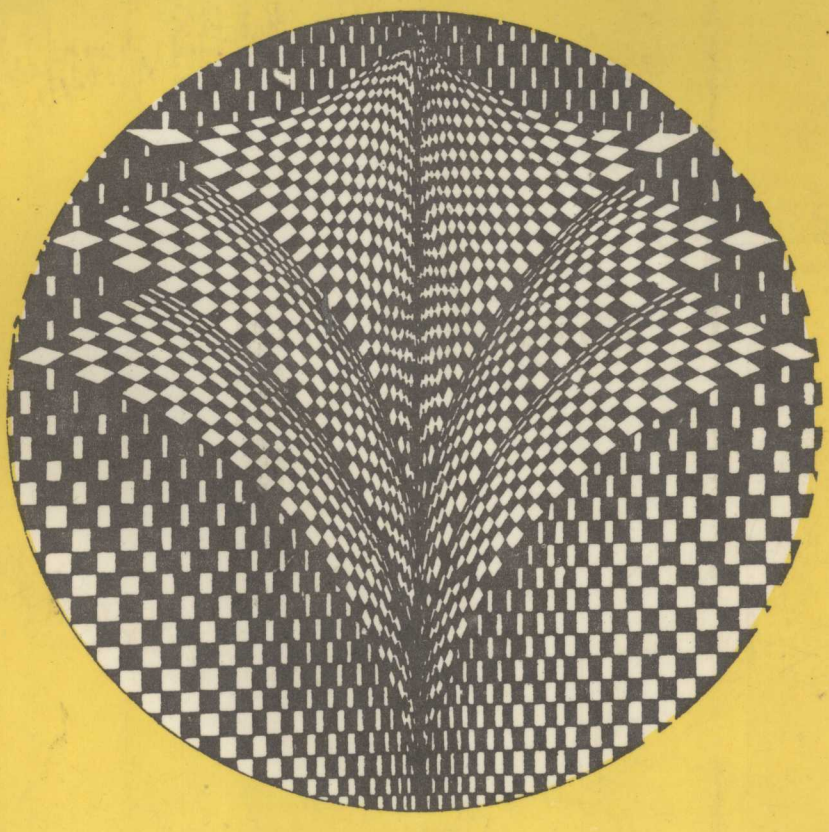
编 ／林成森 盛松柏

高等代数



· 南京大学出版社 ·

高等代数

林成森　盛松柏　编

南京大学出版社

1993·南京

（苏）新登字第011号

内 容 简 介

本书是计算机学科各专业的高等代数教材，内容包括多项式的基本理论、实系数多项式、行列式、向量和矩阵、线性空间、线性变换、线性方程组、矩阵特征值问题、实二次型以及若当标准形简介。

本书除系统地介绍高等代数的基本理论和方法外，还加强了矩阵运算、线性空间概念与理论以及特征值理论。每章选编了大量习题，有利读者掌握基本概念、基础理论和方法。

本书主要适用于计算机学科各专业及计算数学专业，也可供理工科大学师生和科技工作者参考。

高等代数

林成森 盛松柏 编

南京大学出版社出版

（南京大学校内）

江苏省新华书店发行 · 江苏阜宁印刷厂印刷

开本：787×1092 1/16 印张：20.625 字数：515千

1993年10月第1版 1993年10月第1次印刷

印数1—2000

ISBN 7-305-02207-1/O·138

定价：15.80元

前　言

高等代数是理工科大学的一门重要基础数学课程。随着科学技术，特别是计算机的迅速发展，它已渗透到科技、工程、生产、经济和人文等领域中。

本书是根据1985年计算机学科教材会议提出的大纲要求，并参考全国计算数学教材会议精神编写的教材。全书分八章，内容有多项式的基本理论、实系数多项式、行列式、向量和矩阵、线性空间和线性变换、线性方程组、矩阵特征值问题、实二次型，另外还有若当标准形作为附录。

本书初稿分别在南京大学计算机科学系和数学系计算数学及其应用软件专业试用过八次和四次，经过修改和补充定稿。本教材授课时间为一学年，如若安排一学期讲授，可适当删减书中某些内容。

