



普通高等教育“十二五”规划教材

高等代数

内容、方法及典型问题

张盛祝 蔡礼明 胡余旺◎编著



中国石化出版社

[HTTP://WWW.SINOPEC-PRESS.COM](http://www.sinopec-press.com)

教·育·出·版·中·心



普通高等教育“十

高等代数

内容、方法及典型问题

张盛祝 蔡礼明 胡余旺◎编著



中国石化出版社

[HTTP://WWW.SINOPEC-PRESS.COM](http://www.sinopec-press.com)

教·育·出·版·中·心

内 容 提 要

《高等代数内容、方法及典型问题》在主要内容编排上与北京大学数学系编著的《高等代数》基本一致,每章分若干小节对基本概念和重要定理进行叙述,并对关键定理的证明思路作出分析,精选一些典型题目进行解答,并有针对性地安排系列习题供读者训练本课程所涉及的数学思想及方法,这些习题在本章之后作了详细解答。

本书所提供的典型问题主要来自于几个方面:①目前流行教材中的典型题目;②学生学习过程中遇到的重难点问题;③近年来著名高校的经典考研试题。该书在处理问题过程中注重这样几个特点:充分联系基本概念基本理论,典型问题及其方法进行梳理归类,系列知识点实现前后贯通联想,解决问题的方法尽量简明易懂。本书力争让读者能达到举一反三、触类旁通的效果。

本书可作为高等学校数学院系选修课《代数选讲》教材或《高等代数》习题课辅导材料,也可供在校本、专科学生,特别是准备报考研究生的同学学习参考。

图书在版编目(CIP)数据

高等代数内容、方法及典型问题 / 张盛祝编著.
—北京:中国石化出版社,2014.10
ISBN 978-7-5114-3062-5

I. ①高… II. ①张… III. ①高等代数-高等学校-
教学参考资料 IV. ①O15

中国版本图书馆 CIP 数据核字 (2014) 第 228320 号

未经本社书面授权,本书任何部分不得被复制、抄袭,或者以任何形式或任何方式传播。版权所有,侵权必究。

中国石化出版社出版发行

地址:北京市东城区安定门外大街 58 号

邮编:100011 电话:(010)84271850

读者服务部电话:(010)84289974

<http://www.sinopec-press.com>

E-mail:press@sinopec.com

北京科信印刷有限公司印刷

全国各地新华书店经销

*

787×1092 毫米 16 开本 15.25 印张 413 千字
2014 年 10 月第 1 版 2014 年 10 月第 1 次印刷
定价:35.00 元

前 言

会 交 流

高等代数是大学数学专业最重要的基础课程之一,是数学各专业报考研究生的必修课,理工科各专业所学的线性代数课程主要取材于高等代数的代数内容。高等代数主要包括多项式理论、线性代数的代数理论(行列式、线性方程组、矩阵、二次型、 λ -矩阵)及线性代数的几何理论(线性空间、线性变换、欧氏空间、双线性函数)。本课程的内容在工程优化、经济管理、信息管理及计算机科学等许多领域都有重要应用,因此学好本课程显得特别重要。

但是,高等代数这门课程的特点是:概念理论体系繁多,内容具有一般性、概括性及抽象性等,其思想方法独特、灵活、多变,同学们在学习中深感困难。为了帮助同学们学好本门课程,特别是为了帮助考研的同学们提高解决问题的能力,作者根据二十几年来进行教学及辅导考研的丰富经验,特编著了这本书。

本书内容编排上与北京大学数学系编著的《高等代数》教材基本一致,每章对知识点进行简要概述,并对重要定理的证明思想及思路进行说明,然后精心挑选典型问题(源于《高等代数》流行教材中的典型习题以及著名高校的经典考研试题等)进行精解,并分节次安排适量的习题供读者做考研训练之用。通过这样处理,希望能帮助同学们提高解决问题能力,更希望使学生学会读书和思考问题。同学们在使用本书过程中,作者给出如下建议:充分理解《高等代数》教材中的相关内容后,再去看本书的解题过程或思考其中问题,在看问题的过程中也应回过头去联系教材中的相关理论。

在编写本书过程中,得到了信阳师范学院教务处、数学学院、华锐学院等单位领导和老师的帮助和支持,也得到了兄弟院校如中原工学院、黄淮学院等相关院系的领导老师的大力支持,在此作者对他(她)们表示衷心地感谢。

由于作者水平有限及时间仓促,本书中难免会有不妥或谬误之处,诚恳希望读者提出批评指正意见。

作 者

2014 年 7 月

《高等代数内容、方法及典型问题》 编委会

张盛祝 蔡礼明 胡余旺 孙旭明

李小朝 杨金根 郭 振 蒋善利

参 考

B 7 4 +105

目 录

第一章 多项式	(1)
§1 数域、一元多项式及其整除性	(1)
§2 最大公因式与互素	(3)
§3 因式分解和多项式函数	(5)
§4 特殊数域上的多项式的因式分解	(9)
§5 多元多项式	(12)
习题答案	(14)
第二章 行列式	(25)
§1 排列和行列式的定义	(25)
§2 行列式的基本性质及矩阵的行列式	(27)
§3 行列式的行(列)展开性质及应用	(31)
§4 拉普拉斯定理及行列式乘法定理	(36)
习题答案	(41)
第三章 线性方程组	(53)
§1 预备知识	(53)
§2 线性相关性	(55)
§3 矩阵的秩	(61)
§4 线性方程组理论	(64)
习题答案	(69)
第四章 矩阵	(78)
§1 矩阵的运算及其性质	(78)
§2 矩阵的逆	(83)
§3 矩阵的分块及应用	(84)
§4 初等矩阵及矩阵的等价	(89)
习题答案	(92)
第五章 二次型	(101)
§1 二次型及其矩阵表示	(101)
§2 标准形与规范形	(103)
§3 正定二次型	(109)
习题答案	(115)
第六章 线性空间	(130)
§1 线性空间的定义及简单性质	(130)
§2 线性空间中的向量的表示	(131)
§3 线性子空间	(136)
§4 子空间的交与和及其直和	(140)

§ 5 线性空间的同构	(143)
习题答案	(145)
第七章 线性变换	(155)
§ 1 线性变换的定义及运算	(155)
§ 2 线性变换的矩阵	(157)
§ 3 线性变换的矩阵对角化	(162)
§ 4 不变子空间	(168)
§ 5 若尔当标准形与最小多项式	(172)
习题答案	(175)
第八章 λ -矩阵	(189)
§ 1 λ -矩阵的等价标准形理论	(189)
§ 2 矩阵的相似及相似标准形	(190)
习题答案	(195)
第九章 欧几里得空间	(200)
§ 1 定义与基本性质	(200)
§ 2 标准正交基与子空间	(202)
§ 3 同构与正交变换	(206)
§ 4 对称变换与实对称矩阵	(209)
§ 5 酉空间	(214)
习题答案	(216)
第十章 双线性函数与辛空间	(231)

