21世纪高等院校数学指南丛书

高等代数

定理·问题·方法

胡适耕　刘先忠　编著

科学出版社
www.sciencep.com

·21世纪高等院校数学指南丛书·

高等代数

定理·问题·方法

胡适耕　刘先忠　编著

科学出版社

北京

内 容 简 介

高等代数与数学分析并称为最重要的数学基础课程，多年来为教育界所公认。学生从高等代数课程中所获得的知识与方法训练，在其后的数学学习与研究中有不可替代的作用。本书通过 800 道例题分析，透彻地阐释并系统运用了读者在学习过程中所感觉到的优美的思想与方法，务求读者能真正透彻地弄清一些问题。全书共分四章，分别为多项式、矩阵与向量、特征值与标准形、内积空间与二次型，每小节以概念与定理、问题与方法的模式进行阐述。

本书可作为高等院校数学及相关专业本科生的辅导用书，也可供报考研究生的学生和相关科研人员参考。

图书在版编目（CIP）数据

高等代数：定理•问题•方法/胡适耕，刘先忠编著．—北京：科学出版社，2007.1

（21 世纪高等院校数学指南丛书）

ISBN 978-7-03-018288-3

Ⅰ.高… Ⅱ.①胡…②刘… Ⅲ.高等代数－高等学校－教学参考资料 Ⅳ.O15

中国版本图书馆 CIP 数据核字（2006）第 153159 号

责任编辑：江 兰／责任校对：董 丽

责任印制：高 嵘／封面设计：宝 典

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

武汉大学出版社印刷总厂印刷

科学出版社发行 各地新华书店经销

*

2007 年 1 月第 一 版 开本：B5（720×1000）

2007 年 1 月第一次印刷 印张：14 1/4

印数：1—4 000 字数：277 000

定价：19.80 元

（如有印装质量问题，我社负责调换）

前　言

高等代数与数学分析并称为最重要的数学基础课程，多年来为数学教育界所公认，这一格局在可预见的未来也不大可能根本改变. 学生从高等代数课程中所获得的知识与方法训练，在其后的数学学习与研究中有不可替代的作用. 值得耽心的倒是，数学系的大学生从高等代数课程中能获得足够的训练吗？如果在这个为期一年的课程结束之后，学生对于高等代数的核心概念与基本方法仍然难知底里，那么，除了承认这实属正常而予以理解之外，正是该有所建议与帮助了. 在这方面，数学界同仁已有不少佳作可供学生选读. 例如，樊恽教授等人编著的《线性代数学习指导》(科学出版社，2003)就具有很大的可读性，值得特别推荐. 在同一个方向上，作者并不自认会做得更好些而去重复他人的工作. 作者的兴趣完全在另一方面：学生从课程学习中只是有点朦胧感觉的那些优美的思想与方法，一旦被透彻阐释并系统运用，就会真正成为学生基本数学修养中有实质性价值的一部分，成为一种"功夫"，会受益终身. 因此，作者在本书中，不免"喋喋不休"，反复讨论某些问题与方法. 上述意向，主导了本书的构思.

作者的愿望是务求读者真正透彻地弄清楚一些问题，至少在某些问题上达到某种"领悟". 这样的目的并不能兼顾全面，因而我们一开始就未打算包罗所有内容. 论述的重点只是作者认为最重要的东西. 但是，这些内容构成课程的核心部分，涵盖了准备进入硕士学习的读者所关注的内容.

思想与方法总得通过适当的问题来阐述. 本书选择问题的主导想法是：它们应当成为引导读者系统领会若干方法原则的工具. 就具体特色而言，方法依所针对的问题而异；但从方法论的角度考虑，某些几乎普适的原则有着持久的吸引力. 成功的方法应当符合简化原则、转化原则与对称原则，这些原则的科学与美学价值都是不言而喻的. 某个问题或某个方法，局限在某个理论的范围内，可能不是最可取的；但若它所体现的思想带来有某种普遍意义的启示，那么它就可能在数学探索的旅途中留下不可磨灭的印迹，因而是一个非常可取的问题或方法. 要之，我们并非就事论事，而是处处尽力保持一种高瞻远瞩的观点，以小见大，从特殊中发现一般. 这既是作者致力于遵循的原则，也是寄希望于本书读者之所在.

本书内容大体上按其自然顺序安排. 但为收到更大的综合与概括的效果，在某些地方涉及后面的内容. 对于一本并非用作教材的书，这不会是一个很大的问题. 作者的经验是，与读者一道去经历某些思考过程，一起去体验其中的艰辛与得失，

既是一种义务，更是一种真正的乐趣. 因此，本书尽可能采用某种对话式的语体，以期加强与读者的沟通；至于雅俗之议，则不复为虑了. 为了节省篇幅，同时也为了更富有表达力，我们尽可能采用缩记号；不过所有的记号都是通行的(但可能不是唯一的)，且集录在正文之前以供查询. 凡要求证明的问题，都只表述结论，而略去“求证”一类的词. 诸如此类的省略往往一望而知，当不致成为顺利阅读本书的障碍. 当然，改进的余地永远存在，而这正是有待于同行与读者帮助的.