欧阳梓祥、赵金熙、孙文瑜、翟灿芳、傅冬生、周如海等老师曾使用过本教材，并提出了许多宝贵的意见；罗亮生同志为本书精心绘制了插图；南京大学数学系副主任陈仲给予热情的关心；南京大学出版社给予大力支持，编者谨向他们表示衷心的感谢。

由于编者水平有限，在本教材中一定会有错误和不足之处，敬请使用本书的各位老师和读者批评指正。

编　者

1993年4月

目　录

第一章　一元多项式的基本理论

第一节　数　域

许多数学问题的解答与所考虑的数的范围有关，例如，方程$x^2+1=0$在实数范围内没有根，而在复数范围内有根$-\sqrt{-1}$和$\sqrt{-1}$。因此在研究多项式之前，我们先介绍数域概念。

定义1　设F是一个数集，如果其中任意两个数a、b（这两个数也可以相同），它们的和$a+b$、差$a-b$、积ab以及商a/b（$b\neq 0$）仍在F中，则称F为一个**数域**。

显然，全体有理数组成的集合，全体实数组成的集合，以及全体复数组成的集合都是数域。我们分别称它们为**有理数域**，**实数域**和**复数域**，并分别以字母Q、R、C来记这三个数域。

全体整数组成的集合记作Z，它不是数域，因为两个整数的商未必是整数。

例　所有形如

$$a+b\sqrt{2}$$

的数（其中a、b为任何有理数）组成的集合，记作$Q(\sqrt{2})$，它是一个数域。

事实上，设$a+b\sqrt{2}$，$c+d\sqrt{2}$是$Q(\sqrt{2})$中的两个数，则

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$$

因为a、b、c、d都是有理数，因此$a+c$、$b+d$也都是有理数，从而，$(a+c)+(b+d)\sqrt{2}$是$Q(\sqrt{2})$中的数。同理，易知

$$(a+b\sqrt{2})-(c+d\sqrt{2})$$

和

$$(a+b\sqrt{2})(c+d\sqrt{2})$$

也都是$Q(\sqrt{2})$中的数。再假设$c+d\sqrt{2}\neq 0$，则$c-d\sqrt{2}\neq 0$，而

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}$$

$$=\frac{ac-2bd}{c^2-2d^2}+\frac{bc-ad}{c^2-2d^2}\sqrt{2}$$

因$\frac{ac-2bd}{c^2-2d^2}$，$\frac{bc-ad}{c^2-2d^2}$均为有理数，因此$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$是$Q(\sqrt{2})$中的数。

定理　任何数域都包含有理数域Q。

证明 设F是一个数域，由定义1易知：1是F中的数。因此，$1+1=2$，$1+2=3$，…，$1+(n-1)=n$，…全是F中的数。这就是说，F中包含全体自然数。又易知0是F中的数，因此，$0-n=-n$也是F中的数，因而F包含全体整数。任何一个有理数都可以表示成两个整数的商，因此任何一个有理数都是F中的数。定理得证。

定义2 若数域$\overline{F}$包含数域F，则称数域$\overline{F}$为数域F的一个扩展域。

例如，数域C、R、$Q(\sqrt{2})$都是有理数域Q的扩展域。

第二节 一元多项式的定义和运算

定义1 假设x是一个未知量，n为一个非负整数，a_0，a_1，…，a_n（$a_n\neq 0$）都是数域F中的数，形式表达式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \tag{2.1}$$

称为系数在数域F中的关于未知量x的一个**n次多项式**，或称为系数在数域F中的一个**一元n次多项式**，简称为数域F上的**n次多项式**。a_0，a_1，…，a_n称为多项式$f(x)$的**系数**，而a_n又称为$f(x)$的**首项系数**。若$a_n=1$，则称$f(x)$为**首一多项式**。

数域F中任何不等于0的数是x的一个**零次多项式**；数0也是x的一个多项式，称为**零多项式**，记作0，它是唯一没有次数的多项式。

例如

$$f(x)=3x^4+(1+i)x^3+4x^2+ix+(2-i),\qquad i=\sqrt{-1}$$

是复数域C上的一个四次多项式，而

$$g(x)=x^3+\frac{1}{2}x^2+1$$

是有理数域Q上的一个三次多项式，当然$g(x)$也可视为实数域R或复数域C上的一个三次多项式。

数域F上的全体一元多项式构成的集合，记作$F[x]$，F又称为$F[x]$的**系数域**。

设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\qquad a_n\neq 0,\qquad n\geqslant 0 \tag{2.2}$$