第一章 多项式

关键知识点：数域，整除，带余除法定理；最大公因式，最大公因式存在定理，互素，互素的判定及性质；不可约多项式，不可约多项式的性质，因式分解及唯一性定理，重因式(重根)，重因式的性质； $\mathbf{C}[x]$ 中的多项式的因式分解定理， $\mathbf{R}[x]$ 中的多项式的因式分解定理，本原多项式，高斯引理，整系数多项式的性质，艾森斯坦判别定理；对称多项式，对称多项式基本定理。

§1 数域、一元多项式及其整除性

一、数域和一元多项式

定义 1 设 P 是某些复数所组成的集合，如果 P 中至少包含 0 与 1，且 P 对复数的加、减、乘、除四则运算是封闭的，即 $\forall a, b \in P$ ，必有 $a \pm b \in P$ ， $ab \in P$ ，且当 $b \neq 0$ 时， $a/b \in P$ ，则称 P 为一个数域。

典型的数域：复数域 $\mathbf{C}$ ；实数域 $\mathbf{R}$ ；有理数域 $\mathbf{Q}$ 。

数域的一个重要性质：任意数域 P 都包括有理数域 $\mathbf{Q}$ 。

定义 2 所谓数域 P 上的一元多项式，是指形式表达式

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

其中 n 是非负整数， $a_0, a_1, \cdots, a_n \in P$ ， $a_n \neq 0$ 。 $a_n x^n$ 称为 $f(x)$ 的首项， a_n 为首项系数， n 称为多项式 $f(x)$ 的次数，记作 $\partial(f(x)) = n$ 。零多项式不定义次数。

注：零多项式即 $f(x) = 0$ ；零次多项式即 $f(x) = a$ ， $0 \neq a \in P$ 。

规定：多项式的相等即同次项系数的相等；两个多项式的和即同次项系数的相加；两个多项式的乘积按可分配地展开再将同次项合并进行计算。

多项式的次数具如下性质：

1) $\partial(f(x) \pm g(x)) \leq \max(\partial(f(x)), \partial(g(x)))$;

2) 如果 $f(x) \neq 0$ ， $g(x) \neq 0$ ，那么 $f(x)g(x) \neq 0$ ，并且

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

多项式的运算具有的性质：加法交换律；加法结合律；乘法交换律；乘法结合律；乘法对加法的分配律；乘法消去律。数域 P 上的一元多项式的全体，称为数域 P 上的一元多项式环，记为 $P[x]$ 。

例 1.1 证明 $\mathbf{Q}(i) = \{a+bi \mid a, b \in \mathbf{Q}\}$ 是数域(称为 Gauss 数域)，其中 $i = \sqrt{-1}$ 。

证 $0 = 0+0i$ ， $1 = 1+0i \in \mathbf{Q}(i)$ 。

$\forall a+bi, c+di \in \mathbf{Q}(i)$ ，有

$$(a+bi) \pm (c+di) = (a \pm c) + (b \pm d)i \in \mathbf{Q}(i),$$

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i \in \mathbf{Q}(i);$$

若 $a+bi \neq 0$ ，则 $a-bi \neq 0$ ， $a^2+b^2 \neq 0$ ，

$$\frac{c+di}{a+bi} = \frac{(c+di)(a-bi)}{a^2+b^2} = \frac{ac+bd}{a^2+b^2} + \frac{ad-bc}{a^2+b^2}i \in \mathbf{Q}(i),$$

所以 $\mathbf{Q}(i)$ 是一个数域.

例 1.2 设 $f(x), g(x), h(x) \in \mathbf{R}[x]$, 且 $f^2(x) = xg^2(x) + xh^2(x)$, 证明:

$$f(x) = g(x) = h(x) = 0.$$

证 若 $f(x) \neq 0$, 则 $xg^2(x) + xh^2(x) \neq 0$. 那么 $\partial(f^2(x))$ 为偶数, 而 $\partial(xg^2(x) + xh^2(x))$ 为奇数, 矛盾. 所以 $f(x) = 0$, 从而 $g(x) = h(x) = 0$.

二、一元多项式的整除性

带余除法定理设 $f(x), g(x) \in P[x]$, $g(x) \neq 0$, 则存在 $q(x), r(x) \in P[x]$, 使

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

其中 $r(x) = 0$ 或 $\partial(r(x)) < \partial(g(x))$, 且这样的 $q(x), r(x)$ 是唯一决定的. 我们称 $q(x)$ 和 $r(x)$ 分别为用 $f(x)$ 去除 $g(x)$ 所得的商和余式.

多项式的综合除法设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, 则 $x-a$ 除 $f(x)$ 的商式 $q(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_0$ 和余式 r 可按下列计算格式求得:

$$\begin{array}{r|rrrrrr} a & a_n & a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \\ & b_{n-1} & b_{n-2} & b_{n-3} & \cdots & b_0 & r \end{array}$$

其中 $b_{n-1} = a_n$, $b_{n-2} = a_{n-1} + ab_{n-1}$, $b_{n-3} = a_{n-2} + ab_{n-2}$, $\cdots$, $b_0 = a_1 + ab_{n-1}$, $r = a_0 + ab_0$.

定义 3 设 $f(x), g(x) \in P[x]$, 若存在 $q(x) \in P[x]$, 使 $f(x) = q(x)g(x)$, 则称 $g(x)$ 整除 $f(x)$, 记作 $g(x) | f(x)$, $g(x)$ 称为 $f(x)$ 的因式, $f(x)$ 称为 $g(x)$ 的倍式, 否则称 $g(x)$ 不能整除 $f(x)$, 记作 $g(x) \nmid f(x)$.

定理 1 设 $f(x), g(x) \in P[x]$, $g(x) \neq 0$, 则

$$g(x) | f(x) \iff g(x) \text{ 除 } f(x) \text{ 的余式 } r(x) = 0.$$

整除性的常用性质:

1) 若 $g(x) | f(x)$, $f(x) | g(x)$, 则 $f(x) = cg(x)$, 其中 $0 \neq c \in P$;

2) 若 $f(x) | g(x)$, $g(x) | h(x)$, 则 $f(x) | h(x)$;

3) 若 $f(x) | g_i(x)$, 且 $u_i(x) \in P[x] (i=1, 2, \cdots, t)$, 则

$$f(x) | (u_1(x)g_1(x) + u_2(x)g_2(x) + \cdots + u_t(x)g_t(x)).$$

4) 两个多项式之间的整除关系不因为系数域的扩大而改变.