作　者

2006 年 10 月

记号与约定

$A=[a_{ij}]_{m\times n}$ 或 $A_{m\times n}$:$m\times n$ 矩阵.

A^{T}: 矩阵 A 的转置.

A^*: 矩阵 A 的伴随.

$\overline{A}$: 矩阵 A 的共轭.

$|A|$: 矩阵 A 的行列式.

A_{ij}:(i,j) 代数余子式.

$\mathbf{C}$:复数域; $\mathbf{C}^n$:n 维复向量空间.

$\mathbf{C}^{m\times n}$:$m\times n$ 复矩阵之全体.

$D_i(\lambda)$:i 阶子式因子.

$d_i(\lambda)$:i 阶不变因子.

$\mathrm{diag}(a_1,a_2,\cdots,a_n)$ 或 $\mathrm{diag}(a_i)$: 对角形矩阵.

$\mathrm{diag}(A_1,A_2,\cdots,A_k)$ 或 $\mathrm{diag}(A_i)$: 准对角形矩阵.

$\dim V$: 向量空间 V 的维数.

$\Delta_A(\lambda)$: 矩阵 A 的特征多项式.

δ_{ij}: Kronecker 记号.

E_{ij}: 第 i 行第 j 列交叉处为 1 而其余元为零的矩阵.

e:经常用来表示向量 $(1,1,\cdots,1)^{\mathrm{T}}$.

$G(\alpha_1,\alpha_2,\cdots,\alpha_m)$: 向量组 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 的 Gram 矩阵.

$\gcd(f_1,f_2,\cdots,f_k)$: 多项式 $f_1,f_2,\cdots,f_k$ 的最大公因式.

I:单位矩阵; I_n:n 阶单位矩阵.

I: 单位变换.

$\mathrm{Im}\ z$: 复数 z 的虚部.

J:通常记Jordan 矩阵.

$J(a,k)$: 具特征值 a 的 k 阶 Jordan 块.

$\mathbf{K}$:数域,通常取为 $\mathbf{R}$ 或 $\mathbf{C}$.

$\mathbf{K}^{m\times n}$:$\mathbf{K}$ 上的 $m\times n$ 矩阵之全体.

$\mathbf{K}[x]$:$\mathbf{K}$ 上以 x 为变元的多项式环.

$\mathbf{K}_n[x]$:$\mathbf{K}$ 上次数$\leqslant n$ 的多项式之全体.

$L(V)$:V 上线性变换之全体.

$\mathrm{lcm}(f_1,f_2,\cdots,f_k)$: 多项式 $f_1,f_2,\cdots,f_k$ 的最小公倍式.

$m_A(\lambda)$：矩阵 $\boldsymbol{A}$ 的最小多项式.

$\mathbf{N}$：自然数集.

$N(T)$：线性映射 T 的核；$N(\boldsymbol{A})$：矩阵 $\boldsymbol{A}$ 的零空间.

$\mathbf{Q}$：有理数域.

$R(T)$：线性映射 T 之值域；$R(\boldsymbol{A})$：矩阵 $\boldsymbol{A}$ 之列空间.

$\mathbf{R}$：实数域；$\mathbf{R}^n$：实 n 维向量之空间.

$\mathbf{R}^{m\times n}$：$m\times n$ 实矩阵之全体。

$\mathrm{Re}\, z$：复数 z 的实部.

$r(\boldsymbol{A})$ 或 $\mathrm{rank}\, \boldsymbol{A}$：矩阵 $\boldsymbol{A}$ 之秩.

$\mathrm{rank}(\alpha_1,\alpha_2,\cdots,\alpha_m)$：向量组 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 之秩.

$\mathrm{span}\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$：向量组 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 生成的子空间.

$\mathrm{span}\, S$：向量组 S 生成的子空间.

$\sigma(T)$：线性变换 T 的特征值之全体；$\sigma(\boldsymbol{A})$ 仿此.

T,S 等：通常记线性变换.

U,V,W 等：通常记向量空间.

$W^{\perp}$：W 的正交补.

$\begin{pmatrix} m \\ n \end{pmatrix} = C_m^n = \dfrac{m!}{n!(m-n)!}$.

$[x]$：不超过 x 的最大整数.

$\boldsymbol{A}\cong\boldsymbol{B}$：矩阵 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 等价.

$\boldsymbol{A}\sim\boldsymbol{B}$：矩阵 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 相似.

$\boldsymbol{A}(\lambda)\cong\boldsymbol{B}(\lambda)$：$\lambda$ 矩阵 $\boldsymbol{A}(\lambda)$ 与 $\boldsymbol{B}(\lambda)$ 等价.

$f|g$：多项式 f 整除 g.

$A\cup B$：集 A 与 B 之并.

$A\cap B$：集 A 与 B 之交.

$A\backslash B$：集 A 与 B 之差.

