计算代数与应用

周 梦 编著

武汉大学出版社

图书在版编目(CIP)数据

计算代数与应用/周梦编著. —武汉：武汉大学出版社，2002.1

ISBN 7-307-03390-9

Ⅰ.计… Ⅱ.周… Ⅲ.代数几何 Ⅳ.O187

中国版本图书馆 CIP 数据核字(2001)第 077187 号

责任编辑：夏炽元　　**责任校对**：叶　效　　**版式设计**：支　笛

出版：**武汉大学出版社**　(430072　武昌　珞珈山)

(电子邮件：wdp4@whu.edu.cn　网址：www.wdp.whu.edu.cn)

发行：新华书店湖北发行所

印刷：湖北省京山县印刷厂

开本：850×1168　1/32　**印张**：9　**字数**：228 千字

版次：2002 年 1 月第 1 版　　2002 年 1 月第 1 次印刷

ISBN 7-307-03390-9/O・249　　**定价**：13.00 元

前　言

交换代数与代数几何是现代数学的主流分支之一。近二十年来，随着计算机技术的迅速发展，利用计算机符号计算系统对交换代数与代数几何中的可计算问题以及有关应用进行研究，形成了计算代数这个蓬勃发展的新方向。本书论述计算代数与应用理论的主要内容，介绍和反映其最新进展。内容包括 Groebner 基理论，解多项式方程组的算法，结式理论，局部环计算理论，模与同调的计算理论，多面体几何计算理论，在整数规划与组合数学中的应用，在代数编码理论中的应用等。

鉴于计算代数与应用已成为许多应用学科包括工程技术应用领域的重要工具，为适应广大应用领域工作者的需要，本书不要求读者具有专门的抽象代数几何理论知识，仅要求读者掌握微积分、线性代数和初步的代数学及多项式环知识。与此相应，在本书内容的安排上，为保持体系的完整性，对涉及到的一些抽象代数和代数几何有关知识作了简略的概述和介绍。此外，对于少数要利用到大量代数几何专门知识来论证的应用结果，我们仅叙述其证明的主要思想而略去详细证明，并指出了必要的参考书目。

本书的读者为数学、应用数学、理工科、工程技术领域的研究工作者和应用工作者，以及数学、应用数学、理工科高年级学生，研究生和教师。本书可作为教学、研究、应用参考书，也可作为数学系有关专业的研究生教材。

本书的写作出版得到我的同行、武汉大学管理学院教授景奉杰博士及武汉大学出版社的大力支持，在此谨对他们表示衷心的

感谢。由于作者水平所限，对书中的疏漏和不足之处，请读者不吝赐教。

目　录

第一章 Groebner 基理论

交换代数与代数几何是一门利用代数工具研究由多项式方程定义的几何对象的科学. 在它的发展历程中,既出现了作为学科的一般理论,也积累了大量的对于具体对象的详细考证. 近二十年来,随着计算机的出现,交换代数与代数几何的研究出现了重大的变化,即计算代数与应用技术达到新的发展阶段,在许多实际问题中展现出可喜的发展前景. 如几何设计,组合优化,整数规划,编码理论以及机器人学等应用领域,都可以看到计算代数与应用所发挥的作用. 本书的目的是阐述计算代数与应用的基本理论和算法. 为方便应用领域的工作者,也包含了一些基本代数工具的概述.

本章阐述计算代数与应用重要的基本算法之一——Groebner 基算法的理论与应用.

§1.1 多项式理想与环上的模

先回顾多项式环的一些术语. 设 $x_1, x_2, \cdots, x_n$ 是 n 个变元. 这 n 个变元的任一个乘积形式:

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

称为这 n 个变元集上的一个单项式,其中 $\alpha_i (i=1,2,\cdots,n)$ 是非负整数. 有时把单项式简记为 x^α,而 α 表示 n 维向量指数 $(\alpha_1, \alpha_2, \cdots, \alpha_n)$. $\alpha_1 + \alpha_2 + \cdots + \alpha_n$ 称为单项式 x^α 的全次数,记为 $|\alpha|$. 若 K 是一个域,我们可作系数在 K 中的单项式的有限线性组合,称为多项式,其一般形式为

