高等学校教材

Advanced Algebra

高等代数

李慧陵　编

高等教育出版社
Higher Education Press

高等学校教材

高等代数

李慧陵　编

高等教育出版社

内容简介

本书内容共分十章，其中第一章为多项式理论，第二到十章为线性代数，侧重线性空间和线性变换理论，在第十章讲授了 λ - 矩阵的初等因子理论并借此给出 Jordan 标准形定理的证明。此外，本书还包括两则附录，附录一给出了 Jordan 标准形定理的另一证明；附录二提出了二元域上线性代数的问题，并举出它在纠错码中的应用。本书在处理理论问题时力求做到直截了当、抓住关键、线索清楚、说理透彻，在行文上做到语言准确、逻辑严谨、易于阅读。

另外，本书介绍了高等代数理论应用方面的内容，包括平面几何定理机器证明的吴方法、线性规划、组合结构的关联矩阵、纠错码等，以开阔学生的知识面，引起学生的学习兴趣。

本书可作为高等学校数学类专业高等代数课程教材使用，也可作为相关人士的自学读物或参考书。

图书在版编目(CIP)数据

高等代数/李慧陵编. —北京：高等教育出版社，
2009.12

ISBN 978-7-04-014401-7

Ⅰ. 高… Ⅱ. 李… Ⅲ. 高等代数-高等学校-教材
Ⅳ. O15

中国版本图书馆 CIP 数据核字(2009)第 182010 号

策划编辑 于丽娜　**责任编辑** 张耀明　**封面设计** 张　志
责任绘图 吴文信　**版式设计** 余　杨　**责任校对** 杨凤玲
责任印制 尤　静

出版发行	高等教育出版社	**购书热线**	010-58581118
社　　址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
邮政编码	100120	**网　　址**	http://www.hep.edu.cn
总　　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	潮河印业有限公司	**畅想教育**	http://www.widedu.com
开　　本	787×960　1/16	**版　　次**	2009 年 12 月第 1 版
印　　张	20.75	**印　　次**	2009 年 12 月第 1 次印刷
字　　数	390 000	**定　　价**	24.60 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　14401-00

前　言

本书面向高等学校本科数学类专业的学生,在内容上符合数学专业规范中对此课程的基本要求,并涵盖目前数学专业研究生入学考试的通常命题范围。同时,编者在本书取材方面也有自己的考虑,遵循“学得少些,但要学得更好些”的宗旨,在取材上有增有减,有些内容只保证最低要求,有些内容则有所加强。在本书编写过程中,编者主要做了如下几方面的努力:

一、由于本书的读者是本科一年级学生，对于数学理论到底是什么，他们还不清楚。所以书中每开始一个理论的讨论时,都要明确地指出要解决的问题是什么，在解决问题的过程中我们也常常作些回顾,看看路已走了多远。如对于线性方程组理论和 Jordan 标准形理论,书中就做了这样的处理。在第十章我们设置了“什么是 Jordan 标准形”一节,在证明 Jordan 标准形存在定理之前,就对标准形的含义做了认真的思考和深入的挖掘,以使读者对其有较好的理解。

二、理论的抽象性和公理化处理方法是初学者面对的一大困难,对此我们有深切的认识。本书在这方面也做了种种努力。书中充分的讲解和强调、较多的例子、理论和例子的对照，加上学生的努力,我们相信这些困难可以克服。

三、定理的证明是我们特别着力的地方。对于定理，无论是证明方法,还是文字书写，我们都作了精心处理，务求做到证明过程直截了当、抓住关键、条理清楚、易于理解。

四、由于人们接受新事物时，有时会忽略某些方面,有时还会产生误解。本书特别注重语言的准确性,尽量避免含混不清，必要时会对读者做些正面的提醒。

本书共分十章,第一章为多项式理论，后面九章为线性代数的内容，此外还包括两则附录。在线性代数方面,本书侧重于线性空间和线性变换的理论,在第五章讲述了线性空间的理论之后,第六章建立了线性变换的基本概念和事实,第七章讨论了对角化问题,第十章则借助 λ-矩阵的初等因子理论证明了复数域上矩阵的 Jordan 标准形的存在唯一定理,在附录一中通过空间的分解对此定理又给出另一个证明。书中对于行列式和线性方程组理论,以及欧氏空间和二次型,只讲授了最基本的内容，如此处理是因为编者认为线性空间和线性变换理论是最基本、最重要的内容，学生把这部分内容理解透彻了,再学习其

