四川大学“双一流”建设专项经费资助

非线性代数方程组与几何约束问题求解

向晓林◎著

四川大学出版社

四川大学“双一流”建设专项经费资助

非线性代数方程组与几何约束问题求解

向晓林◎著

四川大学出版社

责任编辑:唐　飞
责任校对:蒋　玥
封面设计:严春艳
责任印制:王　炜

图书在版编目(CIP)数据

非线性代数方程组与几何约束问题求解 / 向晓林著.
—成都：四川大学出版社，2018.2
ISBN 978-7-5690-1621-5

Ⅰ.①非… Ⅱ.①向… Ⅲ.①非线性方程-方程组-题解②几何-约束-题解 Ⅳ.①O175-44②O18-44

中国版本图书馆 CIP 数据核字（2018）第 036872 号

书名　**非线性代数方程组与几何约束问题求解**
Feixianxing Daishu Fangchengzu yu Jihe Yueshu Wenti Qiujie

著　　者　向晓林
出　　版　四川大学出版社
地　　址　成都市一环路南一段 24 号 (610065)
发　　行　四川大学出版社
书　　号　ISBN 978-7-5690-1621-5
印　　刷　郫县犀浦印刷厂
成品尺寸　185 mm×260 mm
印　　张　9
字　　数　219 千字
版　　次　2018 年 4 月第 1 版
印　　次　2018 年 4 月第 1 次印刷
定　　价　41.00 元

◆读者邮购本书,请与本社发行科联系。
电话:(028)85408408/(028)85401670/
(028)85408023　邮政编码:610065
◆本社图书如有印装质量问题,请
寄回出版社调换。
◆网址:http://www.scupress.net

引 言

计算机作为人类20世纪的伟大发明，推动了人类社会的快速发展，它正从人们的思想观念、工作方式、工作手段等方面彻底地改变着人类社会，它时时刻刻地改变着人们的生存和工作环境。计算机已经对科学家的研究方法、手段和环境带来了深刻的影响，利用它已经使许多对于科学研究者来说原来不可能或者很难做的研究工作得以实现，现在每天都会有数以万计的新的结论、成果、方法、技术和产品不断涌现，这无疑是与计算机的使用分不开的。

数学和计算机科学具有密切的关系，数学是计算机的灵魂，数学为计算机科学提供理论基础，计算机从数学上来说也仅仅是一个数学模型的具体实现。同时，数学为计算机能够快速、稳定地运算提供高效的算法；计算机也反过来对数学产生着深刻的影响，它使得数学比以往任何时刻都更具有威力，直接影响着数学中的价值观念和方法平衡，并通过其创新性的应用，间接地改变着数学的内容和结构。此外，计算机作为一种先进的工具，也正在改变着数学家的工作方式，它正在逐渐地成为数学家们不可替代的可靠助手和新思想的实验场所，它把数学家从繁复的演算中解放出来，使之能把更多的精力注入新的发现和创造中。

对于实际计算来说，一个好的算法是至关重要的，实际可行性问题不能容忍粗糙的算法，某些算法即使在理论上不管多么完备，如果没有能够接受的时间复杂性和空间复杂性，也只能算是一个空谈。正是在这个意义下，为了扩充有兴趣的计算机应用领域，出现了一个崭新的数学学科——机械化数学。它对实际可行性比对理论可能性更感兴趣，实际可行性已经成为衡量数学进步的一个重要准则。数学的发展已经由抽象的、结构主义的道路转向具体的、构造性的、结合实际的、结合计算机的道路。

迄今为止，定理机器证明领域相继出现了逻辑方法、代数方法以及几何不变量方法，但是，对这一领域的研究可以追溯到古代。数学机械化的主旨是寻求机械化的方法达到解决一类问题的目的，而追求数学的机械化方法正是中国古代数学的特点。中国古代数学研究的中心问题是求解，其方法是把问题分门别类，寻找出每一类的解题模式。《九章算术》就是把问题分成九大类，对每一类问题给出解题的办法[55]。

以希腊的几何学为代表的古代西方数学所研究的中心问题不是问题的分类求解，而是在建立公理体系的基础上一个一个地证明各式各样的数学命题。强调运用公理、假设进行逻辑推理，强烈地依赖于技巧与灵感。

17世纪，法国数学家笛卡儿创立了解析几何，使初等几何问题代数化，在世界上第一次把无章可循的几何证明题纳入了有一定规范形式的代数框架，为后来的几何定理

机器证明打下了基础。后来，德国数学家莱布尼茨也曾提出过“推理机器”的设想。

然而，第一次真正提出对某一类几何命题的假设的机械化检验方法的是数学大师希尔伯特。在距今100多年前的1899年出版的他的名著《几何基础》[175]中，提供了对一类几何命题进行检验的定理。关于希尔伯特机械化定理的证明可参见文献[175]的第六章，其更进一步的阐述参见吴文俊院士的名著《几何定理机器证明的基本原理》[111]的第三章。

1950年，波兰数学家Tarski发表了其著名的成果[172-173]：一切初等几何和初等范围内的命题，都可以用机械化的方法判定其是否成立。Tarski定理后来被Seidenberg[176]进行了简化。据此，对于几何问题，在适当的坐标系下把条件和结论化为纯代数问题，就能使用Tarski-Seidenberg方法。