例 1.3 设 $f(x) = 2x^5 - 5x^3 - 8x$, $g(x) = x + 3$, 用综合除法求商与余式.

证 作综合除法

$$\begin{array}{r|rrrrrr} -3 & 2 & 0 & -5 & 0 & -8 & 0 \\ & 2 & -6 & 13 & -39 & 109 & -327 \end{array}$$

因此 $q(x) = 2x^4 - 6x^3 + 13x^2 - 39x + 109$, $r(x) = -327$.

例 1.4 设 $f(x) \in P[x]$, 证明: $x | f^k(x) (k \in \mathbf{N}) \iff x | f(x)$.

证 ($\Leftarrow$) 设 $f(x) = q(x)x$, 则 $f^k(x) = q^k(x)x^k$, 因此 $x | f^k(x)$.

($\Rightarrow$) 设 $f(x) = q(x)x + r$, 那么

$$f^k(x) = q^k(x)x^k + C_k^1 q^{k-1}(x)x^{k-1}r + \cdots + C_k^{k-1} q(x)xr^{k-1} + r^k,$$

若 $r \neq 0$, 则 $r^k \neq 0$, 导致矛盾, 所以 $x | f(x)$.

习题 1.1

1. 设 $0 \neq f(x) \in P[x]$ 满足: $xf(x-1) = (x-26)f(x)$, 证明: $\partial(f(x)) = 26$.

2. 设 $f(x) = x^4 - 2x^2 + 3$, $x_0 = -2$, 把 $f(x)$ 表示成 $x - x_0$ 的方幂和, 即表示成

$$c_0 + c_1(x - x_0) + c_2(x - x_0)^2 + \cdots + c_n(x - x_0)^n + \cdots$$

的形式.

3. 证明: $x^k - 1 \mid x^n - 1 (k, n \in \mathbf{N}) \iff k \mid n$.

4. 证明: $x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3p+2}$, 其中 $m, n, p \in \mathbf{N}$.

5. 设 $\mathbf{R}, \mathbf{Q}$ 分别表示实数域和有理数域, $f(x), g(x) \in \mathbf{Q}[x]$. 证明: 若在 $\mathbf{R}[x]$ 中有 $g(x) \mid f(x)$, 则在 $\mathbf{Q}[x]$ 中也有 $g(x) \mid f(x)$.

§2 最大公因式与互素

一、最大公因式

定义 4 设 $f(x), g(x) \in P[x]$, 若 $d(x) \in P[x]$, 满足

1) $d(x) \mid f(x), d(x) \mid g(x)$;

2) 任意 $\varphi(x) \in P[x]$ 使 $\varphi(x) \mid f(x)$ 且 $\varphi(x) \mid g(x)$, 均有 $d(x) \mid \varphi(x)$.

则称 $d(x)$ 为 $f(x), g(x)$ 的一个最大公因式(可简记为 GCD).

定理 2 对于任意 $f(x), g(x) \in P[x]$, 则 $f(x)$ 与 $g(x)$ 的最大公因式(即 GCD) $d(x) \in P[x]$ 存在, 且有 $u(x), v(x) \in P[x]$, 使得 $d(x) = u(x)f(x) + v(x)g(x)$.

略证 (1) 若 $f(x) = q(x)g(x) + r(x)$, 则 $(f(x), g(x)) = (g(x), r(x))$;

(2) 若 $f(x), g(x)$ 中有一个为 0, 则结论成立;

(3) 设 $g(x) \neq 0$, 进行辗转带余除, 则可得:

$$f(x) = q_1(x)g(x) + r_1(x), \quad g(x) = q_2(x)r_1(x) + r_2(x), \quad \dots, \quad$$

$$r_{s-2}(x) = q_s(x)r_{s-1}(x) + r_s(x), \quad r_{s-1}(x) = q_{s+1}(x)r_s(x) + 0,$$

那么 $r_s(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式, 通过回代则知 $r_s(x)$ 也是 $f(x)$ 与 $g(x)$ 的一个组合.

对于定理 2, 说明几点:

① 定理中用于求最大公因式(GCD)的方法通常称为辗转相除法;

② 定理中存在的 $u(x), v(x)$ 使 $d(x) = u(x)f(x) + v(x)g(x)$ 一般不唯一;

③ 对于 $f(x), g(x) \in P[x]$, 若存在 $u(x), v(x) \in P[x]$ 使

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

则 $d(x)$ 一般不是 $f(x), g(x)$ 的最大公因式(GCD);

④ 我们用记号 $(f(x), g(x))$ 表示首项系数为 1 的那个最大公因式(GCD).

定义 5 设 $f(x), g(x) \in P[x]$, 若 $m(x) \in P[x]$, 满足

1) $f(x) \mid m(x), g(x) \mid m(x)$;

2) 对 $f(x), g(x)$ 的任一个公倍式 $\varphi(x)$, 都有 $m(x) \mid \varphi(x)$.

则称 $m(x)$ 为 $f(x), g(x)$ 的一个最小公倍式(LCM), 记号 $[f(x), g(x)]$ 表示首项系数为 1 的最小公倍式(LCM).

设 $f_1(x), f_2(x), \dots, f_s(x) \in P[x] (s \geq 2)$, 若 $d(x) \in P[x]$ 满足:

1) $d(x) \mid f_i(x), i = 1, 2, \dots, s$;

2) $\forall \varphi(x) \in P[x]$, 若 $\varphi(x) \mid f_i(x), i = 1, 2, \dots, s$, 则 $\varphi(x) \mid d(x)$.

则称 $d(x)$ 为 $f_1(x), f_2(x), \dots, f_s(x)$ 的最大公因式.

例 1.5 求 $u(x)$, $v(x)$ 使 $u(x)f(x)+v(x)g(x)=(f(x), g(x))$, 其中

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

解 作如下辗转相除:

$$q_2(x)=x+1 \left| \begin{array}{r} x^4+x^3-x^2-2x-2 \\ x^4 \qquad -2x^2 \\ \hline x^3+x^2-2x-2 \\ x^3 \qquad -2x \\ \hline r_2(x)=x^2-2 \end{array} \right| \begin{array}{l} x^4+2x^3-x^2-4x-2 \\ x^4+x^3-x^2-2x-2 \\ \hline r_1(x)=x^3-2x \end{array} \left| \begin{array}{l} q_1(x)=1 \\ r_2(x)=x^2-2 \end{array} \right.$$

所以 $(f(x), g(x))=x^2-2=r_2(x)$.