他内容就不会感到困难。所以本书在线性变换方面花了较多的篇幅。如果学时紧张,可以只讲授本书前九章和第十章第一节的内容。

本书介绍了高等代数理论的一些应用。在多项式理论之后介绍了平面几何定理机器证明的吴(文俊)方法;在线性代数方面介绍了线性规划、线性递归序列、组合结构的关联矩阵等内容;在附录二中介绍了二元域上的线性代数理论在纠错码中的应用。做这些介绍的目的是为了开阔学生的知识面,引起学生的学习兴趣。这些内容中的每一个都代表一个数学分支或课题,展开来就是一个专门的学问。我们这里只介绍这些应用讨论怎样的数学问题,与本课程的理论有怎样的联系等。我们不希望关于这些应用的介绍变成课程的又一部分内容,增加学生的学习负担。所以在学时不够时,可以把有关介绍作为阅读材料使用。

本书在编写过程中,得到浙江大学数学系的支持和帮助,在此表示衷心的感谢。由于编者水平和时间有限,书中难免存在一些不足,诚恳地欢迎读者批评指正。

李慧陵

2009年5月于浙江大学求是村

目　录

第一章 多 项 式

多项式是大家熟悉的数学对象之一. 在中学数学中, 曾学习过一些具体的多项式的因式分解, 但是并没有深入地思考过因式分解问题. 经验使我们相信, 任何多项式总可以表示成不能再分解的因式的乘积, 至于分解的唯一性, 却未曾认真地考虑过. 本章首先讨论因式分解问题, 证明了因式分解及唯一性定理. 在中学时, 也建立了根的概念, 并对某些多项式, 求过它们的根. 根的理论是本章重点讨论的第二个问题. 这两个理论的讨论将帮助我们清理过去对多项式的认识, 把一些正确的通过理论的论证确立起来, 对不确切的要分清是非. 对于多元多项式, 这里只做了非常概括的介绍. 最后, 作为多项式理论的应用, 还介绍了平面几何定理机器证明的吴方法.

§1.1 数 域 和 域

从小学算术开始, 随着数学学习的深入, 所认识的数的范围也越来越宽. 曾学习过的数有正整数, 整数, 有理数, 实数以及复数, 它们有如下包含关系:

$$\text{正整数} \subset \text{整数} \subset \text{有理数} \subset \text{实数} \subset \text{复数}.$$

在正整数范围内, 减法运算不是总能进行的. 例如,2 减去 3 的结果就不再是正整数. 在整数范围内, 除法运算也不是总能进行的. 例如,1 除以 2 的结果不再是整数. 为了建立数学理论, 常常需要先确定某一个数的集合, 要求它具有良好的运算性质. 于是引进数域的概念.

定义 1 设 F 是由一些复数组成的集合, 其中至少包含两个复数. 如果对于 F 中的任意两个数 a, b, 它们的和 $a+b$, 差 $a-b$, 积 $a \times b$, 商 a/b (当 $b \neq 0$ 时) 都仍在 F 内, 则称 F 为一个数域.

说一个给定的集合 S 对某一运算封闭, 是指 S 内的任意两个元素经过此运算后的结果仍在 S 内. 于是一个由数组成的集合 F 成为数域, 必须且只须满足:

1) F 至少包含两个数;

2) F 对加法, 减法, 乘法和除法 (除数不为 0 时) 封闭.

按这个定义, 全体有理数组成的集合 (记做 $\mathbb{Q}$), 全体实数组成的集合 (记做 $\mathbb{R}$), 全体复数组成的集合 (记做 $\mathbb{C}$) 都是数域. 全体整数组成的集合 (记做 $\mathbb{Z}$), 全体正整数组成的集合都不是数域.

数域不止这些.

例 1 用 $F=\mathbb{Q}(\sqrt{2})$ 表示集合 $\{a+b\sqrt{2}|a,b\in\mathbb{Q}\}$, 即全部可以写成 $a+b\sqrt{2}$ 形式的实数所组成的集合, 其中 a,b 为有理数. 证明 $F=\mathbb{Q}(\sqrt{2})$ 是一个数域.

首先注意, 实数 $\sqrt{2}$ 不是有理数 (注意, 这是需要证明的, 请读者给出证明), 所以若 $a+b\sqrt{2}=c+d\sqrt{2}$, 且 $a,b\in\mathbb{Q}$, 则必有 $a=c,b=d$. 特别地, 当 $a,b\in\mathbb{Q}$, 使 $a+b\sqrt{2}=0$ 时, 必有 $a=b=0$.

