Advances in Education 教育进展, 2025, 15(9), 856-860
Published Online September 2025 in Hans. https://www.hanspub.org/journal/ae
https://doi.org/10.12677/ae.2025.1591748

Hans汉斯

Gröbner基在近世代数教学中的应用

古丽沙旦木·玉奴斯

新疆大学数学与系统科学学院，新疆 乌鲁木齐

收稿日期：2025年8月3日；录用日期：2025年9月4日；发布日期：2025年9月12日

摘　要

近世代数是数学专业本科生和研究生的一门基础核心课程。因为此课程内容较抽象，解决问题的思维方式与学生之前学过其他课程不太一样，并且教材里所讨论的问题的处理方法以证明为主，计算性的问题较少，因此很多学生觉得学好此课程比较吃力。据我所知，在很多教材里对一些问题没有提供具体解决方法，比如域论中的极小多项式的计算，判断有限代数扩张是否是单扩张，并且在肯定的情况下计算出扩张本原元等。在本文中，我基于近年来为本科生和研究生讲授近世代数课程时，介绍使用Gröbner基方法解决上述问题的教学实践，分享一些相关的教学认识。

关键词

Gröbnerr基，极小多项式，域扩张，教学效果

The Application of Gröbner Bases in Modern Algebra Teaching

Gulshadam Yunus

College of Mathematics and Systems Science, Xinjiang University, Urumqi Xinjiang

Received: Aug. 3rd, 2025; accepted: Sep. 4th, 2025; published: Sep. 12th, 2025

Abstract

Modern Algebra is one of the foundational core courses for both undergraduate and graduate students in mathematics. Due to its highly abstract nature, the problem-solving approach in modern algebra is distinct from those in other courses students have previously studied. Standard textbooks predominantly focus on theoretical proofs, with limited computational examples. Consequently, many students find mastering the subject a real uphill battle; most textbooks, as far as I know, simply stop short of telling them how to actually compute a minimal polynomial in field theory, how to decide whether a finite algebraic extension is simple, or, if it is, how to exhale a primitive element.

文章引用: 古丽沙旦木·玉奴斯. Gröbner 基在近世代数教学中的应用[J]. 教育进展, 2025, 15(9): 856-860.
DOI: 10.12677/ae.2025.1591748

In this note I draw on my recent experience of teaching both undergraduate and graduate courses in Modern Algebra to describe classroom trials that use Gröbner basis techniques to settle these very questions, and I share the pedagogical lessons that have emerged.

Keywords

Gröbner Basis, Minimal Polynomial, Field Extension, Teaching Effectiveness

1. 前言

大家知道近世代数是大学数学系的本科生和研究生的专业基础课之一。因为近世代数是通过对学生之前学过的各种数学运算进行高度抽象化来提出自己的课程内容，并且解决问题的思维方式也比学生之前学过的课程抽象一些，因此对学生来说是学习比较困难的一门课程。域理论是近世代数的核心内容之一，其中计算元素的极小多项式，判断有限代数扩张是否是单扩张，并且在答案是肯定的情况下如何算出扩张本原元等是域论里的基本问题。遗憾的是很多教科书里对这些问题没有提供明确的方法，极少数教材里介绍了一些方法，但是用的是数学归纳法，因此当添加元素个数较多时计算较麻烦。交换代数的Gröbner 基理论可以提供解决我上面提到的几个问题的操作性很强的方法，另一方面，Gröbner 基理论是Buchberger (见[1])为了解决多项式代数中的約化问题而提出的，确切地说是高等代数中的欧几里得综合除法的推广，因此对学生来说掌握并不困难。在十几年以来从事近世代数的教学工作中给学生介绍使用Gröbner 基方法来回答上面的几个问题，我觉得效果还是很好的。我的教学经验是，如果课时较宽裕的话给学生适当地介绍一些 Gröbner 基的内容，然后介绍用此方法解决以上提到的问题是更好的。如果课时较紧张，那么直接采用 Gröbner 基方法解决以上问题的方法也可以。如果学生感兴趣的话，可以建议他们参阅相关文献。

