工程高等代数

阮传概 编著

北京邮电大学出版社

工程高等代数

北京邮电

工程高等代数

阮传概 编著

北京邮电大学出版社

图书在版编目(CIP)数据

工程高等代数/阮传概编著 .-北京:北京邮电大学出版社,1997.9
ISBN 7-5635-0286-6

Ⅰ. 工… Ⅱ. 阮… Ⅲ. 高等代数-应用-工程技术 Ⅳ. T B111

中国版本图书馆 CIP 数据核字(97)第 08626 号

内容简介

本书介绍了多项式、矩阵、线性空间与线性变换、线性方程组、矩阵的特征值与特征向量、欧氏空间与二次型，以及一些内容在工程中的应用。全书比较注重方法与应用，内容简练，例题较多，每章末均附有习题。

本书可作为信息科学、计算机科学、通信理论与系统工程等有关专业的高等代数或线性代数课程的教材，也可供从事工科有关专业及应用数学、应用物理等专业的科技人员参考。

工程高等代数

编　　著　阮传概

责任编辑　王守平

北京邮电大学出版社出版

新华书店北京发行所发行　各地新华书店经售

河北省高碑店市印刷厂印刷

787×1092 毫米　1/16　印张 13.625　字数 348 千字

1997 年 7 月第一版　1997 年 7 月第一次印刷

印数：1－1500 册

ISBN 7-5635-0286-6/O·15　定价：17.40 元

前　言

高等代数课程不仅在数学的各个分支中有很多应用，而且随着信息科学与计算技术的发展，在工程技术的很多领域中也有广泛的应用。高等代数的基本内容已成为广大科技工作人员的基本工具。现在，国内出版的高等代数教材，一般都是为数学专业的学生编写的，而对于信息科学、计算机科学、通信理论与系统工程等一些专业的学生，他们对高等代数的内容、方法的要求及教学时数与数学专业的学生是不同的，故本书是为工程技术的大学本科生编写的。

本书除包括教委规定的工科学校线性代数课程教学基本要求的内容外，还包括工程中常用的一些内容与方法。如：多项式理论，特别是 $\mathbf{Z}_2$ 上的多项式、矩阵的 Kronecker 积、广义逆、友矩阵、非负矩阵、不可约矩阵、随机矩阵、拉格朗日插值公式、最小二乘法、函数的极值等，以及有些内容在工程中的应用。

本书共六章，分别介绍了多项式、矩阵、线性空间与线性变换、线性方程组、矩阵的特征值与特征向量、欧氏空间与二次型。由于本书是为工科学生编写的，所以比较注重方法与应用，内容简练，有些结论省略了理论证明，例题较多，每章末均附有适合工科学生的习题。一般具有高中数学与物理知识的读者，就可以学习本书。

本书可作为信息科学、计算机科学、通信理论与系统工程等有关专业的高等代数或线性代数课程的教材，也可供从事工科有关专业及应用数学、应用物理等专业的科技人员参考。

本书讲授时数约 58 学时，如果学时不够可根据专业需要，删去一些内容或把某些内容供学生自学。

本书是作者多年来在北京邮电大学讲授此课程讲义的基础上修改而成的。在编写过程中得到了北京邮电大学信息工程系应用数学教研室全体老师、信息工程系办公室同志以及基础部数学教研室杨源淑、赵启松两位教授的大力支持和帮助，在此表示感谢。

北京师范大学郝钢新教授仔细地审阅了本书稿并提出了许多宝贵意见，在此表示衷心的感谢。

由于作者水平有限，定有不妥之处，殷切希望读者指正。

作者
1996.12

目　　录

第一章　一元多项式

多项式是代数学中的一个重要概念,它不但与研究方程的解、矩阵的特征值、二次型等内容有关,而且在数学的其他分支和工程问题中都有广泛的应用。如分析线性系统时,往往需要研究多项式的根。本章所讨论的一元多项式是在中学所学知识的基础上,进一步加深与系统化。

§1.1　集合、数域、映射

一、集合

集合的概念是自然科学中最基本的概念之一,它已深入到各种科学与技术的各领域中。集合就是一些不同对象的总体,集合也简称为集。通常用大写字母 $A,B,C,\cdots$ 表示。组成集合的对象称为该集合的元素。通常用小写字母 $a,b,c,\cdots$ 表示。如果 a 是集合 A 的元素,则称 a 属于 A,或 A 包含 a,记为 $a\in A$。如果 a 不是集合 A 的元素,则称 a 不属于 A,记为 $a\notin A$。确定一个集合 A 就是要确定:哪些元素属于 A,哪些元素不属于 A。