因为 $\mathbb{Q}\subset F$, 所以 F 中有无穷多个元素. 若有 $\alpha=a+b\sqrt{2},\beta=c+d\sqrt{2}\in F$, 则

$$\alpha\pm\beta=(a+b\sqrt{2})\pm(c+d\sqrt{2})=(a\pm c)+(b\pm d)\sqrt{2},$$

$$\alpha\beta=(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}.$$

因为当 a,b,c,d 为有理数时,$a\pm c,b\pm d,ac+2bd,ad+bc$ 也为有理数, 所以 $\alpha\pm\beta,\alpha\beta\in F$. 设 $\beta=c+d\sqrt{2}\neq 0$, 则 c,d 不全为 0, 从而 $c^2-2d^2\neq 0$. 于是

$$\frac{\alpha}{\beta}=\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}=\frac{(ac+2bd)}{c^2-2d^2}+\frac{(bc-ad)}{c^2-2d^2}\sqrt{2}.$$

由于 $\dfrac{(ac+2bd)}{c^2-2d^2},\dfrac{(bc-ad)}{c^2-2d^2}$ 为有理数, 所以 $\dfrac{\alpha}{\beta}\in F$. 依定义 F 为数域. □

定理 1 设 F 为一个数域, 则 $\mathbb{Q}\subseteq F$.

证明 按定义,F 中至少有两个元素, 因而有一个非零元素 $a\in F$. 这样一来 $a/a=1$ 在 F 内. 因 F 对加法封闭, 所以 $1+1=2,2+1=3,\cdots$ 等都在 F 内, 从而全体正整数在 F 内. 因 F 是数域,F 对减法封闭. 故 $0=a-a\in F$, 并且一切负整数也在 F 内. 于是全体整数都在 F 内. 每个有理数是两个整数的商 p/q. 由于 F 对除法封闭,p/q 属于 F, 故 $\mathbb{Q}\subseteq F$. □

于是, 每个数域都是 *无限域*. 这个定理还说明, 有理数域是最小的数域.

在研究数的运算时, 相关的运算律是重要性质. 比如公式

$$(a+b)^2=a^2+2ab+b^2,$$

$$(a+b)^3=a^3+3a^2b+3ab^2+b^3$$

对任意的数 a,b 成立, 是因为数的加法满足交换律和结合律, 乘法满足交换律和结合律, 加法和乘法还满足分配律. 若 F 是一个数域,F 的加法和乘法就满足以下的性质:

加法:

(1) 加法交换律　对一切 $a,b\in F$, 有 $a+b=b+a$;

(2) 加法结合律　对一切 $a,b,c\in F$, 有 $(a+b)+c=a+(b+c)$;

(3) 元素 0 的存在性　有一个元素 0, 它对任何元素 a, 有 $a+0=a$;

(4) 负元素的存在性　对任意元素 a, 有一个元素 b, 使 $a+b=0$.

乘法:

(5) 乘法结合律　对一切 $a,b,c\in F$, 有 $(ab)c=a(bc)$;

(6) 乘法交换律　对一切 $a,b\in F$, 有 $ab=ba$;

(7) 元素 1 的存在性　有一个元素 1, 它对任何元素 a, 有 $1a=a$;

(8) 逆元素的存在性　对任意非零元素 a, 有一个元素 b, 使 $ab=1$.

加法和乘法:

(9) 分配律　对一切 $a,b,c\in F$, 有 $a(b+c)=ab+ac$.

容易看出, 正是 (3), (4) 和 (7), (8), 使数域 F 对减法和除法封闭.

随着研究对象的拓宽, 人们发现, 不只对数可以进行运算, 还有很多的数学对象, 例如多项式, 向量, 函数等, 对它们也可以进行运算. 并且有时也满足某些运算律.

例 2　把 0,1 不看成通常的数, 而仅当成符号. 在它们组成的集合 $F_2=\{0,1\}$ 里, 按下面等式定义加法和乘法:

$$0+0=1+1=0,\quad 1+0=0+1=1;$$

$$0\times 0=1\times 0=0\times 1=0,\quad 1\times 1=1.$$

那么对于这两种运算,F_2 也满足运算律 (1) ~ (9).

