新世纪高等学校规划教材 · 数学系列

高等代数

陈顺民　李金宝◎编著

GAODENG DAISHU

北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

新世纪高等学校规划教材·数学系列

重庆文理学院特色应用型教材建设资助

高等代数

陈顺民　李金宝◎编著

GAODENG DAISHU

北京师范大学出版集团
BEIJING NORMAL UNIVERSITY PUBLISHING GROUP
北京师范大学出版社

内容提要

本书是面向一般本科院校的高等代数课程教材，可作为数学与应用数学专业的教材，也可供其他理工科、经济类专业的教师和学生使用. 全书共分为九章，内容包括多项式、行列式、矩阵、线性方程组解的结构、相似矩阵、线性空间、线性变换、欧式空间、二次型. 根据学生的实际情况和教学要求，精心组织本书内容，既注重高等代数理论的系统性，又注重知识的实用性及知识的前后联系. 同时，本书每小节给出学习目标，合理安排学习内容，并通过针对性强、难度适当的例题和习题加强对基础知识的学习和训练，培养学生能力.

图书在版编目（CIP）数据

高等代数/陈顺民，李金宝编著. --北京：北京师范大学出版社，2017.8

新世纪高等学校规划教材. 数学系列

ISBN 978-7-303-22717-4

Ⅰ. ①高… Ⅱ. ①陈… ②李… Ⅲ. ①高等代数－高等学校－教材 Ⅳ. ①01

中国版本图书馆 CIP 数据核字(2017)第 210998 号

营销中心电话 010-62978190 62979006
北师大出版社科技与经管分社 www.jswsbook.com
电子信箱 jswsbook@163.com

出版发行：北京师范大学出版社 www.bnup.com
北京市海淀区新街口外大街 19 号
邮政编码：100875

印 刷：北京玺诚印务有限公司
经 销：全国新华书店
开 本：787 mm × 1092 mm 1/16
印 张：19.5
字 数：287 千字
版 次：2017 年 8 月第 1 版
印 次：2017 年 8 月第 1 次印刷
定 价：39.80 元

策划编辑：刘凤娟 责任编辑：刘凤娟
美术编辑：刘 超 装帧设计：刘 超
责任校对：赵非非 责任印制：赵非非

前言

《高等代数》是数学类各专业一门重要的基础课.《高等代数》教材作为保证和提高教学质量的重要支柱和基础，作为体现教学内容和教学方法的知识载体，在当前培养应用型人才中的作用是显而易见的. 大学教育已由精英教育转变为大众教育，而现有的《高等代数》教材主要是面对重点本科院校的学生编写的，这样的教材已不适合一般本科院校的学生. 因此，教材建设就显得十分重要. 本书是在总结作者多年高等代数教学实践的基础上，定位在一般本科院校数学类专业的教学要求，并吸取其他有关高等代数教材的优点，经过多次修改而成. 各章配有适量的、针对性强、应用性强、难度适当的例题和习题，本书适合理论课与习题课合二为一的一般本科院校教学班选用.

考虑到一般本科院校数学类专业培养的是应用型人才，在本书的编写过程中，我们在保证教材内容的科学性与完整性的前提下，删除或调整传统教材中的某些内容，合理的安排课程内容，注意前后知识的关联，并在各章节给出学习目标. 在内容的编排上，既注重代数学基础知识和代数学基本思想方法，突出矩阵、向量、方程组的基础工具性，又注重知识的运用，重视代数基本知识及代数基本方法的训练，重视培养学生的能力.

本书教学时数为 160 学时左右，带有“*”号的内容为选学内容. 对教学时数安排为 145 学时左右的教学班，可不讲结式、多元多项式、 Jordan 标准形的理论证明，也可不讲后 4 章中证明过程比较复杂、证明方法应用较少的一些定理的证明过程. 对教学时数较少的理工科、经济类专业的教学班，可不讲多项式、结式、线性空间、线性变换等内容，可根据专业需求简介 Jordan 标准形的内容及计算.

本书还具有以下几个特点.

1. 考虑到多项式的内容与中学知识的衔接紧密，且高等代数的后续内容要用到多项式的知识，我们将第 1 章安排为多项式. 在本章中，简化了多元多项式中对称多项式的内容，增强了根与系数的关系的例题与习题. 给出了多项式的知识及方法在多项式的因式分解上的应用.

