

高等 学 校 教 材

# 高等代数 与解析几何

同济大学应用数学系 编



高等教育出版社  
HIGHER EDUCATION PRESS

## 内容提要

本书正文包括一元多项式、空间解析几何、矩阵代数、方阵的行列式、矩阵的秩与线性方程组、线性空间、线性变换与相似矩阵、 $\lambda$ -矩阵、内积空间、双线性函数与二次型等共十章。本书强调初等变换与初等矩阵的作用，引进了阶梯矩阵首元的概念，使得许多问题简单明了。我们力求做到内容由浅入深，由易及难，由具体到抽象。本书深广度适宜，结构严谨，文笔流畅，例题丰富且具代表性，便于教学。所配习题和补充题有利于学生巩固提高所学内容。

本书可作为一般普通高校数学系的本科一年级“高等代数与解析几何”课程的教材。

## 图书在版编目 (CIP) 数据

高等代数与解析几何/同济大学应用数学系编. —北

京: 高等教育出版社, 2005.5

ISBN 7-04-016627-5

I. 高... II. 同... III. ①高等代数-高等学校-教材②解析几何-高等学校-教材 IV. ①O15②O182

中国版本图书馆 CIP 数据核字(2005)第 036298 号

策划编辑 王 强      责任编辑 董达英      封面设计 于文燕  
责任绘图 郝 林      版式设计 范晓红      责任校对 朱惠芳  
责任印制 孔 源

---

出版发行 高等教育出版社  
社 址 北京市西城区德外大街 4 号  
邮政编码 100011  
总 机 010-58581000

经 销 北京蓝色畅想图书发行有限公司  
印 刷 北京铭成印刷有限公司

开 本 787 × 960 1/16  
印 张 24.75  
字 数 450 000

购书热线 010-58581118  
免费咨询 800-810-0598  
网 址 <http://www.hep.edu.cn>  
<http://www.hep.com.cn>  
网上订购 <http://www.landaco.com>  
<http://www.landaco.com.cn>

版 次 2005 年 5 月第 1 版  
印 次 2005 年 5 月第 1 次印刷  
定 价 25.90 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。

版权所有 侵权必究

物料号 16627-00

# 前 言

高等代数与解析几何是数学与应用数学等专业的一门重要基础课程,对其基本知识和内容的掌握程度将直接影响到许多后继课程(如抽象代数、微分方程等)的学习。作为体现教学内容和教学方法的知识载体,教材对教学效果起着重要作用。本书编写时遵循了以下原则:

1. 由浅入深,由易及难,由具体到抽象,注意与中学内容的衔接。对不少学生来说,由中学升到大学是一次大的跳跃,很多一年级的学生还需要一个调整适应期。其中大学与中学在教材的处理、教学方式和学习方式的差异是重要原因。因此,我们首先讲授中学生较为熟悉的一元多项式,空间解析几何,而将较抽象的行列式放在了稍后的位置。

2. 充分体现解析几何与高等代数的内在联系,以简单而具体的几何例子引出抽象的代数概念,反过来再以代数工具来解决几何问题。为了保持解析几何的完整性,我们在第二章讲授空间解析几何的基本内容,但有些几何内容我们穿插在代数的相关章节中处理。比如:三个平面的位置关系安插在方程组一节,用矩阵的秩以及方程组解的理论讨论;二次曲面分类放在正交变换与二次型的标准形部分讲授。

3. 特别强调行初等变换和初等矩阵的作用,引入了阶梯形矩阵首元(素)的概念。教学实践证明,初等矩阵作用强大,首元(素)简单明了,学生更易于接受掌握。

4. 强调理论的应用,在相关章节介绍了一些实用的例子。比如:在讲授多项式与线性空间的基变换时,介绍了常用的拉格朗日插值公式;结合施密特正交化方法,介绍了矩阵的正交三角分解;通过半正定矩阵可以相似于对角矩阵,引入了矩阵的奇异值分解与广义逆等等。这些内容都是十分有用的。

5. 增加了介绍 Mathematica 和 MATLAB 数学软件中有关代数与几何运算操作命令的两个附录。随着计算机及其软件的发展,很多高等代数与解析几何中的计算问题都可以通过相关的软件利用计算机来实现。Mathematica 不仅可以提供精确的计算结果,甚至可以进行符号运算;而 MATLAB 虽主要只提供近似的计算结果,但具有强大的绘图功能。在学好本课程的基本理论和方法的同时,掌握一些现代的工具是有益的。