这里只证明加法结合律, 即证明对一切 $a,b,c\in F_2$, 有等式

$$(a+b)+c=a+(b+c)$$

成立. 其余的请读者自己证明.

首先若 $a=0$, 则等式左边为 $(0+b)+c=b+c$, 右边为 $0+(b+c)=b+c$, 等式成立. 若 $c=0$, 同样知等式成立. 若 $b=0$, 则两边都等于 $a+c$. 最后若 $a=b=c=1$, 则左右都等于 1. 所以等式在一切情况下成立. □

由于 F_2 以及许多其他的例子都满足数域所满足的运算律, 可以把数域的概念推广成更一般的“域”的概念.

定义 2 设 F 为至少有两个元素的集合, 在 F 内定义了加法 (即对任意取定的两个元素 $a,b\in F$, 在 F 内都有一个元素, 称为它们的和, 与之对应,a,b 的和记做 $a+b$) 和乘法 (即对任意取定的两个元素 $a,b\in F$, 在 F 内都有一个元素, 称为它们的积, 与之对应,a,b 的积记做 $a\cdot b$), 并且满足运算律 (1) ~ (9), 则 F 称为一个域.

定义中的 F 不一定是数组成的集合. 它可能与数 0,1 毫无联系. 应把运算律 (3) 理解成: F 内有一个特别的元素, 它与任意元素 a 的和仍为 a, 借用数字 0 来表示它. 对运算律 (7) 也可以有类似地理解. 运算律 (3) 中的 0 称为 F 的零元素, 运算律 (4) 中的 b 称为 a 的负元素, 运算律 (7) 中的 1 称为 F 的单位元素, 运算律 (8) 中的 b 称为 a 的逆元素.

于是例 1 中的 F_2 是一个域, 它仅有两个元素, 称为二元域. 本节前面定义的数域都是域. 数域的特殊性在于它们的元素都来自复数集合.

例 3 任取一个素数 p. 对于 $i\in\{0,1,2,\cdots,p-1\}$, 用 $\overline{i}$ 表示被 p 除余数为 i 的整数组成的集合. 观察发现, 在 $\overline{i}$ 中随便取元素 i', 在 $\overline{j}$ 中随便取元素 j', 它们的和 $i'+j'$ 总落在 $\overline{k}$ 内, 这里 k 是 $i+j$ 被 p 除所得的余数. 基于上述观察可以规定: $\overline{i}+\overline{j}=\overline{k}$. 同样, 若用 l 表示 $i\times j$ 被 p 除所得的余数, 则 $\overline{i}$ 中任意数与 $\overline{j}$ 中任意数的乘积落在 $\overline{l}$ 内. 规定: $\overline{i}\times\overline{j}=\overline{l}$. 可以证明, 在 $F_p=\{\overline{0},\overline{1},\cdots,\overline{p-1}\}$ 内如上定义了加法和乘法以后,F_p 也成为一个域. 证明要用到许多数论的事实, 限于篇幅, 证明省略. 在 F_p 内,$\overline{0}$ 是零元素, 而 $\overline{1}$ 是单位元素.

于是对每个素数 p, 都有一个 p 元域, 它们都是有限域.

作为基础课, 在本书内只在数域上讨论问题. 虽然前七章的绝大多数结论在任意域上都成立.

与域的概念平行的还有环的概念.

定义 3 设 R 是一个非空集合, 在其中定义了加法和乘法两种运算, 并且满足运算律 (1) ~ (5), (9), 则 R 称为一个环. 若 R 还满足运算律 (6), 则 R 称为交换环

按照这个定义, 全体整数组成整数环 $\mathbb{Z}$. 下节将看到, 数域上的全体多项式组成多项式环.

§1.2 一元多项式的运算 带余除法

定义 4 设 F 为一个数域,x 为一文字. 或称不定元. 形如

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n,\quad a_i\in F \tag{1}$$

的表达式称为 x 在 F 上的多项式.

在上面的表达式中,a_ix^i 称为 i 次项 (或简单地称为项),a_i 称为系数. 若 $a_n \neq 0$, 则多项式 $f(x)$ 称为 n 次的, n 称为 $f(x)$ 的次数, 表作 $\partial^0 f(x)$, 而 a_nx^n 称为首项,a_n 称为首项系数. 若一个多项式的所有系数全为 0, 则称为零多项式, 记作 0. 零多项式的次数规定为 $-\infty$.

多项式常简单地记作 $f(x), g(x), \cdots$.F 上全体多项式所成的集合记作 $F[x]$.