2. 在行列式这一章中，重点体现行列式的主要计算方法及具体计算，对需用递推加归纳法计算的行列式只作简单体现；对克莱姆法则，采取了行列式和逆矩阵两种方法进行证明；保留了应用性较强的两多项式的结式内容；去掉了行列式的拉普拉斯定理(矩阵乘积的行列式定理用行列式的性质证明).

3. 在矩阵及线性方程组解的结构这两章中，强调了矩阵初等变换的突出作用；突出了矩阵的行分块及列分块的作用及运用；加强了矩阵的秩及齐次线性方程组解结构的运用.

4. 将相似矩阵单独安排为一章，不与线性变换的对角化安排在一起，一是降低学生学习矩阵相似对角化、线性变换对角化的难度，二是便于其他数学类专业的教学和学习.

5. 在线性空间和线性变换中，通过恰当适量的例子加深学生对线性空间基本知识的理解，注重体现研究代数结构的基本思想方法. 涉及的概念及结论除特殊情况外，只要在前面章节出现，通常直接平移；有时，为了使学生熟悉线性变换的运用，仍以线性变换的形式给出相应的证明.

6. 以较少的篇幅给出了矩阵(线性变换)可准对角化的特殊情形，Jordan 标准形的理论推导和计算方法，因而去掉了 $\lambda-$ 矩阵的内容.

7. 二次型安排在最后一章，可使二次型的内容比较系统. 同时，增加了用代数方法研究几何图形的内容二次曲面的化简.

重庆文理学院对本书的出版给以资助，数学与财经学院的领导和代数教研室的同事们对本书的编写给予了大力的支持. 特别是施武杰教授对本书的编写给予了极大地指导和支持，余大鹏教授、龙述德教授提出了一些具体的修改意见. 在此我们一并表示衷心的感谢！

由于作者的水平有限，不当之处恳请读者提出宝贵的批评意见和建议，使本书不断得到完善. 来函邮件请发至 sminchen@126.com .

陈顺民　李金宝

2017 年 4 月

目 录

第一章　多项式

多项式是高等代数的重要组成部分，它不但与高次方程有关，而且是进一步学习代数及其他数学分支的基础. 本章系统地学习多项式的基本知识.

§1.1　数域

学习目标：(1) 能判定一个数集是否是数环、数域；

(2) 知道任何数域都包含有理数域.

我们过去熟悉的数集有：正整数集 $\mathbb{N}^*$, 自然数集 $\mathbb{N}$, 整数集 $\mathbb{Z}$, 有理数集 $\mathbb{Q}$, 实数集 $\mathbb{R}$, 复数集 $\mathbb{C}$. 本书中，我们固定使用上述符号.

在给定的数集中，我们常关心两个数的运算结果是否仍然在这个数集中. $\mathbb{Q}$ 中的任何两个数相加、减、乘、除（除数不为零）的结果都在 $\mathbb{Q}$ 中，我们称之为有理数集 $\mathbb{Q}$ 对这些运算封闭.

定义 1.1.1　设 $\boldsymbol{S}$ 是一个非空数集，若 $\boldsymbol{S}$ 中任意两个数作某种运算的结果仍在 $\boldsymbol{S}$ 中，则称 $\boldsymbol{S}$ 对该运算是封闭的.

定义 1.1.2　设 $\boldsymbol{S}$ 是一个非空数集，若 $\boldsymbol{S}$ 对数的加法、减法及乘法都是封闭的，则称 $\boldsymbol{S}$ 是一个 **数环**.

定义 1.1.3　设 $\boldsymbol{F}$ 是含有 0 和 1（或含有非零数）的数集. 若 $\boldsymbol{F}$ 对数的加法、减法、乘法及除法（除数不为 0）都是封闭的，则称 $\boldsymbol{F}$ 是一个 **数域**.

显然，数域是数环. $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ 都是数环， $\mathbb{Z}$ 常称为 **整数环** . $\mathbb{N}$ 不是数环. $\mathbb{Q},\mathbb{R},\mathbb{C}$ 是数域. $\mathbb{N},\mathbb{Z}$ 不是数域.

例 1.1.1　取定整数 a, 令 $\boldsymbol{S}=\{na\,|\,n\in\mathbb{Z}\}$, 则 $\boldsymbol{S}$ 是一个数环.