如果两个集合 A,B 所包含的元素完全一样,则称 A 和 B 相等,记为 $A=B$。

集合的表示法主要有两种:列表法与构造法。所谓列表法,就是列出集合的所有元素。例如,$A=\{x,y,z\}$ 表示 A 是由元素 x,y,z 构成的;所谓构造法,就是描述出集合中元素适合的条件。例如,$A=\{x\mid x^2-1=0,x\text{ 为实数}\}$,表示 A 是由 $-1,1$ 两个数构成的。

下面介绍几个常用的数集及所表示的字母:

全体整数构成的集,称为整数集,记为 $\mathbf{Z}$;

全体有理数构成的集,称为有理数集,记为 $\mathbf{Q}$;

全体实数构成的集,称为实数集,记为 $\mathbf{R}$;

全体复数构成的集,称为复数集,记为 $\mathbf{C}$。

例 1.1.1　$A=\{x\mid x\in\mathbf{Z},x^2-5x+6=0\}=\{2,3\}$. □

设 A,B 是两个集合,如果 A 的每个元素也是 B 的元素,则称 A 是 B 的子集,记为 $A\subseteq B$。例如 $A=\{a,c\},B=\{a,b,c,d\}$,则 A 是 B 的子集。又如,有理数集 $\mathbf{Q}$ 是实数集 $\mathbf{R}$ 的子集。任意集 A 是自己的子集。

设 A,B 是两个集合,$A=B\Leftrightarrow A\subseteq B$ 且 $B\subseteq A$。

不含任何元素的集称为空集,例如 $A=\{x\mid x\in\mathbf{R},x^2+1=0\}$ 是空集。规定:空集是任何集的子集。

定义 1.1.1　设 A,B 是两个集,由 A 和 B 的所有共同元素组成的集,称为 A 和 B 的交集,记为 $A\cap B$,即

$$A\cap B=\{x\mid x\in A\text{ 并且 }x\in B\}$$

例 1.1.2　设 $A=\{a,b,c,d\},B=\{a,c,e\}$,则 $A\cap B=\{a,c\}$. □

定义 1.1.2 设 A,B 是两个集,由属于 A 或属于 B 的所有元素组成的集,称为 A 和 B 的并集,记为 $A\cup B$,即

$$A\cup B=\{x\mid x\in A\text{ 或 }x\in B\}$$

例 1.1.3 设 $A=\{1,2,3\}$,$B=\{1,4\}$,则 $A\cup B=\{1,2,3,4\}$. □

定义 1.1.3 设 A,B 是两个集,由属于 A 而不属于 B 的所有元素组成的集,称为 A 与 B 的差集或称 B 在 A 中的余集,即

$$A-B=\{x\mid x\in A\text{ 并且 }x\notin B\}$$

例 1.1.4 设 $A=\{1,2,3,4\}$,$B=\{1,2,5\}$,则 $A-B=\{3,4\}$,$B-A=\{5\}$. □

二、数域

定义 1.1.4 设 P 是复数集的子集,并且至少含有一个不为零的数,如果对于 P 中的任何两个数 a,b(可写成 $\forall\, a,b\in P$),有 $a+b\in P$,$a-b\in P$,$ab\in P$,且当 $b\neq 0$ 时,$\frac{a}{b}\in P$,则称 P 为一个数域。

例 1.1.5 有理数集 **Q**、实数集 **R**、复数集 **C** 都是数域,整数集 **Z** 不是数域。□

由于一个数域 P 至少含有一个不为零的数,设 $a\in P$ 且 $a\neq 0$,则 $a-a=0\in P$,$a/a=1\in P$,于是任何数域包含数 0 与 1。

例 1.1.6 集 $\{a+b\sqrt{3}\mid a,b\in\mathbf{Q}\}$,记为 $\mathbf{Q}(\sqrt{3})$,即 $\mathbf{Q}(\sqrt{3})=\{a+b\sqrt{3}\mid a,b\in\mathbf{Q}\}$,$\mathbf{Q}(\sqrt{3})$ 包含数 0,1。设 $\alpha,\beta\in\mathbf{Q}(\sqrt{3})$ 且 $\alpha=a_1+b_1\sqrt{3}$,$\beta=a_2+b_2\sqrt{3}$,其中