两个多项式称为相等的, 当且仅当对任何 $i = 0, 1, 2, \cdots$, 它们的 i 次项系数都相同. 这样规定是因为通常把多项式看成形式表达式而不是看成函数. 按定义, 两个函数 $f(x), g(x)$ 称为相等的, 当且仅当对自变量 x 的每个取值 x_0, 函数值 $f(x_0), g(x_0)$ 都相等. 而在下面的多项式理论中, 形式上不同的表达式就认为是不同的多项式, 而不考虑它们是否给出不同的函数.

(1) 式中的多项式 $f(x)$ 也可按降幂方式写成

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

的形式. 它和 (1) 式中的升幂写法同样有效. 可以根据讨论问题时的需要来选择使用.

两个多项式可以相加, 设 $f(x)$ 由 (1) 式给出, $g(x)$ 由下式给出

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, \tag{2}$$

它们的和规定为多项式

$$h(x) = c_0 + c_1x + c_2x^2 + \cdots + c_lx^l. \tag{3}$$

其中 $l = \max\{n, m\}$, 而且对 $i = 0, 1, \cdots, l$, $c_i = a_i + b_i$. 这里当 $n > m$ 时, 取 $b_{m+1} = \cdots = b_n = 0$; 当 $n < m$ 时, 取 $a_{n+1} = \cdots = a_m = 0$. $f(x), g(x)$ 的和记作 $f(x) + g(x)$.

易知, 若 $f(x), g(x) \in F[x]$, 则其和 $f(x) + g(x)$ 的系数都在 F 内, 故 $f(x) + g(x) \in F[x]$. 并且 $\partial^0(f(x) + g(x)) \leqslant \max\{\partial^0 f(x), \partial^0 g(x)\}$. 加法满足交换律, 结合律. 此外在 $F[x]$ 内零多项式扮演零元素的角色, 而每个多项式都有负元素, 如果 $f(x)$ 为形如式 (1) 的多项式, 则它的负元素 (记做 $-f(x)$) 的次数也是 n, 其 i 次项的系数为 $-a_i$. 减法是加法的逆运算, 即

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

这里 $-g(x)$ 是 $g(x)$ 的负元素.

两个多项式可以相乘. 设 $f(x), g(x)$ 分别由 (1) 式和 (2) 式给出, 则它们的乘积记作 $f(x)g(x)$, 且

$$f(x)g(x) = d_0 + d_1x + d_2x^2 + \cdots + d_{n+m}x^{n+m}. \tag{4}$$

这里

$$\begin{aligned} d_0 &= a_0b_0, \\ d_1 &= a_0b_1 + a_1b_0, \\ d_2 &= a_0b_2 + a_1b_1 + a_2b_0, \\ &\cdots\cdots\cdots\cdots \\ d_{n+m} &= a_nb_m. \end{aligned}$$

一般项系数满足

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

上式表示对所有满足 $i+j=k$ 的 i,j 求和.

例 1

$$\begin{aligned} &(2+3x^2+2x^3)(-1-x-x^2-x^3) \\ =&2(-1)+(2(-1))x+(2(-1)+3(-1))x^2 \\ &+(2(-1)+3(-1)+2(-1))x^3+(3(-1)+2(-1))x^4 \\ &+(3(-1)+2(-1))x^5+(2(-1))x^6 \\ =&-2-2x-5x^2-7x^3-5x^4-5x^5-2x^6. \end{aligned}$$ □

显然若 $f(x),g(x)\in F[x]$, 则 $f(x)g(x)$ 的系数都在 F 内, 故 $f(x)g(x)\in F[x]$. 乘法满足交换律, 结合律. 容易看出, 若 $f(x)=0$ 为零多项式, 或 $g(x)=0$ 为零多项式, 则乘积也为零多项式. 而若 $f(x),g(x)$ 都不是零多项式时,$f(x)g(x)$ 也不是零多项式, 且 $\partial^0(f(x)g(x))=\partial^0 f(x)+\partial^0 g(x)$. 此外, 加乘还满足分配律: 设 $a(x),b(x),c(x)$ 为三个多项式, 则

$$(a(x)+b(x))c(x)=a(x)c(x)+b(x)c(x).$$

由此知, 若 $f(x)\neq 0$, 而 $f(x)g(x)=f(x)h(x)$ 时, 就有 $f(x)(g(x)-h(x))=0$, 进而 $g(x)-h(x)=0$, 于是 $g(x)=h(x)$. 即乘法消去律成立.

