高等代数教程

蓝以中 编

北京大学出版社

高等代数教程

蓝以中 编

北京大学出版社

内 容 提 要

本书是《线性代数引论》一书的续篇，两书合在一起可作为大学数学系高等代数课的教材。本书除包含通常高等代数教材的共同内容（一元与多元多项式，矩阵的Jordan标准形，群、环、域的基本概念）外，又根据现代数学发展对专业数学工作者代数学基本训练所提出的要求，拓广了书的深度和广度。编者以其多年的教学经验为基础，参考了国外优秀教材，由浅入深地介绍了形式幂级数，矩阵函数，p-adic 数域，线性结合代数，多线性代数与外代数，n维仿射空间与射影空间，仿射、射影代数曲线等在近代数学中起重要作用的概念。书中包含了不少富有启发性的例题和习题。本书还有部分内容可供学生课外阅读和钻研。

高等代数教程

蓝以中　编

责任编辑　徐信之

*

北京大学出版社出版

（北京大学校内）

北大印刷厂印刷

新华书店北京发行所发行　各地新华书店经售

*

850×1168毫米　32开本　8.375印张　200千字

1988年11月第一版　　1988年11月第一次印刷

印数：00001—5000册

ISBN 7-301-00347-1/O·062

定价2.05元

前　言

本书是以编者几年来在北京大学数学系讲授高等代数课程的教学实践经验为基础写成的。其目的是使它和我以前编写的“线性代数引论”一书（北京大学出版社1981年 8 月出版）合并成综合性大学数学系高等代数课程的一套完整教材。

当前，代数学的影响不但已经遍及数学各个领域，而且深入到自然科学、技术科学的许多方面，因而，加强综合大学数学系学生代数学基本理论和基本方法的训练的问题，正日益受到人们的重视。高等代数课程是代数学的入门课，它所面对的是刚刚步入数学科学领域的青年，因而，必须针对初学者的特点，由浅入深，由具体而抽象，以尽可能自然和尽可能直观的方式，来引进代数学中的一系列抽象的概念和一套处理问题的方法，使学生能洞察问题的本质，不致被众多的概念、定理、命题所压倒。这是编者在教学中和写作“线性代数引论”一书及本书时所遵循的一个总的指导思想。

本书前面三章是在“线性代数引论”一书的基础上，继续引入代数学的一些基本概念。第一、二两章是多项式的理论。多项式作为函数，学生在数学分析中就已经熟知了，而在这里，则是从代数的观点，把它们作为环这一抽象代数系统的特例来阐述的。线性代数中所研究的线性空间和本书前面两章所讨论的多项式是两类最为初等、较为直观和具体的代数系统，在学生具备了这方面的知识之后，第三章从理论上作了一个总的概括，上升到一般，引进了一般的代数系统——群、环、体、域的基本概念。在这里，学生开始接触到现代代数学的主要研究对象，并初步领会了它的基本方法。这样，本课程就完成了将学生领进代数学的大

门的任务，为他们今后的发展打下了基础。本书的后面三章，则是回过头去讨论线性代数的一些较深入的课题：线性变换与矩阵的若当标准形，矩阵函数，高维的仿射空间和射影空间，线性空间的张量积和外代数。这是在学生具备了代数学的基础训练之后，在理论上提出了深一步的要求，学习并掌握这部分内容，无疑将使学生得到进一步的锻炼，使他们更加熟悉代数学的研究对象及其特点。