$a_1,b_1,a_2,b_2,\in\mathbf{Q}$,则 $\alpha+\beta=(a_1+a_2)+(b_1+b_2)\sqrt{3}\in\mathbf{Q}(\sqrt{3})$;

$\alpha-\beta=(a_1-a_2)+(b_1-b_2)\sqrt{3}\in\mathbf{Q}(\sqrt{3})$;

$\alpha\beta=(a_1+b_1\sqrt{3})(a_2+b_2\sqrt{3})=(a_1a_2+3b_1b_2)+(a_1b_2+a_2b_1)\sqrt{3}\in\mathbf{Q}(\sqrt{3})$;

如果 $\beta=a_2+b_2\sqrt{3}\neq 0$,即 a_2,b_2 不全为零,则

$$\begin{aligned}\frac{\alpha}{\beta}=\frac{a_1+b_1\sqrt{3}}{a_2+b_2\sqrt{3}}&=\frac{(a_1+b_1\sqrt{3})(a_2-b_2\sqrt{3})}{(a_2+b_2\sqrt{3})(a_2-b_2\sqrt{3})}\\&=\frac{a_1a_2-3b_1b_2}{a_2^2-3b_2^2}+\frac{a_1b_2-a_2b_1}{a_2^2-3b_2^2}\sqrt{3}\end{aligned}$$

由于 $a_1,a_2,b_1,b_2\in\mathbf{Q}$,从而 $\frac{a_1a_2-3b_1b_2}{a_2^2-3b_2^2},\frac{a_1b_2-a_2b_1}{a_2^2-3b_2^2}\in\mathbf{Q}$,所以 $\frac{\alpha}{\beta}\in\mathbf{Q}(\sqrt{3})$。

综上,$\mathbf{Q}(\sqrt{3})$ 是一个数域。□

例 1.1.7 集 $\mathbf{Z}(\sqrt{3})=\{a+b\sqrt{3}\mid a,b\in\mathbf{Z}\}$,$\mathbf{Z}(\sqrt{3})$ 包含数 0,1。设 $\alpha,\beta\in\mathbf{Z}(\sqrt{3})$ 且 $\alpha=a_1+b_1\sqrt{3}$,$\beta=a_2+b_2\sqrt{3}$,其中 $a_1,a_2,b_1,b_2\in\mathbf{Z}$,则 $\alpha+\beta,\alpha-\beta,\alpha\beta\in\mathbf{Z}(\sqrt{3})$;

如果 $\beta=a_2+b_2\sqrt{3}\neq 0$,即 a_2,b_2 不全为零,则

$$\frac{\alpha}{\beta}=\frac{a_1a_2-3b_1b_2}{a_2^2-3b_2^2}+\frac{a_1b_2-a_2b_1}{a_2^2-3b_2^2}\sqrt{3}$$

综上,虽然 $a_1,a_2,b_1,b_2\in\mathbf{Z}$,但 $\frac{a_1a_2-3b_1b_2}{a_2^2-3b_2^2}$,$\frac{a_1b_2-a_2b_1}{a_2^2-3b_2^2}$ 不一定属于 **Z**,所以 $\frac{\alpha}{\beta}$ 不一定属于 $\mathbf{Z}(\sqrt{3})$。因此,$\mathbf{Z}(\sqrt{3})$ 不是数域. □

定理 1.1.1 任何数域都包含有理数域 **Q**。

证 设 P 是一个数域,$0,1\in P$。$1+1=2\in P,2+1=3\in P,\cdots$,继续下去,可得所有正整数都属于 P。由此得 $0,n\in P$(n 为任意正整数),于是 $0-n=-n\in P$,即所有负整数也属于 P,从而 $\mathbf{Z}\subseteq P$。由于任意一个有理数都可表示成两个整数 m,n 的商 $\frac{m}{n}(n\neq 0)$,而 $\frac{m}{n}\in P$。因此,有理数域 $\mathbf{Q}\subseteq P$。

三、映射

定义 1.1.5 设 A,B 是两个非空集合,如果存在一个法则 f,使得对于 A 中任何一个元素 x,按照法则 f,在 B 中有唯一的元素 y 与 x 对应,则称法则 f 是 A 到 B 的映射或函数,记为 $f:A\rightarrow B$。