把上面的讨论总结一下, 知道集合 $F[x]$ 满足运算律 (1) ~ (7) 和 (9). $F[x]$ 不满足 (8), 所以它不是域, 是交换环. 把 $F(x)$ 称为数域 F 上的一元多项式环.

在 $F(x)$ 内两个多项式不是总能相除的.

定义 5 设 $f(x),g(x)$ 为 F 上的两个多项式, 若有 F 上的一个多项式 $q(x)$, 使

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

成立, 则称 $g(x)$ 整除 $f(x)$. 此时也说 $f(x)$ 为 $g(x)$ 的倍式,$g(x)$ 为 $f(x)$ 的因式. $g(x)$ 整除 $f(x)$ 记作 $g(x)\mid f(x)$. 若 $g(x)$ 不能整除 $f(x)$, 则记作 $g(x)\nmid f(x)$.

整除有下列性质:

(1) 任一多项式都整除零多项式. 若零多项式整除 $f(x)$, 则 $f(x)$ 为零多项式;

(2) 若 $f(x) \mid g(x)$,$g(x) \mid f(x)$, 则有 F 中的非零元素 c 使 $f(x)=cg(x)$;

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

(4) 若 $f(x) \mid g_1(x)$,$f(x) \mid g_2(x)$, 则对 F 中的任意多项式 $u_1(x), u_2(x)$, 有

$$f(x) \mid u_1(x)g_1(x)+u_2(x)g_2(x),$$

其中, 表达式 $u_1(x)g_1(x)+u_2(x)g_2(x)$ 叫做多项式 $g_1(x), g_2(x)$ 的组合.

这里给出性质 (2) 的证明. 设 $f(x) \mid g(x)$ 和 $g(x) \mid f(x)$ 同时成立. 易知 $f(x)=0$ 当且仅当 $g(x)=0$.此时任取 $c \in F, c \neq 0$, 即有 $f(x)=cg(x)$. 今设 $f(x), g(x)$ 均非 0, 因 $f(x) \mid g(x)$, 有 $u(x) \in F[x]$, 使 $g(x)=u(x)f(x)$. 同样由 $g(x) \mid f(x)$, 知有 $v(x) \in F[x]$, 使 $f(x)=v(x)g(x)$. 这样一来,$g(x)=u(x)v(x)g(x)$. 因 $g(x) \neq 0$, 比较次数知,$\partial^0(u(x)v(x))=0$. 因此 $u(x), v(x)$ 均为 F 的非零元. 设 $v(x)=c, c \neq 0$. 对此 c,$f(x)=cg(x)$ 成立. 性质 (2) 得证.

给定 $f(x), g(x), g(x) \neq 0$, $g(x)$ 不一定能整除 $f(x)$. 有下列定理:

定理 2 设 $f(x), g(x)$ 为数域 F 上的两个多项式, 其中 $g(x) \neq 0$, 则有 F 上的多项式 $q(x)$ 和 $r(x)$, 满足

$$\begin{cases} f(x)=q(x)g(x)+r(x), \\ r(x)=0, \quad 或 \quad \partial^0 r(x) < \partial^0 g(x), \end{cases} \tag{5}$$

并且满足上述条件的 $q(x)$,$r(x)$ 由 $f(x), g(x)$ 唯一确定.

证明 如果 $g(x)$ 是零次的, 那么 $q(x), r(x)$ 的存在性是明显的. 以下假设 $g(x)$ 的次数 m 为正数. 于是可设 $f(x), g(x)$ 就是由 (1)(2) 两式所给出的多项式, 其中 $b_m \neq 0$. 先证明 $q(x)$ 和 $r(x)$ 的存在性.

如果 $n<m$, 令 $q(x)=0, r(x)=f(x)$, 则它们满足 (5) 中条件.

今设 $n=\partial^0 f(x) \geqslant m$, 对 n 用归纳法. 设对 $g(x)$ 和 $F[x]$ 中次数小于 n 的一切多项式, 如 $q(x)$,$r(x)$ 那样的满足条件 (5) 的多项式是存在的. 作多项式

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

由于 $f(x), g(x) \in F[x]$, 且 $a_n b_m^{-1} \in F$, 上面的 $f_1(x)$ 在 $F[x]$ 内. 又 $f(x)$ 与 $a_n b_m^{-1} x^{n-m} g(x)$ 都是 n 次多项式,而且首项系数相同. 因而 $f_1(x)$ 的次数小于 n.