矩阵通常记为黑体大写英文字母，如 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}$；向量通常记为小写黑体希腊字母，如 $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}$；$n$ 维向量（即 $\mathbf{K}^n$ 中的元素）有时也用记号 $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}$ 等. $\boldsymbol{0}$ 表示零向量或零空间，依具体情况而定.

行列式与矩阵中的空白部分为零元素，而 $*$ 号则代表某些不必明确写出的元素.

和式 $\sum\limits_{i=1}^{n} a_i$ 依情况简写作 $\sum\limits_{i} a_i$，$\sum_1^n a_i$ 或 $\sum a_i$，在不致误解的情况下尽可能取简单的写法；乘积式 $\prod\limits_{i=1}^{n} a_i$ 仿此.

目　　录

第一章 多 项 式

从多项式开始高等代数的学习，看来再合适不过了. 你会感到这是一个熟悉的对象：在初等代数中，已讨论过二次多项式及某些简单的高次多项式了. 但如何一般地处理多项式，却是一个全新的课题，初等代数的简单方法远不足以为用. 现在你将面对一套完全不同的语言与处理模式，其突出特点就是将所有概念与结论建立在完全一般化的逻辑基础上. 学习多项式理论，既是对一个老课题的深化，也是熟悉高等代数方法的一个起点.

本章自然地分为两部分：一般理论，它不涉及基域 **K** 的特殊性质；复与实多项式(包括更特殊的有理多项式)，它用到复数域、实数域及有理数域的特殊性质.

§1.1 一 般 理 论

I 概念与定理

本书中，总以 **K** 记一给定的数域，它通常指实数域 **R** 或复数域 **C**，但也不排除指其他数域(如有理数域 **Q**). 以 $\mathbf{K}[x]$ 记以 x 为变元而系数在 **K** 中的多项式之全体. $f(x) \in \mathbf{K}[x]$ 的一般形式为

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

其中 $a_i \in \mathbf{K}$ $(0 \leqslant i \leqslant n)$. 当 $a_n \neq 0$ 时，称 $f(x)$ 为 n 次多项式，记为 $\deg f = n$；若 $a_n = 1$，则称 f 为**首一多项式**. 若 $f = 0$，则 f 没有次数，此时约定 $\deg f = -\infty$. 若 $f \in \mathbf{K}[x]$，则当 $\mathbf{K} = \mathbf{C}, \mathbf{R}$ 与 $\mathbf{Q}$ 时，分别称 f 为复多项式、实多项式与有理多项式.

关于多项式的最基本的事实是：对多项式可施行加法与乘法，且满足如同相应的数运算一样的运算规则，如交换律、结合律与分配律等，这使 $\mathbf{K}[x]$ 构成一个性质良好的代数系统，即所谓**多项式环**. 但我们立即发现，$\mathbf{K}[x]$ 毕竟不如 **K** 那么完美，其主要缺陷就是除法并非总能施行，常常有“除不尽”的时候，多项式理论的核心问题就是围绕这一事实展开的. 要回答的一个基本问题是，对于给定的 $f, g \in \mathbf{K}[x]$，在什么条件下 f“除尽”g？这一问题引出一系列概念.

1.1.1 定义 设 $f, g, h, f_1, \cdots, f_k \in \mathbf{K}[x]$.

(i) 若 $f = gh$，则称 g 为 f 的因式，而称 f 为 g 的倍式.

(ii) 若 g 是 f 的因式，$g \neq 0$，则说 g **整除** f，记作 $g|f$.

(iii) 若 $h|f_i$ $(1 \leqslant i \leqslant k)$，则称 h 为 $f_1, f_2, \cdots, f_k$ 的**公因式**；次数最高的公因式称为**最大公因式**，约定以 $\gcd(f_1, f_2, \cdots, f_k)$ 记 $f_1, f_2, \cdots, f_k$ 的首一最大公因式. 若 $\gcd(f_1, f_2, \cdots, f_k) = 1$，则说 $f_1, f_2, \cdots, f_k$ **互质**.

(iv) 与(iii)对偶地，若 $f_i|g$ $(1 \leqslant i \leqslant k)$，则称 g 为 $f_1, f_2, \cdots, f_k$ 的**公倍式**；次数最低的公倍式称为**最小公倍式**，约定以 $\mathrm{lcm}(f_1, f_2, \cdots, f_k)$ 记 $f_1, f_2, \cdots, f_k$ 的首一最小公倍式.

(v) 若 $\deg f > 0$，f 除同次与零次因式之外别无其他因式，则称 f 为 $\mathbf{K}$ 上的**不可约多项式**.

理解上述概念的一个重要辅助方法是与整数的相应概念进行对照：因式与倍式分别对应整数的因数与倍数；最大公因式与最小公倍式分别对应于最大公约数与最小公倍数；不可约多项式则颇类似于质数. 下面的除法定理也可看作关于整数除法相应结论的推广.

1.1.2 定理　设 $f, g \in \mathbf{K}[x]$.

(i) **带余除法**：若 $g \neq 0$，则存在由 f, g 唯一决定的 $q, r \in \mathbf{K}[x]$，使得 $\deg r < \deg g$，且

$$f = gq + r \tag{1}$$

上述的 q 与 r 分别称为 g 除 f 的商与余式；$g|f \Leftrightarrow r = 0$.