由于

$$f(x)=q_1(x)g(x)+r_1(x), \quad g(x)=q_2(x)r_1(x)+r_2(x),$$

所以

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

则得 $u(x)=-q_2(x)=-x-1$, $v(x)=1+q_1(x)q_2(x)=1+1 \cdot (x+1)=x+2$.

例 1.6 证明: 如果 $d(x) \mid f(x)$, $d(x) \mid g(x)$, 且 $d(x)$ 为 $f(x)$ 与 $g(x)$ 的组合, 那么 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式.

证 设 $\varphi(x)$ 是 $f(x)$ 与 $g(x)$ 的任一公因式, 由于 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个组合, 则存在多项式 $u(x)$ 与 $v(x)$, 使 $d(x)=u(x)f(x)+v(x)g(x)$, 则 $\varphi(x) \mid d(x)$, 所以 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式.

例 1.7 证明: $(f(x), g(x))=(f(x)+u(x)g(x), g(x))$.

证 设 $(f(x), g(x))=d(x)$, 则 $d(x) \mid f(x)$, $d(x) \mid g(x)$, $d(x) \mid f(x)+u(x)g(x)$.

设 $\varphi(x) \mid f(x)+u(x)g(x)$, $\varphi(x) \mid g(x)$, 则 $\varphi(x) \mid f(x)$, 那么 $\varphi(x) \mid d(x)$, 所以 $d(x)$ 是 $f(x)+u(x)g(x)$ 与 $g(x)$ 的一个最大公因式.

二、互素

定义 6 设 $f(x), g(x) \in P[x]$, 若 $(f(x), g(x))=1$, 则称 $f(x), g(x)$ 在数域 P 上互素(也可称互质).

如果 $(f_1(x), f_2(x), \dots, f_n(x))=1$, 那么称 $f_1(x), f_2(x), \dots, f_n(x)$ 互素.

定理 3 设 $f(x), g(x) \in P[x]$, 则 $f(x), g(x)$ 互素 $\Leftrightarrow$ 存在 $u(x), v(x) \in P[x]$ 使

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

定理 4 如果 $(f(x), g(x))=1$, 且 $f(x) \mid g(x)h(x)$, 那么 $f(x) \mid h(x)$.

推论 若 $f_1(x) \mid g(x)$, $f_2(x) \mid g(x)$, 且 $(f_1(x), f_2(x))=1$, 则 $f_1(x)f_2(x) \mid g(x)$.

例 1.8 证明: 若 $(f(x), g(x))=1$, $(f(x), h(x))=1$, 则 $(f(x), g(x)h(x))=1$.

证 由假设, 存在 $u_1(x), v_1(x)$ 及 $u_2(x), v_2(x)$ 使得

$$u_1(x)f(x)+v_1(x)g(x)=1, \quad u_2(x)f(x)+v_2(x)h(x)=1,$$

将两式相乘则得

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

其中 $u(x)=u_1(x)u_2(x)f(x)+v_1(x)u_2(x)g(x)+u_1(x)v_2(x)h(x)$, $v(x)=v_1(x)v_2(x)$,

所以 $(f(x), g(x)h(x))=1$.

例 1.9 设 $f(x), g(x)$ 不全为零, 记 $(f(x), g(x))=d(x)$, 且 $f(x)=d(x)f_1(x)$,

$g(x) = d(x)g_1(x)$, 证明: $(f_1(x), g_1(x)) = 1$.

证 由定理 2, 则存在 $u(x), v(x)$ 使得

$$u(x)f(x) + v(x)g(x) = d(x), \text{ 即 } u(x)d(x)f_1(x) + v(x)d(x)g_1(x) = d(x),$$

由于 $f(x), g(x)$ 不全为 0, 因此 $(f(x), g(x)) = d(x) \neq 0$, 由消去律则

$$u(x)f_1(x) + v(x)g_1(x) = 1,$$

所以 $(f_1(x), g_1(x)) = 1$.

例 1.10 设多项式 $f(x), g(x), h(x) \in P[x]$ 满足

$$(x^2+1)h(x) + (x-1)f(x) + (x-2)g(x) = 0,$$

$$(x^2+1)h(x) + (x+1)f(x) + (x+2)g(x) = 0,$$

证明: $x^2+1 \mid f(x), x^2+1 \mid g(x)$.

证 两式分别相减、相加, 则得

$$f(x) = -2g(x), (x^2+1)h(x) = -xg(x).$$

由于 $(x^2+1) \mid xg(x)$, 且 $(x^2+1, x) = 1$, 所以 $(x^2+1) \mid g(x), x^2+1 \mid f(x)$.

习题 1.2

1. 设 $f(x) = x^3 + (1+t)x^2 + 2x + 2u$, $g(x) = x^3 + tx + u$ 的最大公因式是一个二次多项式, 求 t, u 的值.

2. 设 $h(x)$ 的首项系数为 1, 证明: $(f(x)h(x), g(x)h(x)) = (f(x), g(x))h(x)$.

3. 证明: 若 $(f(x), g(x)) = 1$, 则 $(f(x)g(x), f(x)+g(x)) = 1$.

4. 设 $(f_i(x), g_j(x)) = 1, (i=1, 2, \dots, m; j=1, 2, \dots, n)$, 求证:

$$(f_1(x)f_2(x)\cdots f_m(x), g_1(x)g_2(x)\cdots g_n(x)) = 1.$$

5. 设 $(f_1(x), f_2(x), \dots, f_{s-1}(x))$ 存在, 证明: $(f_1(x), f_2(x), \dots, f_{s-1}(x), f_s(x))$ 也存在, 且当 $f_1(x), f_2(x), \dots, f_s(x)$ 全不为零时有

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

6. 设 $f_1(x), f_2(x), f_3(x) \in P[x]$ 均为非零多项式, 证明: $f_1(x), f_2(x), f_3(x)$ 两两互素的充分必要条件是存在多项式 $u(x), v(x), w(x)$ 使得

$$u(x)f_1(x)f_2(x) + v(x)f_1(x)f_3(x) + w(x)f_2(x)f_3(x) = 1.$$

7. 设 $f_1(x), f_2(x), \dots, f_n(x) \in P[x]$. 证明: $f_1(x), f_2(x), \dots, f_n(x)$ 的最大公因式 $d(x)$ 必存在, 且 $d(x)$ 是 $f_1(x), f_2(x), \dots, f_n(x)$ 的一个组合.