$$f=\sum_{\alpha}c_{\alpha}x^{\alpha}$$

其中 $c_{\alpha}\in K$，$c_{\alpha}\neq 0$，$c_{\alpha}x^{\alpha}$ 称为 f 的项，f 有有限多项. 在很多具体问题中遇到的域 K 是有理数域 Q，实数域 R，复数域 C，或有限域 K. K 上所有多项式集合记为 $K[x_1,\cdots,x_n]$，其中的多项式可按显然方式相加和相乘，从而 $K[x_1,\cdots,x_n]$ 是一个有单位元的交换环. 由于其中只有非零常数有乘法逆，故它不是域，而有理函数集 $\{f/g\mid f,g\in[x_1,\cdots,x_n],g\neq 0\}$ 是一个域，记为 $K(x_1,\cdots,x_n)$.

如果一个多项式 f 的每项具有相同的全次数，称 f 为齐次多项式. 齐次多项式在一些问题中起着重要作用.

任给有限个多项式 $f_1,f_2,\cdots,f_s$，用任意其他多项式去乘它们并任意作和，这样得到的多项式集合在许多实际问题中有重要意义. 由此得到多项式理想的概念.

1.1.1 定义：设 $I\subseteq K[x_1,\cdots,x_n]$ 是一个非空子集，如果满足

(1) 对任意 $f\in I,g\in I$ 有 $f+g\in I$，

(2) 对任意 $f\in I,p\in K[x_1,\cdots,x_n]$，有 $pf\in I$，

则称 I 为一个多项式理想.

若任给有限个多项式 $f_1,\cdots,f_s$，作 $\langle f_1,\cdots,f_s\rangle=\{p_1f_1+\cdots+p_sf_s\mid p_i\in R[x_1,\cdots,x_n]\}$，则可直接验证 $\langle f_1,\cdots,f_s\rangle$ 满足定义(1.1.1)的条件，从而是一个多项式理想，称为由 $f_1,f_2,\cdots,f_s$ 生成的理想. $f_1,\cdots,f_s$ 称为生成元. 它是 $K[x_1,\cdots,x_n]$ 中包含 $f_1,\cdots,f_s$ 的最小理想.

在几何上有重要意义的一种理想是根理想.

1.1.2 定义：设 $I\subseteq K[x_1,\cdots,x_n]$ 是理想，令

$$\sqrt{I}=\{g\in K[x_1,\cdots,x_n]\mid g^m\in I\text{对某个 }m\geqslant 1\},$$

称 $\sqrt{I}$ 为 I 的根. 若 $\sqrt{I}=I$，称 I 为根理想.

易见 $\sqrt{I}\supseteq I$，但一般地 I 并不等于 $\sqrt{I}$.

例如，$I=\langle x^2+3xy,3xy+y^2\rangle$，由于 $(x+y)^3=x(x^2+3xy)+y(3xy+y^2)\in I$，故 $x+y\in\sqrt{I}$，但由于 I 的生成元是二次齐次

的，显见 $x+y\notin I$，故 $I\subsetneqq\sqrt{I}$.

关于多项式理想有以下经典结果，它们的详细证明可在任何一本交换代数教材中找到. 例如[1].

1.1.1 定理：(Hilbert 基定理)每个理想 $I\subseteqq K[x_1,\cdots,x_n]$ 有有限生成元集. 即对每个理想 I 存在有限多个多项式 $f_1,\cdots,f_s$，使 $I=\langle f_1,f_2,\cdots,f_s\rangle$.

1.1.2 定理：($K[x]$中除法算法)任给多项式 $f,g\in K[x]$，必存在多项式 q,r 使

$$f=qg+r,$$

其中 $r=0$ 或 r 的次数小于 g 的次数. $K[x]$是一元多项式环.

以下我们阐述环上的模的有关概念，这是在计算代数与应用中起重要作用的代数概念.

1.1.3 定义：设 R 是有单位元的交换环. 一个环 R 上的模(或称为 R 模)是一个集合 M，其上定义了加法运算和 R 对 M 的数乘运算，即对任意 $f,g\in M$ 有 $f+g\in M$，对任意 $a\in R,f\in M$ 有 $af\in M$，且满足以下性质：

(1)M 对加法成为 Abel 群；

(2)对任意 $a\in R,f,g\in M$ 有 $a(f+g)=af+ag$；

(3)对任意 $a,b\in R,f\in M$ 有 $(a+b)f=af+bf$；

(4)对任意 $a,b\in R,f\in M$ 有 $(ab)f=a(bf)$；

(5)对任意 $f\in M$，用 R 的单位元 1 去乘 f 仍得 f：$1f=f$.