(ii) **余数定理**：$\forall\, a \in \mathbf{K}$，存在唯一的 $q \in \mathbf{K}[x]$，使得

$$f(x) = (x - a)q(x) + f(a). \tag{2}$$

显然 $f|f$ (自反性)；$f|g$ 且 $g|h \Rightarrow f|h$ (传递性)；$f|g$ 且 $g|f (gf \neq 0) \Leftrightarrow f$ 与 g 仅差一常数因子(某种意义上的反对称性). 这些都是很明显的简单事实. 下面的定理则综合了有关整除性的较深入的结论.

1.1.3 定理　设 $f, g, h, f_1, \cdots, f_k \in \mathbf{K}[x]$，则以下结论成立：

(i) 设 $f_1, f_2, \cdots, f_k$ 不全为零；则 $f_1, f_2, \cdots, f_k$ 的最大公因式存在，当不计常数因子的差别时是唯一的；特别地，$d = \gcd(f_1, f_2, \cdots, f_k)$ 唯一地存在，它是 $f_1, f_2, \cdots, f_k$ 的任何公因式的倍式. 存在 $p_1, p_2, \cdots, p_k \in \mathbf{K}[x]$，使得

$$f_1p_1 + f_2p_2 + \cdots + f_kp_k = d \tag{3}$$

若 d 是 $f_1, f_2, \cdots, f_k$ 的首一公因式且满足(3)，则必有

$$d = \gcd(f_1, f_2, \cdots, f_k).$$

(ii) $f_1, f_2, \cdots, f_k$ 互质 $\Leftrightarrow$ 存在 $p_1, p_2, \cdots, p_k \in \mathbf{K}[x]$，使得

$$f_1p_1 + f_2p_2 + \cdots + f_kp_k = 1. \tag{4}$$

(iii)(与(i)对照) 设 $f_1, f_2, \cdots, f_k$ 不全为零，则 $f_1, f_2, \cdots, f_k$ 的最小公倍式存在，当不计常数因子的差别时是唯一的；特别地，$m = \mathrm{lcm}(f_1, f_2, \cdots, f_k)$ 唯一地存在，它是 $f_1, f_2, \cdots, f_k$ 的任何公倍式的因式.

(iv) 若 $f|gh$，f 与 g 互质，则 $f|h$；若 $f|h$，$g|h$，f 与 g 互质，则 $fg|h$.

(v) 若 $h|f_1f_2\cdots f_k$，h 是不可约多项式，则 h 整除某个 f_i $(1\leqslant i\leqslant k)$.

若 $f_1f_2\cdots f_k\neq 0$，$k>1$，则有

$$\gcd(f_1,f_2,\cdots,f_k)=\gcd(\gcd(f_1,\cdots,f_{k-1}),f_k).$$

因此，原则上只要有求两个多项式的最大公因式的方法就够了. 为求 $\gcd(f,g)$，可用如下的**辗转相除法**：

$$\begin{aligned} f&=gq_1+r_1,\\ g&=r_1q_2+r_2,\\ &\cdots\cdots\\ r_{n-2}&=r_{n-1}q_n+r_n,\\ r_{n-1}&=r_nq_{n+1}. \end{aligned}$$

利用以上等式相继消去 $r_{n-1},r_{n-2},\cdots,r_1$，可得

$$r_n=f\tilde{p}_1+g\tilde{p}_2,$$

r_n 即为 f 与 g 的最大公因式. 上式两端除以适当常数后即得所需的

$$\gcd(f,g)=fp_1+gp_2.$$

1.1.4 因式分解定理 任何非常数多项式 $f\in \mathbf{K}[x]$ 有分解式：

$$f=ap_1p_2\cdots p_m,\tag{5}$$

其中 $0\neq a\in\mathbf{K}$；p_i $(1\leqslant i\leqslant m)$ 是 $\mathbf{K}$ 上的首一不可约多项式. 若不计因式排列次序，分解式(5)是唯一的.

可将(5)改写成如下标准分解式：

$$f=ap_1^{n_1}p_2^{n_2}\cdots p_k^{n_k},\tag{5$'$}$$

其中 $p_1,p_2,\cdots,p_k$ 是互异的首一不可约多项式；$n_i\geqslant 1$ $(1\leqslant i\leqslant k)$. 若 $n_i=1$，则称 p_i 为单因式；若 $n_i>1$，则称 p_i 为 n_i 重因式. 直接计算导数易得如下结论：p 是 f 的 n 重因式 $\Leftrightarrow p$ 是 f 的因式，且是 f' 的 $n-1$ 重因式 $\Leftrightarrow p$ 是 $f,f',\cdots,f^{(n-1)}$ 的公因式但不是 $f^{(n)}$ 的因式.