由归纳法假设知, 有 $q_1(x), r_1(x) \in F[x]$, 使

$$\begin{cases} f_1(x) = q_1(x)g(x) + r_1(x), \\ r_1(x) = 0, \quad 或 \quad \partial^0 r_1(x) < \partial^0 g(x). \end{cases}$$

令

$$q(x) = a_n b_m^{-1} x^{n-m} + q_1(x),$$
$$r(x) = r_1(x).$$

显然, $r(x) \in F[x]$. 因为 $a_n b_m^{-1} \in F$, 故 $q(x) \in F[x]$. 此时即有

$$\begin{cases} f(x) = q(x)g(x) + r(x), \\ r(x) = 0, \quad 或 \quad \partial^0 r(x) < \partial^0 g(x). \end{cases}$$

说明 $q(x), r(x)$ 符合条件 (5) 的要求.

再证 $q(x), r(x)$ 的唯一性. 设又有 $q'(x), r'(x) \in F[x]$, 也满足

$$\begin{cases} f(x) = q'(x)g(x) + r'(x), \\ r'(x) = 0, \quad 或 \quad \partial^0 r'(x) < \partial^0 g(x). \end{cases}$$

比较 $f(x)$ 的两个表达式, 有

$$(q(x) - q'(x))g(x) = r'(x) - r(x). \tag{6}$$

若 $r'(x) \neq r(x)$, 则 $r'(x) - r(x) \neq 0$. 这样一来 (6) 式左端的次数不小于 $\partial^0 g(x)$, 而右端次数

$$\partial^0(r'(x) - r(x)) \leqslant \max\{\partial^0 r'(x), \partial^0 r(x)\} < \partial^0 g(x),$$

这是不可能的.

于是 $r'(x) = r(x)$, 进而 $q'(x) = q(x)$. 唯一性得证. □

定理 2 中的满足条件 (5) 的 $q(x)$ 称为 $g(x)$ 除 $f(x)$ 的**商式**, 而 $r(x)$ 称为 $g(x)$ 除 $f(x)$ 的**余式**. 已知 $f(x), g(x)$ 求 $q(x), r(x)$ 的这种运算称为**带余除法**.

推论 1 $g(x) \neq 0$ 时, $g(x) \mid f(x)$ 当且仅当 $g(x)$ 除 $f(x)$ 的余式为 0.

例 2 带余除法可按下面的格式进行: 用 $g(x)$ 除 $f(x)$, 求商式和余式, 其中

$$f(x) = 4x^4 + 3x^3 - x^2 + x + 5; \quad g(x) = 2x^2 - x + 1.$$

$$
\begin{array}{r|l}
 & 2x^2+\frac{5}{2}x-\frac{1}{4} \\
2x^2-x+1 & 4x^4+3x^3-x^2+x+5 \\
 & 4x^4-2x^3+2x^2 \\
\hline
 & 5x^3-3x^2+x \\
 & 5x^3-\frac{5}{2}x^2+\frac{5}{2}x \\
\hline
 & -\frac{1}{2}x^2-\frac{3}{2}x+5 \\
 & -\frac{1}{2}x^2+\frac{1}{4}x-\frac{1}{4} \\
\hline
 & -\frac{7}{4}x+\frac{21}{4}
\end{array}
$$

计算结果为: 商式为 $q(x)=2x^2+\frac{5}{2}x-\frac{1}{4}$; 余式为 $r(x)=-\frac{7}{4}x+\frac{21}{4}$. □

读者对带余除法可能并不陌生, 小学时就学过正整数的带余除法. 下面将看到, 正是带余除法成为多项式因式分解理论的起点.

§1.3 最大公因式

设 $f(x),g(x)$ 都是 $F[x]$ 内的多项式, 若有 $d(x)\in F[x]$, 使 $d(x)\mid f(x)$ 且 $d(x)\mid g(x)$, 则说 $d(x)$ 为 $f(x),g(x)$ 的公因式.

定义 6 设 $f(x),g(x)$ 都是 $F[x]$ 内的多项式, 若 $d(x)\in F[x]$, 满足:

(1) $d(x)$ 为 $f(x),g(x)$ 的公因式;

(2) 只要 $e(x)$ 为 $f(x),g(x)$ 的公因式, 则 $e(x)\mid d(x)$,

则称 $d(x)$ 为 $f(x),g(x)$ 的最大公因式.