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0,\qquad b_m\neq 0,\qquad m\geqslant 0 \tag{2.3}$$

是$F[x]$中的两个多项式。

定义2 多项式$f(x)$与$g(x)$**相等**（或**恒等**），记作$f(x)=g(x)$，是指它们的同次数的未知量的系数都彼此相等，即$n=m$，$a_n=b_m$，$a_{n-1}=b_{m-1}$，…，$a_1=b_1$，$a_0=b_0$。

零多项式只能与零多项式相等。

定义3 多项式$f(x)$与$g(x)$的**和**，记作$f(x)+g(x)$，定义为

$$f(x)+g(x)=a_nx^n+\cdots+a_{m+1}x^{m+1}+c_mx^m+c_{m-1}x^{m-1}+\cdots+c_1x+c_0,\qquad n>m$$

其中$c_i=a_i+b_i$，$i=0$，1，…，m；

$$f(x)+g(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0,\qquad n=m$$

其中$c_i=a_i+b_i$，$i=0$，1，…，n；

$$f(x)+g(x)=b_mx^m+\cdots+b_{n+1}x^{n+1}+c_nx^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0,\qquad n<m$$

其中$c_i=a_i+b_i$，$i=0$，1，……，n；

$0+f(x)=f(x)+0=f(x)$。

定义4 多项式$f(x)$与$g(x)$的乘积，记作$f(x)g(x)$，定义为

$$f(x)g(x)=d_{n+m}x^{n+m}+d_{n+m-1}x^{n+m-1}+\cdots+d_1x+d_0 \tag{2.4}$$

其中

$$d_k=\sum_{i+j=k}a_ib_j$$

$$=a_kb_0+a_{k-1}b_1+\cdots+a_1b_{k-1}+a_0b_k \qquad (0\leqslant k\leqslant n+m)$$

若$i>n$，则$a_i=0$；若$j>m$，则$b_j=0$。

$$0f(x)=f(x)0=0。$$

据定义4，我们有

$$f(x)g(x)=a_nb_mx^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)x^{n+m-1}$$
$$+\cdots+(a_1b_0+a_0b_1)x+a_0b_0$$

$$\alpha f(x)=f(x)\alpha=\alpha a_nx^n+\alpha a_{n-1}x^{n-1}+\cdots+\alpha a_1x+\alpha a_0。$$

其中$\alpha\in F$。

我们把$-1\cdot f(x)$简记作$-f(x)$。

定义5 多项式$f(x)$与$g(x)$之差，记作$f(x)-g(x)$定义为

$$f(x)-g(x)=f(x)+(-g(x))$$

例 求多项式

$$f(x)=x^3+2x^2+x+1与g(x)=2x^2+3x+2$$

之乘积$f(x)g(x)$。

解 据(2.4)式

$$f(x)g(x)=2x^5+(3+4)x^4+(2+6+2)x^3+(4+3+2)x^2+(2+3)x+2$$
$$=2x^5+7x^4+10x^3+9x^2+5x+2$$

我们也可这样来计算：

$$\begin{array}{r}f(x)=x^3+2x^2+x+1\\ \times\ g(x)=2x^2+3x+2\\ \hline 2x^5+4x^4+2x^3+2x^2\\ 3x^4+6x^3+3x^2+3x\\ 2x^3+4x^2+2x+2\\ \hline f(x)g(x)=2x^5+7x^4+10x^3+9x^2+5x+2\end{array}$$