映射 f 使 $x\in A$ 对应 $y\in B$,记为 $f(x)=y$,y 称为 x 在映射 f 下的象,x 称为 y 在映射 f 下的一个原象。A 称为映射 f 的定义域。所有 $x\in A$ 在映射 f 下的全体象组成的集,称为 A 在 f 下的象集,记为 $f(A)$ 或 $Im(A)$,即 $f(A)=\{f(x)\mid x\in A\}$。A 到 A 的映射也称为 A 上的变换。如果 A 到 A 的映射 f,使 $\forall x\in A,f(x)=x$,则称 f 为 A 上的恒等映射或恒等变换或单位映射。

两个映射 $f:A_1\rightarrow B_1,g:A_2\rightarrow B_2$,当且仅当 $A_1=A_2,B_1=B_2$,且对于任何 $x\in A_1$ 均有 $f(x)=g(x)$时,才认为它们是相等的,记为 $f=g$。

例 1.1.8 设 $A=\{a,b,c\},B=\{1,2,3,4\}$。规定 $f:A\rightarrow B$ 为 $f(a)=2,f(b)=3,f(c)=2$,则 f 是 $A\rightarrow B$ 的映射。因为 A 中的每个元素在 B 中都有象,并且象是唯一的。□

例 1.1.9 设 $A=B=\mathbf{R}$,规定 $f:\mathbf{R}\rightarrow\mathbf{R}$ 为 $\forall x\in\mathbf{R},f(x)=x+1$,则 f 是 $\mathbf{R}\rightarrow\mathbf{R}$ 的映射,也是 $\mathbf{R}$ 上的变换,因为 $\mathbf{R}$ 中的每个数在 $\mathbf{R}$ 中都有象,并且象是唯一的。□

例 1.1.10 设 $\mathbf{R}^+$ 是正实数集,$\mathbf{R}$ 为实数集,规定 $f:\mathbf{R}^+\rightarrow\mathbf{R}$ 为 $\forall x\in\mathbf{R}^+,f(x)=\pm\sqrt{x}$,则 f 不是 $\mathbf{R}^+\rightarrow\mathbf{R}$ 的映射,因为 x 的象不是唯一的。□

定义 1.1.6 设 f 是集合 A 到 B 的一个映射,如果 $\forall b\in B$,均有 $a\in A$ 使 $f(a)=b$,即 $f(A)=B$,则称 f 为 A 到 B 的满映射,简称满射或称映上的。

定义 1.1.7 设 f 是集 A 到 B 的一个映射,如果 $\forall x,y\in A,x\neq y$ 有 $f(x)\neq f(y)$,则称 f 为 A 到 B 的单映射,简称单射或称 1-1 的。

定义 1.1.8 设 f 是集 A 到 B 的一个映射,如果 f 既是满射又是单射,则称 f 为 A 到 B 的双射或一一映射。

例 1.1.11 设 $A=\{a,b,c,d\},B=\{1,2,3,4,5\}$,规定 $f:A\rightarrow B$ 为 $f(a)=2,f(b)=1,f(c)=5,f(d)=4$,则 f 是 A 到 B 的单射,但不是满射,因为 B 中的元素 3 在 A 中没原象。□

例 1.1.12 设 $A=\{a,b,c,d\},B=\{1,2,3\}$,规定 $f:A\rightarrow B$ 为 $f(a)=2,f(b)=1,f(c)=3,f(d)=3$,则 f 是 A 到 B 的满射,但不是单射,因为 A 中的不同元素 c,d,存在 $f(c)=f(d)=3$。□

例 1.1.13 设 $A=\mathbf{Z},B=2\mathbf{Z}=\{2n\mid n\in\mathbf{Z}\}$,规定 $f:A\rightarrow B$ 为 $\forall x\in\mathbf{Z},f(x)=2x$,则 f 是 $\mathbf{Z}$ 到 $2\mathbf{Z}$ 的双射。□

设 A,B,C 为集合,映射 $f:A\rightarrow B,g:B\rightarrow C$,由 f,g 确定的 $A\rightarrow C$ 的映射 h,$\forall x\in A,h(x)=g[f(x)]$称为映射 f,g 的合成或复合,也称 f,g 的乘积,记为 $h=g\circ f$ 或 gf,即 $\forall x\in A$,$(gf)(x)=g[f(x)]$。

设 A,B,C,D 为集合,映射 $f:A\rightarrow B,g:B\rightarrow C,h:C\rightarrow D$,则合成映射 $h(gf)$与$(hg)f$ 都是