证明　任取 $na, ma\in\boldsymbol{S}$, 其中 $n,m\in\mathbb{Z}$, 有

$$na\pm ma=(n\pm m)a\in\boldsymbol{S},\ (na)(ma)=(nma)a\in\boldsymbol{S},$$

因此 $\boldsymbol{S}$ 是一个数环. □

特别地，当 $a=2$ 时， $\boldsymbol{S}$ 是全体偶数组成的数环，通常称之为 **偶数环** ；当 $a=0$ 时， $\boldsymbol{S}=\{0\}$ 是最小的数环. 当然，例 1.1.1 中的 $\boldsymbol{S}$ 对除法不封闭，$\boldsymbol{S}$ 不是一个数域.

例 1.1.2 证明： $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Q}\}$ 是一个数域.

证明 任取 $a+b\sqrt{2},c+d\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, 有

$$(a+b\sqrt{2})\pm(c+d\sqrt{2})=(a\pm c)+(b\pm d)\sqrt{2}\in\mathbb{Q}(\sqrt{2}),$$
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in\mathbb{Q}(\sqrt{2}),$$

从而 $\mathbb{Q}(\sqrt{2})$ 是一个数环.

显然， $0=0+0\times\sqrt{2}$, $1=1+0\times\sqrt{2}\in\mathbb{Q}(\sqrt{2})$. 任取 $0\neq c+d\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, 则 $c-d\sqrt{2}\neq 0$. 否则，当 $d=0$ 时， $c=0$, 从而 $c+d\sqrt{2}=0$, 矛盾；当 $d\neq 0$ 时， $\sqrt{2}=c/d\in\mathbb{Q}$, 矛盾. 因此，

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}=\frac{ac-2bd}{c^2-2d^2}+\frac{bc-ad}{c^2-2d^2}\sqrt{2}\in\mathbb{Q}(\sqrt{2}),$$

这就证明了 $\mathbb{Q}(\sqrt{2})$ 是一个数域. □

最后，我们证明数域的一个重要性质.

定理 1.1.1 任何数域都包含有理数域 $\mathbb{Q}$.

证明 设 $\boldsymbol{F}$ 是任意一个数域，由数域定义， $\boldsymbol{F}$ 含有数 0,1. 因 $\boldsymbol{F}$ 对加法封闭，知 $1+1,1+1+1,\cdots$ 均属于 $\boldsymbol{F}$, 即全体正整数属于 $\boldsymbol{F}$. 又因 $\boldsymbol{F}$ 对减法封闭，知对任意 $n\in\mathbb{N}^*$, 有 $-n=0-n\in\boldsymbol{F}$, 即任意负整数属于 $\boldsymbol{F}$, 这样，$\boldsymbol{F}$ 含有全体整数.

又任意一个有理数可表示为除数不为 0 的两个整数之商，所以由数域关于除法的封闭性，知 $\boldsymbol{F}$ 含有全体有理数. 因此，任何数域 $\boldsymbol{F}$ 都包含有理数域 $\mathbb{Q}$. □

习 题 1.1

1. 下列数集哪些是数域？哪些是数环？哪些既非数域也非数环？
   (1) 所有正实数组成的数集 $\mathbb{R}^+$;
   (2) $A=\{a+b\mathrm{i}\,|\,a,\ b\in\mathbb{Z},\ \mathrm{i}^2=-1\}$;
   (3) 所有奇数构成的数集 B ;
   (4) $\mathbb{Q}(\sqrt{p})=\{a+b\sqrt{p}\,|\,a,b\in\mathbb{Q}\}$, 其中 p 是素数.
2. 证明： $\boldsymbol{F}=\{a+b\mathrm{i}\,|\,a,b\in\mathbb{Q},\mathrm{i}^2=-1\}$ 是一个数域.
3. (1) 证明：两个数域的交是一个数域;
   (2) 两个数域的并是否是一个数域？并说明理由.

§1.2 一元多项式

学习目标: (1) 知道一元多项式的相关概念;
(2) 理解次数定理, 并能进行简单运用.

定义 1.2.1 数域 $\boldsymbol{F}$ 上的关于 x 的一元多项式是指表达式

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \tag{1.1}$$

其中 x 是一个文字 (符号), n 为非负整数, $a_0, a_1, \cdots, a_n \in \boldsymbol{F}$.

在多项式 (1.1) 中, 称 $\boldsymbol{a_i x^i}$ 为 **i 次项**, $\boldsymbol{a_i}$ 为 **i 次项的系数**, $\boldsymbol{a_0}$ 为 **零次项或常数项**. 我们可以在多项式中任意添上或去掉一些系数为 0 的项. 除常数项外的系数为 1 的项, 系数 1 省略不写. 以后常用 $f(x), g(x), \cdots$ 来表示一元多项式, 在不引起混淆的情况下, 也简记为 $f, g, \cdots$.