分解式(5)或(5)$'$可用来解决多项式理论中的种种问题. 例如，利用因式分解可简单地求出最大公因式与最小公倍式：设

$$f_i=a_ip_1^{n_{i1}}p_2^{n_{i2}}\cdots p_k^{n_{ik}}\quad(1\leqslant i\leqslant m),$$

其中 $0\neq a_i\in\mathbf{K}$；p_j 是 $\mathbf{K}$ 上互异的首一不可约多项式；$n_{ij}\geqslant 0$ $(1\leqslant i\leqslant m;\ 1\leqslant j\leqslant k)$，则

$$\begin{cases}\gcd(f_1,f_2,\cdots,f_m)=p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k},\\ \operatorname{lcm}(f_1,f_2,\cdots,f_m)=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k},\end{cases}\tag{6}$$

其中 $s_j=\min\limits_i n_{ij}$；$t_j=\max\limits_i n_{ij}$ $(1\leqslant j\leqslant k)$.

以上简单结论容易造成一个错觉：似乎求最大公因式的问题有了一个比辗转

相除法更简捷的解法.问题在于,如何求得分解式(5)呢?我们仅知道它原则上存在,但如何实际求出它,则并无任何普遍可行的方法.

多项式理论的相当一部分内容无关乎对变元 x 的解释.你大概已注意到,多项式定义中甚至未赋予 x 确切的含义,这与你从初等代数继承下来的直观理解有很大不同.这样做的好处是,唯有不将 x 定死,才使得多项式理论可作多种应用的可能.你在接触到矩阵多项式、线性变换多项式等内容之后,对此将会有更深的体会.

与上述高度一般化的观点相比较,限制 x 在数域$\mathbf{K}$ 内变动就略显狭窄了.但这种朴素的观点有一个明显的好处,那就是可将 $f(x)\in\mathbf{K}[x]$ 看作定义在$\mathbf{K}$ 上的函数,因而可充分利用函数论方法的种种便利,这一点在下节中将显得突出.这一观点的深入展开当然有赖于利用域$\mathbf{K}$ 的特殊性质.在不对$\mathbf{K}$ 作任何特殊假定的条件下,亦可提出某些简单的概念与结论,其中某些正是下面就要提及的.

给定 $f\in\mathbf{K}[x]$. 若 $a\in\mathbf{K}$ 使得 $f(a)=0$,则称 a 为 f 在$\mathbf{K}$ 中的一个根或零点.显然 a 是 f 的根 $\Leftrightarrow x-a$ 是 f 的因式(依(2));f 有根 $\Leftrightarrow f$ 有一次因式.若 $x-a$ 是 f 的 k 重因式,$k\geqslant 1$,则称 a 为 f 的 k 重根.

1.1.5 定理　设 $f\in\mathbf{K}[x]$ 是一个 n 次多项式,$n\geqslant 1$,则以下结论成立:

(i) f 在$\mathbf{K}$ 中至多有 n 个根(计算重数);f 的根的个数就是 f 的分解式中一次因式的个数.

(ii) 若存在 $n+1$ 个互异的数 x_i,使得 $f(x_i)=0\ (0\leqslant i\leqslant n)$,则 $f=0$.

II　问题与方法

A. 整除性

如已指出的,多项式理论可以说始于除法.不消说,作多项式除法的技巧是基本的.带余除法是一种完全机械的操作,并不难掌握.但它往往过于繁琐,并不特别令人喜爱,只要有其他替代办法,就不妨绕过它.关键的事实是,表达式(1)的结构并不依赖于除法演算过程,其中的 $q(x)$ 与 $r(x)$ 可通过其他方法(如待定系数法)确定.

在未明确说明时,以下出现的 f,g,h 等均假定属于 $\mathbf{K}[x]$.

1. 设 $a,b\in\mathbf{K}$ 互异,求 $f(x)$ 除以 $(x-a)(x-b)$ 的余式 $r(x)$.

解　因 $r(x)$ 至多是一次多项式,故可写出

$$f(x)=(x-a)(x-b)q(x)+cx+d,$$

其中系数 c,d 待定.分别取 $x=a$ 与 $x=b$ 代入得

$$f(a)=ca+d,f(b)=cb+d.$$

联立以上两式解出 c,d,即得

$$r(x)=\frac{f(a)-f(b)}{a-b}x+\frac{af(b)-bf(a)}{a-b}.\qquad\square$$

2. 求 $f(x^3+1)$ 除以 x^2-1 的余式 $r(x)$.

提示 用题1之解法；

$$r(x)=\{[f(2)-f(0)]x+f(2)+f(0)\}/2.$$

3. 设 $f(x)=x^3+px+q, g(x)=x^2+bx-1, g|f$，求 b,p,q 之间的关系.

解I(待定系数法) 仿照题1的解法，令

$$f(x)=(x^2+bx-1)(x+a),$$

比较等式两端系数得

$$b+a=0,\quad p=ab-1,\quad q=-a.$$

从以上等式消去 a 得 $b=q, b^2+p+1=0$.

解II(带余除法) 以 g 除 f 得余式

$$r(x)=(b^2+p+1)x+q-b.$$

于是由 $r=0$ 可得 $b^2+p+1=0, b=q$. □

以上两种解法实质上一致，形式上则各有特点，均可采用.