本书每节都配备了适量的习题,每章末附有一定量的补充题。对立志从事

数学研究和准备攻读研究生的同学,做完全部习题是相当有益的。

本书不仅可以作为普通高校数学与应用数学专业高等代数与解析几何课程一学年的教材(根据我们的实践,每周五学时(包括习题课及上机实习)可以完成全部教学内容),也可用作对数学要求较高的某些理工科专业(如理论物理,计算机及软件)本科生线性代数课程及硕士研究生矩阵论课程的教材或教学参考书。(同济大学在计算机软件专业的强数学基础试点班上,试用过本教材,效果不错。)

本书是在刘昌堃,叶世源,叶家琛,陈承东编《高等代数》(同济大学出版社,1995年)的基础上修改扩充而成的。由靳全勤策划,陈承东、蒋志洪、靳全勤、叶家琛参加了本书的修改编写工作。很多老师如陈猛、兰辉等试用过本教材,并提出了很好的建议,陈猛还曾编写过解析几何部分的初稿,在此深表谢意。我们要感谢同济大学应用数学系的领导及老师对教材编写及出版工作的关心,也要感谢高等教育出版社的徐刚和王强为本书的出版所付出的辛勤劳动。使用过本书原稿的许多老师、同学曾提出过许多宝贵建议,在此一并致谢。

本书作为同济大学“十五”规划教材,得到了“同济大学教材、学术著作出版基金委员会”的资助。

作者

2005年1月

于上海·同济园

# 目 录

<b>第一章 一元多项式</b> .....	1
§ 1.1 一元多项式 .....	1
习题 1.1 .....	4
§ 1.2 多项式的最高公因式 .....	4
习题 1.2 .....	8
§ 1.3 因式分解与唯一性定理 .....	9
习题 1.3 .....	13
§ 1.4 复系数、实系数、有理系数多项式 .....	14
习题 1.4 .....	20
补充题 .....	21
<b>第二章 空间解析几何</b> .....	23
§ 2.1 坐标系、三维向量 .....	23
习题 2.1 .....	29
§ 2.2 向量的数量积、向量积、混合积 .....	29
习题 2.2 .....	36
§ 2.3 平面、直线方程, 平面束 .....	37
习题 2.3 .....	40
§ 2.4 点、直线、平面之间的位置关系 .....	41
习题 2.4 .....	48
§ 2.5 柱面、锥面、旋转面、空间曲线在坐标面上的投影 .....	50
习题 2.5 .....	53
§ 2.6 二次曲面、直纹面 .....	55
习题 2.6 .....	58
补充题 .....	59
<b>第三章 矩阵代数</b> .....	61
§ 3.1 矩阵及其运算 .....	61
习题 3.1 .....	67
§ 3.2 矩阵的分块与初等方阵 .....	69
习题 3.2 .....	74

§ 3.3 矩阵的逆 .....	75
习题 3.3 .....	84
§ 3.4 线性方程组 .....	87
习题 3.4 .....	93
补充题 .....	93
<b>第四章 方阵的行列式</b> .....	<b>95</b>
§ 4.1 行列式的定义 .....	95
习题 4.1 .....	99
§ 4.2 行列式的性质 .....	100
习题 4.2 .....	108
§ 4.3 行列式展开 .....	109
习题 4.3 .....	118
§ 4.4 用行列式求 $A^{-1}$ 与 Cramer (克拉默) 法则 .....	120
习题 4.4 .....	124
补充题 .....	125
<b>第五章 矩阵的秩与线性方程组</b> .....	<b>127</b>
§ 5.1 向量组的线性相关性 .....	127
习题 5.1 .....	132
§ 5.2 向量组的秩 .....	134
习题 5.2 .....	138
§ 5.3 矩阵的秩 .....	138
习题 5.3 .....	149
§ 5.4 线性方程组解的结构 .....	150
习题 5.4 .....	157
补充题 .....	160
<b>第六章 线性空间</b> .....	<b>163</b>
§ 6.1 线性空间的定义与简单性质 .....	163
习题 6.1 .....	166
§ 6.2 子空间 .....	167
习题 6.2 .....	169
§ 6.3 生成元集、线性相关性、基与维数 .....	170
习题 6.3 .....	178
§ 6.4 基变换与坐标变换 .....	179
习题 6.4 .....	182