近几十年来，代数学的发展是十分迅速的。现在的代数学和三十年代、四十年代相比，已经面目全非。这种状况，在高等代数课程中也应得到反映，拘守几十年前教材的老框框，显然已经不能适应现代科学的要求。使高等代数教材现代化是一个刻不容缓的任务。本书在这方面作了较多的努力。这就是在书中尽可能地吸收了一些反映近代代数学的新思想的重要材料，例如，在本书中介绍了在代数学中起着重要作用的中国剩余定理；介绍了域的赋值的概念（有理数域，有理函数域，形式幂级数域的赋值），并在这个基础上，作为环的理论的一个重要应用，引进了 p-adic 数域这一新的数系的基本概念；鉴于代数几何在现代数学中所处的重要地位，本书加强了多元多项式的理论，并在第五章介绍了代数几何的两类基本研究对象——仿射代数集和射影代数集，利用结式理论证明了仿射代数曲线交点的贝朱定理，等等。介绍这些概念和定理有两方面的目的，一是扩大学生的眼界，启发他们的思路，例如，p-adic 赋值和 p-adic 数域的引进，可以使学生看到，除了通常熟知的数的绝对值概念和实数、复数体系之外，还有着另一个大不相同的新天地；二是培养学生利用所学知识处理问题的能力。由于在论述这些较深的材料时，所运用的工具仅仅是高等代数中所讲授过的知识，这就为学生提供了许多处理问题的方法和技巧。例如第三章§6介绍的实数域上有限维可除代数的弗洛宾尼乌斯定理的证明，就是一个运用线性代数知识处理问题的优秀范例。相信这样做，比起单纯讲授某些难题的解题技

巧来，会有较好的效果.

本书的体例和“线性代数引论”一书大致相同。由于本书的对象是数学系的学生，而且他们已经学过线性代数的理论，有了一定的数学训练，所以书中有些地方写的较为简略，这就要求读者在阅读时，要动脑筋思考，自己动手作一些简单的推理。这样做，对于理解书中的内容，培养自学的能力是十分必要的。本书的一部分内容，对于低年级学生，相对地是比较深的，因此，并没有必要将全部材料都在课堂上讲授。当采用本书作教材时，教师可选择书中的大部分材料讲授，而将其它材料留给程度较高的学生自行阅读，或留到后继课程使用时再回头讲授（例如第六章张量积与外代数）。

石生明教授仔细地审阅了全书，提出了许多宝贵的意见。编者在此向他表示感谢.最后，诚恳地希望读者对本书的不当之处提出批评指正。

编　者

1985.11.于北京大学

目　录

第一章　一元多项式

本章的主要内容包括：一元多项式的因式分解理论，实系数多项式根的分布，单变量有理函数域，最后介绍单变量形式幂级数的基本概念。这些内容在代数学中都具有基本的意义。在学习一元多项式的因式分解理论时，读者将会发现它们和整数的因式分解理论极其相似，而在一元多项式基础上产生出来的单变量有理函数域，又和在整数基础上产生出来的有理数域极其相似，这表明它们在本质上有许多共同之处。在本书的第三章中，我们将从更高的观点上揭示出它们在本质上的相同点。因此，学好本章的内容，也就为学习后面章节的内容打好了基础。

§1　一元多项式的因式分解

读者在数学分析课程中已经熟知实系数一元多项式的概念和许多基本性质．但我们这里所要讨论的一元多项式，其概念的内涵更为广泛，所讨论的主要课题也跟数学分析大不相同（虽然在许多地方又有密切的联系），所以读者应当把数学分析中已接受的实系数一元多项式的概念暂时抛开。下面，我们就先来给出一元多项式的一般定义。

一元多项式的定义及运算

定义　设K是一个数域，x是一个不定元（或称文字），以K中的元素为系数的形式表达式

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n \qquad (a_i\in K)$$

称为数域K上的一个一元多项式。

以x为不定元的数域K上的全体一元多项式组成一个集合，

记之为 $K[x]$。$a_0, a_1, \cdots, a_n$ 称为 $f(x)$ 的系数。在 $f(x)$ 的形式表达式中出现的 $x, x^2, \cdots, x^n$ 等等只是用来表示系数的排列次序（或位置），现在它们还不具有方幂的含意。因此，$f(x)$ 实际上也可以写成 $(a_0, a_1, a_2, \cdots, a_n)$。但是，等于零的系数今后我们将不写出，因而使用定义中的记号（即借助于不定元 x）较为方便。例如，我们有

$$0 + 1x + (-3)x^2 + 0x^3 = x + (-3)x^2.$$

根据上面的约定，我们也可以把 $f(x)$ 写成无穷多项连加的形式：

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n + a_{n+1}x^{n+1} + \cdots = \sum_{i=0}^{+\infty} a_i x^i,$$