1959年，数理逻辑学家王浩教授设计了一个程序，用计算机证明了罗素、怀特海的名著《数学原理》中的几百条定理，总共仅用了9 min。1976年，美国的两位年轻数学家阿佩尔和黑肯，在高速电子计算机上，用1200 h的时间证明了数学家100多年中未能证明的数学难题“地图四色定理”。

然而，人们期待的是能把初等几何定理成批地证明出来。但自Tarski的定理发表后的20多年中，初等几何定理的机器证明并未取得人们预期的进展。用Tarski的原有方法甚至连中学课本中的许多定理也证不出来。无论是Tarski原来的方法还是其后Seidenberg的简化都是极其复杂的，这些方法不仅难见实效，而且所得的解答也不能完全符合几何上的要求。及至中国数学家的加入，几何定理机器证明的研究取得了迅猛的发展。其中，张景中和他的课题组在定理的可读证明方面的工作[177-179]，杨路等在几何不等式型定理的机器证明方面的工作[54,118-119,122-124,180-184]等，世界瞩目。

然而，制约数学机械化领域研究发展的核心是非线性代数方程组的求解，它更是非线性科学的核心，很多来自工程、机械、科学研究等的实际问题最终都化为求解一个非线性代数方程组。非线性代数方程组的求解方法大体上分为非线性方程组的符号解法和数值解法，而其符号解法相对年轻且在数学机械化领域具有极其重要的地位。虽然非线性代数方程组的符号求解方法在国际国内有众多的科技工作者做了大量的工作[51-57]，但它还是一个至今没有彻底解决的数学难题；对非线性代数方程组求解研究的每一个成果，都将为数学机械化领域研究乃至非线性科学的每一个领域带来突破性的进展。

来自工程、机械等的几何约束问题，最终都将产生一个非线性代数方程组，同时该代数方程组中方程和未知量的个数都非常多，且往往其中的未知量的次数还非常高。因此，解决这些几何约束问题非常困难。目前，有很多学者在这方面做了大量的工作[122-123,134-144,150-152,164-166]，但是目前还没有实质性的突破，其根源在于没有一个好的非线性方程组的求解算法。

1953年，Leonard M. Blumenthal出版了距离几何的专著*Theory and Applications of Distance Geometry*[131]。1989年，杨路研究员和张景中院士进一步研究了距离几何的一些重要理论[126]，之后继续对其中的嵌入理论进行了深入的讨论[127-128,148]。最近，杨路研究员发觉使用距离几何的基本理论将有助于几何约束问题的求解的研究[130]，书中作者在杨路研究员现有工作的基础上，对非线性代数方程组，

特别对一类在机械、工程和技术等中出现的几何约束问题，利用距离几何的基本理论进行了系统深入的研究，取得了一定成效。

本书分4章。第1章对非线性代数方程组的求解算法进行了深入研究，给出了一个求一元高次代数方程组实根的定位算法，并用结式的基本理论给出了求代数数根界的一个有效算法；同时还给出了多项式的商环的对偶空间的基的显式表示的一个基本定理。第2章介绍了数值最优化的算法和理论，并在数值最优化的理论上作了一定的工作，所有这些对于我们的非线性代数方程组的求解都是必须的。第3章首先介绍了距离几何的基本理论，并在此基础上给出了能够对几何约束问题产生极少的方程个数的系统方法和理论；给出了将距离坐标转化为直角坐标的系统方法；进一步对几何元素在欧氏空间的实现的理论，用构造性的方法进行了发展；研究了非线性代数方程组的求解问题，并结合数值方法和符号方法的优势，给出了一个几何约束问题求解的系统、有效的算法。第4章将我们的系统方法用计算机代数系统编制了计算机程序，解决了几个典型的几何约束问题的求解。其中有些问题的求解还给出了其符号解，而这些问题按原有的方法根本不能得到其符号解。最后，书后附录给出了Maple代数系统编程基础和主要源程序清单。

本书在撰写过程中参考了大量的文献和资料，在此谨向相关作者表示衷心的感谢。由于作者水平有限，书中难免存在不足之处，敬请广大读者批评指正。

作者

2017年12月

目 录

第 1 章　非线性代数方程组的符号解法

21 世纪是非线性科学的世纪，方法论大师笛卡儿(R. Descartes)在其著作《思维与法则》里提出了一个大胆的设想：一切问题可以化为数学问题，一切数学问题可以化为代数问题，一切代数问题可以化为方程求解问题。事情当然不都可以这样“一刀切”，但科学研究的实践已经使科学家逐步意识到：非线性代数方程组的求解乃是非线性科学的核心；很多来自工程、机诫、科学研究等的实际问题最终都化为求解一个非线性代数方程组；而非线性代数方程组的求解，是一个至今没有彻底解决的数学难题；对非线性代数方程组求解研究的每一个成果，都将为非线性科学的每一个领域带来突破性的进展。非线性代数方程组的求解方法大体上分为非线性方程组的符号解法和数值解法。其中的符号解法有其独特的优势，如它能求出非线性代数方程组的所有解，且是精确的，但更加年轻；其数值解法[1-3,18-19,58-59]较为成熟，但也有其致命的弱点，例如，一般数值解法都只能求得非线性方程组的一个解，且只能求得近似解等。非线性代数方程组的符号解法目前大体分为 3 类，即 Groebner 基方法[51-53,56-57]、吴方法[51,54-55,57]和基于结式的方法[51,54]等。