显然，$F[x]$中的两个多项式$f(x)$和$g(x)$的和、差、乘积仍是$F[x]$中的多项式。

定理1 若$f(x)$、$g(x)$和$h(x)$都是$F[x]$中的多项式，则有

（1）加法交换律：$f(x)+g(x)=g(x)+f(x)$；

（2）加法结合律：$(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$；

（3）乘法交换律：$f(x)g(x)=g(x)f(x)$；

（4）乘法结合律：$(f(x)g(x))h(x)=f(x)(g(x)h(x))$；

（5）乘法对加法的分配律：$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$；

（6）记$f^1(x)=f(x)$，$f^2(x)=f^1(x)f(x)$，……，$f^k(x)=f^{k-1}(x)f(x)$，k是大于1的自然数，则

$$f^k(x)f^m(x)=f^{k+m}(x)$$

$$(f^k(x))^m=f^{km}(x)$$

其中$f^k(x)$称为$f(x)$的k**次方幂**。

关于多项式的和与乘积的次数，我们容易得到下面的定理。

定理2 若$f(x)$，$g(x)$都是$F[x]$中的多项式，则$f(x)\pm g(x)$的次数不大于$f(x)$与$g(x)$的次数之较大数，而当$f(x)$与$g(x)$的次数不相等时，$f(x)\pm g(x)$的次数等于$f(x)$与$g(x)$之次数的较大数；乘积$f(x)g(x)$的次数为$f(x)$与$g(x)$的次数之和。

推论1 $f(x)g(x)=0$的充分必要条件为$f(x)$和$g(x)$中至少有一个是零多项式。

证明 若$f(x)$和$g(x)$中至少有一个是零多项式，则由定义4立即得$f(x)g(x)=0$。若$f(x)\neq 0$，且$g(x)\neq 0$，则由定理2可知$f(x)g(x)\neq 0$。

推论2 若$f(x)g(x)=f(x)h(x)$，且$f(x)\neq 0$，则$g(x)=h(x)$。

证明 由$f(x)g(x)=f(x)h(x)$得$f(x)(g(x)-h(x))=0$，但$f(x)\neq 0$，据推论1知，必有$g(x)-h(x)=0$，即$g(x)=h(x)$。

第三节 多项式的整除性

定义1 设$f(x)$和$g(x)$是$F[x]$中的两个多项式。若存在$F[x]$中的多项式$q(x)$，使得

$$f(x)=g(x)q(x) \qquad (3.1)$$

则称$g(x)$**整除**（**能除尽**）$f(x)$，记作$g(x)\mid f(x)$。$g(x)$，$q(x)$都称为$f(x)$的因式。若$g(x)$不能整除$f(x)$，则记作$g(x)\nmid f(x)$。

由定义1，容易推出关于多项式整除性的一些基本性质（所提到的多项式均指$F[x]$中的多项式）：

1） 若$g(x)\mid f(x)$，$f(x)\mid h(x)$，则$g(x)\mid h(x)$；

证明 由假设条件知，必存在多项式$u(x)$，$v(x)$使

$$f(x)=g(x)u(x),\quad h(x)=f(x)v(x)$$

因此

$$h(x)=g(x)u(x)v(x)$$

即$g(x)\mid h(x)$。

2） 若$g(x)\mid f(x)$，$g(x)\mid h(x)$，则$g(x)\mid(f(x)\pm h(x))$；

3） 若$g(x)\mid f(x)$，则$g(x)\mid f(x)h(x)$，$h(x)$为任一多项式；

4）若$g(x)\mid f_i(x)$，$i=1,2,\cdots,k$，则对$F[x]$中任意的多项式$h_i(x)$，$i=1,2,\cdots,k$，

$$g(x)\Big|\sum_{i=1}^{k}f_i(x)h_i(x)$$

5） 零次多项式整除任一多项式；任一多项式整除零多项式；

6） $g(x)|f(x)$且$f(x)|g(x)$的充分必要条件是$g(x)=cf(x)$，其中$c\in F$为一个不等于0的数；

7） 若$g(x)$与$f(x)$的次数相同，且$g(x)\mid f(x)$，则$g(x)=cf(x)$，$c\in F$。

对于$F[x]$中任意的两个多项式$f(x)$、$g(x)$，一般地，$g(x)$未必能整除$f(x)$，即找不到$F[x]$中的一个多项式$q(x)$使（3.1）成立，但却有下面的带余除法。

定理1（带余除法） 设$f(x)$和$g(x)$为$F[x]$中的任意两个多项式，且$g(x)\neq 0$，则必存在$F[x]$中的唯一多项式$q(x)$和$r(x)$，使

$$f(x)=g(x)q(x)+r(x) \tag{3.2}$$

其中或者$r(x)=0$，或者$r(x)$的次数小于$g(x)$的次数。

证明 若$f(x)=0$，则取$q(x)=0$，$r(x)=0$，（3.2）式便成立。在下面的讨论中，我们假定$f(x)\neq 0$，并设$g(x)$的次数是m，则显然有$m\geqslant 0$。我们用归纳法来完成定理的证明。