而令 $a_{n+1} = \cdots = 0$，即上式中只有有限多个系数不为零。

下面，我们在 $K[x]$ 内定义加法和乘法运算。

一、加法

设 $f(x), g(x) \in K[x]$。如果 $f(x) = \sum_{i=0}^{+\infty} a_i x^i$，$g(x) = \sum_{i=0}^{+\infty} b_i x^i$（这里当然假定 a_i, b_i 中只有有限多项不为零），则定义

$$f(x) + g(x) = \sum_{i=0}^{+\infty} (a_i + b_i) x^i.$$

显然，$f(x) + g(x) \in K[x]$，称它为 $f(x)$ 与 $g(x)$ 的和。

容易验证，上面定义的加法运算具有下列基本性质：

1）满足结合律：$(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$；

2）存在一个多项式 $0(x) = 0 + 0x + 0x^2 + \cdots$，使对所有 $f(x) \in K[x]$，都有 $f(x) + 0(x) = f(x)$。$0(x)$ 将称为零多项式，并简单地记为 0；

3）任给 $f(x) = \sum_{i=0}^{+\infty} a_i x^i \in K[x]$，令 $\bar{g}(x) = \sum_{i=0}^{+\infty} (-a_i) x^i$，

则 $f(x)+g(x)=0(x)=0$。下面将 $g(x)$ 记为 $-f(x)$；

4）满足交换律：$f(x)+g(x)=g(x)+f(x)$（$\forall f(x), g(x) \in K[x]$）。

今后，把 $f(x)+(-g(x))$ 记为 $f(x)-g(x)$，并称它为 $K[x]$ 内的**减法运算**。显然，若

$$f(x)=\sum_{i=0}^{+\infty} a_i x^i, \qquad g(x)=\sum_{i=0}^{+\infty} b_i x^i,$$

则

$$f(x)-g(x)=\sum_{i=0}^{+\infty}(a_i-b_i)x^i.$$

在 $f(x)$ 的表达式里，如果只有一个系数不为零，即若 $f(x)=a_n x^n$，则称为**单项式**。显然，一个多项式可以认为是由许多单项式按上面的加法法则连加得出的，即一般有

$$\begin{aligned} f(x) &= a_0+a_1x+a_2x^2+\cdots+a_nx^n \\ &= (a_0)+(a_1x)+(a_2x^2)+\cdots+(a_nx^n). \end{aligned}$$

由于加法可交换次序，于是又有

$$f(x)=(a_nx^n)+\cdots+(a_2x^2)+(a_1x)+(a_0).$$

这样，$f(x)$ 也可写成：$f(x)=a_nx^n+\cdots+a_2x^2+a_1x+a_0$。

现在，在一元多项式定义中，$f(x)$ 的形式表达式内出现的记号"+"已经具有加法的含意，并遵循上面列举的四条基本运算法则了。

二、乘法

设 $f(x), g(x) \in K[x]$，若 $f(x)=\sum_{i=0}^{+\infty} a_i x^i$，$g(x)=\sum_{j=0}^{+\infty} b_j x^j$，

定义

$$f(x)g(x)=\sum_{k=0}^{+\infty} c_k x^k, \qquad c_k=\sum_{i+j=k} a_i b_j.$$

显然，$f(x)g(x)\in K[x]$，称它为 $f(x)$ 与 $g(x)$ 的**乘积**。

如果 $a_{n+1}=a_{n+2}=\cdots=0$；$b_{m+1}=b_{m+2}=\cdots=0$，则 $c_{m+n+1}=c_{m+n+2}=\cdots=0$。