实数上的 n 维向量空间 R^n 是最简单的实数环 R 上的模的例子. 含单位元的交换环 R 上任一理想 I 也是一个 R 模.

1.1.1 例：设 R 是含单位元的交换环. 由 R 中元素组成的 n 元列向量全体 R^n 按通常向量加法和 R 数乘成为一个 R 模. 若 A 是一个 R 上的 $m\times n$ 矩阵，对任意 $f\in R^n$，按通常矩阵乘法，有 $Af\in R^m$，令

$$\ker A=\{f\mid f\in R^n,Af=0\},$$

$$\mathrm{im}A=\{g\mid g\in R^m,g=Af\text{ 对某个 }f\in R^n\},$$

分别称之为 A 的核与 A 的象，它们都是 R-模，且分别是 R^n、R^m 的 R-子模.

若 M 是一个 R-模，任取 $f_1,\cdots,f_s\in M$，作 $\langle f_1,\cdots,f_s\rangle=\{a_1f_1+\cdots+a_sf_s\mid a_i\in R\}$，易验证它也作成一个 R-模，称为由 $f_1,\cdots,f_s$ 生成的 M 的 R-子模. $f_1,\cdots,f_s$ 称为生成元. 更一般地，设 F 是 R-模 M 的一个子集，作 $\langle F\rangle=\{a_1f_1+\cdots+a_nf_n\mid a_i\in R, f_i\in F, n\in Z^+\}$，则 $\langle F\rangle$ 是 M 的 R-子模，称为由 F 生成的子模. 若 $\langle F\rangle=M$，称 M 由 F 张成(或生成). 如果存在有限集 F 使 $\langle F\rangle=M$，称 M 为有限生成模.

设 M,N 是两个 R-模，作 $M\oplus N=\{(f,g)\mid f\in M,g\in N\}$，按二维向量的加法和数乘定义其上加与数乘运算，则 $M\oplus N$ 成为 R-模，称为 M 与 N 的直和. 由于 R 可作为自身模，易见 $R^n=R\oplus R\oplus\cdots\oplus R$. R^n 称为 R 上的自由模.

若 $N\subseteq M$ 都是 R-模，对每个 $f\in M$，记 $[f]=\{g\in M\mid g-f\in n\}$ 称为 f 的模 N 等价类. 全体等价类所成集合记为 M/N. 定义 $[f]+[g]=[f+g]$，$a[f]=[af]$，则 M/N 作成 R-模，称为 M 对 N 的商模. 商模的概念稍专业化，但非常重要.

1.1.4 定义：设 M,N 是两个 R-模，$\varphi:M\to N$ 是一个映射，若对任意 $a\in R, f,g\in M$ 有

$$\varphi(af+g)=a\varphi(f)+\varphi(g),$$

则称 φ 为一个 M 到 N 的 R-模同态.

此定义自然隐含着 $\varphi(f+g)=\varphi(f)+\varphi(g)$ 和 $\varphi(af)=a\varphi(f)$，对任意 $a\in R, f,g\in M$.

当 M,N 是自由模时，M 到 N 的模同态可表示为线性映射. 如果 $M=N=R$，则每个 R-模同态，$\varphi:R\to R$ 中必有 $\varphi(1)=f\in R$，从而对任何 $a\in R$，有

$$\varphi(a)=\varphi(a\cdot 1)=a\cdot\varphi(1)=af=fa,$$

即 φ 可由 R 中某个元素 f 的左乘来实现.

更一般地，$\varphi:R^m\to R^n$ 是模同态，当且仅当存在

$f_1, f_2, \cdots, f_m \in R^n$ 使 $\varphi((a_1, \cdots, a_m)^T) = a_1 f_1 + \cdots + a_m f_m$ 对任何 $(a_1, \cdots, a_m)^T \in R^m$ 成立. 事实上，设 $e_1, e_2, \cdots, e_m$ 是 R^m 的标准基，即 e_i 是 R^m 中第 i 个分量为 1 其余为 0 的向量，则必有 f_i 使 $\varphi(e_i) = f_i$. 由于 $(a_1, \cdots, a_m)^T$ 可惟一表示为 $a_1 e_1 + \cdots + a_m e_m$ 的形式，而 φ 为模同态，故必有 $\varphi((a_1, \cdots, a_m)^T) = a_1 \varphi(e_1) + \cdots + a_m \varphi(e_m) = a_1 f_1 + \cdots + a_m f_m$.