2. 用 Gröbner 基方法计算极小多项式及本原元

2.1. Gröbner 基

设 k 是一个域，$X=\{x_1,\cdots,x_n\}$ 是一个有序集，其中 $x_1>\cdots>x_n$。我们用 X^* 表示由 X 生成的可交换单项式的幺半群。我们在 X^* 上选取序 $>$，使得对任意 $a,b,c\in X^*$，如果 $a>b$，则有 $ac>bc$。对任意 $f\in k[x_1,\cdots,x_n]$，我们用 $\overline{f}$ 表示多项式 f 关于序 $>$ 的首项。

对任意 $f,g\in k[x_1,\cdots,x_n]$，如果 $(\overline{f},\overline{g})\neq 1$，则我们定义 f 和 g 之间的合成 $(f,g)_w$ 如下：

$$(f,g)_w=af-bg,$$

其中 $a\overline{f}=b\overline{g}=w=[\overline{f},\overline{g}]$ 是 $\overline{f}$ 和 $\overline{g}$ 的最小公倍式，且 $a,b\in X^*$。

设 G 是 $k[x_1,\cdots,x_n]$ 的由一些首项系数为 1 的多项式组成的非空子集，对于 $f,g\in k[x_1,\cdots,x_n]$，如果存在 $s_1,\cdots,s_m\in G$ 和 $a_1,\cdots,a_m\in X^*$ 使得

$$(f,g)_w=\alpha_1a_1s_1+\cdots+\alpha_ma_ms_m,$$

其中 $\alpha_1,\cdots,\alpha_m\in k$，并且对每一个 $i\in\{1,\cdots,m\}$，a_is_i 的首项小于 w，则我们说合成 $(f,g)_w$ 模 (G,w) 平凡，

并且记为$(f,g)_w \equiv 0 \bmod (G,w)$。

设 J 是 $k[x_1,\cdots,x_n]$ 中由 G 生成的理想。如果对任意 $f,g \in G$，当 $(f,g)_w$ 存在时，均有 $(f,g)_w \equiv 0 \bmod (G,w)$，则称 G 为理想 J 在 $k[x_1,\cdots,x_n]$ 中的一个 Gröbner 基。如果对于 Gröbner 基 G 中的任意 f,g 不存在 $a \in X^*$ 使得 $\overline{f} = a\overline{g}$ 或者 $\overline{g} = a\overline{f}$，则我们把 G 称为约化 Gröbner 基。

给定理想 J 的一个生成集 G，我们通过把所有的非平凡的合成添加到 G 得到更大的生成集 G^c 使得 G^c 是 J 的一个 Gröbner 基。此过程称为 Buchberger 算法。具体计算方法如下：

首先要看合成 $(f,g)_w$ 的首项 $\overline{(f,g)_w}$ 是否被 G 中的某一个多项式 $h \in G$ 的首项 $\overline{h}$ 整除，即 $\overline{(f,g)_w} = a\overline{h}$，$a \in X^*$。如果是，那么把 $a\overline{h}$ 带入到 $(f,g)_w$ 的表达式中。重复此过程(称为约化)。最终如果得到零，那么合成 $(f,g)_w$ 对于模 (G_1,w) 平凡，因此我们考虑另外一个合成。如果最终得到的多项式的首项不能被 G_1 中的任何多项式的首项整除，那么我们把此多项式(称为不可约多项式)的首项系数化为 1 后添加到 G_1 中去，这里的 G_1 是前几步的约化中得到的所有不可约多项式添加到 G 而得到的多项式集合。

消元序是为多项式环 $k[x_1,\cdots,x_n,y_1,\cdots,y_m]$ (或更一般地，$k[X,Y]$)中单项式排序的一种规则。其核心特性是：若一个非零多项式 f 的首项(关于该序)仅由目标变量组 $Y = y_1,\cdots,y_m$ 中的变量构成，则 f 本身也必定仅含 Y 变量(即 $f \in k[Y]$)。

消元定理：设 J 是 $k[X,Y]$ 上的理想，若 G 是 J 关于某个消元序的 Gröbner 基，则对于任意 $t(0 \le t \le n)$，集合 $G_t = G \cap k[x_{t+1},\cdots,x_n,Y]$ 恰好是消元理想 $J_t = J \cap k[x_{t+1},\cdots,x_n,Y]$ 的 Gröbner 基。特别地，当消去全部 X 变量时，$G_Y = G \cap k[Y]$ 生成 $J \cap k[Y]$，即 $\langle G_Y \rangle = J \cap k[Y]$。