首先，当$f(x)$是零次多项式时，即$f(x)=c\neq 0$，如果$g(x)$不是零次多项式，那么可取$q(x)=0$，$r(x)=f(x)=c\neq 0$，因而（3.2）式成立；如果$g(x)$也是零次多项式，即$g(x)=c_1\neq 0$，则可以取$q(x)=\dfrac{c}{c_1}$，而取$r(x)=0$，因而(3.2)也成立。这就证明了当$f(x)$是零次多项式时定理成立。

其次，假设对于不超过$n-1$次的多项式$f(x)$，定理结论成立。我们来证明，当$f(x)$是n次多项式时，定理结论也成立。如果$n<m$，则显然可取$q(x)=0$，$r(x)=f(x)$，于是(3.2)式成立。如果$n\geqslant m$，令a_n和b_m分别是$f(x)$和$g(x)$的首项系数，则显然$b_m^{-1}a_nx^{n-m}g(x)$与$f(x)$有相同的首项，因此

$$f_1(x)=f(x)-b_m^{-1}a_nx^{n-m}g(x)$$

或者是零多项式，或者次数小于n。由已经讨论过的情况或归纳法假设，对于$f_1(x)$，$g(x)$而言，必存在$q_2(x)$和$r(x)$使

$$f_1(x)=g(x)q_2(x)+r(x)$$

成立，其中或者$r(x)=0$，或者$r(x)$的次数小于m，于是令

$$q(x)=b_m^{-1}a_nx^{n-m}+q_2(x)$$

就有

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

即得（3.2）式。由此可知，对一切n次多项式$f(x)$，（3.2）式成立。

现在来证明唯一性。

设另有$q_1(x)$，$r_1(x)$使

$$f(x)=g(x)q_1(x)+r_1(x)$$

其中$r_1(x)=0$或者$r_1(x)$的次数小于$g(x)$的次数，于是

$$g(x)q(x)+r(x)=g(x)q_1(x)+r_1(x)$$

即

$$(q(x)-q_1(x))g(x)=r_1(x)-r(x) \tag{3.3}$$

若$q(x)\neq q_1(x)$，则$q(x)-q_1(x)\neq 0$。因此（3.3）式左端的次数不小于$g(x)$的次数。因为$r_1(x)$与$r(x)$或者等于0，或者它们的次数小于$g(x)$的次数，因此，$r_1(x)-r(x)$的次数

小于$g(x)$的次数。这样，（3.3）式便不能成立。故$q_1(x)=q(x)$，因而$r_1(x)=r(x)$。

定义2 （3.2）式中的$q(x)$称为$f(x)$除以$g(x)$的**商**，$r(x)$称为**余式**。

在定理1的证明过程中，用$\frac{a_n}{b_m}x^{n-m}g(x)$来消去$f(x)$的首项的办法是具体求$q(x)$，$r(x)$过程的步骤。

例 设

$$f(x)=2x^4-3x^3+4x^2-5x+6$$
$$g(x)=x^2-3x+1$$

求商$q(x)$及余式$r(x)$。

解

$$\begin{array}{l|l|l}
x^2-3x+1 & 2x^4-3x^3+4x^2-5x+6 & 2x^2+3x+11 \\
 & 2x^4-6x^3+2x^2 & \\
\hline
 & 3x^3+2x^2-5x+6 & \\
 & 3x^3-9x^2+3x & \\
\hline
 & 11x^2-8x+6 & \\
 & 11x^2-33x+11 & \\
\hline
 & 25x-5 &
\end{array}$$

$$q(x)=2x^2+3x+11$$
$$r(x)=25x-5$$

实际上，带余除法就是初等代数中用一个多项式去除另一个多项式求商及余式的方法。

推论1 若商非零，则商的次数等于被除式的次数与除式的次数之差。

推论2 对于$F[x]$中任意两个多项式$f(x)$，$g(x)$，$g(x)\neq 0$，$g(x)|f(x)$的充分必要条件是$g(x)$除$f(x)$得余式为零。

若数域$\overline{F}$是数域F的一个扩展域，则$F[x]$中的一个多项式$f(x)$也是$\overline{F}[x]$中的一个多项式。例如$Q[x]$中的多项式x^2+3x+1也是$R[x]$和$C[x]$中的多项式。