1.1.3 命题：设 $\varphi: R^m \to R^n$ 是 R-模同态，则存在 R 上的 $n \times m$ 矩阵 A 使得对一切 $f \in R^m$ 有 $\varphi(f) = Af$. 反之，任一个 $n \times m$ 矩阵 A 也可由 $\varphi(f) = Af$ 定义一个 R^m 到 R^n 的模同态 φ.

证：由前述已知 $\varphi: R^m \to R^n$ 的模同态可表为 $\varphi((a_1, \cdots, a_m)^T) = a_1 f_1 + \cdots + a_m f_m$，由于每个 f_j 又可惟一地由 R^n 的标准基 $\varepsilon_1, \cdots, \varepsilon_n$ 表示：$f_j = a_{1j}\varepsilon_1 + \cdots + a_{nj}\varepsilon_n$，记 $f = (a_1, \cdots, a_m)^T$，则 $\varphi(f) = (f_1, \cdots, f_m) = (\varepsilon_1, \cdots, \varepsilon_n) Af = Af$，其中 $A = (a_{ij})_{r \times m}$. 反之，$\varphi(f) = Af$ 定义了一个 R^m 到 R^n 的模同态是显见的结论. 证毕.

1.1.5 定义：设 $\varphi: M \to N$ 是 R-模同态，记

$$\ker(\varphi) = \{f \in M \mid \varphi(f) = 0\},$$

$$\mathrm{im}(\varphi) = \{g \in N \mid \text{存在 } f \in M \text{ 使 } \varphi(f) = g\},$$

分别称为模同态 φ 的核与象.

若模同态 φ 是一一对应，称 φ 为模同构，此时也称 M 与 N 同构，记为 $M \cong N$.

1.1.4 命题：设 $\varphi: M \to N$ 是模同态，则

(1) $\varphi(0) = 0$.

(2) $\ker(\varphi)$ 是 M 的子模.

(3) $\mathrm{im}(\varphi)$ 是 N 的子模.

(4) φ 是单射当且仅当 $\ker(\varphi) = \{0\}$，φ 是满射当且仅当 $\mathrm{im}(\varphi) = N$.

在 R 不是域的情形下引入线性组合和线性相关性的概念(例如 $R = K[x_1, \cdots, x_n]$)，模理论就真正开始不同于线性空间理论了. 借用线性代数的术语，我们称模 M 的子集 $F = \{f_1, \cdots, f_n\}$ 是

在 R 上线性无关的，如果任一线性组合 $a_1f_1+\cdots+a_nf_n=0$ 时必有 $a_1=\cdots=a_n=0$ 成立. 如果 $F\subseteq M$ 线性无关且生成 M，称 F 为 M 的一个基.

在线性代数中，每个域上的线性空间都有基，而模则未必.

1.1.2 例：令 $R=K[x,y,z]$，$M\subseteq R^3$，$M=\langle f_1,f_2,f_3\rangle$，其中

$$f_1=\begin{pmatrix}y\\-x\\0\end{pmatrix},f_2=\begin{pmatrix}z\\0\\-x\end{pmatrix},f_3=\begin{pmatrix}0\\z\\-y\end{pmatrix},$$

则 f_1,f_2,f_3 线性相关，因为 $zf_1-yf_2+xf_3=0$ 而 $z,-y,x\in R=K[x,y,z]$. 由于 f_1,f_2 的任何非 0 线性组合都得不到 f_3，故 f_1,f_2,f_3 中任何两个都不可能生成 M. 即 $\{f_1,f_2,f_3\}$ 是极小生成元集. 但由于它线性相关，因此不是 M 的基. 更进一步地，M 不可能有线性无关的生成元集，即 M 不存在基.

一般地，$R=K[x_1,\cdots,x_n]$ 的任一理想 M，如果它必须由不少于两个生成元生成，则 M 作为 R-模必定不存在基. 因为在 R 中，任何两个 f_1,f_2 必线性相关：$f_1f_2-f_2f_1=0$. 如果 $\{f_1,f_2\}$ 是 M 作为理想的基，它必定不是 M 作为 R-模的基.