4. 设 $(x^2+bx+1)|(x^4+px^2+q)$，求 b,p,q 之间的关系.

提示 参照题3；$b^2+p=q+1, b=bq$.

5. 设 $(x^2+bx-1)|[x^3-(a^2+1)x+a]$，求 a,b 之关系. $(a=b)$

6. 设 $m,n\geqslant 1$，则 $(x^m-1)|(x^n-1)\Leftrightarrow m|n$.

提示 设 $n=mq+r, 0\leqslant r<m$，则

$$x^{n-1}=x^r(x^{mq}-1)+x^r-1.$$

7. 设 $f(x)=x^2-4x+a$，存在唯一的3次首一多项式 g，使得 $f|g$ 且 $g|f^2$，求 a 与 g.

解 首先仍用待定系数法，写出

$$g(x)=f(x)(x-b),\quad f^2(x)=g(x)(x-c),$$

其中 b,c 待定. 结合以上两式得 $f^2(x)=f(x)(x-c)(x-b)$，于是 $h(x)=f(x)(x-c)$ 满足 $f|h$ 与 $h|f^2$，因而由题设中的唯一性条件得出 $h=g$，即 $f(x)(x-c)=f(x)(x-b)$，由此推出 $c=b$（何故？）. 这又推出 $f^2(x)=f(x)(x-b)^2$，从而 $f(x)=(x-b)^2$，这与 $f(x)=x^2-4x+a$ 比较得 $a=4, b=2$，$g(x)=(x-2)^3$. □

对于给定的 $f,g\in \mathbf{K}[x]$，判定 $f|g$ 的方法如下：

(i) **因式分解法**：直接将 g 分解因式，得出 $g=fh$，这只在很特殊的情况下才能做到.

(ii) **验根法**：若能求出 f 的全部复根 $a_1,a_2,\cdots,a_n$，且这些根互异，则 $f|g\Leftrightarrow g(a_i)=0\ (1\leqslant i\leqslant n)$.

应注意，尽管 $f|g$ 是一可以在**K** 中确立的事实，但仅求出 f 在**K** 中的根不足以检验 $f|g$. 例如，$f(x)=(x-1)(x^2+1)$ 并不整除 $g(x)=(x-1)^3$，但 $f(x)$ 的

唯一实根 1 满足 $g(1)=0$!

8. 设 $f(x)=1+x^2+\cdots+x^{2n}$,$g(x)=1+x^4+\cdots+x^{4n}$,则有 $f|g \Leftrightarrow n$ 为偶数.

证　容易想到首先应化简 f 与 g 的表达式:

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

$$g(x)=\frac{x^{4(n+1)}-1}{x^4-1}=f(x)\frac{x^{2(n+1)}+1}{x^2+1}.$$

由此得出 $f|g$ 的充要条件是

$$q(x)(x^2+1)=x^{2(n+1)}+1,$$

$q(x)$ 是一多项式. 以 $x=\mathrm{i}$ 代入得 $0=(-1)^{n+1}+1$,因此 $f|g \Leftrightarrow n$ 为偶数. □

9. 设 $f(x)=(x+1)^{2n}+2x(x+1)^{2n-1}+\cdots+2^n x^n(x+1)^n$,$g(x)=(x-1)f(x)+(x+1)^{2n+1}$,则 $x^{n+1}|g(x)$.

提示　推出 $(x-1)f(x)=(x+1)^n[(2x)^{n+1}-(x+1)^{n+1}]$.

10. 设 $(x^2+x+1)|[f(x^3)+xg(x^3)]$,则 $x-1$ 整除 $\gcd(f,g)$.

证　x^2+x+1 有一对共轭复根 $\varepsilon,\bar{\varepsilon}$,它们都是 1 的立方根. 以 $\varepsilon,\bar{\varepsilon}$ 代入 $f(x^3)+xg(x^3)$ 得

$$\begin{cases} f(1)+\varepsilon g(1)=0, \\ f(1)+\bar{\varepsilon} g(1)=0. \end{cases}$$

将这看作关于 $f(1)$,$g(1)$ 的线性方程组,解出 $f(1)=0=g(1)$,因此 $(x-1)|f$,$(x-1)|g$,从而 $(x-1)|\gcd(f,g)$. □

11. 设 $(x-1)|f(x^n)$,则 $(x^n-1)|f(x^n)$.

提示　利用 $f(1)=0$.

12. $(x^2+x+1)|[x^{n+2}+(x+1)^{2n+1}]$,$n\geqslant 0$.

提示　设 $\varepsilon^2+\varepsilon+1=0$,则 $\varepsilon^3=1$,$\varepsilon+1=-\varepsilon^2$.

13. $(x^2+x+1)|(x^{3m}+x^{3n+1}+x^{3p+2})$,$m,n,p\geqslant 0$.

提示　参照题 12.

14. 设 $(x^2+x+1)|[(x+1)^n-x^n-1]$,$n\geqslant 1$,求 n.