推论3 设$f(x)$，$g(x)$是$F[x]$中的两个多项式。若$g(x)$不能整除$f(x)$，则在$\overline{F}[x]$中$g(x)$亦不能整除$f(x)$，此处$\overline{F}$是F的一个扩展域。

第四节 多项式的最高公因式

定义1 设$f(x)$，$g(x)$为$F[x]$中的两个多项式。若$F[x]$中的多项式$\varphi(x)$既是$f(x)$的因式，又是$g(x)$的因式，即$\varphi(x)|f(x)$，$\varphi(x)|g(x)$，则$\varphi(x)$称为$f(x)$与$g(x)$的**公因式**。

$F[x]$中任何两个多项式$f(x)$与$g(x)$都有公因式，因为至少每一零次多项式都是$f(x)$与$g(x)$的公因式。一般地，$f(x)$与$g(x)$还有其它公因式。

定义2 设$f(x)$，$g(x)$是$F[x]$中的两个多项式。若$F[x]$中的多项式$d(x)$是$f(x)$与

$g(x)$的一个公因式，且$d(x)$能被$f(x)$与$g(x)$的每一个公因式整除，则$d(x)$称为$f(x)$与$g(x)$的一个**最高公因式，或最大公因式。**

定理1 $F[x]$中任何两个多项式$f(x)$与$g(x)$一定有最高公因式。而且，$f(x)$与$g(x)$的最高公因式，除一个零次因式外，是唯一的。这就是说，若$d(x)$是$f(x)$与$g(x)$的一个最高公因式，则对数域F中的任何一个不为零的数c，$cd(x)$也是$f(x)$与$g(x)$的一个最高公因式，且只有这样的乘积$cd(x)$是$f(x)$与$g(x)$的最高公因式。

证明 我们将构造性地证明最高公因式的存在性。若$f(x)=g(x)=0$，则$f(x)$与$g(x)$的最高公因式就是0；若$f(x)$与$g(x)$中有一个为0，则另一个便是它们的最高公因式。现假设$f(x)$与$g(x)$都不为0，应用带余除法，以$g(x)$除$f(x)$，得商$q_1(x)$及余式$r_1(x)$。若$r_1(x)\neq 0$，则再以$r_1(x)$除$g(x)$，得商$q_2(x)$及余式$r_2(x)$。若$r_2(x)\neq 0$，再以$r_2(x)$除$r_1(x)$。如此继续下去。由于$r_1(x)$，$r_2(x)$…的次数一次比一次低，因此，进行到某一步时，余式必为零，比方说$r_{k+1}(x)=0$。这样，我们得到一组等式：

$$
\begin{aligned}
f(x)&=g(x)q_1(x)+r_1(x)\\
g(x)&=r_1(x)q_2(x)+r_2(x)\\
r_1(x)&=r_2(x)q_3(x)+r_3(x)\\
&\cdots\cdots\qquad\cdots\cdots\\
r_{k-3}(x)&=r_{k-2}(x)q_{k-1}(x)+r_{k-1}(x)\\
r_{k-2}(x)&=r_{k-1}(x)q_k(x)+r_k(x)\\
r_{k-1}(x)&=r_k(x)q_{k+1}(x)
\end{aligned}
$$

从上述最后一个等式知，$r_k(x)\mid r_{k-1}(x)$，因而从倒数第二个等式知，$r_k(x)\mid r_{k-2}(x)$，由此倒推上去便知

$$r_k(x)\mid f(x),\quad r_k(x)\mid g(x)$$

因此$r_k(x)$是$f(x)$与$g(x)$的一个公因式。

其次，假设$h(x)$是$f(x)$与$g(x)$的任一公因式，则从上述等式组的第一个等式可知，$h(x)\mid r_1(x)$。同理，据第二个等式知，$h(x)\mid r_2(x)$。如此逐次往下推，最后得到$h(x)\mid r_k(x)$。因此$r_k(x)$是$f(x)$与$g(x)$的一个最高公因式。

假设$d(x)$也是$f(x)$与$g(x)$的一个最高公因式，则$d(x)\mid f(x)$，$d(x)\mid g(x)$，且$d(x)\mid r_k(x)$，$r_k(x)\mid d(x)$，据第三节中性质6知$d(x)=cr_k(x)$。