1.1.5 命题：设 M 是 R-模，$F\subseteq M$. 则 F 是 M 作为模的基，当且仅当每个 $f\in M$ 可由 F 中元素惟一表出：$f=a_1f_1+\cdots+a_nf_n$. 此处 $a_i\in R,f_i\in F$.

证：F 生成 M 是显然的，只要证 F 的线性无关性，设 $a_1f_1+\cdots+a_nf_n=0$，由于 $0\in M$，故 0 只能有惟一表示方式 $0=0f_1+\cdots+0f_n$，即 $a_1=a_2=\cdots=a_n=0$. 证毕.

1.1.6 定义：设 M 是 R-模，如果 M 存在基（即线性无关生成元集），则称 M 为自由模.

前面给出过的 R^n 是自由模，因为标准基 $e_1,\cdots,e_n$ 是线性无关的. 只有一个生成元的模未必是自由模. 例如 R 为多项式环时取非零多项式 f，$M=R/\langle f\rangle$ 是 R-模，M 只有一个生成元 $[1]$，但它不是线性无关的，因为 $f\cdot[1]=[f]=0\in M$，而 $f\neq 0$.

决定一个 R^n 的子模是否为自由模是相当困难的. 下列定理是 1976 年由 Quillen 和 Suslin 给出的.

1.1.6 定理:(Quillen-Suslin)设 $R=K[x_1,\cdots,x_n]$, $a_1,\cdots,a_m\in R$ 且生成整个 R(即$\langle a_1,\cdots,a_m\rangle=R$),则线性方程 $a_1z_1+\cdots+a_mz_m=0$ 的解集合$(z_1,\cdots,z_m)^{\mathrm{T}}\subseteq R^m$, 作为 R-模是自由的.

Logar 和 Starmfels 在 1992 年给出了上述定理的算法证明. 1994 年 Park 和 Woodburn 给出了计算这个模的基的算法. 我们在后面将论及这一相当复杂的算法.

模未必有基,而且有些存在基的模也未必能找出它的基,这就引出了如何对一个模进行准确计算的问题. 我们不仅需要知道模的生成元集,还需要知道这些生成元之间的关系. 这种关系对于判断 M 中由生成元表示的两个元素是否相等是至关重要的. 例如,设 M 为一个 $Q[x,y]$模,$\{f_1,f_2,f_3\}$为 M 的生成元集,那么 $4f_1+5f_2+6f_3$ 与 $f_1+3f_2+4f_3$ 是否代表 M 中同一个元素? 只有知道了 $3f_1+2f_2+2f_3$ 在 M 中是否代表零元素,才能回答这个问题. 如果给出 f_1,f_2,f_3 之间的关系:

$$\begin{cases}3f_1+(1+x)f_2=0\\ f_1+(2x+3)f_2+4yf_3=0\\ (2-2x)f_2+4f_3=0\end{cases}$$

则容易直接计算出 $3f_1+2f_2+2f_3=0$ 在 M 中成立,从而 $4f_1+5f_2+6f_3$ 与 $f_1+3f_2+4f_3$ 在 M 中是同一个元素.

一般地,设 M 是一个 R-模,$f_1,f_2,\cdots,f_t\in M$,$F=(f_1,\cdots,f_t)$ 是 M 中 t 个元素组成的有序元素组. 若关于 f_i 的一个 R-线性组合等于 0:

$$a_1f_1+\cdots+a_tf_t=0\in M,$$

称此式为 F 上的一个关系,我们可以把这个关系看做由 R 中 t 个元素$(a_1,\cdots,a_t)$决定的. 这样,我们又可把 F 上一个关系等价地看

做 R^t 的一个元素 $(a_1,\cdots,a_t)$. 这种关系称为 Syzygies，这个词来源于希腊文，意为“约束”.

1.1.7 命题：设 $(f_1,\cdots,f_t)$ 是 R-模 M 的有序 t 元素组，所有使 $a_1f_1+\cdots+a_tf_t=0$ 成立的 $(a_1,\cdots,a_t)^{\mathrm{T}}\in R^t$ 组成一个 R^t 的 R-子模，称为 $(f_1,\cdots,f_t)$ 的第一约束模，记为 $Syz(f_1,\cdots,f_t)$.