定义 1.2.2 若数域 $\boldsymbol{F}$ 上的两个多项式 $f(x)$ 与 $g(x)$ 的同次项系数都相等, 则称多项式 $f(x)$ 和 $g(x)$**相等**, 记为 $f(x) = g(x)$.

按照定义 1.2.2, 一个数域 $\boldsymbol{F}$ 上系数不全为零的多项式可以写成

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, a_n \neq 0 \tag{1.2}$$

的形式, 并且这种写法是唯一的. 又称

$$-f(x) = -a_n x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$$

为 $f(x)$ 的 **负多项式**.

我们称式 (1.2) 中的 $a_n x^n$ 为多项式 $f(x)$ 的 **首项**, a_n 为 **首项系数**(首项系数为 1 的多项式简称 **首 1 式**), n 为多项式 $f(x)$ 的 **次数**, 记为 $\deg(f(x)) = n$. 特别地, 对首项为零次项的多项式 $a(a \neq 0)$, 有 $\deg(a) = 0$; 而系数全为零的多项式称为 **零多项式**, 记为 0, 它是唯一不定义次数的多项式.

以后在谈到多项式 $f(x)$ 的次数时, 总假定 $f(x) \neq 0$.

定义 1.2.3 设

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

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

是数域 $\boldsymbol{F}$ 上两多项式, 不妨假定 $m \leqslant n$, 则定义

(1) $f(x)$ 与 $g(x)$ 的 **和(差)** 为

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

当 $m<n$ 时， $b_n=\cdots=b_{m+1}=0$.

(2) $f(x)$ 与 $g(x)$ 的 **乘积** 为

$$f(x)g(x)=\sum_{s=0}^{n+m}\Big(\sum_{i+j=s}a_ib_j\Big)x^s,$$

其中 s 次项的系数 $\sum\limits_{i+j=s}a_ib_j=a_sb_0+a_{s-1}b_1+\cdots+a_1b_{s-1}+a_0b_s$.

显然，数域 $\boldsymbol{F}$ 上的两个多项式的和、差、乘积为数域 $\boldsymbol{F}$ 上的多项式，且易验证多项式的加法和乘法满足下列运算律：

(1) 加法交换律： $f(x)+g(x)=g(x)+f(x)$；

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

(3) 乘法交换律： $f(x)g(x)=g(x)f(x)$；

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

(5) 乘法分配律： $f(x)\big(g(x)+h(x)\big)=f(x)g(x)+f(x)h(x)$.

对于如上定义的加法与乘法，数域 $\boldsymbol{F}$ 上的关于文字 x 的一元多项式全体构成数域 $\boldsymbol{F}$ 上的 **一元多项式环**, 记作 $\boldsymbol{F}[x]$, $\boldsymbol{F}$ 称为 $\boldsymbol{F}[x]$ 的 **系数域**.

多项式的次数在多项式理论中占有重要地位.

定理 1.2.1 设 $f(x), g(x)\in\boldsymbol{F}[x]$, 且 $f(x)\neq 0$, $g(x)\neq 0$, 则

(1) 当 $f(x)\pm g(x)\neq 0$ 时,

$$\deg\big(f(x)\pm g(x)\big)\leqslant\max\big\{\deg\big(f(x)\big),\deg\big(g(x)\big)\big\};$$

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

证明 因为 $f(x)\neq 0$, $g(x)\neq 0$, 所以可令

$$f(x)=\sum_{i=0}^{n}a_ix^i,\qquad g(x)=\sum_{j=0}^{m}b_jx^j,$$

其中 $a_n\neq 0$, $b_m\neq 0$, 于是 $\deg\big(f(x)\big)=n,\deg\big(g(x)\big)=m$. 不妨假定 $m\leqslant n$. 我们有

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

其中当 $m<n$ 时， $b_n=\cdots=b_{m+1}=0$.

由于 $f(x)\pm g(x)\neq 0$, 于是 $\deg\big(f(x)\pm g(x)\big)\leqslant n$.

因为 $a_n \neq 0$, $b_m \neq 0$, 所以 $f(x)g(x)$ 的首项系数 $a_nb_m \neq 0$, 于是

$$\deg\big(f(x)g(x)\big) = n + m. \qquad \square$$

推论 1.2.2 设 $f(x), g(x) \in \boldsymbol{F}[\boldsymbol{x}]$, 则 $f(x)g(x) = 0$ 当且仅当 $f(x) = 0$ 或 $g(x) = 0$.