两个零多项式的最高公因式是0，它是唯一确定的。两个不全为零的多项式的最高公因式总是非零多项式，它们之间只相差一个常数因子。通常以$(f(x),\ g(x))$来表示$f(x)$与$g(x)$的首项系数为1的最高公因式。显然，该最高公因式是唯一的。

定理1证明中用来求最高公因式的方法，通常称为**辗转相除法。**

由于$f(x)$与$cf(x)$（$c\neq 0$）有相同的因式，因此有

$$(f(x),\ g(x))=(cf(x),\ g(x))$$

这说明，在计算过程中，有时可用一个非零常数去乘某一多项式，并不影响计算结果。

例1 求$Q[x]$中多项式

$$
\begin{aligned}
f(x)&=x^4+3x^3-x^2-4x-3\\
g(x)&=3x^3+10x^2+2x-3
\end{aligned}
$$

的最高公因式。

解 辗转相除法可按下列格式来进行：

$q_2(x)=-\frac{9}{5}x+3$	$3x^3+10x^2+2x-3$	$3x^4+9x^3-3x^2-12x-9$	$q_1(x)=x-\frac{1}{3}$
	$3x^3+15x^2+18x$	$3x^4+10x^3+2x^2-3x$	
	$-5x^2-16x-3$	$-x^3-5x^2-9x-9$	
	$-5x^2-25x-30$	$-x^3-\frac{10}{3}x^2-\frac{2}{3}x+1$	
	$r_2(x)=9x+27$	$r_1(x)=-\frac{5}{3}x^2-\frac{25}{3}x-10$	$q_3(x)=-\frac{5}{3}x-\frac{10}{3}$
	$\frac{1}{9}r_2(x)=x+3$	$-\frac{5}{3}x^2-\frac{15}{3}x$	
		$-\frac{10}{3}x-10$	
		$-\frac{10}{3}x-10$	
		0	

因此

$$(f(x),\ g(x))=\frac{1}{9}r_2(x)=x+3$$

定理2 设$f(x)$，$g(x)$是$F[x]$中的两个多项式。若$d(x)$是$f(x)$与$g(x)$的最高公因式，则在$F[x]$中存在两个多项式$u(x)$与$v(x)$，使得$d(x)$表示成$f(x)$和$g(x)$的一个组合：

$$d(x)=u(x)f(x)+v(x)g(x) \qquad (4.1)$$

证明 若$f(x)=g(x)=0$，则$d(x)=0$，这时，任何两个多项式都可取作$u(x)$与$v(x)$；若$f(x)$与$g(x)$有一个为0，比方说，$g(x)=0$，则$d(x)=f(x)$，因此可取$u(x)=1$，而任何一个多项式都可取作$v(x)$。

现假设$f(x)$，$g(x)$均不为0，考察定理1证明过程中的辗转相除等式组。由第一个等式有

$$r_1(x)=f(x)+(-q_1(x))g(x)$$

将它代入第二个等式得

$$r_2(x)=(-q_2(x))f(x)+(1+q_1(x)q_2(x))g(x)$$

如此继续下去，最后便可把$r_k(x)$表示成

$$r_k(x)=u_1(x)f(x)+v_1(x)g(x)$$

而$d(x)=cr_k(x)$，因此，取$u(x)=cu_1(x)$，$v(x)=cv_1(x)$，即得所要证明的等式(4.1)。

例2 就例1而言

$$r_2(x)=9x+27=\left(\frac{9}{5}x-3\right)3\,f(x)+\left[1+\left(x-\frac{1}{3}\right)\left(-\frac{9}{5}x+3\right)\right]g(x)$$

$$=3\left(\frac{9}{5}x-3\right)f(x)+\left(-\frac{9}{5}x^2+\frac{18}{5}x\right)g(x)$$

于是

$$(f(x),\ g(x))=x+3$$

$$=\left(\frac{3}{5}x-1\right)f(x)+\left(-\frac{1}{5}x^2+\frac{2}{5}x\right)g(x)$$

定义 3 设$f(x)$，$g(x)$为$F[x]$中的两个多项式，若$(f(x),\ g(x))=1$，则称$f(x)$与$g(x)$**互质**（或**互素**）。