证：设 $(a_1,\cdots,a_t)^{\mathrm{T}},(b_1,\cdots,b_t)^{\mathrm{T}}\in Syz(f_1,\cdots,f_t),c\in R$，则

$$a_1f_1+\cdots+a_tf_t=0,$$

$$b_1f_1+\cdots+b_tf_t=0,$$

从而得到，$(ca_1+b_1)f^1+\cdots+(ca_t+b_t)^t=0$，这表示 $(ca_1+b_1,\cdots,ca_t+b_t)\in Syz(f_1,\cdots,f_t)$，即 $Syz(f^1,\cdots,f^t)$ 是 R^t 的子模. 证毕.

这一命题告诉我们如何去描述和决定一个模的生成元集上的关系. 当 R 为 Noether 环时，它的每个理想是有限生成的 ($K[x_1,\cdots,x_n]$ 是 Noether 环)，从而 R^t 的每个子模有限生成. 如果我们能决定一个模 M 的生成元集的第一约束模的(有限)生成元，我们就在某种程度上把握了 M 的生成元集上的关系. 既然 R^t 中元素是 t 元列向量，那么有限多个约束关系就作成一个矩阵. 设 M 是 R-模且由 $f_1,\cdots,f_t$ 生成，$Syz(f_1,\cdots,f_t)$ 是 R^t 的子模，它的有限生成元集组成矩阵 A，称为 M 的表示矩阵. 也称 A 为模 M 的表示. A 的行数等于 M 的生成元个数，A 的列数等于 $Syz(f_1,\cdots,f_t)$ 的生成元个数.

1.1.8 命题：设 A 为 R 上的 $m\times n$ 矩阵，且是两个不同的 R-模 M,N 的表示矩阵，则

(1) M 与 N 是同构 R-模.

(2) M 与 N 都同构于商模 R^m/AR^n.

证：(1)由于 A 是 M 的表示，存在 M 中元素 $f_1,\cdots,f_m$ 使 A 的列生成 $Syz(f_1,\cdots,f_m)$，同样存在 N 中元素 $g_1,\cdots,g_m$ 使 A 的列生成 $Syz(g_1,\cdots,g_m)$. 作映射 $\varphi:M\to N$ 使 $\varphi(f_i)=g_i,i=1,\cdots,m$，并线性地扩充到整个 M. φ 显然是满的. 若 $\varphi(a_1f_1+\cdots+a_mf_m)=$

$\varphi(b_1g_1+\cdots+b_mg_m)$，则 $a_1g_1+\cdots+a_mg_m=b_1g_1+\cdots+b_mg_m$，从而 $(a_1-b_1)g_1+\cdots+(a_m-b_m)g_m=0$，这样 $(a_1-b_1,\cdots,a_m-b_m)^T\in Syz(g_1,\cdots,g_m)$，故 $(a_1-b_1,\cdots,a_m-b_m)^T\in Syz(f_1,\cdots,f_m)$，得到 $a_1f_1+\cdots+a_mf_m=b_1f_1+\cdots+b_mf_m$. 这证明了 φ 是单的. 由 φ 的作法显见它是模同态. 故 φ 是同构.

(2)由于 AR^n 是 R^m 的由 A 的列生成的子模，故商模 R^m/AR^m 由 $e_1+AR^n,e_2+AR^n,\cdots,e_m+AR^n$ 生成，此处 $e_1,\cdots,e_m$ 是 R^m 的标准基. 由于 $(c_1,\cdots,c_m)^T\in Syz(e_1+AR^n,\cdots,e_m+AR^n)$ 当且仅当 $(c_1,\cdots,c_m)^T\in AR^n$，而这又等价于 $(c_1,\cdots,c_m)^T$ 是 A 的列的线性组合，这就是说 A 是 R-模 R^m/AR^n 的表示. 由(1)即得 M 与 N 皆同构于 R^m/AR^n. 证毕.

一个 R-模 M 的表示矩阵并不是惟一的. 它取决于所选择的 M 的生成元集以及生成元集上的第一约束模的生成元. 重要的是，一旦有了一个表示矩阵，我们就有了 M 的一个具体的生成元集和关系，从而可具体地刻画 M. 例如，可刻画从 M 到自由模的同态.