注意, 在小学算术中, 把正整数 n,m 的最大公因子理解为 n 和 m 的绝对值最大的公因子. 按同样的思路,$f(x),g(x)$ 的最大公因式似应定义成 $f(x),g(x)$ 的次数最高的公因式. 但按现在的定义, 最大公因式不但必须是次数最高的公因式, 而且还必须是所有公因式的共同倍式. 于是这样的最大公因式的存在性就不是明显的了. 相反, 这样的最大公因式在如下意义下是唯一的.

命题 1 若 $d_1(x),d_2(x)$ 都是 $f(x),g(x)$ 的最大公因式, 则它们只差一个非零的常数倍, 即有非零元 $c\in F$, 使 $d_1(x)=cd_2(x)$.

证明 $d_1(x), d_2(x)$ 都满足定义 6 中 (1), (2) 两个条件. 由于 $d_1(x)$ 满足条件 (1),$d_2(x)$ 满足条件 (2), 则有 $d_1(x) \mid d_2(x)$. 同样, 由于 $d_2(x)$ 满足条件 (1),$d_1(x)$ 满足条件 (2), 又有 $d_2(x) \mid d_1(x)$. 于是命题得证. □

下面来证明最大公因式是存在的.

定理 3 *设 $f(x), g(x)$ 为数域 F 上的两个多项式, 则 $f(x), g(x)$ 在 $F[x]$ 内有最大公因式.*

证明 首先注意, 若 $g(x) \mid f(x)$, 则 $g(x)$ 满足定义 6 中 (1), (2) 两个条件, 因而是 $f(x), g(x)$ 的最大公因式. 同样 $f(x) \mid g(x)$ 时,$f(x)$ 为最大公因式. 特别,$f(x), g(x)$ 中有一个为零多项式时, 另一个就是最大公因式.$f(x), g(x)$ 中有一个是零次多项式时, 它就是最大公因式.

今设 $f(x), g(x)$ 均为非零多项式, 并且次数均大于 0.

设 $n = \partial^0 f(x), m = \partial^0 g(x)$, 并设 $n \geqslant m$.

用 $g(x)$ 去除 $f(x)$, 若 $g(x) \mid f(x)$, 则 $g(x)$ 为最大公因式. 不然, 有 $q_1(x), r_1(x) \in F[x]$, 使

$$f(x) = q_1(x)g(x) + r_1(x),$$
$$0 \leqslant \partial^0 r_1(x) < \partial^0 g(x).$$

再用 $r_1(x)$ 去除 $g(x)$, 得 $q_2(x), r_2(x) \in F[x]$, 使

$$g(x) = q_2(x)r_1(x) + r_2(x).$$

这里要么 $r_2(x) = 0$, 要么 $r_2(x) \neq 0, \partial^0 r_2(x) < \partial^0 r_1(x)$.

若 $r_2(x) \neq 0$, 则用 $r_2(x)$ 去除 $r_1(x)$, 有 $q_3(x), r_3(x) \in F[x]$, 使

$$r_1(x) = q_3(x)r_2(x) + r_3(x),$$
$$r_3(x) = 0, \quad \text{或} \quad \partial^0 r_3(x) < \partial^0 r_2(x).$$

继续这一过程, 由于按上面的步骤所得到的“余式” $r_1(x), r_2(x), r_3(x), \cdots$ 的次数越来越小, 这样的过程不会无休止的继续下去. 于是有正整数 $s \geqslant 2$, 使 $r_{s-1}(x) \neq 0$, 而 $r_s(x) = 0$. 这意味着, 当用 $r_{s-1}(x)$ 去除 $r_{s-2}(x)$ 时, 余式为 0. 这样一来, 就得到一串等式

$$\begin{aligned}
f(x) &= q_1(x)g(x) + r_1(x),\\
g(x) &= q_2(x)r_1(x) + r_2(x),\\
r_1(x) &= q_3(x)r_2(x) + r_3(x),\\
&\cdots\cdots\cdots\cdots\\
r_{s-4}(x) &= q_{s-2}(x)r_{s-3}(x) + r_{s-2}(x),\\
r_{s-3}(x) &= q_{s-1}(x)r_{s-2}(x) + r_{s-1}(x),\\
r_{s-2}(x) &= q_s(x)r_{s-1}(x).
\end{aligned} \tag{1}$$