显然，若两个多项式互质，则它们除去零次多项式外没有其它公因式；反之亦成立。

定理 3 $F[x]$中两个多项式$f(x)$，$g(x)$互质的充分必要条件是在$F[x]$中存在两个多项式$u(x)$和$v(x)$，使

$$u(x)f(x)+v(x)g(x)=1 \qquad (4.2)$$

证明 必要性是定理 2 的直接推论。现证充分性。设有多项式$u(x)$和$v(x)$使

$$u(x)f(x)+v(x)g(x)=1$$

而$d(x)=(f(x),\ g(x))$，则$d(x)\mid f(x)$，$d(x)\mid g(x)$，从而$d(x)\mid 1$。故$d(x)=1$，即$f(x)$与$g(x)$互质。

从定理 3，可以得到关于互质多项式的一些重要结论：

推论 1 若$(f(x),\ g(x))=1$，$(f(x),\ h(x))=1$，则$(f(x),\ g(x)h(x))=1$。

证明 据（4.2），存在$u(x)$，$v(x)$使

$$u(x)f(x)+v(x)\ g(x)=1$$

因而有

$$u(x)f(x)h(x)+v(x)g(x)h(x)=h(x) \qquad (4.3)$$

令 $d(x)=(f(x),\ g(x)h(x))$，则$d(x)\mid u(x)f(x)h(x)$，$d(x)\mid v(x)g(x)h(x)$，因而$d(x)\mid h(x)$，故$d(x)\mid(f(x),\ h(x))$，但$(f(x),\ h(x))=1$，故$d(x)=1$。

推论 2 若$f(x)\mid g(x)h(x)$，$(f(x),\ g(x))=1$，则$f(x)\mid h(x)$。

证明 据假设条件$(f(x),\ g(x))=1$，知（4.3）式成立。因$f(x)\mid u(x)f(x)h(x)$，$f(x)\mid v(x)g(x)h(x)$，故$f(x)\mid h(x)$。

推论 3 若$f(x)\mid h(x)$，$g(x)\mid h(x)$，$(f(x),\ g(x))=1$，则$f(x)g(x)\mid h(x)$。

证明 据假设条件$(f(x),\ g(x))=1$，知（4.3）式成立。由于$g(x)\mid h(x)$，因此$f(x)g(x)\mid u(x)f(x)h(x)$；又因$f(x)\mid h(x)$，因此$f(x)g(x)\mid v(x)g(x)h(x)$，故$f(x)g(x)\mid h(x)$。

最高公因式的定义可推广到任何一组有限多个多项式的情形。

若多项式$f(x)$整除多项式$f_1(x)$，…，$f_k(x)$中的每一个，即$f(x)\mid f_1(x)$，$f(x)\mid f_2(x)$，…，$f(x)\mid f_k(x)$，则称$f(x)$为$f_1(x)$，$f_2(x)$，…，$f_k(x)$的一个公因式。若，$f_1(x)$，$f_2(x)$，…，$f_k(x)$的公因式$d(x)$能被这k个多项式的每一个公因式整除，则称$d(x)$为多项式$f_1(x)$，$f_2(x)$，…，$f_k(x)$的一个**最高公因式**。

定理 4 $F[x]$中多项式$f_1(x)$，$f_2(x)$，…，$f_k(x)$的最高公因式，等于多项式$f_k(x)$与多项式$f_1(x)$，$f_2(x)$，…，$f_{k-1}(x)$的最高公因式的最高公因式（其中$k>1$）。

证明 用归纳法证明。当$k=2$时，定理显然成立。假定它对$k-1$个多项式是正确的。设$d_{k-1}(x)$是多项式$f_1(x)$，…，$f_{k-1}(x)$的一个最高公因式，则$d_{k-1}(x)\mid f_1(x)$，…，$d_{k-1}(x)\mid f_{k-1}(x)$。用$d_k(x)$表示$d_{k-1}(x)$与$f_k(x)$的一个最高公因式，于是$d_k(x)\mid d_{k-1}(x)$，$d_k(x)\mid f_k(x)$。因此，$d_k(x)\mid f_1(x)$，$d_k(x)\mid f_2(x)$，…，$d_k(x)\mid f_k(x)$。另一方面，设$\varphi(x)$