§ 6.5 子空间的直和 .....	182
习题 6.5 .....	185
§ 6.6 线性空间的同构 .....	185
习题 6.6 .....	186
§ 6.7 线性函数与对偶空间 .....	187
习题 6.7 .....	190
补充题 .....	190
<b>第七章 线性变换与相似矩阵</b> .....	<b>192</b>
§ 7.1 线性变换的定义与性质 .....	192
习题 7.1 .....	199
§ 7.2 线性变换的矩阵与相似矩阵 .....	201
习题 7.2 .....	209
§ 7.3 特征值与特征向量 .....	211
习题 7.3 .....	219
§ 7.4 可对角化条件 .....	221
习题 7.4 .....	231
§ 7.5 不变子空间与根空间分解 .....	232
习题 7.5 .....	240
补充题 .....	241
<b>第八章 <math>\lambda</math>-矩阵</b> .....	<b>243</b>
§ 8.1 $\lambda$ -矩阵及其标准形 .....	243
习题 8.1 .....	252
§ 8.2 $\lambda$ -矩阵的余式定理 .....	254
习题 8.2 .....	259
§ 8.3 初等因子 .....	260
习题 8.3 .....	263
§ 8.4 若尔当标准形 .....	264
习题 8.4 .....	271
补充题 .....	271
<b>第九章 内积空间</b> .....	<b>273</b>
§ 9.1 内积空间的定义与基本性质 .....	273
习题 9.1 .....	277
§ 9.2 标准正交基与矩阵的 $QR$ 分解 .....	278
习题 9.2 .....	285

§ 9.3 正交子空间与最小二乘问题 .....	286
习题 9.3 .....	290
§ 9.4 保长同构与酉变换(正交变换) .....	290
习题 9.4 .....	294
§ 9.5 埃尔米特(实对称)矩阵与酉相似标准形 .....	294
习题 9.5 .....	302
§ 9.6 二次曲面分类、主轴问题 .....	303
习题 9.6 .....	309
补充题 .....	309
<b>第十章 双线性函数与二次型</b> .....	<b>311</b>
§ 10.1 双线性函数与二次型 .....	311
习题 10.1 .....	315
§ 10.2 化二次型为标准形 .....	315
习题 10.2 .....	320
§ 10.3 规范形与惯性定理 .....	321
习题 10.3 .....	324
§ 10.4 正定二次型与正定矩阵 .....	324
习题 10.4 .....	331
§ 10.5 矩阵的奇异值分解与广义逆 .....	332
习题 10.5 .....	339
补充题 .....	340
<b>附录一 补充知识</b> .....	<b>342</b>
§ A.1 集合 .....	342
习题 .....	343
§ A.2 映射 .....	344
习题 .....	347
§ A.3 等价关系 .....	347
习题 .....	349
§ A.4 群、环、域的定义与例子 .....	350
习题 .....	352
§ A.5 连加号 $\Sigma$ 与连乘号 $\Pi$ .....	352
习题 .....	354
<b>附录二 软件 Mathematica 中与高等代数有关的命令</b> .....	<b>355</b>
§ B.1 基本操作和数的计算 .....	355



---

§ B.2	矩阵的代数运算 .....	356
§ B.3	矩阵的初等行变换、线性方程组求解 .....	359
§ B.4	多项式代数 .....	361
§ B.5	方阵的特征值和特征向量、方阵的分解 .....	363
<b>附录三</b>	<b>软件 MATLAB 中与高等代数有关的命令 .....</b>	<b>368</b>
§ C.1	数的计算 .....	368
§ C.2	矩阵运算 .....	370
§ C.3	线性方程组求解 .....	373
§ C.4	方阵的特征值和特征向量 .....	374
§ C.5	方阵的分解 .....	376
§ C.6	符号运算 .....	380
	习题 .....	381
	<b>参考文献 .....</b>	<b>383</b>

# 第一章 一元多项式

多项式代数是高等代数课程中最基本的研究对象之一，它对于进一步学习代数学以及其他数学分支都有很重要的意义，本章将讨论数域上多项式代数的代数结构，整除性与因式分解理论。

## § 1.1 一元多项式

设  $F$  是数域，例如  $F = \mathbb{Q}$  (有理数域)， $\mathbb{R}$  (实数域) 或  $\mathbb{C}$  (复数域)， $x$  是一个变量(或者称为不定元)， $n$  是一个非负整数， $a_0, a_1, \dots, a_n \in F$ ，我们称

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (1.1.1)$$

为系数在数域  $F$  中的一元多项式，或简称为数域  $F$  上的一元多项式；数域  $F$  上的一元多项式全体组成的集合记为  $F[x]$ 。

在多项式(1.1.1)中， $a_i x^i$  称为  $i$  次项， $a_i$  称为  $i$  次项的系数，通常用  $f(x), g(x), \dots$ ，或简单地用  $f, g, \dots$  来表示多项式。

如果多项式  $f(x)$  与多项式  $g(x)$  的同次项的系数全相等，则称  $f(x)$  与  $g(x)$  相等，记为  $f(x) = g(x)$ 。系数全为零的多项式称为零多项式，记为  $0$ 。