消元定理揭示了 Gröbner 基计算与代数消元的内在联系。字典序是消元序的典型例子，字典序的规则为变量赋予了一种严格的层级关系：任何包含高阶变量的项，其优先级都绝对高于所有不包含该变量的项。Gröbner 理论的核心在于对首项的分析，因为首项决定了多项式在除法运算中的行为。当采用字典序计算 Gröbner 基时，计算过程会自然生成一些多项式，它们的首项被约束在低维变量空间(即仅含低阶变量的子环)中，最终所得的 Gröbner 基 G 呈现出清晰的分层结构，此时只需提取其中属于目标低维子环的多项式，即可完整描述消元后的系统。这一方法将原本依赖技巧的消元问题，转化为一种可机械化执行的标准化计算任务——即 Gröbner 基的计算。

2.2. 应用

域论，特别是域的扩张，是近世代数课程的重要内容之一。因为单代数扩张的本原元的极小多项式的次数刚好是此域扩张的扩张次数，因此计算本原元的极小多项式在域论里很重要。

在很多近世代数教材里(见[2]-[4])没有介绍计算极小多项式的方法，或者介绍的方法当本原元的形式较复杂时很繁琐。此外，由于域的单扩张是最简单的扩张，因此有时我们需要解决以下问题：设 $K = k(\alpha_1,\cdots,\alpha_n)$ 是 k 的一个代数扩张，那么我们计算极小多项式的元素 $\beta \in k(\alpha_1,\cdots,\alpha_n)$ 能否满足 $k(\alpha_1,\cdots,\alpha_n) = k(\beta)$？我们上面介绍的 Gröbner 基同时回答这些问题。

设 $K = k(\alpha_1,\cdots,\alpha_n)$ 是域 k 的一个代数扩张。对每一个 $i = 1,\cdots,n$，设 $p_i(x) \in k(\alpha_1,\cdots,\alpha_{i-1})[x_i]$ 是 α_i 在 $k(\alpha_1,\cdots,\alpha_{i-1})$ 上的极小多项式。我们设

$$\beta = \frac{f(\alpha_1,\cdots,\alpha_n)}{g(\alpha_1,\cdots,\alpha_n)} \in k(\alpha_1,\cdots,\alpha_n),$$

其中 $f,g \in k[x_1,\cdots,x_n]$。我们考虑 $k[x_1,\cdots,x_n,y]$ 的理想

$$J = \langle p_1(x_1),\cdots,p_n(x_n), gy - f \rangle.$$

这时理想 J 的约化 Gröbner 基 G 中不包含 $x_1,\cdots,x_n$ 的首项系数为 1 的多项式就是 β 在 k 上的极小多

项式，并且 $k(\beta)=k(\alpha_1,\cdots,\alpha_n)$ 当且仅当存在多项式 $g_1,\cdots,g_n\in G$ 使得 $g_i=x_i-h_i(1\le i\le n)$，其中 $h_i\in k[y](1\le i\le n)$。进一步地有 $\alpha_i=h_i(\beta)$。

Gröbner 基的存在性与算法终止性证明可参见经典文献(详见[5])，本文重点讨论其在教学中的具体应用。

下面我们通过几个例子来介绍具体求法。

例题 1 讨论域扩张 $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$。因为 $\sqrt{2}$ 在 $\mathbb{Q}$ 上的极小多项式为 $x_1^2-2\in\mathbb{Q}[x_1]$，$\sqrt[3]{5}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的极小多项式为 $x_2^3-5\in\mathbb{Q}(\sqrt{2})[x_2]$。设 $X=\{x_1,x_2,y\}$，我们取序 $x_1>x_2>y$，则此序在 X^* 上诱导出字典排序，我们仍用 $>$ 来表示字典排序。通过计算我们得到理想 $J=\langle x_1^2-2,x_2^3-5,y-(x_1+x_2)\rangle$ 关于序 $>$ 的约化 Gröbner 基为

$$\begin{aligned}G=\Big\{&x_1^2-2,x_2^3-5,x_1+x_2-y,y^6-6y^4-10y^3+12y^2-60y+17,\\&x_1-\frac{48}{1187}y^5-\frac{45}{1187}y^4+\frac{320}{1187}y^3+\frac{780}{1187}y^2-\frac{735}{1187}y+\frac{1820}{1187},\\&x_2+\frac{48}{1187}y^5+\frac{45}{1187}y^4-\frac{320}{1187}y^3-\frac{780}{1187}y^2-\frac{452}{1187}y-\frac{1820}{1187}\Big\}.\end{aligned}$$