§1.1　Groebner 基方法

记 $K[x_1, x_2, \cdots, x_n]$为数域 K 上的 n 元多项式环，$f_1, f_2, \cdots, f_s \in K[x_1, x_2, \cdots, x_n]$，记 $I \triangleq < f_1, f_2, \cdots, f_s > = \{f: f = \sum_{i=1}^{s} h_i f_i, h_i \in K[x_1, \cdots, x_n], i = 1, 2, \cdots, s\}$ 为多项式序列 $f_1, f_2, \cdots, f_s$ 在多项式环 $K[x_1, x_2, \cdots, x_n]$上生成的理想。记 $x^\alpha \triangleq x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ 为在多项式环 $K[x_1, x_2, \cdots, x_n]$上的单项式，其中 $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)^{\mathrm{T}} \in Z_{\geqslant 0}^n$称为单项式 x^α 的指数。

§1.1.1　理想的 Groebner 基

定义 1.1.1.1　单项式序：设“$>$”为 $Z_{\geqslant 0}^n$上的任意关系(或单项式 x^α，$\alpha \in Z_{\geqslant 0}^n$上的任意关系)，如果：

(1)“$>$”为 $Z_{\geqslant 0}^n$上的全序关系。

(2)如果 $\alpha > \beta$，$\alpha, \beta, \gamma \in Z_{\geqslant 0}^n$，那么 $\alpha + \gamma > \beta + \gamma$。

(3)“$>$”为$Z_{\geqslant 0}^{n}$上的良序关系，即：$Z_{\geqslant 0}^{n}$上的任意非空集合在关系“$>$”上都有最小元素。

那么，称关系“$>$”为多项式环$K[x_1, x_2, \cdots, x_n]$上的一个**单项式序**。

常用的单项式序有以下3种：

(1)若“$>_{lex}$”：$\alpha >_{lex} \beta \Leftrightarrow \alpha - \beta \in Z^n$，并且该差向量最左边的第一个非零数为正数，如果$\alpha >_{lex} \beta$，那么我们记$x^{\alpha} >_{lex} x^{\beta}$。可以证明，“$>_{lex}$”满足单项式序的定义1.1.1.1的3个条件。该序称为**字典序**。

(2)若“$>_{grlex}$”：$\alpha >_{grlex} \beta \Leftrightarrow |\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$，或者$|\alpha| = |\beta|$和$\alpha >_{lex} \beta$。如果$\alpha >_{grlex} \beta$，那么我们记$x^{\alpha} >_{grlex} x^{\beta}$。可以证明，“$>_{grlex}$”也满足单项式序的定义1.1.1.1的3个条件。该序称为**分级字典序**。

(3)若“$>_{grevlex}$”：$\alpha >_{grevlex} \beta \Leftrightarrow |\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$，或者 $|\alpha| = |\beta|$并且$\alpha - \beta \in Z^n$，该差向量最右边的第一个非零数为负数。如果$\alpha >_{gevrlex} \beta$，那么我们记$x^{\alpha} >_{grevlex} x^{\beta}$。可以证明，“$>_{grevlex}$”也满足单项式序的定义1.1.1.1的3个条件。该序称为**分级逆字典序**。

定义1.1.1.2 令$f = \sum_{\alpha} a_{\alpha} x^{\alpha}$为多项式环$K[x_1, x_2, \cdots, x_n]$上的多项式，关系“$>$”为多项式环$K[x_1, x_2, \cdots, x_n]$上的一个单项式序。

(1)多项式f的**多元次数**定义为：$multi\ \deg(f) = \max(\alpha \mid \alpha \in Z_{\geqslant 0}^{n},\ a_{\alpha} \neq 0)$，其中的最大是指关于序“$>$”取最大。

(2)多项式f的**首项系数**定义为：$LC(f) = a_{multi\ \deg(f)} \in K$。

(3)多项式f的**首单项式**定义为：$LM(f) = x^{multi\ \deg(f)}$。

(4)多项式f的**首项**定义为：$LT(f) = LC(f) \cdot LM(f)$。

算法1.1.1.1 [52](除法算法)

(输入：$f_1, f_2, \cdots, f_s, f$；输出：$a_1, a_2, \cdots, a_s, r$)

```
BEGIN
    a_1 = 0, a_2 = 0, ..., a_s = 0, r = 0
    p = f
    WHILE  p ≠ 0  DO
        i = 1
        divisionoccurred = false
        WHILE  i ≤ s AND divisionoccurred = false  DO
            IF  LT(f_i)  divides  LT(p)  THEN
                a_i = a_i + LT(p)/LT(f_i)
                p = p - (LT(p)/LT(f_i)) f_i
                divisionoccurred = true
            ELSE
                i = i + 1
```

FI;
IF $divisionoccurred = false$ THEN
$r = r + LT(p)$
$p = p - LT(p)$
FI;
OD;
OD;
END.