A 到 D 的映射，并且有 $h(gf)=(hg)f$，即映射的合成满足结合律。

定义 1.1.9 设映射 $f:A\to B$，如果存在映射 $g:B\to A$，使 $gf=I_A, fg=I_B$，其中 I_A 与 I_B 分别为 A 与 B 上的恒等映射，则 g 称为 f 的逆映射，记为 f^{-1}。

注：映射 $f:A\to B$ 有逆的充分必要条件是 f 为双射。

例 1.1.14 设 $A=\mathbf{Z}, B=2\mathbf{Z}$，规定 $f:A\to B$ 为 $\forall x\in\mathbf{Z}, f(x)=2x$，从例 1.1.13 中得 f 是 $A\to B$ 的双射。规定 $g:B\to A$ 为 $\forall y\in B, g(y)=y/2$，由于 y 是偶数，所以 $\frac{y}{2}\in\mathbf{Z}$。

$\forall x\in A, gf(x)=g[f(x)]=g(2x)=x$，于是 $gf=I_A$；$\forall y\in B, fg(y)=f[g(y)]=f(y/2)=y$，于是 $fg=I_B$。因此，g 是 f 的逆映射。□

§1.2 一元多项式的概念与运算

定义 1.2.1 设 P 是一个数域，x 为一个符号(或称文字)，n 是一个非负整数，形式表达式

$$a_nx^n+\cdots+a_1x+a_0 \tag{1.2.1}$$

其中 $a_0,a_1,a_2,\cdots,a_n$ 属于 P 中的数，称为系数在数域 P 中的 x 的一元多项式，或简称为数域 P 上的 x 的一元多项式。

在(1.2.1)式中，a_ix^i 称为 i 次项，a_i 称为 i 次项的系数。

如果多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 与 $g(x)=b_nx^n+\cdots+b_1x+b_0$ 中，同次项的系数都相等，即 $a_i=b_i(i=0,1,\cdots,n)$，则称多项式 $f(x)$ 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(1.2.1)式中，如果 $a_n\neq 0$，则 a_nx^n 称为多项式(1.2.1)的最高次项，a_n 称为最高次项系数，n 称为多项式(1.2.1)的次数。零多项式不规定次数。若 $f(x)$ 不是零多项式，$f(x)$ 的次数记为 $\partial[f(x)]$ 或 $\deg f(x)$。

例 1.2.1 $f(x)=4x^3-\frac{1}{2}x^2+3x+2$ 是有理数域上的 3 次多项式，$g(x)=x^4+2x^3-2\mathrm{i}x^2+\mathrm{i}$ 是复数域上的 4 次多项式。□

在数域 P 上的多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 也可简记为 $f(x)=\sum\limits_{i=0}^{n}a_ix^i$。

在数域 P 上的所有一元多项式组成的集合记为 $P[x]$，即

$$P[x]=\{a_nx^n+\cdots+a_1x+a_0 \mid a_i\in P, i=0,1,\cdots,n; n \text{ 为非负整数}\}$$

设 $f(x),g(x)\in P[x]$

$$f(x)=a_nx^n+\cdots+a_1x+a_0=\sum_{i=0}^{n}a_ix^i$$

$$g(x)=b_mx^m+\cdots+b_1x+b_0=\sum_{i=0}^{m}b_ix^i$$

如果 $n\geqslant m$ 时，$g(x)$ 也可写为

$$g(x)=0x^n+\cdots+0x^{m+1}+b_mx^m+\cdots+b_1x+b_0=\sum_{i=0}^{n}b_ix^i$$

定义两个多项式 $f(x),g(x)$ 的和与积分别为

$$f(x)+g(x)=(a_n+b_n)x^n+\cdots+(a_1+b_1)x+(a_0+b_0)=\sum_{i=0}^{n}(a_i+b_i)x^i$$

$$f(x)g(x) = a_nb_mx^{n+m} + (a_nb_{m-1} + a_{n-1}b_m)x^{n+m-1} + \cdots + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0$$

其中 x^k 的系数

$$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_1b_{k-1} + a_0b_k = \sum_{i+j=k} a_ib_j$$

于是

$$f(x)g(x) = c_{n+m}x^{n+m} + \cdots + c_kx^k + \cdots + c_1x + c_0 = \sum_{k=0}^{n+m} c_kx^k = \sum_{k=0}^{n+m}\Big(\sum_{i+j=k} a_ib_j\Big)x^k$$