所以 $\sqrt{2}+\sqrt[3]{5}$ 的极小多项式为 $y^6-6y^4-10y^3+12y^2-60y+17$，并且 $\mathbb{Q}(\sqrt{2}+\sqrt[3]{5})=\mathbb{Q}(\sqrt{2},\sqrt[3]{5})$。

例题 2 讨论域扩张 $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[4]{2},i)$。因为 $\sqrt[4]{2}$ 在 $\mathbb{Q}$ 上的极小多项式为 $x_1^4-2\in\mathbb{Q}[x_1]$，$i$ 在 $\mathbb{Q}(\sqrt[4]{2})$ 上的极小多项式为 $x_2^2+1\in\mathbb{Q}(\sqrt[4]{2})[x_2]$。设 $\beta=1+\frac{i}{\sqrt[4]{2}}$，通过计算我们得到理想 $J=\langle x_1^4-2,x_2^2+1,x_1y-(x_1+x_2)\rangle$ 关于序 $x_1>x_2>y$ 的约化 Gröbner 基为

$$G=\left\{x_1-2y^3x_2+6y^2x_2-6yx_2+2x_2,x_2^2+1,y^4-4y^3+6y^2-4y+\frac{1}{2}\right\}.$$

所以 $\beta=1+\frac{i}{\sqrt[4]{2}}$ 的极小多项式为 $y^4-4y^3+6y^2-4y+\frac{1}{2}$。尽管元素 $\beta=1+\frac{i}{\sqrt[4]{2}}$ 在 $\mathbb{Q}$ 上的极小多项式是 4 次多项式，但由它生成的域 $\mathbb{Q}(\beta)$ 实际上等于整个扩域 $\mathbb{Q}(\sqrt[4]{2},i)$。因此，$\beta$ 是扩域 $\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q}$ 的一个本原元。

2.3. 教学效果

为了更好地理解 Gröbner 基方法在近世代数教学中的应用效果，我们进行了一项对比实验。研究选取了 20 名前期成绩无显著差异的数学专业本科生，并分为实验组(采用 Gröbner 基教学法)和对照组(传统教学法)。研究发现，在解决域论中的极小多项式计算，单扩张判定和本原元构造等问题上，实验组表现出显著优势。这种优势主要体现在三个方面：

第一，算法化流程降低了抽象问题的求解难度。Gröbner 基方法将依赖技巧性构造的抽象域论问题(如求极小多项式)，转化为可机械执行的 Buchberger 算法步骤。这使得解题过程变得清晰，可操作，调研数据显示，采用此方法后，相关计算题的正确率至少提升 2 倍。

第二，计算工具增强了几何直观理解。借助 Maple 等计算机代数系统，学生能够可视化代数簇等概念。实验组学生反馈表明，这种可视化功能帮助他们深刻理解了本原元等核心概念的几何意义，这是传统纯符号推导教学难以达到的效果。

第三，统一的理论框架促进了知识迁移。该方法自然地构建了域论与代数几何之间的知识桥梁，为学生提供了一个更强大的统一视角。正因如此，多达三分之二的实验组学生能够将所学方法成功迁移至

课堂上未讲授的有限域构造问题，展现了良好的知识拓展能力。

相比之下，对照组学生在传统教学中遇到了明显困难。大部分学生无法独立完成像本原元存在性这样的构造性证明，反映出他们难以理解证明背后的动机和技巧。

综上所述，Gröbner 基方法不仅提升了学生的解题效率和正确率，更通过其算法化，可视化和理论统一性的特点，深化了学生对近世代数核心思想的理解，并培养了他们的知识迁移能力。

基金项目

国家自然科学基金地区基金项目(12061068)。

参考文献

[1] Buchberger, B. (1965) An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Ideal. Ph.D. Thesis, University of Innsbruck.

[2] 熊全淹. 近世代数[M]. 武汉: 武汉大学出版社, 1991.

[3] 冯克勤, 李尚志, 章璞. 近世代数引论[M]. 合肥: 中国科学技术大学出版社, 2013.

[4] 张禾瑞. 近世代数基础[M]. 北京: 高等教育出版社, 2001.

[5] Adams, W. and Loustaunau, P. (1994) An Introduction to Gröbner Bases. American Mathematical Society.