在(1.1.1)式中，如果  $a_n \neq 0$ ，则  $a_n x^n$  称为多项式(1.1.1)的首项， $a_n$  称为首项系数， $n$  称为多项式(1.1.1)的次数。注意：我们规定零多项式的次数为  $-\infty$ 。多项式  $f(x)$  的次数记为  $\deg(f(x))$ 。

设

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

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0 = \sum_{j=0}^m b_j x^j.$$

定义加法为

$$f(x) + g(x) = \sum_{i=0}^{\max\{m, n\}} (a_i + b_i) x^i,$$

其中，当  $i > n$  时， $a_i = 0$ ；当  $i > m$  时， $b_i = 0$ 。

由加法的定义，显然有  $\deg(f(x) + g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\}$ 。

定义乘法为

$$f(x)g(x) = \sum_{s=0}^{m+n} \left( \sum_{i+j=s} a_i b_j \right) x^s.$$

由乘法的定义容易看出, 如果  $f(x) \neq 0$ ,  $g(x) \neq 0$ , 则  $f(x)g(x) \neq 0$ , 并且

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

容易验证: 对于上面定义的多项式加法 “+” 和乘法 “ $\cdot$ ”,  $(\mathbb{F}[x], +, \cdot)$  构成了一个具有单位元的交换环(关于环的定义请参考后面的附录中的 § A.4), 因此我们也称  $\mathbb{F}[x]$  为多项式环.

下面我们讨论多项式的带余除法, 它是  $\mathbb{F}[x]$  的一个基本性质.

**定理 1.1.1 (带余除法)** 设  $f(x), g(x) \in \mathbb{F}[x]$ , 其中  $g(x) \neq 0$ , 则一定存在唯一的  $q(x), r(x) \in \mathbb{F}[x]$ , 使

$$f(x) = q(x)g(x) + r(x) \quad (1.1.2)$$

成立, 其中  $\deg(r(x)) < \deg(g(x))$ , 或者  $r(x) = 0$ .

**证明** (1.1.2) 式中  $q(x)$  与  $r(x)$  的存在性可以对  $\deg(f(x))$  进行数学归纳来完成, 我们把它留给读者自己来完成.

下面证明唯一性, 设如果另有  $q'(x), r'(x) \in \mathbb{F}[x]$ , 使

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

成立, 其中  $\deg(r'(x)) < \deg(g(x))$  或者  $r'(x) = 0$ . 于是

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

所以

$$(q(x) - q'(x))g(x) = r'(x) - r(x).$$

如果  $q(x) \neq q'(x)$ , 又因为  $g(x) \neq 0$ , 则  $r'(x) - r(x) \neq 0$ , 并且

$$\deg(r'(x) - r(x)) = \deg(q(x) - q'(x)) + \deg(g(x)) \geq \deg(g(x)).$$

这一矛盾证明了  $q(x) = q'(x)$ , 从而  $r'(x) = r(x)$ . ■

带余除法中所得的  $q(x)$  称为  $g(x)$  除  $f(x)$  的商, 称  $r(x)$  为  $g(x)$  除  $f(x)$  的余式.

**例 1.1.2** 设  $f(x) = x^4 + 3x^3 - x^2 - 4x - 3$ ,  $g(x) = 3x^3 + 10x^2 + 2x - 3$ , 用  $g(x)$  除  $f(x)$ , 求商  $q(x)$  与余式  $r(x)$ .

**解** 立算式

$$\begin{array}{r|rrrrr}
 & \frac{1}{3}x & & & & \\
 & -\frac{1}{9} & & & & \\
 \hline
 3x^3 + 10x^2 + 2x - 3 & x^4 & + 3x^3 & - x^2 & - 4x & - 3 \\
 & x^4 & + \frac{10}{3}x^3 & + \frac{2}{3}x^2 & - x & \\
 \hline
 & & -\frac{1}{3}x^3 & - \frac{5}{3}x^2 & - 3x & - 3 \\
 & & -\frac{1}{3}x^3 & - \frac{10}{9}x^2 & - \frac{2}{9}x & + \frac{1}{3} \\
 \hline
 & & & -\frac{5}{9}x^2 & - \frac{25}{9}x & - \frac{10}{3}
 \end{array}$$

用式子表示:

$$f(x) = \left(\frac{1}{3}x - \frac{1}{9}\right)g(x) + \left(-\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3}\right),$$

所以商  $q(x) = \frac{1}{3}x - \frac{1}{9}$ , 余式  $r(x) = -\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3}$ . ■

**定义 1.1.3** 设  $f(x), g(x) \in \mathbb{F}[x]$ , 如果存在  $h(x) \in \mathbb{F}[x]$ , 使得  $f(x) = g(x)h(x)$ , 则称  $g(x)$  整除  $f(x)$ , 用  $g(x) | f(x)$  表示  $g(x)$  整除  $f(x)$ , 用  $g(x) \nmid f(x)$  表示  $g(x)$  不整除  $f(x)$ , 并用  $\frac{f(x)}{g(x)}$  表示  $g(x)$  整除  $f(x)$  的商. 特别当  $g(x) | f(x)$  时,  $g(x)$  称为  $f(x)$  的因式,  $f(x)$  称为  $g(x)$  的倍式.