容易验证，上面定义的乘法运算具有下面几条基本性质：

1）结合律：$(f(x)g(x))h(x)=f(x)(g(x)h(x))$；

2）对于多项式 $I(x)=1+0x+0x^2+\cdots$，显然有

$$f(x)I(x)=f(x),\quad \forall\ f(x)\in K[x].$$

今后，将 $I(x)$ 简单地记为 1。

3）交换律：$f(x)g(x)=g(x)f(x)$。

根据上面的定义，如取 $f(x)=x^n$，$g(x)=x^m$，则有 $x^nx^m=x^{n+m}$，于是

$$x^n=\overbrace{x\,x\cdots x}^{n\text{ 项}}.$$

现在，在一元多项式定义中 $f(x)$ 的形式表达式内，$x^k(k=2,\cdots,n)$ 已经具有方幂的含意了。为方便计，今后约定 $f(x)^0=1(f(x)\neq 0$ 时)。

对任意 $a\in K$，令 $a(x)=a+0x+0x^2+\cdots$，称为**常数多项式**，简记为 a。显然，$a(x)\cdot x^n=ax^n$，这表明：单项式 ax^n 可看作常数多项式 a 与多项式 x^n 的乘积。

一元多项式的加法与乘法运算之间，存在着一种基本的关系，称为分配律：

$$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x).$$

从上面的关系式，利用数学归纳法，不难证明：

$$\begin{aligned}&f(x)(g_1(x)+g_2(x)+\cdots+g_k(x))\\&\quad=f(x)g_1(x)+f(x)g_2(x)+\cdots+f(x)g_k(x).\end{aligned}$$

到此为止，我们已经把读者在初等代数中就已熟知的一元多项式的一些基本运算规律重新确立起来了。我们之所以在这里不厌其烦地详细讲这些东西，是为了向读者说明：我们所熟知的这些运算，其理论上的依据就是上面所指出的加法运算的四条基本

性质，乘法运算的三条基本性质，以及加法和乘法之间的关系——分配律。这些东西在本书的第三章内，将作为一种全新的理论体系的出发点，因此，读者不要因为已经熟知这些运算规律而忽视它们。

从现在开始，我们就可以把一元多项式当作一般的代数式来作运算了。对一元多项式，我们常常采用另一种表达式——按不定元x的降幂来排列它：

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n \qquad (a_i\in K)。$$

如果$a_0\neq 0$，则称$f(x)$是n次多项式，或称$f(x)$的次数为n，并用记号$\deg f(x)=n$来表示它。有时，我们也把$f(x)$简单地写成f（当其不定元从上下文看很清楚，不会混淆时），于是其次数可简记为$\deg f=n$。a_0称为$f(x)$的首项系数，而a_n称为常数项。另外，我们约定$x^0=1$，故常数项a_n可看作x的零次方幂的系数。常数多项式$a(x)=a\neq 0$为零次多项式。零多项式0的次数沒有定义（有时为了方便，把零多项式次数定义为$-\infty$）。

在这一段的最后，我们来指出现在所讨论的一元多项式和分析中的实系数多项式之间的两个重要区别：1）这里所讨论的是任意数域K上的一元多项式，并不限于实系数多项式。因而，以实数的连续性为基础的一些概念（如$f(x)$的连续性、极限、微商、积分等等）不能照搬到K上的一元多项式上来；2）这里的一元多项式$f(x)$并不当作函数看，x只是一个“未定元”或“文字”，并不看作自变量。因此，我们下面要讨论的主要课题也与数学分析不同，我们所要讨论的，是与上面所定义的两种多项式运算相联系的问题：一元多项式的因式分解理论。

整除理论

全体整数组成的集合$\mathbb{Z}$内有两种运算：加法和乘法。这和$K[x]$相同，而且它们也满足上一段所指出的几条基本运算规律。从加法的四条性质不难知道，$\mathbb{Z}$内和$K[x]$内的加法都存在逆运

算：减法。那么，乘法是否有逆运算呢？在算术课程中就已经指出，$\mathbf{Z}$内的乘法沒有逆运算，即任给$a,b\in\mathbf{Z}$，不一定存在$x\in\mathbf{Z}$，使$ax=b$，即使$a\neq0$也是如此。$K[x]$内的乘法与此类似。在这一段中，我们就来讨论这个问题。