解　仍然用验根法,但这次计算要复杂些. x^3-1 的复根为 $\varepsilon=\mathrm{e}^{\pm 2\pi\mathrm{i}/3}$. 由整除性条件有

$$0=(\varepsilon+1)^n-\varepsilon^n-1=(-1)^n\varepsilon^{-n}-\varepsilon^n-1.$$

若 n 为偶数,则 $1=\varepsilon^{-n}-\varepsilon^n=$ 纯虚数,必予排除. 当 n 为奇数时,

$$-1=\varepsilon^n+\varepsilon^{-n}=2\cos\frac{2n\pi}{3},$$

这推出 $n=3m\pm 1$. 但要使 n 为奇数,应取 $m=2k$,故 $n=6k+1$ $(k\geqslant 0)$ 或 $n=6k-1$ $(k\geqslant 1)$. □

在所涉及的多项式完全未给出具体表达式的情况下，整除性只能依据适当的定性推导进行判断. 这一类的问题无疑有很大的多样性，未必能归纳出某种一般解法. 不过，求助于定义 1.1.1 与定理 1.1.3 是要优先考虑的.

15. 设 $f|gh$，f 与 g 互质，则 $f|h$.

证 涉及互质性的问题不免要联系于等式（依(4)）

$$fp + gq = 1 \quad (p,q\text{ 为多项式})；$$

由此得 $fhp + ghq = h$. 因左端每项含因式 f，故 $f|h$. □

16. 设 $f|g_1\cdots g_k h$，f 与每个 g_i $(1\leqslant i\leqslant k)$ 互质，则 $f|h$.

提示 指明 f 与 $g_1g_2\cdots g_k$ 互质（参看题 36）.

17. 设 $f|h$，$g|(h/f)$，则 $fg|h$.

提示 令 $h = fp$，$p = gq$.

18. 设 $f|h$，$g|h$，f 与 g 互质，则 $fg|h$.

提示 注意 $g|f(h/f)$，综合运用题 15 与 17.

19. 设 $f_i|h$ $(1\leqslant i\leqslant k)$，$f_1,f_2,\cdots,f_k$ 两两互质，则 $f_1f_2\cdots f_k|h$.

提示 对 k 用归纳法并用题 18.

20. 设 $fg|\varphi h$，$\varphi|f$，则 $g|h$.

证 在没有其他明显依据可用的情况下，就只有直接援用整除性的定义了. 写出

$$\varphi h = fgp,\quad f = \varphi q \quad (p,q\text{ 为多项式}),$$

由此得 $\varphi h = \varphi gpq$，两端约去 φ 后得 $h = gpq$，这正表明 $g|h$.

B. 最大公因式

为求 $d = \gcd(f,g)$，可考虑如下方法：

(i) 辗转相除法：此法虽无技巧可言，但首先要求已给出 f 与 g 的具体表达式，且当多项式次数较高时计算可能很繁琐，甚至无法完成.

(ii) 观察法：由观察推断出某个多项式 d，然后验证 $d|f$，$d|g$，且 f 与 g 的任何公因式整除 d.

(iii) 利用关于最大公因式的某些已知公式，如本段中的题 28，29，32 等.

21. 设 $f(x) = 3x^3 - 2x^2 + x + 2$，$g(x) = x^2 - x + 1$，求 $d = \gcd(f,g)$ 与分解式 $d = fp + gq$.

解 用辗转相除法得出

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

综合以上两式得

$$\begin{aligned}1 &= -x(x-1) + g(x)\\ &= x[f(x) - g(x)(3x+1)] + g(x)\end{aligned}$$

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

可见 $\gcd(f,g) = 1$，且已得出所需分解式. □

22. 设 $f(x) = x^4 - x^3 - 4x^2 + 4x + 1, g(x) = x^2 - x - 1$，求 $d = \gcd(f,g)$ 与分解式 $d = fp + gq$.

提示 用辗转相除法；

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

23. 设 $f(x) = x^3 + 2x^2 + 2x + 1, g(x) = x^4 + x^3 + 2x^2 + x + 1$，求 $\gcd(f,g)$. $(= x^2 + x + 1)$

24. 设 $f(x) = x^n + a_1x^{n-1} + \cdots + a_n, g(x) = x^{n-1} + a_1x^{n-2} + \cdots + a_{n-1}$, $n > 1$，求 $\gcd(f,g)$.

解 关键是注意到

$$f(x) = xg(x) + a_n.$$

若 $a_n = 0$，则 $g|f$，因而 $\gcd(f,g) = g$；若 $a_n \neq 0$，则 f 与 g 不可能有非常数公因式，因此 $\gcd(f,g) = 1$. □

25. 设 $f(x) = x^{m+n} - x^m - x^n - 1, g(x) = x^m - x^{m-n} - 2, m > n$，求 $\gcd(f,g)$.

提示 注意 $f(x) = x^n g(x) + x^n - 1$，而 $f(x), g(x)$ 与 $x^n - 1$ 无公根.

26. 设 $f(x) = x^2 + (a+6)x + 4a + 2, g(x) = x^2 + (a+2)x + 2a, d = \gcd(f,g)$ 是一次多项式，求 a.