8. 设 $(f_1(x), f_2(x)) = 1$. 证明: 任给 $g_1(x), g_2(x) \in P[x]$, 则存在 $g(x) \in P[x]$ 使得 $f_i(x) \mid g(x) - g_i(x), (i=1, 2)$.

9. 设 $f(x), g(x) \in \mathbf{Q}[x]$. 证明: $f(x), g(x)$ 在 $\mathbf{Q}[x]$ 中互素, 当且仅当 $f(x), g(x)$ 在 $\mathbf{R}[x]$ 中互素.

10. 证明: 若 $f(x), g(x)$ 的首项系数都是 1, 则 $[f(x), g(x)] = \frac{f(x)g(x)}{(f(x), g(x))}$.

§3 因式分解和多项式函数

一、不可约多项式与因式分解定理

定义 7 设 $p(x) \in P[x], \partial(p(x)) \geq 1$, 称 $p(x)$ 为数域 P 上的不可约多项式, 如果 $p(x)$ 不能表

示成 $P[x]$ 中两个次数较低的多项式的乘积.

设 $p(x) \in P[x]$ 是不可约多项式, 则 $p(x)$ 具性质: 对于任意 $f(x) \in P[x]$, 则 $p(x) \mid f(x)$ 或 $(p(x), f(x)) = 1$.

定理 5 设 $p(x) \in P[x]$ 是不可约多项式, 那么 $p(x)$ 具性质: 对于 $P[x]$ 中任意 $f(x), g(x)$, 若 $p(x) \mid f(x)g(x)$, 则 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$.

推广: 若不可约多项式 $p(x) \mid f_1(x)f_2(x)\cdots f_s(x)$, 则 $f_1(x), f_2(x), \dots, f_s(x)$ 中必有某个 $f_i(x)$ 使得 $p(x) \mid f_i(x)$.

因式分解及唯一性定理任给 $f(x) \in P[x], \partial(f(x)) \geq 1$, 则 $f(x)$ 可唯一地分解成数域 P 上一些不可约多项式的乘积. 所谓唯一性是指, 若有两个分解式

$$f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)\cdots q_t(x),$$

则 $s=t$, 且适当调整次序后, 有 $p_i(x) = c_i q_i(x)$, 其中 $c_i (i=1, 2, \dots, s)$ 是非零常数.

设 $f(x) \in P[x], \partial(f(x)) \geq 1$, 则 $f(x)$ 的标准分解式为

$$f(x) = cp_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x),$$

其中 c 为 $f(x)$ 的首项系数, $p_i(x)$ 为互不相同的首项系数为 1 的不可约多项式, r_i 是正整数.

例 1.11 设 $p(x) \in P[x], \partial(p(x)) \geq 1$, 且 $p(x)$ 满足性质: 任给 $f(x) \in P[x]$, 都有 $p(x) \mid f(x)$ 或 $(p(x), f(x)) = 1$. 证明: $p(x)$ 是不可约多项式.

证 (反证) 设 $p(x)$ 是可约多项式, 则 $p(x)$ 可分解成两个次数较低的多项式的乘积 $p(x) = f_1(x)f_2(x)$, 取 $f(x) = f_1(x)$, 则 $p(x) \nmid f(x)$ 且 $(p(x), f(x)) \neq 1$, 矛盾.

例 1.12 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in P[x] (a_n \neq 0, a_0 \neq 0)$, 且 $f(x)$ 是不可约多项式, 证明: $g(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ 也是不可约多项式.

证 (反证) 设 $g(x)$ 是可约多项式, 则 $g(x)$ 可分解成两个次数较低的多项式的乘积 $g(x) = g_1(x)g_2(x)$, 记 $\partial(g_1(x)) = r$, 则 $0 < r < n$.

因为 $f(x) = x^n g(1/x)$, 所以 $f(x) = x^r g_1(1/x) \cdot x^{n-r} g_2(1/x)$, 说明 $f(x)$ 也可分解成两个次数较低的多项式的乘积, 此与 $f(x)$ 不可约矛盾.

例 1.13 设 $f(x) \in P[x], \partial(f(x)) \geq 1$, 且首项系数为 1. 证明: $f(x)$ 是一个不可约多项式的方幂的充分必要条件是: 任给 $g(x) \in P[x]$, 必有 $(f(x), g(x)) = 1$ 或者 $f(x) \mid g^m(x)$, 其中 m 为某一正整数.

证 ($\Rightarrow$) 设 $f(x) = p^n(x)$, 其中 $p(x)$ 为不可约多项式, n 为正整数.

任给 $g(x) \in P[x]$, 则 $(p(x), g(x)) = 1$, 或者 $p(x) \mid g(x)$. 若前者成立, 则有 $(p^n(x), g(x)) = 1$, 即得 $(f(x), g(x)) = 1$; 若后者成立, 则有 $p^n(x) \mid g^n(x)$, 即得 $f(x) \mid g^n(x)$.

($\Leftarrow$) (反证) 设 $f(x)$ 不能表示成一个不可约多项式的方幂, 则 $f(x)$ 至少有两个不同的不可约因式, 分别设它们为 $p(x), q(x)$, 取 $g(x) = p(x)$, 则

$$(f(x), g(x)) \neq 1, \text{ 且 } f(x) \nmid g^m(x),$$

其中 m 为任一正整数, 矛盾.

二、重因式

定义 8 设 $p(x)$ 为数域 P 上的不可约多项式, $f(x) \in P[x]$, 称 $p(x)$ 为 $f(x)$ 的 k 重因式, 如果 $p^k(x) \mid f(x)$, 但 $p^{k+1}(x) \nmid f(x)$.

定理 6 如果不可约多项式 $p(x)$ 是 $f(x)$ 的 k 重因式 ($k \geq 1$), 那么它是导数多项式 $f'(x)$ 的 $k-1$ 重因式.

由此可得重因式的下述性质:

1) 若不可约多项式 $p(x)$ 是 $f(x)$ 的 k 重因式 ($k \geq 1$), 则 $p(x)$ 是 $f(x), f'(x), f''(x), \dots, f^{(k-1)}(x)$ 的因式, 但不是 $f^{(k)}(x)$ 的因式;

2) 不可约多项式 $p(x)$ 是 $f(x)$ 的重因式 $\Leftrightarrow p(x)$ 是 $f(x)$ 与 $f'(x)$ 的公因式;

3) 多项式 $f(x)$ 没有重因式 $\Leftrightarrow (f(x), f'(x)) = 1$.