下面我们用带余除法给出整除的一个判别法:

**定理 1.1.4** 设  $f(x), g(x) \in \mathbb{F}[x]$ , 其中  $g(x) \neq 0$ , 则  $g(x)$  整除  $f(x)$  的充分必要条件是  $g(x)$  除  $f(x)$  的余式为 0.

**证明** 如果  $r(x) = 0$ , 则  $f(x) = q(x)g(x)$ , 即  $g(x) | f(x)$ . 反过来, 如果  $g(x) | f(x)$ , 则存在  $q(x) \in \mathbb{F}[x]$ , 使得  $f(x) = q(x)g(x) = q(x)g(x) + 0$ , 即  $r(x) = 0$ . ■

下面叙述整除的几个常用的性质:

**性质 1.1.1** 设  $f(x) \in \mathbb{F}[x]$ ,  $a \in \mathbb{F}$ , 并且  $a \neq 0$ , 则

$$f(x) | f(x), \quad f(x) | 0, \quad a | f(x).$$

**性质 1.1.2** 设  $f(x), g(x) \in \mathbb{F}[x]$ ,  $f(x) | g(x)$  并且  $g(x) | f(x)$ , 则存在  $c \in \mathbb{F}$ ,  $c \neq 0$ , 使得  $f(x) = cg(x)$ .

**证明** 由于  $f(x) | g(x)$ ,  $g(x) | f(x)$ , 所以存在  $h_1(x), h_2(x) \in \mathbb{F}[x]$ , 使得

$$g(x) = h_1(x)f(x), \quad f(x) = h_2(x)g(x),$$

于是

$$f(x) = h_2(x)h_1(x)f(x).$$

如果  $f(x) = 0$ , 则  $g(x) = 0$ , 结论成立. 如果  $f(x) \neq 0$ , 则由

$$f(x)(h_2(x)h_1(x) - 1) = 0$$

可得

$$h_1(x)h_2(x) = 1,$$

从而

$$\deg(h_1(x)) + \deg(h_2(x)) = 0.$$

由此即得  $\deg(h_1(x)) = 0$ ,  $\deg(h_2(x)) = 0$ . 这就是说  $h_1(x)$  是一个非零常数  $c$ . ■

**性质 1.1.3** 设  $f(x), g(x), h(x) \in \mathbb{F}[x]$ . 如果  $f(x) | g(x)$ ,  $g(x) | h(x)$ , 则  $f(x) | h(x)$ .

**证明** 因为  $g(x) = g_1(x)f(x)$ ,  $h(x) = h_1(x)g(x)$ , 所以

$$h(x) = h_1(x)g_1(x)f(x). \quad \blacksquare$$

**性质 1.1.4** 设  $f(x), g_1(x), \dots, g_r(x) \in \mathbb{F}[x]$ . 如果  $f(x) \mid g_i(x)$ ,  $i = 1, 2, \dots, r$ , 则对任意的  $u_1(x), u_2(x), \dots, u_r(x) \in \mathbb{F}[x]$ ,

$$f(x) \mid (u_1(x)g_1(x) + \dots + u_r(x)g_r(x)).$$

**证明** 由  $g_i(x) = h_i(x)f(x)$ ,  $i = 1, 2, \dots, r$ , 得

$$\begin{aligned} u_1(x)g_1(x) + u_2(x)g_2(x) + \dots + u_r(x)g_r(x) \\ = [u_1(x)h_1(x) + u_2(x)h_2(x) + \dots + u_r(x)h_r(x)]f(x), \end{aligned}$$

其中  $h_1(x), h_2(x), \dots, h_r(x) \in \mathbb{F}[x]$ .  $\blacksquare$

根据性质 1.1.2, 在讨论多项式与整除性相关的问题时, 常常可以假定多项式的首项系数是 1 (通常称这样的多项式为首 1 多项式).