解 首先注意到 $f - g$ 有简单表达式：

$$f(x) - g(x) = 4x + 2a + 2.$$

另一方面，$d|(f-g)$，因此 d 与 $f-g$ 仅差常数因子，这就得出 $d(x) = x + (a+1)/2$. 然后由 $f(-(a+1)/2) = 0$ 解出 $a = 1$ 或 3. □

27. 设 $f(x) = x^3 + (a+1)x^2 + 4x + b, g(x) = x^3 + ax^2 + b, \gcd(f,g)$ 是 2 次多项式，求 a,b.

提示 用辗转相除法得余式 $4(4-a)x + b$；$a = 4, b = 0$.

与最大公因式有关的公式并不是很多，下面是几个有用的例子.

28. 设 g 是首一多项式，则

$$g \cdot \gcd(f_1, f_2, \cdots, f_k) = \gcd(gf_1, gf_2, \cdots, gf_k).$$

证 令 $d = \gcd(f_1, f_2, \cdots, f_k)$，则有多项式 p_i $(1 \leqslant i \leqslant k)$ 使式(3)成立. 因

$$gd = gf_1p_1 + gf_2p_2 + \cdots + gf_kp_k,$$

且显然 $gd | gf_i$ $(1 \leqslant i \leqslant k)$，故依定理 1.1.3(i)有

$$gd = \gcd(gf_1, gf_2, \cdots, gf_k).$$ □

29. $\gcd(f^n, g^n) = [\gcd(f,g)]^n$.

提示 用题 28 之证法.

30. 设 $d=\gcd(f_1,f_2,\cdots,f_k)\neq 0$，则

$$\gcd(f_1/d,f_2/d,\cdots,f_k/d)=1.$$

提示 由题28有 $d\gcd(f_1/d,\cdots,f_k/d)=d$.

31. 设 $ad\neq bc$，则 $\gcd(af+bg,cf+dg)=\gcd(f,g)$.

证 不妨设 $\gcd(f,g)=1$（用题30），且 $ad-bc=1$（否则按比例改变 a,b,c,d）. 取多项式 p,q，使 $1=fp+gq$，则可验证

$$1=(dp-cq)(af+bg)+(aq-bp)(cf+dg)$$

这表明 $\gcd(af+bg,cf+dg)=1$. □

32. 设 $g_i=\sum\limits_j a_{ij}f_j\ (1\leqslant i\leqslant k)$，行列式 $|a_{ij}|\neq 0$，则

$$\gcd(g_1,g_2,\cdots,g_k)=\gcd(f_1,f_2,\cdots,f_k).$$

提示 原则上仍用题31之证法，但用矩阵记号会表述得简明些.

33. 设 $g\neq 0$，则 $\gcd(f,g)=\gcd(f-gh,g)$.

提示 验证等式两端互相整除.

下面是关于互质性的几个问题. 因为这不过是最大公因式问题的特殊情况，因而所有关于最大公因式的已知结果都可以考虑利用.

34. 设 $n\geqslant 1$，则 f 与 g 互质 $\Leftrightarrow f^n$ 与 g^n 互质.

提示 可用题29，但作为练习，最好直接证明.

35. 设 $f_1,f_2,\cdots,f_k$ 互质，$g_i=\sum\limits_j a_{ij}f_j(1\leqslant i\leqslant k)$，而行列式 $|a_{ij}|\neq 0$，则 $g_1,g_2,\cdots,g_k$ 互质.

提示 用题32.

36. 设 f 与每个 $g_i\ (1\leqslant i\leqslant k)$ 互质，则 f 与 $g\triangleq g_1g_2\cdots g_k$ 互质.

证 取多项式 p_i,q_i，使得 $fp_i+g_iq_i=1\ (1\leqslant i\leqslant k)$，则

$$1=(fp_1+g_1q_1)\cdots(fp_k+g_kq_k)=fp+gQ,$$

其中 $Q=q_1q_2\cdots g_k$；P 是一个多项式，其表达式不必写出. 这已表明 f 与 g 互质. □

37. 设 f 与 g 互质，则 $f+g$ 与 fg 互质.

提示 只要证 $f+g$ 与 f 互质，可参照题36之证法.

38. 设 $f_1,f_2,\cdots,f_k$ 中每一个与 $g_1,g_2,\cdots,g_m$ 中每一个互质，则 $f_1f_2\cdots f_k$ 与 $g_1g_2\cdots g_m$ 互质.

提示 相继两次利用题36.

39. f 与 g 互质 $\Leftrightarrow\forall\ h\in\mathbf{K}[x]$，存在 $p,q\in\mathbf{K}[x]$，使得 $h=fp+gq$.

提示 证充分性时特别取 $h=1$.

40. $f(x)$ 与 $g(x)$ 互质 $\Leftrightarrow f(x^n)$ 与 $g(x^n)$ 互质（n 是任给自然数）.

提示 f 与 g 互质 $\Leftrightarrow f$ 与 g 在复数域内互质 $\Leftrightarrow f$ 与 g 在复数域内无公根.