证明 若 $f(x) = 0$ 或 $g(x) = 0$, 由多项式的乘法定义, 有 $f(x)g(x) = 0$. 反之, 若 $f(x) \neq 0$, 且 $g(x) \neq 0$, 由定理 1.2.1, 有 $f(x)g(x) \neq 0$. □

推论 1.2.3 (乘法消去律) 设 $f(x), g(x), h(x) \in \boldsymbol{F}[\boldsymbol{x}]$. 若 $f(x) \neq 0$, 且 $f(x)g(x) = f(x)h(x)$, 则 $g(x) = h(x)$.

证明 因为 $f(x)g(x) = f(x)h(x)$, 所以 $f(x)\big(g(x) - h(x)\big) = 0$, 由推论 1.2.2 及 $f(x) \neq 0$, 我们有 $g(x) - h(x) = 0$, 于是 $g(x) = h(x)$. □

例 1.2.1 若 $f(x), g(x), h(x) \in \mathbb{R}[x]$, 且 $f^2(x) = x\big(g^2(x) + h^2(x)\big)$, 证明: $f(x) = g(x) = h(x) = 0$. 试举出在 $\mathbb{C}$ 上结论不成立的例子.

证明 若 $f(x) \neq 0$, 则 $f^2(x) \neq 0$, $g^2(x) + h^2(x) \neq 0$, 于是 $\deg\big(f^2(x)\big)$, $\deg\big(g^2(x) + h^2(x)\big)$ 都为偶数, 根据定理 1.2.1, 知

$$\deg\big(x(g^2(x) + h^2(x))\big) = 1 + \deg\big(g^2(x) + h^2(x)\big)$$

为奇数, 矛盾. 因此, $f(x) = 0$, 于是

$$x\big(g^2(x) + h^2(x)\big) = 0, \ g^2(x) + h^2(x) = 0.$$

从而在实数域 $\mathbb{R}$ 上必有 $g^2(x) = h^2(x) = 0$, 所以 $g(x) = h(x) = 0$.

在复数域 $\mathbb{C}$ 上, 取 $f(x) = 0, g(x) = x, h(x) = \mathrm{i}x$, 它们满足

$$f^2(x) = x\big(g^2(x) + h^2(x)\big).$$

因此, 在复数域 $\mathbb{C}$ 上结论不成立. □

习 题 1.2

1. 计算数域 $\boldsymbol{F}$ 上多项式 $f(x)$ 与 $g(x)$ 的乘积, 其中
   $f(x) = x^7 + 2x^4 + 3x + 1, g(x) = 3x^2 + 2x + 4.$
2. 设 $f(x), g(x), h(x) \in \boldsymbol{F}[\boldsymbol{x}]$, 且 $f(x) = g(x)h(x)$, 其中
   $f(x) = x^4 - 5x^3 + 11x^2 + ax + b$, $g(x) = (x-1)^2$, 试确定 a, b.
3. 设 $f(x), g(x) \in \mathbb{R}[\boldsymbol{x}]$, 且 $f^2(x) + g^2(x) = 0$. 证明: $f(x) = g(x) = 0$.

§1.3 多项式的整除

学习目标: (1) 掌握两个多项式整除的概念及其性质;

(2) 能熟练地使用带余除法求商式与余式.

$\boldsymbol{F}[x]$ 中任意两个多项式的和、差、积仍然是 $\boldsymbol{F}[x]$ 中的一个多项式, 一元多项式环 $\boldsymbol{F}[x]$ 对于加法、减法和乘法是封闭的. 但是我们知道两个多项式相除(除式不为零多项式)不一定得到多项式. 因此, 关于多项式的整除性的研究, 在多项式的理论中占有重要的地位.

§1.3.1 多项式的整除

定义 1.3.1 令 $f(x), g(x) \in \boldsymbol{F}[x]$, 若存在 $q(x) \in \boldsymbol{F}[x]$, 使得

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

则称 $\boldsymbol{g(x)}$ **整除** $\boldsymbol{f(x)}$, 记作 $g(x)\big|f(x)$. 否则, 称 $\boldsymbol{g(x)}$ **不整除** $\boldsymbol{f(x)}$, 记作 $g(x) \nmid f(x)$. 当 $g(x)\big|f(x)$ 时, 称 $g(x)$ 是 $f(x)$ 的一个 **因式**, 反之称 $f(x)$ 是 $g(x)$ 的一个 **倍式**.

整除只是多项式间的一种关系而并非一种运算. 由定义 1.3.1, 易知零多项式 0 是任何多项式的倍式, 零多项式只能是零多项式的因式.