例 1.14 设 $p(x) \in P[x]$ 为不可约多项式, $k > 1$, $(f(x), f'(x)) = d(x)$. 证明: $p(x)$ 是 $f(x)$ 的 k 重因式 $\Leftrightarrow p^{k-1}(x) \mid d(x)$, $p^k(x) \nmid d(x)$.

证 ($\Rightarrow$) 由于 $p(x)$ 是 $f(x)$ 的 k 重因式, 那么 $p^k(x) \mid f(x)$, $p^{k+1}(x) \nmid f(x)$, 由定理 6, 则 $p^{k-1}(x) \mid f'(x)$, $p^k(x) \nmid f'(x)$, 因此 $p^{k-1}(x) \mid d(x)$, $p^k(x) \nmid d(x)$.

($\Leftarrow$) 由于 $p(x)$ 是 $d(x)$ 的 $k-1$ 重因式, 则 $p(x) \mid f(x)$, $p(x) \mid f'(x)$, 因此 $p(x)$ 必是 $f(x)$ 的重因式, 假设此重数为 s ($s > 1$), 由必要性, 则 $p(x)$ 是 $d(x)$ 的 $s-1$ 重因式, 所以 $s-1 = k-1$, 从而 $s = k$.

例 1.15 设 $f(x)$ 的标准分解式为

$$f(x) = cp_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x),$$

其中 c 为 $f(x)$ 的首项系数, $p_i(x)$ 为互不相同的首项系数为 1 的不可约多项式, r_i 是正整数. 证明:

$$\frac{f(x)}{(f(x), f'(x))} = cp_1(x)p_2(x)\cdots p_s(x).$$

证 由于 $p_i(x)$ 是 $f(x)$ 的 r_i 重因式, 那么 $p_i(x)$ 是 $f'(x)$ 的 r_i-1 重因式, 因此可设

$$f'(x) = dp_1^{r_1-1}(x)p_2^{r_2-1}(x)\cdots p_s^{r_s-1}(x)g(x),$$

其中 d 为 $f'(x)$ 的首项系数, 且 $(p_i(x), g(x)) = 1$, 所以

$$(f(x), f'(x)) = p_1^{r_1-1}(x)p_2^{r_2-1}(x)\cdots p_s^{r_s-1}(x),$$

结论得证.

三、多项式函数

设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in P[x]$, $\alpha \in P$, 记

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

则称 $f(\alpha)$ 为 $f(x)$ 当 $x = \alpha$ 时的值, 并且 $f: \alpha \mapsto f(\alpha)$ 定义了 P 到 P 的函数, 称为多项式函数.

若 $f(x)$ 在 $x = \alpha$ 时值 $f(\alpha) = 0$, 则称 α 为 $f(x)$ 的一个根或零点.

定理 7 (余数定理) 用一次多项式 $x - \alpha$ 去除多项式 $f(x)$, 所得的余式是一个常数, 这个常数等于函数值 $f(\alpha)$.

定理 8 $P[x]$ 中的 n 次多项式 ($n \geq 0$) 在数域 P 中的根至多为 n 个, 重根按重数计算.

定理 9 设 $f(x), g(x) \in P[x]$, 且它们的次数 $\partial(f(x)), \partial(g(x)) \leq n$, 若存在 n 个不同的数 $\alpha_1, \alpha_2, \dots, \alpha_{n+1} \in P$ 使得 $f(\alpha_i) = g(\alpha_i)$ ($i = 1, 2, \dots, n+1$), 则 $f(x) = g(x)$.

例 1.16 利用重因式重根的性质解答下列问题:

1) 设 $(x-1)^2 \mid ax^4 + bx^2 + 1$, 求 a, b ;

2) 试求多项式 $x^{2009} + 1$ 除以 $(x-1)^2$ 所得的余式.

解 1) 令 $f(x) = ax^4 + bx^2 + 1$, 则 $f'(x) = 4ax^3 + 2bx$, 由题设知, 1 是 $f(x)$ 的根, 也是 $f'(x)$ 的根, 则有 $\begin{cases} a+b+1=0 \\ 4a+2b=0 \end{cases}$, 解得 $a=1, b=-2$.

2) 可设 $x^{2009} + 1 = q(x)(x-1)^2 + ax + b$, 记 $f(x) = (x^{2009} + 1) - (ax + b)$, 则 1 是 $f(x)$ 的根, 也是 $f'(x) = 2009x^{2008} - a$ 的根, 则可解得 $a = 2009, b = -2007$, 所以余式为 $2009x - 2007$.

例 1.17 求多项式 $f(x) = x^3 + px + q$ 有重根的条件.

解 $f'(x) = 3x^2 + p$, 由于 $f(x)$ 是一个三次多项式, 那么 $f(x)$ 有重根 $\Leftrightarrow f(x)$ 有重因式 $\Leftrightarrow (f(x), f'(x)) \neq 1$.

作如下辗转相除:

$$f(x) = q_1(x)f'(x) + r_1(x), \quad f'(x) = q_2(x)r_1(x) + r_2(x),$$

其中

$$q_1(x) = \frac{1}{3}x, \quad r_1(x) = \frac{2}{3}px + q, \quad q_2(x) = \frac{9}{2p}x - \frac{27q}{4p^2}, \quad r_2(x) = p + \frac{27q^2}{4p^2},$$

上述运算中, 若 $p=0$, 则需 $q=0$, 否则 $(f(x), f'(x)) = 1$, 矛盾; 若 $p \neq 0$, 则可运算到第二步带余除, 此时需 $r_2(x) = 0$, 即需 $p + \frac{27q^2}{4p^2} = 0$. 总之 $4p^3 + 27q^2 = 0$.

例 1.18 设 α 是 $f'''(x)$ 的一个 k 重根, 证明: α 是 $g(x)$ 的一个 $k+3$ 重根, 其中

$$g(x) = \frac{x - \alpha}{2} [f''(x) + f''(\alpha)] - f(x) + f(\alpha).$$

证 对 $g(x)$ 连续求两次导得

$$g'(x) = \frac{x - \alpha}{2} f'''(x) - \frac{1}{2} [f''(x) - f''(\alpha)], \quad g''(x) = \frac{x - \alpha}{2} f'''(x),$$

由于 α 是 $f'''(x)$ 的 k 重根, 即 $x - \alpha$ 是 $f'''(x)$ 的 k 重因式, 因此, 则 $x - \alpha$ 是 $g''(x)$ 的 $k+1$ (≥ 1) 重因式.