对于除法算法 1.1.1.2，有下面基本定理[51,57]：

定理 1.1.1.1　固定 $Z_{\geqslant 0}^{n}$ 上的单项式序“$>$”，令 $F=(f_1, f_2, \cdots, f_s)$ 为多项式环 $K[x_1, x_2, \cdots, x_n]$ 上的 s 个多项式组成的有序的 s −元组，那么，由算法 1.1.1.1，任意的 $f \in K[x_1, x_2, \cdots, x_n]$，都存在 $a_i (i=1, 2, \cdots, s)$，$r \in K[x_1, x_2, \cdots, x_n]$，使：

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r \tag{1.1.1.1}$$

这里，要么 $r=0$，要么 r 是环 $K[x_1, x_2, \cdots, x_n]$ 上的单项式的线性组合，并且，其中的每一项都不能被任意的 $LT(f_i)(i \in \{1, 2, \cdots, s\})$ 整除，我们称 r 为 F 除以 f 的**余数**，或称 r 为 f 关于 F 的**约化多项式**，记为 $\overline{f}^{F}$。此外，如果 $a_i f_i \neq 0$，那么必有：

$$multi\ \deg(f) \geqslant multi\ \deg(a_i f_i)$$

注 1.1.1.1　对于不同的单项式序，及 $f_1, f_2, \cdots, f_s$ 的不同顺序，一般会得到不同的 r。即余数 r 不唯一。

对于多项式环 $K[x_1, x_2, \cdots, x_n]$ 上的理想，有下面重要的 Hilbert 基定理：

定理 1.1.1.2　[51](Hilbert 基定理)多项式环 $K[x_1, x_2, \cdots, x_n]$ 上的每一个理想 $I \subset K[x_1, x_2, \cdots, x_n]$ 都有一个有限生成集，即：存在 $g_1, g_2, \cdots, g_t \in I$，使：

$$I = < g_1, g_2, \cdots, g_t >$$

我们称 $g_1, g_2, \cdots, g_t$ 为理想 I 的**基**。

令 $I \subset K[x_1, x_2, \cdots, x_n]$ 为多项式环 $K[x_1, x_2, \cdots, x_n]$ 上一个理想且 $I \neq \{0\}$，记理想 I 中的元素的首项的集合为 $LT(I)$，即：$LT(I) = \{cx^{\alpha} \mid$ 存在 $f \in I$ 使 $LT(f) = cx^{\alpha}\}$。记 $<LT(I)>$ 为由 $LT(I)$ 的元素生成的理想。

定义 1.1.1.3　[51](Groebner 基)固定一个单项式序，$I \subset K[x_1, x_2, \cdots, x_n]$ 为多项式环 $K[x_1, x_2, \cdots, x_n]$ 上的一个理想，$g_1, g_2, \cdots, g_t \in I$，如果：

$$< LT(g_1), LT(g_2), \cdots, LT(g_t) > = < LT(I) >$$

那么，我们称有限子集 $G = \{g_1, g_2, \cdots, g_t\}$ 为理想 I 的 Groebner **基或标准基**。

定义 1.1.1.4　[51-52](S −多项式)令 $f, g \in K[x_1, x_2, \cdots, x_n]$ 为非零多项式，固定一个多项式序，设 $LT(f) = cx^{\alpha}$，$LT(g) = dx^{\beta}$，这里 $c, d \in K$；令 x^{γ} 为单项式 x^{α} 和 x^{β} 的最小公倍式。我们称：

$$S(f, g) \triangleq \frac{x^{\gamma}}{LT(f)} \cdot f - \frac{x^{\gamma}}{LT(g)} \cdot g$$

为多项式 f，g 的 $S-$**多项式**。

关于 $S-$多项式，有下列重要的 Buchberger 定理：

定理 1.1.1.3 [51,60-61](Buchberger 定理)理想 I 的有限子集 $G=\{g_1, g_2, \cdots, g_t\}$ 是理想 I 的 Groebner 基，当且仅当对所有的 $i, j \in \{1, 2, \cdots, t\}$，$i \neq j$，$\overline{S(g_i, g_j)}^G=0$。

据此，有下列重要的求理想 I 的 Groebner 基的基本算法：

算法 1.1.1.2 [51-52,60-61](Groebner 基算法)

(输入：$F=(f_1, f_2, \cdots, f_s)$；输出：理想 $I=<F>$的 Groebner 基 $G=\{g_1, g_2, \cdots, g_t\}$，这里 $F \subset G$)

```
BEGIN
    G=F;
    REPEAT
        G'=G;
        FOR G'中的每对 p, q DO
            S=S(p, q)^G';
            IF S≠0 THEN
                G=G∪{S};
            FI;
        OD;
    UNTIL G=G';
END.
```

以上 Groebner 基算法仅仅为一较粗糙的算法，它的运行效率较低，对它的进一步修正可参考 Buchberger1985 年的工作[62]、Gebauer 和 Moller1988 年的工作[63]。