例 1.2.2 设 $f(x), g(x) \in \mathbf{Q}[x]$, $f(x) = 2x^3 + x^2 + 2x + 1$, $g(x) = x^2 - 3x - 1$,于是

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

$$f(x)g(x) = 2x^5 - 5x^4 - 3x^3 - 6x^2 - 5x - 1 \quad \Box$$

两个多项式 $f(x), g(x)$ 相减,定义为 $f(x) - g(x) = f(x) + [-g(x)]$。

数域 P 上的两个多项式的和、差、积仍然是 P 上的多项式。即 $\forall f(x), g(x) \in P[x]$, $f(x) \pm g(x) \in P[x]$, $f(x)g(x) \in P[x]$。

数域 P 上多项式的加法与乘法满足下列规律,$\forall f(x), g(x), h(x) \in P[x]$

(1) 加法交换律

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

(2) 加法结合律

$$[f(x) + g(x)] + h(x) = f(x) + [g(x) + h(x)]$$

(3) 乘法交换律

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

(4) 乘法结合律

$$[f(x)g(x)]h(x) = f(x)[g(x)h(x)]$$

(5) 乘法对加法的分配律

$$f(x)[g(x) + h(x)] = f(x)g(x) + f(x)h(x)$$

定理 1.2.1 设 $f(x), g(x) \in P[x]$,且 $f(x) \neq 0$, $g(x) \neq 0$,则

(1) 当 $f(x) + g(x) \neq 0$ 时

$$\partial[f(x) + g(x)] \leqslant \max\,[\partial f(x), \partial g(x)]$$

(2) $\partial[f(x)g(x)] = \partial[f(x)] + \partial[g(x)]$

证 设

$$f(x) = a_nx^n + \cdots + a_1x + a_0, \qquad a_n \neq 0$$

$$g(x) = b_mx^m + \cdots + b_1x + b_0, \qquad b_m \neq 0$$

(1) 设 $n \geqslant m$

$$f(x) + g(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

其中 $b_{m+1} = b_{m+2} = \cdots = b_n = 0$,于是 $f(x) + g(x)$ 的次数不能超过 n,即

$$\partial[f(x) + g(x)] \leqslant \max\,[f(x), g(x)]$$

(2) $f(x)g(x) = a_nb_mx^{n+m} + \cdots + (a_1b_0 + a_0b_1)x + a_0b_0$

由于 $a_n \neq 0$, $b_m \neq 0$,所以 $a_nb_m \neq 0$,即 $f(x)g(x)$ 的次数为 $n + m$。

§1.3 最大公因式

在数域 P 上的两个多项式 $f(x)$，$g(x)$ 相加、相减与相乘后还是 P 上的多项式，但相除就不一定是 P 上的多项式了。若 $g(x)\neq 0$，则 $f(x)$ 除以 $g(x)$ 在 P 上可得唯一的商式 $q(x)$ 与余式 $r(x)$，即

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

其中 $r(x)=0$ 或 $\partial r(x)<\partial g(x)$。

例 1.3.1 设 $f(x)$，$g(x)\in \mathbf{Q}[x]$，且

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

求 $f(x)$ 除以 $g(x)$ 的商式与余式。

解

$$\begin{array}{r|l}
 & x^2-3 \\ \hline
x^2-x-1 & x^4-x^3-4x^2+4x+1 \\
 & x^4-x^3-x^2 \\ \hline
 & \qquad -3x^2+4x+1 \\
 & \qquad -3x^2+3x+3 \\ \hline
 & \qquad\qquad\quad x-2
\end{array}$$

于是 $f(x)=(x^2-3)g(x)+(x-2)$，即 $f(x)$ 除以 $g(x)$ 的商式 $q(x)=x^2-3$，余式 $r(x)=x-2$。上式的除法也可用以下格式

$$\begin{array}{r|l|l}
x^2-x-1 & x^4-x^3-4x^2+4x+1 & x^2-3=q(x) \\
 & x^4-x^3-x^2 & \\ \hline
 & \qquad -3x^2+4x+1 & \\
 & \qquad -3x^2+3x+3 & \\ \hline
 & \qquad r(x)=\ x-2 &
\end{array}$$