易验证 $g(\alpha) = g'(\alpha) = 0$, 因此 α 是 $g(x)$ 的重根, 即 $x - \alpha$ 是 $g(x)$ 的重因式, 可设其重数为 s ($s \geq 2$), 那么 $x - \alpha$ 是 $g''(x)$ 的 $s-2$ 重因式, 由重数的唯一性, 因此 $s-2 = k+1$, 所以 $s = k+3$, 即 α 是 $g(x)$ 的 $k+3$ 重根.

例 1.19 设 $\alpha \in \mathbb{C}$, 且 α 是数域 P 上某非零多项式 $g(x)$ 的根, 记

$$W = \{f(x) \in P[x] \mid f(\alpha) = 0\},$$

证明: 存在 $p(x) \in W$, 使 $p(x) \mid f(x)$, $\forall f(x) \in W$, 且 $p(x)$ 在 P 上不可约.

证 由于 $0 \neq g(x) \in W$, 则 W 中有很多非零多项式, 因此 W 中必存在次数最低的多项式, 取其一记为 $p(x)$, 对于任意多项式 $f(x) \in W$, 用 $p(x)$ 对 $f(x)$ 作带余除:

$$f(x) = q(x)p(x) + r(x), \quad \text{其中 } r(x) = 0 \text{ 或 } \partial(r(x)) < \partial(p(x)),$$

则 $r(\alpha) = f(\alpha) - q(\alpha)p(\alpha) = 0$, 因此 $r(x) \in W$, 说明 $\partial(r(x)) < \partial(p(x))$ 不可能成立, 所以 $r(x) = 0$, 即得 $p(x) \mid f(x)$.

(反证) 假设 $p(x)$ 在 P 上可约, 则 $p(x)$ 可分解成 P 上的两个次数较低的多项式的乘积即 $p(x) = p_1(x)p_2(x)$, 那么 $p(\alpha) = 0$, 则 $p_1(\alpha) = 0$ 或 $p_2(\alpha) = 0$, 立即可推得 $p_1(x) \in W$ 或 $p_2(x) \in W$, 矛盾.

习题 1.3

1. 设 $p(x)$ 是次数大于零的多项式, 如果对于任何多项式 $f(x)$, $g(x)$, 由 $p(x) \mid f(x)g(x)$ 可以推出 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$, 则 $p(x)$ 是不可约多项式.

2. 设 $f(x) \in P[x]$, $\partial(f(x)) \geq 1$, 且首项系数为 1. 证明: $f(x)$ 是一个不可约多项式的方幂的充分必要条件是: 对任意的多项式 $g(x)$, $h(x)$, 由 $f(x) \mid g(x)h(x)$, 可以推出 $f(x) \mid g(x)$, 或 $f(x) \mid h^m(x)$ (其中 m 为某一正整数).

3. 求 t 值使 $f(x) = x^3 - 3x^2 + tx - 1$ 有重根.

4. 试求一个 3 次多项式 $f(x)$ 使得 $(x-1)^2 \mid f(x)+1$, $(x+1)^2 \mid f(x)-1$.

5. 证明 $f(x)$ 不可能有重根:

1) $f(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$; 2) $f(x) = 1 - x + \frac{x^2}{2!} + \cdots + (-1)^n \frac{x^n}{n!}$

6. 证明: α 是 $f(x)$ 的 k 重根 $\Leftrightarrow f(\alpha) = f'(\alpha) = \cdots = f^{(k-1)}(\alpha) = 0$, 但 $f^{(k)}(\alpha) \neq 0$.

7. 证明: 如果 $(x-1) \mid f(x^n)$, 那么 $(x^n-1) \mid f(x^n)$.

8. 证明: $f(x) = x^n + ax^{n-m} + b$ 不存在非零的重数大于 2 的根.

9. 证明: 如果 $f(x) \mid f(x^n)$, 那么 $f(x)$ 的根只能是零或单位根.

10. 证明: 如果 $f'(x) \mid f(x)$, 那么 $f(x)$ 有 n 重根, 其中 $n = \partial(f(x))$.

11. 设 $\partial(f(x)) = n$, $\frac{f(x)}{(f(x), f'(x))} = c(x-a)(x-b)$, 求 $f(x)$.

12. 设复数 $c \neq 0$ 为某一有理多项式的根, 令 $M = \{f(x) \in \mathbf{Q}[x] \mid f(c) = 0\}$.

1) 证明: 存在唯一的首项系数等于 1 的在 $\mathbf{Q}$ 上不可约的多项式 $p(x) \in M$, 使得 $p(x) \mid f(x)$, $\forall f(x) \in W$, 对于 $c = \sqrt{3} + i$, 求相应的 $p(x)$;

2) 证明: 存在 $g(x) \in \mathbf{Q}[x]$ 使得 $g(c) = 1/c$;

13. 设 $0 \neq \alpha \in \mathbf{C}$, 证明: α 是某非零 $g(x) \in \mathbf{Q}[x]$ 的根 $\Leftrightarrow$ 存在 $f(x) \in \mathbf{Q}[x]$ 使得 $f(\alpha) = 1/\alpha$.

14. 设 $f(x)$ 是 $\mathbf{Q}[x]$ 中的不可约多项式, 证明: $f(x)$ 的根都是单根.

§4 特殊数域上的多项式的因式分解

一、复系数和实系数多项式的因式分解

代数基本定理次数 ≥ 1 的 $f(x) \in \mathbf{C}[x]$ 在复数域 $\mathbf{C}$ 上必有根.

复系数多项式因式分解定理对于任意 $f(x) \in \mathbf{C}[x]$, 若 $\partial(f(x)) \geq 1$, 则 $f(x)$ 在复数域 $\mathbf{C}$ 上都可唯一地分解成一次因式的乘积. 复系数多项式具有标准分解式

$$f(x) = a_n (x - \alpha_1)^{l_1} (x - \alpha_2)^{l_2} \cdots (x - \alpha_s)^{l_s},$$

其中 $\alpha_1, \alpha_2, \cdots, \alpha_s$ 是不同的复数, $l_1, l_2, \cdots, l_s$ 是正整数.

如果 α 是 $f(x) \in \mathbf{R}[x]$ 的复根, 那么 α 的共轭复数 $\bar{\alpha}$ 也是 $f(x)$ 的复根.