定义 1.1.1.5 [51]$I \subset K[x_1, x_2, \cdots, x_n]$为多项式环 $K[x_1, x_2, \cdots, x_n]$上的一个理想，$G=\{g_1, g_2, \cdots, g_t\}$ 是理想 I 的 Groebner 基；如果对任意的 $p, q \in G$，多项式 p 中的每一个单项式都不能整除 $LT(q)$，则称 G 为理想 I 的**约化 Groebner 基**；进一步，若还有 G 中的每一个多项式的首项系数都是 1，则称 G 为理想 I 的**首一的 Groebner 基**。

一般地，一个理想的 Groebner 基不是唯一的，但每一个理想一定只有唯一的一个首一的 Groebner 基[51-52]。

§1.1.2 用理想的 Groebner 基解非线性代数方程组

定义 1.1.2.1 [51]设 I 为多项式环 $K[x_1, x_2, \cdots, x_n]$上的一个理想，我们称：

$$I_l = I \cap K[x_{l+1}, x_{l+2}, \cdots, x_n]$$

为理想 I 的第 l 个**消元理想**。

直观地，如果 $I=<f_1, f_2, \cdots, f_s>$，那么 I_l 中的每一个元素都为 $f_1, f_2, \cdots, f_s$ 以多项式为系数的线性组合，并且，这些元素都已经从方程组 $f_1=f_2$

$=\cdots=f_s=0$ 中消去了变量 x_1，x_2，…，x_l。

记 $V(I)$ 为理想 I 的仿射簇，若 $I=<f_1, f_2, \cdots, f_s>$，则 $V(I)=zero(f_1, f_2, \cdots, f_s)$，也就是方程组 $f_1=f_2=\cdots=f_s=0$ 的解。

定理 1.1.2.1 [51-52]（消元定理）如果 G 是理想 I 关于字典序（或其他含有变量 x_1，x_2，…，x_l 的任何单项式都大于只含有其余变量的单项式）的 Groebner 基（其中 $x_1>x_2>\cdots>x_n$），那么：

$$G_l = G \cap K[x_{l+1}, x_{l+2}, \cdots, x_n]$$

必为理想 I 的第 l 个消元理想的 Groebner 基。

定义 1.1.2.2 [51]（部分解）称点 $(a_{l+1}, a_{l+2}, \cdots, a_n) \in V(I_l) \subset K^{n-l}$ 为一个部分解。

任意解 $(a_1, a_2, \cdots, a_n) \in V(I) \subset K^n$ 均可以截出一个部分解；反之，对任意的 $f \in K[x_1, x_2, \cdots, x_n]$，如果将 f 在理想 I 的第 l 个消元理想中记为：

$$f = c_q(x_{l+1}, x_{l+2}, \cdots, x_n)x_l^q + \cdots + c_0(x_{l+1}, x_{l+2}, \cdots, x_n)$$

这里 q 是 x_l 在 f 中出现的最高次幂，我们称 c_q 为 f 的首系数多项式。我们有下面的扩展定理：

定理 1.1.2.2 [51-52]（扩展定理）如果 K 为一个代数闭域（如 $K=C$），若 I_{l-1} 关于字典序的 Groebner 基的元素的首系数多项式在点 $(a_{l+1}, \cdots, a_n)$ 处不全为 0，那么 $V(I_l)$ 中的部分解 $(a_{l+1}, \cdots, a_n)$ 必能扩展为 $V(I_{l-1})$ 中的部分解 $(a_l, a_{l+1}, \cdots, a_n)$。

上面两个 Groebner 基的基本定理给出了一个解非线性代数方程组的一个简单方法：先求理想 I 的字典序 Groebner 基 G，然后从解 G 的含有最少变量（如一个变量）的多项式开始，逐次解 G 中增加一个变量的多项式，反复用扩展定理，直到找到理想 I 的解为止。这样解非线性多项式方程组的问题就转化为解序列一元高次多项式的问题了。

算法 1.1.2.1　（Groebner 基算法）

（输入：$F=(f_1, f_2, \cdots, f_s)$；输出：多项式方程组 $f_1=f_2=\cdots=f_s=0$ 的解）

BEGIN

　求理想 $I=<f_1, f_2, \cdots, f_s>$ 关于字典序的 Groebner 基 $G=\{g_1, g_2, \cdots, g_t\}$；

　FOR $r=1$ TO n DO

　　求 $G_l=G \cap K[x_{l+1}, x_{l+2}, \cdots, x_n]$，$l=n-r$；

　　将部分解 $(a_{l+2}, \cdots, a_n)$ 代入 G_l，得到只含有变元 x_{l+1} 的多项式 h_1，h_2，…，h_m；

　　IF G_l 的元素的首多项式不全为 0 THEN

　　求 $h_1, h_2, \cdots, h_m$ 的最大公因式 $h=\mathrm{GCD}(h_1, h_2, \cdots, h_m)$；

　　解 $h=0$ 得解 a_{l+1}，从而得到部分解 $(a_{l+1}, \cdots, a_n)$；

　　ELSE

　　方法失败，算法停止；

　　FI；

　OD；

END.