首先指出两条简单的事实。

1）根据$K[x]$内元素的定义，我们有

$$\sum_{i=0}^{+\infty}a_ix^i=\sum_{i=0}^{+\infty}b_ix^i\Longleftrightarrow a_i=b_i\quad(i=0,1,2,\cdots)$$

（注意我们约定上面的无穷和式中只有有限多项系数不为零）。

2）对任意$f(x)\in K[x]$，$0\cdot f(x)=0$。而若$f(x)\neq0$，$g(x)\neq0$，则$\deg f(x)g(x)=\deg f(x)+\deg g(x)$，即两个非零多项式相乘时，其次数相加。容易看出，$f(x)g(x)$的首项系数恰为$f(x)$和$g(x)$首项系数的乘积。因而两个非零多项式的乘积仍为非零多项式。

现在我们不难知道：$K[x]$内的乘法也沒有逆运算，即任给$f(x),g(x)\in K[x]$，不一定能找到$h(x)\in K[x]$，使$f(x)h(x)=g(x)$，即使$f(x)\neq0$时也是如此。特别是当$\deg g(x)<\deg f(x)$时，上面的第2条事实告诉我们，此时肯定不存在满足上述要求的$h(x)$。

由于$\mathbf{Z}$和$K[x]$内的乘法沒有逆运算，于是就产生出一套整除性理论。这个理论以下面的命题为出发点。

命题1.1 设$f(x),g(x)\in K[x]$，$f(x)\neq0$。则存在唯一的$q(x),r(x)\in K[x]$，使

$$g(x)=q(x)f(x)+r(x),$$

其中$r(x)=0$或$\deg r(x)<\deg f(x)$。

证 存在性。设

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\qquad(a_0\neq0).$$

如果$n=0$，则取$q(x)=\frac{1}{a_0}g(x)$，$r(x)=0$即可。下面假定$n>0$。

对$g(x)$的次数作数学归纳法：如果$g(x)=0$或$\deg g(x)<n$，则令$q(x)=0$，$r(x)=g(x)$即满足要求。设$g(x)$次数$<m$时，命题正确。则当$g(x)$次数为m时，有

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m \qquad (b_0\neq 0)$$

（这里$m\geqslant n$），令

$$g_1(x)=g(x)-\frac{b_0}{a_0}x^{m-n}f(x).$$

若$g_1(x)=0$，则取$q(x)=\frac{b_0}{a_0}x^{m-n}, r(x)=0$。否则，因$\deg g_1(x)<m$，按归纳假设，存在$q_1(x), r_1(x)\in K[x]$，使

$$g_1(x)=q_1(x)f(x)+r_1(x),$$

这里$r_1(x)=0$或$\deg r_1(x)<\deg f(x)$。现在令

$$q(x)=\frac{b_0}{a_0}x^{m-n}+q_1(x), \quad r(x)=r_1(x),$$

显然有$q(x)f(x)+r(x)=g(x)$。

唯一性。设又有$\bar{q}(x), \bar{r}(x)$满足命题要求，那么

$$q(x)f(x)+r(x)=\bar{q}(x)f(x)+\bar{r}(x),$$

$$[q(x)-\bar{q}(x)]f(x)=\bar{r}(x)-r(x).$$

比较两边的次数，即可知$\bar{r}(x)-r(x)=0, q(x)-\bar{q}(x)=0$。 ▎

命题1.1中的$q(x)$和$r(x)$分别称为用$f(x)$去除$g(x)$所得的**商**和**余式**。命题证明过程中实际上已给出了求$q(x)$和$r(x)$的方法。在具体计算时，可采用第8页所示的除法算式：

下面所叙述的计算通常称为**带余除法**。

请读者仿照下面的办法自行证明：在$\mathbf{Z}$内也有类似的带余除法，即设$a, b\in\mathbf{Z}, a\neq 0$，则存在唯一的$q, r\in\mathbf{Z}$，使$b=qa+r$，其中$0\leqslant r<|a|$。