2x^2y^2z^2+2x^2yz^3+xy^3z\\&+2xyz^2+2xy+2xz+2.\end{aligned}$$

按照算法的原则，我们应将其递归为一个二元问题. 为此随机地取 $z=2,-5,-3,5$，先考虑 $z=2$ 的情形，有

$$\begin{aligned}A_{11}(x,y,2)=&-2x^5+4x^4y-4x^3y^3+5x^3y\\&+3x^3-3x^2y^4-x^2y^2-4x^2\end{aligned}$$