最后我们要指出的是两个多项式之间的整除关系不会因为系数域  $\mathbb{F}$  的扩大而改变. 例如:  $f(x), g(x) \in \mathbb{R}[x]$ , 则  $f(x), g(x) \in \mathbb{C}[x]$ . 如果  $f(x)$  在  $\mathbb{C}[x]$  中整除  $g(x)$ , 则  $f(x)$  在  $\mathbb{R}[x]$  中也整除  $g(x)$ .

## 习题 1.1

**习题 1.1.1** 用  $g(x)$  除  $f(x)$ , 求商  $q(x)$  与余式  $r(x)$

(1)  $f(x) = x^3 - 3x^2 - x - 1$ ,  $g(x) = 3x^2 - 2x + 1$ ;

(2)  $f(x) = x^4 - 2x + 5$ ,  $g(x) = x^2 - x + 2$ .

**习题 1.1.2**  $m, p, q$  适合什么条件时, 有下式成立?

(1)  $x^2 + mx - 1 \mid x^3 + px + q$ ;

(2)  $x^2 + mx + 1 \mid x^4 + px^2 + q$ .

**习题 1.1.3** 证明: 在域  $\mathbb{F}$  上,  $x^d - 1 \mid x^n - 1$ , 当且仅当  $d \mid n$  成立.

## § 1.2 多项式的最高公因式

如果多项式  $\varphi(x)$  既是  $f(x)$  的因式, 又是  $g(x)$  的因式, 那么  $\varphi(x)$  称为  $f(x)$  与  $g(x)$  的一个公因式, 我们最感兴趣的自然是所谓的最高公因式.

**定义 1.2.1** 设  $f(x), g(x), d(x) \in \mathbb{F}[x]$ , 如果满足条件:

(1)  $d(x)$  是  $f(x)$  与  $g(x)$  的公因式;

(2)  $f(x)$  与  $g(x)$  的公因式都是  $d(x)$  的因式,

则称  $d(x)$  为  $f(x), g(x)$  的一个最高公因式.

例如, 对任意的  $f(x) \in \mathbb{F}[x]$ ,  $f(x)$  是  $f(x)$  与 0 的一个最高公因式. 特别, 两个零多项式的最高公因式是 0.

下面我们解决最高公因式的存在性问题.

**定理 1.2.2** 对任意  $f(x), g(x) \in \mathbb{F}[x]$ , 存在最高公因式  $d(x) \in \mathbb{F}[x]$ , 而且存在  $u(x), v(x) \in \mathbb{F}[x]$  使得

$$d(x) = u(x)f(x) + v(x)g(x).$$

**证明** 如果  $f(x), g(x)$  有一个为 0, 例如  $g(x) = 0$ , 则  $f(x)$  就是一个最高公因式, 而且

$$f(x) = 1 \cdot f(x) + 1 \cdot 0.$$

对于一般情形, 不妨设  $g(x) \neq 0$ . 按带余除法, 用  $g(x)$  除  $f(x)$ , 得到商  $q_1(x)$ , 余式  $r_1(x)$ ; 如果  $r_1(x) \neq 0$ , 再用  $r_1(x)$  除  $g(x)$ , 得到商  $q_2(x)$ , 余式  $r_2(x)$ ; 又如果  $r_2(x) \neq 0$ , 用  $r_2(x)$  除  $r_1(x)$ , 得到商  $q_3(x)$ , 余式  $r_3(x)$ ; 如此辗转相除下去, 显然所得的余式的次数不断降低, 即

$$\deg(g(x)) > \deg(r_1(x)) > \deg(r_2(x)) > \cdots,$$

因此, 在有限次以后, 必然使余式为 0, 于是, 我们得到了一串等式:

$$\begin{aligned} f(x) &= q_1(x)g(x) + r_1(x), \\ g(x) &= q_2(x)r_1(x) + r_2(x), \\ r_1(x) &= q_3(x)r_2(x) + r_3(x), \\ &\dots\dots \\ r_{s-2}(x) &= q_s(x)r_{s-1}(x) + r_s(x), \\ r_{s-1}(x) &= q_{s+1}(x)r_s(x) + 0. \end{aligned} \tag{1.2.1}$$

根据习题 1.2.7,  $f(x), g(x)$  与  $g(x), r_1(x)$  有相同的公因式,  $g(x), r_1(x)$  与  $r_1(x), r_2(x)$  有相同的公因式,  $\cdots, r_{s-2}(x), r_{s-1}(x)$  与  $r_{s-1}(x), r_s(x)$  有相同的公因式,  $r_{s-1}(x), r_s(x)$  与  $r_s(x), 0$  有相同的公因式, 但是  $r_s(x)$  与 0 的最高公因式是  $r_s(x)$ , 由此推出  $r_s(x)$  是  $f(x)$  与  $g(x)$  的一个最高公因式.