多项式的整除有如下的一些基本性质.

设 $f(x), g(x), h(x) \in \boldsymbol{F}[x]$, 则有

(1) 若 $f(x)\big|g(x), g(x)\big|h(x)$, 则 $f(x)\big|h(x)$.

(2) 若 $h(x)\big|f(x), h(x)\big|g(x)$, 则 $h(x)\big|\big(f(x) \pm g(x)\big)$.

(3) 若 $h(x)\big|f(x)$, 则 $h(x)\big|f(x)g(x)$.

(4) 若$f_i(x), g_i(x) \in\boldsymbol{F}[x]$, $h(x)\big|f_i(x)$, $i = 1, 2, \cdots, s$, 则 $h(x)\big|\sum\limits_{i=1}^{s} f_i(x)g_i(x)$.

(5) $c\big|f(x), f(x)\big|cf(x), cf(x)\big|f(x)$, 其中 $0 \neq c \in \boldsymbol{F}$.

(6) 若 $f(x)\big|g(x), g(x)\big|f(x)$, 则 $f(x) = cg(x)$, 其中 $0 \neq c \in \boldsymbol{F}$.

证明 这里我们只证明性质 (1) 和性质 (6), 其余证明留给读者去完成.

性质 (1): 由条件, 知存在 $u(x), v(x) \in \boldsymbol{F}[x]$, 使得 $g(x) = f(x)u(x)$, $h(x) = g(x)v(x)$, 于是 $h(x) = f(x)\big(u(x)v(x)\big)$, 即 $f(x)\big|h(x)$.

性质 (6): 由条件, 知存在 $u(x), v(x) \in \boldsymbol{F}[x]$, 使得

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

若 $f(x)=0$, 由 $g(x)=f(x)u(x)$, 有 $g(x)=0$, 于是 $f(x)=cg(x)$, 其中 c 可为任意一取定非零常数;

若 $f(x)\neq 0$, 由 $g(x)=f(x)u(x)$ 及 $f(x)=g(x)v(x)$, 有

$$f(x)=f(x)u(x)v(x),$$

于是由消去律有 $u(x)v(x)=1$, 从而 $\deg\big(u(x)\big)+\deg\big(v(x)\big)=0$, 这表明

$$\deg\big(u(x)\big)=\deg\big(v(x)\big)=0,$$

所以 $v(x)=c$ 是 $\boldsymbol{F}$ 中一非零常数, 因此, $f(x)=cg(x)$. □

§1.3.2 带余除法

当两个多项式之间不整除时, 我们可利用带余除法来考察两多项式之间的联系.

定理 1.3.1 (**带余除法定理**) 设 $f(x),g(x)\in \boldsymbol{F}[\boldsymbol{x}]$, 且 $g(x)\neq 0$, 则存在唯一的一对多项式 $q(x),r(x)\in \boldsymbol{F}[\boldsymbol{x}]$, 使得

$$f(x)=g(x)q(x)+r(x), \tag{1.3}$$

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

式 (1.3) 中的 $q(x)$ 和 $r(x)$ 分别称为 $f(x)$ 除以 $g(x)$ 所得的 **商式** 和 **余式**.

证明 首先, 我们证明 $q(x)$ 和 $r(x)$ 的存在性.

若 $f(x)=0$, 则取 $q(x)=r(x)=0$ 即可.

若 $f(x)\neq 0$, 令 $\deg\big(f(x)\big)=n$, $\deg\big(g(x)\big)=m$. 我们对 $f(x)$ 的次数 n 用归纳法来证明 $q(x)$ 和 $r(x)$ 的存在性.

(1) 当 $n=0$, 即 $f(x)=a$ 为非零常数时, 若 $m>0$, 则取 $q(x)=0,r(x)=a$ 即可; 若 $m=0$, 则 $g(x)=b$ 为非零常数, 从而 $a=b\cdot\frac{a}{b}+0$, 取 $q(x)=\frac{a}{b},r(x)=0$ 即可.

(2) 假设结论对次数小于 n 的多项式成立, 则对次数为 n 的 $f(x)$,

若 $n<m$, 则取 $q(x)=0,r(x)=f(x)$ 即可;

若 $n\geqslant m$, 令 ax^n 和 bx^m 为 $f(x)$ 和 $g(x)$ 的首项, 则 $\frac{a}{b}x^{n-m}g(x)$ 的首项为 ax^n. 现令 $f_1(x)=f(x)-\frac{a}{b}x^{n-m}g(x)$.