1.1.9 命题：设 A 是一个 $m\times n$ 矩阵，且是 R-模 M 的表示. 则任何 R-模同态 $\varphi:M\to R^t$ 可由一个 $t\times m$ 矩阵 B 表示，B 满足 $BA=0$. 反之，若 B 是一个满足 $BA=0$ 的元素在 R 中的 $t\times m$ 矩阵，则 B 可定义一个 R-模同态 $\varphi:M\to R^t$.

证：由于 A 是 M 的表示，故 M 有 m 个生成元 $f_1,\cdots,f_m$，从而 φ 由 $\varphi(f_1),\cdots,\varphi(f_m)$ 决定. 它给出一个以 $\varphi(f_1),\cdots,\varphi(f_m)$ 为各列的 $t\times m$ 矩阵 B. φ 对元素 $a_1f_1+\cdots+a_mf_m$ 的作用相当于 B 左乘 $(a_1,\cdots,a_m)^T$，对 A 的任一列 $(c_1,\cdots,c_m)^T$ 有 $c_1f_1+\cdots+c_mf_m=0$，故 $B(c_1,\cdots,c_m)^T=\varphi(c_1f_1+\cdots+c_mf_m)=\varphi(0)=0$，从而 $BA=0$.

反之，若 A 是 R-模 M 对于生成元集 $\{f_1,\cdots,f_m\}$ 的表示矩阵，B 是 $t\times m$ 矩阵使 $BA=0$，则由 $B(c_1,\cdots,c_m)^T$ 定义 $\varphi(c_1f_1+\cdots+c_mf_m)$. 若 $a_1f_1+\cdots+a_mf_m=b_1f_1+\cdots+b_mf_m$，则 $(a_1-b_1)f_1+\cdots+(a_m-b_m)f_m=0$，即 $(a_1-b_1,\cdots,a_m-b_m)^T$ 是 A 的列的线性组合，从

而 $B(a_1-b_1,\cdots,a_m-b_m)^{\mathrm{T}}=0$，得 $B(a_1,\cdots,a_m)^{\mathrm{T}}=B(b_1,\cdots,b_m)^{\mathrm{T}}$，即 $\varphi(a_1f_1+\cdots+a_mf_m)=\varphi(b_1f_1+\cdots+b_mf_m)$. 这证明 φ 是有定义的映射. 显然 φ 是模同态. 证毕.

关于模的较一般的初步理论，读者可参阅文献[2].

§1.2 单项式序，多项式约化与 Groebner 基

在 $K[x_1,\cdots,x_n]$ 中，已给一个理想 $I=\langle f_1,\cdots,f_s\rangle$，决定某个 f 是否属于 I，以及另一个理想 $J=\langle g_1,\cdots,g_t\rangle$ 是否等于 I，一般来说并不容易. 现在我们给出确定这类情形的一般方法. 首先给出单项式序概念.

1.2.1 定义：$K[x_1,\cdots,x_n]$ 上的一个单项式序是一个单项式集合上的序关系“$>$”，且满足：

(1) “$>$”是一个全序关系，即对任意单项式 x^α, x^β 必有 $x^\alpha>x^\beta$ 或 $x^\beta>x^\alpha$.

(2) “$>$”与单项式乘积相容，即当 $x^\alpha>x^\beta$ 时，对任意单项式 x^γ 有 $x^\alpha x^\gamma>x^\beta x^\gamma$.

(3) “$>$”是一个良序，即每个非空的单项式集合中必有“$>$”关系下的最小元素.

单项式序定义的意义在于：条件(1)使我们能把任一多项式 f 的各项按序的大小惟一排列；条件(2)保证这种排列不因为用另一个单项式 x^γ 去乘 f 而改变；条件(3)则使我们处理单项式集合的有关问题时能在有限步内结束.

在一元多项式环 $K[x]$ 的除法算法中，我们实际上隐含着使用了其中的单项式序：我们总是比较 f 和 g 的首项次数. 事实上，很容易验证，一元多项式环 $K[x]$ 上只有惟一一种单项式序，即分次序：

$$\cdots>x^{n+1}>x^n>\cdots>x^2>x>1.$$

对于多元多项式环 $K[x_1,\cdots,x_m]$，却有许多单项式序可供选择. 我