注意在实际用该算法解非线性代数方程组时，$h=0$ 往往有多个根，因而一个部分解$(a_{l+2}, \cdots, a_n)$最后扩展为多个部分解$(a_{l+1}, \cdots, a_n)$。因此，如果扩展定理的条件总是满足，那么该算法能求出非线性代数方程组的所有解。当然，要求解 $h=0$ 也是很困难的，在求解过程中往往扩展定理的条件会不满足而导致算法失败。同时，该算法由于计算量太大，实际计算时往往很慢。

§1.1.3 用理想的商代数解非线性代数方程组

设 $G=\{g_1, g_2, \cdots, g_t\}$ 为理想 I 的 Groebner 基，对于任意的 $f \in K[x_1, x_2, \cdots, x_n]$，由多项式的除法算法 1.1.1.1 知：

$$f = a_1 g_1 + a_2 g_2 + \cdots + a_t g_t + \overline{f}^G$$

由 Groebner 基理论，$\overline{f}^G$ 为单项式 $x^\alpha \notin <LT(I)>$的线性组合。并且[51-52]：

$$\overline{f}^G = \overline{g}^G \Leftrightarrow f - g \in I$$

$$\overline{f}^G + \overline{g}^G = \overline{f+g}^G$$

$$\overline{\overline{f}^G \cdot \overline{g}^G}^G = \overline{fg}^G$$

在商环 $K[x_1, x_2, \cdots, x_n]/I$ 中，记$[f]=f+I=\{f+h: h \in I\}$，显然有$[f]=[g] \Leftrightarrow f-g \in I$，商环 $K[x_1, x_2, \cdots, x_n]/I$ 由所有的$[f]$组成，这里 $f \in K[x_1, x_2, \cdots, x_n]$。由上知 $\overline{f}^G \in [f]$，并且 $\overline{f}^G$，$[f]$之间具有一一对应关系：$\overline{f}^G \leftrightarrow [f]$，因此，$\overline{f}^G$ 可以作为商环 $K[x_1, x_2, \cdots, x_n]/I$ 中的陪集$[f]$的标准表示。若在商环 $K[x_1, x_2, \cdots, x_n]/I$ 中加入数乘运算[商环中的常数为$[c](c \in K)$]，商环又具有向量空间结构，因此，商环 $K[x_1, x_2, \cdots, x_n]/I$ 为一个代数，称为商代数，记为 A。因为 A 中的元素的标准表示均为单项式 $x^\alpha \notin <LT(I)>$的线性组合，且这些单项式在 A 中线性无关，因此可将它们组成的集合看成 A 的基，即 A 的基为：$B=\{x^\alpha: x^\alpha \notin <LT(I)>\}$。

定理 1.1.3.1 [51-52,60-61](有限定理)令 $K \subset C$ 为一个域，$I \subset K[x_1, x_2, \cdots, x_n]$ 为一个理想，那么，下面几条必等价：

(1)代数 $A=K[x_1, x_2, \cdots, x_n]/I$ 为有限维代数。

(2)仿射簇 $V(I) \subset C^n$ 为有限集。此时称理想 I 为**零维理想**。

(3)如果 G 是理想 I 的 Groebner 基，那么，对任意的 $i(1 \leqslant i \leqslant n)$，必存在 $m_i \geqslant 0$，$g \in G$，使 $x_i^{m_i} = LT(g)$。

该定理的一个直接推论是：

推论 1.1.3.1 理想 I 为零维理想，当且仅当，对任意的 $i(1 \leqslant i \leqslant n)$，必存在一个非零的多项式 g，使 $g \in I \cap K[x_i]$，并且 g 生成消去理想 $I \cap K[x_i]$。多项式 g 称为理想 I 关于变量 x_i 的**最小多项式**。

只需用定理 1.1.3.1 的第三条，在求理想 I 的 Groebner 基时，选用字典序，并将变量 x_i 作为最小变量，便得推论 1.1.3.1。

该推论的一个应用是用它可以很容易地求零维理想对应的商代数的基。因为 G 是理想 I 的 Groebner 基，$x_i^{m_i} = LT(g)$，所以 $x_i^{m_i} \in <LT(I)>$，从而有代数 A 的基 B

中的元素的幂应在下面矩形框内：$D=\{\alpha \mid \alpha \in Z_{\geqslant 0}^{n},\ \forall i,\ 0 \leqslant \alpha_i \leqslant m_{i-1}\}$。因此，我们只需在矩形区域 D 内检验是否有 $\overline{x^{\alpha G}}=x^{\alpha}$，便可求得基 B，即 $B=\{x^{\alpha} \mid \alpha \in D,\ \overline{x^{\alpha G}}=x^{\alpha}\}$，若使用计算机代数系统 Maple 的 Groebner 包中的函数 *findunic*，求理想工关于变量 x_i 的最小多项式，检查理想 I 是否是零维的，使用函数 *finite*( )，便有如下求代数 A 的基 B 的算法。

算法 1.1.3.1　(求代数 A 的基 B 算法)

(输入：$plist=(f_1, f_2, \cdots, f_s)$，$vlist=(x_1, x_2, \cdots, x_n)$单项式序 *torder*；输出：代数 A 的基 B)

```
BEGIN
    IF finite(plist, vlist)THEN
        G=gbasis(plist, vlist, torder);
        B=[1];
        FOR v IN vlist DO
            m=degree(finduni(v, G, vlist), v);
            C=B;
            FOR t IN C DO
                FOR L FROM 1 TO m-1 DO
                    t =t * v;
                    IF normalf(t, G, vlist, torder)=t THEN
                        B=[op(B), t];
                    FI;
                OD;
            OD;
        OD;
        return(B);
    ELSE
        error(ideal is not zero-dimensional, no finitebasis');
    FI;
END.
```