若 $f_1(x)=0$, 则取 $q(x)=\frac{a}{b}x^{n-m},r(x)=0$ 即可.

若 $f_1(x)\neq 0$, 则 $\deg\big(f_1(x)\big)<n$, 由归纳假设, 对 $f_1(x),g(x)$ 存在一对多项式 $q_1(x),r_1(x)\in \boldsymbol{F}[\boldsymbol{x}]$, 使得

$$f_1(x)=g(x)q_1(x)+r_1(x),$$

从而
$$f(x)=g(x)\big(q_1(x)+\tfrac{a}{b}x^{n-m}\big)+r_1(x),$$
其中 $r_1(x)=0$ 或者 $\deg\big(r_1(x)\big)<\deg\big(g(x)\big)$.

因此，取 $q(x)=q_1(x)+\frac{a}{b}x^{n-m}$, $r(x)=r_1(x)$ 即可.

下证唯一性. 若另有一对多项式 $q_2(x),r_2(x)\in \boldsymbol{F}[x]$, 使得
$$f(x)=g(x)q_2(x)+r_2(x),$$
其中 $r_2(x)=0$ 或者 $\deg\big(r_2(x)\big)<\deg\big(g(x)\big)$, 则
$$g(x)q(x)+r(x)=g(x)q_2(x)+r_2(x),$$
$$r(x)-r_2(x)=g(x)\big(q_2(x)-q(x)\big).$$
如果 $q_2(x)\neq q(x)$, 因为 $g(x)\neq 0$, 所以 $r(x)-r_2(x)\neq 0$, 这将导致
$$\begin{aligned}\deg\big(r(x)-r_2(x)\big)&=\deg\big(g(x)\big)+\deg\big(q_2(x)-q(x)\big)\\&\geqslant \deg\big(g(x)\big),\end{aligned}$$
这与 $\deg\big(r(x)-r_2(x)\big)<\deg\big(g(x)\big)$ 矛盾.

因此， $q(x)=q_2(x)$, 进而 $r(x)=r_2(x)$. 唯一性得证. □

利用带余除法定理，我们易得如下结论.

推论 1.3.2 设 $f(x),g(x)\in \boldsymbol{F}[x]$, 且 $g(x)\neq 0$, $f(x)$ 除以 $g(x)$ 的余式为 $r(x)$, 则 $g(x)\big|f(x)\Leftrightarrow r(x)=0$.

两个多项式之间的整除关系不因系数域的扩大而改变.

例 1.3.1 设 $f(x)=3x^4+9x^3-3x^2-9$, $g(x)=3x^3+10x^2+2x-3$ 为数域 $\boldsymbol{F}$ 上的多项式，求 $f(x)$ 除以 $g(x)$ 所得的商式 $q(x)$ 和余式 $r(x)$.

解 由带余除法，有
$$\begin{array}{c|l|l}
g(x) & \qquad\qquad f(x) & q(x)\\
3x^3+10x^2+2x-3 & 3x^4\ +9x^3\ -3x^2\ +0x\ -9 & x-\frac{1}{3}\\
 & 3x^4+10x^3+2x^2\ -3x & \\
\hline
 & \qquad -x^3-\ 5\ x^2\ +3x-9 & \\
 & \qquad -x^3-\frac{10}{3}x^2-\frac{2}{3}x+1 & \\
\hline
 & \qquad r(x)=-\frac{5}{3}x^2+\frac{11}{3}x-10 &
\end{array}$$
所以商式 $q(x)=x-\frac{1}{3}$, 余式 $r(x)=-\frac{5}{3}x^2+\frac{11}{3}x-10$. □

例 1.3.2 设 $f(x)=x^4-5x^3+11x^2+ax+b$, $g(x)=(x-1)^2$, 试确定 a, b, 使得 $g(x)\big|f(x)$.