由(1.2.1)的倒数第二个等式, 有

$$r_s(x) = r_{s-1}(x) - q_s(x)r_{s-1}(x),$$

再由(1.2.1)的倒数第三式,  $r_{s-1}(x) = r_{s-3}(x) - q_{s-1}(x)r_{s-2}(x)$ , 代入上式可以消去  $r_{s-1}(x)$ , 得到

$$r_s(x) = (1 + q_s(x)q_{s-1}(x))r_{s-2}(x) - q_s(x)r_{s-3}(x).$$

根据同样的方法用它上面的等式逐个地消去  $r_{s-2}(x), \cdots, r_1(x)$ , 再并项就得

$$r_s(x) = u(x)f(x) + v(x)g(x). \quad \blacksquare$$

由最高公因式的定义和性质 1.1.2 可得, 两个多项式的最高公因式相差一个非零常数倍数, 所以两个多项式的首项系数是 1 的最高公因式是唯一确定的, 我们用

$$(f(x), g(x))$$

来表示 $f(x)$ 与 $g(x)$ 的首项系数是1的最高公因式. 定理1.2.2的证明给出了一个求最高公因式的方法: 辗转相除法.

**例 1.2.3** 设 $f(x) = x^4 + 3x^3 - x^2 - 4x - 3$ ,  $g(x) = 3x^3 + 10x^2 + 2x - 3$ . 求 $(f(x), g(x))$ , 并求 $u(x)$ ,  $v(x)$ 使得

$$(f(x), g(x)) = u(x)f(x) + v(x)g(x).$$

**解** 辗转相除法可按下面的格式来做:

	$g(x)$ $3x^3 + 10x^2 + 2x - 3$ $3x^3 + 15x^2 + 18x$	$f(x)$ $x^4 + 3x^3 - x^2 - 4x - 3$ $x^4 + \frac{10}{3}x^3 + \frac{2}{3}x^2 - x$	$\frac{1}{3}x - \frac{1}{9}$ $= q_1(x)$
$-\frac{27}{5}x + 9$ $= q_2(x)$	$-5x^2 - 16x - 3$ $-5x^2 - 25x - 30$	$-\frac{1}{3}x^3 - \frac{5}{3}x^2 - 3x - 3$ $-\frac{1}{3}x^3 - \frac{10}{9}x^2 - \frac{2}{9}x + \frac{1}{3}$	
	$r_2(x) = 9x + 27$	$r_1(x) = -\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3}$ $-\frac{5}{9}x^2 - \frac{5}{3}x$	$-\frac{5}{81}x - \frac{10}{81}$ $= q_3(x)$
		$-\frac{10}{9}x - \frac{10}{3}$ $-\frac{10}{9}x - \frac{10}{3}$	
			0

用等式写出来, 就是

$$\begin{aligned} f(x) &= \left(\frac{1}{3}x - \frac{1}{9}\right)g(x) + \left(-\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3}\right) \\ g(x) &= \left(-\frac{27}{5}x + 9\right)\left(-\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3}\right) + (9x + 27) \\ &\quad -\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3} = \left(-\frac{5}{81}x - \frac{10}{81}\right)(9x + 27), \end{aligned}$$

因此

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

而

$$\begin{aligned}
 9x + 27 &= g(x) - \left(-\frac{27}{5}x + 9\right) \left(-\frac{5}{9}x^2 - \frac{25}{9}x - \frac{10}{3}\right) \\
 &= g(x) - \left(-\frac{27}{5}x + 9\right) \left[f(x) - \left(\frac{1}{3}x - \frac{1}{9}\right)g(x)\right] \\
 &= \left(\frac{27}{5}x - 9\right)f(x) + \left[1 - \left(\frac{27}{5}x - 9\right)\left(\frac{1}{3}x - \frac{1}{9}\right)\right]g(x) \\
 &= \left(\frac{27}{5}x - 9\right)f(x) + \left(-\frac{9}{5}x^2 + \frac{18}{5}x\right)g(x),
 \end{aligned}$$

于是

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

**定义 1.2.4** 设  $f(x), g(x) \in \mathbb{F}[x]$ , 如果  $(f(x), g(x)) = 1$ , 则称  $f(x)$  与  $g(x)$  互素.

显然, 如果两个多项式互素, 则它们除去零次多项式外, 没有其他的公因式, 反之也对.