在以上算法中，还使用了计算机代数系统 Maple 的如下函数：①*gbasis*( )：求理想的 Groebner 基；②*degree*( )：求一元多项式关于其变元的次数；③*normalf*( )：求多项式关于多项式组的约化；④*op*( )：取出列的元素；⑤*return*( )：返回结果；⑥*error*( )：返回错误信息等。关于更多的计算机代数系统 Maple 及其函数，参见文献[64-66]。

该推论的应用之二是，我们可以通过求最小多项式的根来计算非线性代数方程组的解的每一个分量的值。但是这些分量要怎样匹配才是要求的解，却是一件很难的事情。

定义 1.1.3.1　令 $I \subset K[x_1, x_2, \cdots, x_n]$为多项式环 $K[x_1, x_2, \cdots, x_n]$上一个理想，如果对任意的整数 $m \geqslant 1$，$f^m \in I \Rightarrow f \in I$，那么我们称理想 I 为**根理想**。

定义 1.1.3.2 令 $I \subset K[x_1, x_2, \cdots, x_n]$ 为多项式环 $K[x_1, x_2, \cdots, x_n]$ 上一个理想，理想 I 的根理想，记为 $\sqrt{I}$，由下列集合组成：$\{f: f^m \in I, m \geqslant 1$ 为某一正数$\}$。

定理 1.1.3.2 [51-52] 令 $I \subset K[x_1, x_2, \cdots, x_n]$ 为多项式环 $K[x_1, x_2, \cdots, x_n]$ 上一个理想，那么，$\sqrt{I}$ 为多项式环 $K[x_1, x_2, \cdots, x_n]$ 上的理想，$I \subset \sqrt{I}$，且 $\sqrt{I}$ 为一个根理想。

对于一般的理想 $I = <f_1, f_2, \cdots, f_s>$，目前已经有很有效的计算机算法计算其根理想及其生成元 $g_1, g_2, \cdots, g_t$，使 $\sqrt{I} = <g_1, g_2, \cdots, g_t>$，并且已在计算机代数系统 Axiom、Macauly、Singular、SCRATCHPAD 上实现(参见文献[72－73])。当理想 I 为零维理想时，计算其根理想变得极其简单，文献[52]给出了一个简单算法，利用该算法，很容易在计算机代数系统 Maple 上求一个零维理想的根理想。

理想的根理想的零点与原理想的零点相同，但已没有重零点。同时还有下列漂亮的结论：

定理 1.1.3.3 令 $I \subset C[x_1, x_2, \cdots, x_n]$ 为一个零维理想，且令 $A = C[x_1, x_2, \cdots, x_n]/I$，那么，$\dim_c(A)$ 大于等于仿射族 $V(I)$ 中的点的数目，当且仅当理想 I 为根理想时等号成立。

任给多项式 $f \in K[x_1, x_2, \cdots, x_n]$，这里 K 为一个代数闭域(如复数域 C)，我们可以用乘法定义代数 $K[x_1, x_2, \cdots, x_n]/I$ 到自身的映射 m_f 如下：

$$m_f: A \to A, \forall [g] \in A, m_f([g]) = [f][g] = [fg] \in A$$

那么，映射 m_f 必有下面的基本性质：

定理 1.1.3.4 [51] 令 $f \in C[x_1, x_2, \cdots, x_n]$，那么

(1)映射 m_f 是代数 A 到 A 的线性映射。

(2)$m_f = m_g$，当且仅当 $f - g \in I$。因此，两个多项式给出相同的线性映射，当且仅当相差一个理想 I 的元素；特别地，m_f 为零映射，当且仅当 $f \in I$。

当代数 A 为复数域 K 上的有限维向量空间时，我们可以按算法 1.1.3.1 求出代数 A 的基 B，然后计算出基 B 的每一个元素在映射 m_f 下的像，从而得到映射 m_f 的矩阵(记为 m_f)。

例 1.1.3.1 令 $G = \left\{x^2 + \frac{3}{2}xy + \frac{1}{2}y^2 - \frac{3}{2}x - \frac{3}{2}y,\ xy^2 - x,\ y^3 - y\right\}$，那么用分级逆字典序，并且令 $x > y$，通过用 Maple 计算知，G 为理想 $I = <G> \subset C[x, y]$ 的 Groebner 基，由算法 1.1.3.1 知代数 A 的基为 $B = \{1, x, y, xy, y^2\}$，令 $f = x$，则矩阵：

$$\boldsymbol{m}_x = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & \frac{3}{2} & 0 & -\frac{3}{2} & 1 \\ 0 & \frac{3}{2} & 0 & -\frac{1}{2} & 0 \\ 0 & -\frac{3}{2} & 1 & \frac{3}{2} & 0 \\ 0 & -\frac{1}{2} & 0 & \frac{3}{2} & 0 \end{bmatrix}$$