解 由带余除法，有

$$
\begin{array}{c|r|c}
g(x) & f(x) \quad\quad\quad & q(x) \\
x^2-2x+1 & x^4-5x^3+11x^2+ax+b & x^2-3x+4 \\
 & x^4-2x^3+\ \ x^2 \quad\quad\quad\quad & \\
\cline{2-2}
 & -3x^3+10x^2+ax+b & \\
 & -3x^3+\ \ 6x^2-3x \quad & \\
\cline{2-2}
 & 4x^2+(a+3)x+b & \\
 & 4x^2 \quad\quad -8x+4 & \\
\cline{2-2}
 & r(x)=(a+11)x+(b-4) &
\end{array}
$$

因为 $g(x)\big|f(x)$, 所以 $r(x)=(a+11)x+(b-4)=0$, 故 $a+11=0$, 且 $b-4=0$, 即 $a=-11$, $b=4$. □

例 1.3.3 设 $f(x)\in \boldsymbol{F}[x]$, 且正整数 $k\geqslant 2$, 证明：

$$x\big|f^k(x)\Leftrightarrow x\big|f(x).$$

证明 “$\Rightarrow$” 由带余除法定理，知存在 $q(x), r(x)\in \boldsymbol{F}[x]$, 使得

$$f(x)=xq(x)+r(x),$$

其中 $r(x)=0$, 或 $\deg\big(r(x)\big)=0$, 即 $r(x)=r$ 为 $\boldsymbol{F}$ 中常数，于是

$$f(x)=xq(x)+r,$$

$$
\begin{aligned}
f^k(x)\ &=\big(xq(x)\big)^k+\mathrm{C}_k^1 r\big(xq(x)\big)^{k-1}+\cdots+\mathrm{C}_k^{k-1}r^{k-1}\big(xq(x)\big)+r^k\\
&=x\big[x^{k-1}q^k(x)+\mathrm{C}_k^1 r x^{k-2}q^{k-1}(x)+\cdots+\mathrm{C}_k^{k-1}r^{k-1}q(x)\big]+r^k,
\end{aligned}
$$

其中 r^k 为 $\boldsymbol{F}$ 常数. 由商式和余式的唯一性，知 r^k 为 $f^k(x)$ 除以 x 的余式，又因 $x\big|f^k(x)$, 于是 $r^k=0, r=0$, 所以 $x\big|f(x)$.

“$\Leftarrow$” 若 $x\big|f(x)$, 则存在 $q(x)\in \boldsymbol{F}[x]$, 使得 $f(x)=xq(x)$, 于是

$$f^k(x)\ =x^kq^k(x)=x\big(x^{k-1}q^k(x)\big),$$

从而 $x\big|f^k(x)$. □

习 题 1.3

1. 求 $f(x)$ 除以 $g(x)$ 的商式 $q(x)$ 及余式 $r(x)$：

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

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

2. 当 m,n,p 满足什么条件时，有 $x^2+mx-1\mid x^3+px+q$ ？

3. (1) 若 $h(x)\mid f(x), h(x)\nmid g(x)$, 能否推出 $h(x)\nmid f(x)+g(x)$ ？

    (2) 若 $h(x)\nmid f(x), h(x)\nmid g(x)$, 能否推出 $h(x)\nmid f(x)+g(x)$ ？

4. 在数域 $\boldsymbol{F}$ 上，证明： $x^d-1\mid x^n-1 \Leftrightarrow d\mid n$.

§1.4 最大公因式

学习目标：(1) 掌握最大公因式、互素等概念及其性质；

(2) 能熟练地求两个多项式的最大公因式.

§1.4.1 最大公因式

定义 1.4.1 设 $f(x),g(x),d(x)\in \boldsymbol{F}[x]$, 若 $d(x)$ 满足

(1) $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个公因式，即 $d(x)\mid f(x), d(x)\mid g(x)$,

(2) 对 $f(x),g(x)$ 的任意公因式 $h(x)$, 有 $h(x)\mid d(x)$,

则称 $d(x)$ 为 $f(x),g(x)$ 的一个 **最大公因式**.

按定义 1.4.1, 若 $g(x)\mid f(x)$, 则 $g(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式；特别地，任意多项式 $g(x)$ 与 0 的最大公因式有 $g(x)$.

定理 1.4.1 若在数域 $\boldsymbol{F}$ 上有 $f(x)=g(x)q(x)+h(x)$, 则 $f(x)$ 与 $g(x)$, $g(x)$ 与 $h(x)$ 有相同的（最大）公因式.

证明 若 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的任意一个公因式，即

$$d(x)\mid f(x), d(x)\mid g(x),\ \text{又因}\ f(x)=g(x)q(x)+h(x),$$

于是 $d(x)\mid h(x)$, 从而 $d(x)$ 是 $g(x)$ 与 $h(x)$ 的一个公因式. 同理， $g(x)$ 与 $h(x)$ 的公因式也是 $f(x)$ 与 $g(x)$ 的公因式. 因此， $f(x)$ 与 $g(x)$, $g(x)$ 与 $h(x)$ 有相同的（最大）公因式. □