**定理 1.2.5**  $\mathbb{F}[x]$  中两个多项式  $f(x), g(x)$  互素的充分必要条件是在  $\mathbb{F}[x]$  中存在多项式  $u(x), v(x)$ , 使得

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

**证明** 必要性是定理 1.2.2 的直接推论.

现在证明充分性. 设存在  $u(x), v(x)$  使得

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

如果  $\varphi(x)$  是  $f(x)$  与  $g(x)$  的一个最高公因式, 于是  $\varphi(x) \mid f(x)$ ,  $\varphi(x) \mid g(x)$ , 由性质 1.1.4 推出  $\varphi(x) \mid 1$ , 即  $f(x)$  与  $g(x)$  互素. ■

**定理 1.2.6** 如果  $(f(x), g(x)) = 1$ , 并且  $f(x) \mid g(x)h(x)$ , 则  $f(x) \mid h(x)$ .

**证明** 由  $(f(x), g(x)) = 1$  可知, 存在  $u(x), v(x)$  使得

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

等式两边乘  $h(x)$ , 得到

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

由于  $f(x) \mid g(x)h(x)$ , 所以  $f(x)$  可整除上式, 从而  $f(x) \mid h(x)$ . ■

**推论 1.2.7** 如果  $f_1(x) \mid g(x)$ ,  $f_2(x) \mid g(x)$ , 并且  $(f_1(x), f_2(x)) = 1$ , 则  $f_1(x)f_2(x) \mid g(x)$ .

**证明** 由  $f_1(x) \mid g(x)$  推出

$$g(x) = f_1(x)h_1(x).$$

因为  $f_2(x) \mid f_1(x)h_1(x)$ , 并且  $(f_1(x), f_2(x)) = 1$ , 所以根据定理 1.2.6 知  $f_2(x) \mid h_1(x)$ , 即



$$h_1(x) = f_2(x)h_2(x).$$

代入上式即得

$$g(x) = f_1(x)f_2(x)h_2(x).$$

这就是说,

$$f_1(x)f_2(x) \mid g(x). \quad \blacksquare$$

到现在为止,关于最高公因式与互素的概念,都是对两个多项式定义的.事实上,对于任意有限个多项式 $f_1(x), f_2(x), \dots, f_s(x)$ , ( $s \geq 2$ ), 也可以同样定义(见习题 1.2.8 和习题 1.2.9). 最后我们还需要指出的是多项式互素是与系数数域无关的.

## 习题 1.2

**习题 1.2.1** 求 $f(x)$ 与 $g(x)$ 的最高公因式:

(1)  $f(x) = x^4 + x^3 - 3x^2 - 4x - 1, g(x) = x^3 + x^2 - x - 1;$

(2)  $f(x) = x^4 - 4x^3 + 1, g(x) = x^3 - 3x^2 + 1.$

**习题 1.2.2** 求 $u(x), v(x)$ 使得 $u(x)f(x) + v(x)g(x) = (f(x), g(x))$ .

(1)  $f(x) = x^4 + 2x^3 - x^2 - 4x - 2, g(x) = x^4 + x^3 - x^2 - 2x - 2;$

(2)  $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9, g(x) = 2x^3 - x^2 - 5x + 4.$

**习题 1.2.3** 证明: 如果 $d(x) \mid f(x), d(x) \mid g(x)$ 并且 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个组合(即 $d(x) = u(x)f(x) + v(x)g(x)$ ), 则 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最高公因式.

**习题 1.2.4** 设 $h(x)$ 是首 1 多项式, 证明:

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

**习题 1.2.5** 如果 $f(x), g(x)$ 不全为 0, 证明:

$$\left( \frac{f(x)}{(f(x), g(x))}, \frac{g(x)}{(f(x), g(x))} \right) = 1.$$

**习题 1.2.6** 证明: 如果 $f(x), g(x)$ 不全为 0, 且 $(f(x), g(x)) = u(x)f(x) + v(x)g(x)$ , 则 $(u(x), v(x)) = 1$ .

**习题 1.2.7** 证明: 如果等式 $f(x) = q(x)g(x) + r(x)$ 成立, 则 $f(x), g(x)$ 与 $g(x), r(x)$ 有相同的公因式.

**习题 1.2.8** 写出 $f_1(x), f_2(x), \dots, f_s(x)$ 的最高公因式的定义和 $f_1(x), f_2(x), \dots, f_s(x)$ 互素的定义.

**习题 1.2.9** 证明: 如果 $f_1(x), f_2(x), \dots, f_{s-1}(x)$ 的最高公因式存在, 则 $f_1(x), f_2(x), \dots, f_{s-1}(x), f_s(x)$ 的最高公因式也存在, 而且

$$(f_1(x), f_2(x), \dots, f_{s-1}(x), f_s(x)) = ((f_1(x), f_2(x), \dots, f_{s-1}(x)), f_s(x)),$$