理想 I 的仿射族 $V(I)$ 与矩阵 $\boldsymbol{m}_f$ 之间有如下重要定理[51]：

定理 1.1.3.5　令 $I \subset C[x_1, x_2, \cdots, x_n]$ 为一个零维理想，$f \in C[x_1, x_2, \cdots, x_n]$，那么对于任意的 $\lambda \in C$，λ 为矩阵 $\boldsymbol{m}_f$ 的特征值，当且仅当 λ 为多项式 f 在 $V(I)$ 上的值。

由定理 1.1.3.1 容易知道，当 $f = x_i$ 时，矩阵 $\boldsymbol{m}_{x_i}$ 的特征值与仿射族 $V(I)$ 的 x_i 坐标相同，因此，我们通过计算所有矩阵 $\boldsymbol{m}_{x_i}$ 及其特征值，就能计算出仿射族 $V(I)$ 中的所有点的 x_i 坐标，从而求解非线性代数方程组。这样就把解非线性代数方程主的问题转化为就解线性代数中的矩阵特征值的问题了[67-68]。所有求解矩阵特征值的数值算法[69-70]都可以用于解非线性代数方程组了。

这种通过计算矩阵特征值来解非线性代数方程组的方法，与通过消去理论来解非线性代数方程组的算法 1.1.2.1 相比，有下面显著的优势：

(1)由于在矩阵 $\boldsymbol{m}_f$ 的计算与所用单项式序无关，而消去法理论必须使用字典序(或类似的序)，因此，该方法计算量要小得多。尽管我们可先不用字典序求理想的 Groebner 基，再用基转化算法将所求的基转化为字典序的 Groebner 基[61,71]，但计算量仍然很大。

(2)该方法更加稳定。

(3)由于是独立地求点的每一个分量，因此，它们之间的舍入误差不会互相影响。

在实际计算中，不需要计算 n 次矩阵 $\boldsymbol{m}_{x_i}$ 及其特征值，而只需要选择一个合适的线性多项式，从而计算一次矩阵 $\boldsymbol{m}_{c_1x_1+\cdots+c_nx_n}$ 及其特征值就行了。

定义 1.1.3.3　设 $\boldsymbol{M}$ 为一个 $n \times n$ 的矩阵，对于某一个数 $\lambda \in C$，若存在非零向量 $\boldsymbol{v} \neq 0$，使 $\boldsymbol{Mv} = \lambda \boldsymbol{v}$，那么称 $\boldsymbol{v}$ 为矩阵的**左特征向量**，相应地称数 λ 为矩阵 $\boldsymbol{M}$ 的**特征值**。由于矩阵 $\boldsymbol{M}$ 与其转置矩阵 $\boldsymbol{M}^{\mathrm{T}}$ 有相同的特征值，对于特征值 λ，我们可以找到非零向量 $\boldsymbol{v}' \neq 0$，使 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{v}' = \lambda \boldsymbol{v}'$，将式两边转置，并令 $\boldsymbol{v}'^{\mathrm{T}} = \boldsymbol{w}$，得 $\boldsymbol{wM} = \lambda \boldsymbol{w}$，则称 $\boldsymbol{w}$ 为矩阵 $\boldsymbol{M}$ 的**右特征向量**。

定理 1.1.3.6　[51]选取 $f \in C[x_1, x_2, \cdots, x_n]$，使对于不同的点 $p \in V(I)$，$f(p)$ 不同，那么，矩阵 $\boldsymbol{m}_f$ 的右特征向量空间由行向量 $(p^{\alpha(1)}, p^{\alpha(2)}, \cdots, p^{\alpha(m)})$ 张成。这里 $B = \{[x^{\alpha(1)}], [x^{\alpha(2)}], \cdots, [x^{\alpha(m)}]\}$ 为代数 A 看成向量空间的基。

若理想 $I = \langle f_1, f_2, \cdots, f_s \rangle$ 为任意的零维理想，以上定理可以用来求解非线性代数方程组 $f_1 = f_2 = \cdots = f_s = 0$(或仿射族 $V(I)$ 的点)。我们可以由数值方法计算矩阵 $\boldsymbol{m}_f$ 的任意特征值 λ 及相应的右特征向量 $\boldsymbol{v} \neq 0$，由定理 1.1.3.6，对某常数 λ 及某点 $p \in V(I)$，有

$$\boldsymbol{v} = \lambda(p^{\alpha(1)}, p^{\alpha(2)}, \cdots, p^{\alpha(m)}) \tag{1.1.3.1}$$

记 $p = (a_1, a_2, \cdots, a_n)$，我们可以由式(1.1.3.1)求出点 p 的坐标。

由有限定理 1.1.3.1，如果 G 是理想 I 的 Groebner 基，那么，对任意的 i，$1 \leqslant i \leqslant n$，必存在 $m_i \geqslant 0$，$g \in G$，使 $x_i^{m_i} = LT(g)$；如果 $m_i > 1$，那么必有 $[x_i] \in B$，因此 λa_i 必是 $\boldsymbol{v}$ 的坐标，而 $[1] \in B$，所以 λ 也是 $\boldsymbol{v}$ 的坐标，由 $a_i = \dfrac{\lambda a_i}{\lambda}$ 便可以求得点 p 的第 i 个坐标 a_i。当 $m_i = 1$ 时，由于基 B 中不含有该变量，为了计算点 p 的第 I 个变量，我