实系数多项式因式分解定理对于任意 $f(x) \in \mathbf{R}[x]$, 若 $\partial(f(x)) \geq 1$, 则 $f(x)$ 在复数域 $\mathbf{R}$ 上都可唯一地分解成一次因式与二次不可约因式的乘积. 实系数多项式具有标准分解式

$$f(x) = a_n (x - c_1)^{l_1} \cdots (x - c_s)^{l_s} (x^2 + p_1x + q_1)^{k_1} \cdots (x^2 + p_rx + q_r)^{k_r},$$

其中 $c_1, \cdots, c_s, p_1, \cdots, p_r, q_1, \cdots, q_r$ 全是实数, $l_1, \cdots, l_s, k_1, \cdots, k_r$ 全是正整数, 且 $p_i^2 - 4q_i < 0$ 即 $x^2 + p_ix + q_i (i=1, 2, \cdots, r)$ 为 $\mathbf{R}$ 上的不可约多项式.

例 1.20 分别在 $\mathbf{C}[x]$ 、 $\mathbf{R}[x]$ 中对 $f(x) = x^6 - 1$ 进行不可约分解.

解 $f(x) = (x+1)(x-1)\left(x + \frac{1-\sqrt{3}i}{2}\right)\left(x + \frac{1+\sqrt{3}i}{2}\right)\left(x - \frac{1+\sqrt{3}i}{2}\right)\left(x - \frac{1-\sqrt{3}i}{2}\right)$

$$f(x) = (x+1)(x-1)(x^2 - x + 1)(x^2 + x + 1).$$

例 1.21 设 $f_n(x) = x^{n+2} - (x+1)^{2n+1}$, 其中 n 为非负整数, 证明:

$$(x^2 + x + 1, f_n(x)) = 1.$$

证 记 $\omega = \cos(2\pi/3) + i\sin(2\pi/3)$, 则 $x^2 + x + 1 = (x - \omega)(x - \bar{\omega})$, 那么

$$f_n(\omega) = \omega^{n+2} - (\omega + 1)^{2n+1} = \omega^{n+2} - (-\omega^2)^{2n+1} = \omega^{n+2}(1 + \omega^{3n}) = 2\omega^{n+2} \neq 0,$$

而 $f_n(x) \in R[x]$, 则 $f_n(\bar{\omega}) \neq 0$, 故 $(x^2+x+1) \nmid f_n(x)$, 则 $(x^2+x+1, f_n(x)) = 1$.

二、有理系数多项式的因式分解

设 $g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$ 为非零整系数多项式, 如果 $b_n, b_{n-1}, \cdots, b_0$ 没有异于 ± 1 的公因子, 即 $b_n, b_{n-1}, \cdots, b_0$ 互素, 那么称 $g(x)$ 为本原多项式.

定理 10 (Gauss 引理) 两个本原多项式的乘积积仍是本原多项式.

略证 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$ 均为本原多项式, 则 $h(x) = f(x)g(x) = d_{n+m} x^{n+m} + d_{n+m-1} x^{n+m-1} + \cdots + d_0$, $d_s = \sum_{i+j=s} a_i b_j$.

(反证) 假设 $h(x)$ 不是本原的, 则存在素数 p 使得 $p \mid d_s (s=0, 1, \cdots, n+m)$, 但 $f(x), g(x)$ 均本原, 则可设 $p \nmid a_0, \cdots, p \nmid a_{i-1}, p \nmid a_i, p \nmid b_0, \cdots, p \nmid b_{j-1}, p \nmid b_j$. 考查

$$d_{i+j} = \cdots + a_{i-2} b_{j+2} + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \cdots,$$

则导致矛盾.

定理 11 若一非零的整系数多项式可分解成两个次数较低的有理系数多项式的乘积, 则它一定可分解成两个次数较低的整系数多项式的乘积.

定理 12 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 是一个整系数多项式, 而 r/s 是它的一个有理根, 其中 r, s 是互素的, 则必有 $s \mid a_n, r \mid a_0$.

定理 13 (Eisenstein 判别法) 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 是整系数多项式, 若有一个素数 p , 使 $p \nmid a_n, p \mid a_{n-1}, p \mid a_{n-2}, \cdots, p \mid a_0, p^2 \nmid a_0$, 则 $f(x)$ 在有理数域上是不可约的.

略证 (反证) 设 $f(x)$ 在有理数域上可约, 则 $f(x)$ 可分解为两个次数较低的整系数多项式的乘积, 设 $f(x) = (b_l x^l + b_{l-1} x^{l-1} + \cdots + b_0)(c_m x^m + c_{m-1} x^{m-1} + \cdots + c_0)$, 其中 $0 < l, m < n$, 且 $l+m=n$. 因此 $a_n = b_l c_m, a_0 = b_0 c_0$.

由于 $p \nmid b_l c_m, p \mid b_0 c_0, p^2 \nmid b_0 c_0$, 则可不妨设 $p \nmid b_l, p \nmid c_m, p \mid b_0, p \nmid c_0$, 那么可假设 $p \mid b_0, p \mid b_1, \cdots, p \mid b_{k-1}, p \nmid b_k$. 利用 $a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k$, 则得矛盾.

例 1.22 求多项式 $f(x) = x^5 + x^4 - 6x^3 - 14x^2 - 11x - 3$ 的有理根.

解 设 $f(x)$ 的有理根为 r/s , 其中 r, s 互素, 则 $r \mid (-3), s \mid 1$, 那么 $f(x)$ 可能的有理根为 $-1, 1, -3, 3$. 作下述综合除法

$$\begin{array}{r|rrrrrr} -1 & 1 & 1 & -6 & -14 & -11 & -3 \\ -1 & 1 & 0 & -6 & -8 & -3 & (0) \\ -1 & 1 & -1 & -5 & -3 & (0) & \\ -1 & 1 & -2 & -3 & (0) & & \\ & 1 & -3 & (0) & & & \end{array}$$

则知 $f(x)$ 的有理根为 $-1, -1, -1, -1, 3$.

例 1.23 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 为整系数多项式, 而 p/q 是它的一个有理根, 其中 p, q 是互素的, 证明: 对于任意整数 m , 则 $(p-mq) \mid f(m)$.

证 由于 $f(p/q) = 0$, 因此在 $\mathbb{Q}[x]$ 中 $(x-p/q) \mid f(x)$, 从而 $(qx-p) \mid f(x)$, 则存在 $g(x) \in \mathbb{Q}[x]$ 使得

$$f(x) = (qx - p) \cdot g(x),$$

但 p, q 互素, 则 $(qx-p)$ 是本原多项式, 所以 $g(x)$ 是整系数多项式, 上式中以 m 代 x , 则得