有时也可只用系数表示多项式，即

$$\begin{array}{rrr|rrrrr|rrr}
1 & -1 & -1 & 1 & -1 & -4 & 4 & 1 & 1 & 0 & -3 \\
 & & & 1 & -1 & -1 & & & & & \\ \hline
 & & & & & -3 & 4 & 1 & & & \\
 & & & & & -3 & 3 & 3 & & & \\ \hline
 & & & & & & 1 & -2 & & &
\end{array}$$

表示 $f(x)$ 除以 $g(x)$ 的商式 $q(x)=x^2-3$，余式 $r(x)=x-2$。□

定义 1.3.1 设 $f(x)$，$g(x)\in P[x]$，如果存在 P 上的多项式 $h(x)$，使 $f(x)=g(x)h(x)$，则称 $f(x)$ 能被 $g(x)$ 整除，或称 $g(x)$ 整除 $f(x)$，记为 $g(x)\mid f(x)$。$g(x)$ 不能整除 $f(x)$，记为 $g(x)\nmid f(x)$。当 $g(x)\mid f(x)$ 时，$g(x)$ 称为 $f(x)$ 的因式，$f(x)$ 称为 $g(x)$ 的倍式。

显然，数域 P 上的两个多项式 $f(x)$，$g(x)\neq 0$，$g(x)$ 整除 $f(x)$ 的充分必要条件是 $f(x)$ 除以 $g(x)$，得到的余式为 0。

例 1.3.2 试问 s,t 为什么数时，下列 $f(x)$ 能被 $g(x)$ 整除？

$$f(x)=x^4+sx^3+2x^2+5x+t$$
$$g(x)=x^2-x-2$$

解法一

$$
\begin{array}{r|l|l}
x^2-x-2 & x^4+sx^3+2x^2+5x+t & x^2+(s+1)x+(s+5) \\
 & x^4-x^3-2x^2 & \\
\hline
 & (s+1)x^3+4x^2+5x+t & \\
 & (s+1)x^3-(s+1)x^2-2(s+1)x & \\
\hline
 & \quad (s+5)x^2+(2s+7)x+t & \\
 & \quad (s+5)x^2-(s+5)x-2(s+5) & \\
\hline
 & \qquad (3s+12)x+t+2s+10 &
\end{array}
$$

我们要求 $f(x)$ 能被 $g(x)$ 整除，则余式必为零，即

$$(3s+12)x+t+2s+10=0$$

$$\begin{cases}3s+12=0\\ t+2s+10=0\end{cases}$$

解出 $s=-4,t=-2$。因此，当 $s=-4,t=-2$ 时，$f(x)$ 能被 $g(x)$ 整除。

解法二 设 $x^4+sx^3+2x^2+5x+t=(x^2-x-2)(x^2+kx+l)=x^4+(k-1)x^3+(l-k-2)x^2-(l+2k)x-2l$，于是

$$\begin{cases}k-1=s\\ l-k-2=2\\ l+2k=-5\\ -2l=t\end{cases}$$

解出

$$\begin{cases}l=1\\ k=-3\\ t=-2\\ s=-4\end{cases}$$

因此，当 $s=-4,t=-2$ 时，$f(x)$ 能被 $g(x)$ 整除。□

下面讨论在数域 P 上的多项式整除的简单性质。

(1) 如果 $g(x)\mid f(x)$ 且 $f(x)\mid g(x)$，则 $g(x)=cf(x)$，其中 $c\in P$，且 $c\neq 0$。

例 1.3.3 设 $f(x),g(x)$ 为有理数域 **Q** 上的多项式，且 $f(x)=x^2-2x+4$，$g(x)=\frac{1}{2}x^2-x+2$，多项式满足 $g(x)\mid f(x)$ 且 $f(x)\mid g(x)$，显然 $g(x)=\frac{1}{2}f(x)$。□

(2) 如果 $g(x)\mid f_1(x),g(x)\mid f_2(x),\cdots,g(x)\mid f_k(x)$，则

$$g(x)\mid u_1(x)f_1(x)+u_2(x)f_2(x)+\cdots+u_k(x)f_k(x)$$

其中 $u_i(x)(i=1,2,\cdots,k)$ 为 P 上的多项式。

(3) 如果 $h(x)\mid g(x)$ 且 $g(x)\mid f(x)$，则 $h(x)\mid f(x)$。

定义 1.3.2 设 $f(x),g(x)\in P[x]$，P 上的多项式 $d(x)$ 满足：

(1) $d(x) \mid f(x)$, $d(x) \mid g(x)$，即 $d(x)$是 $f(x)$与 $g(x)$的公因式；

(2) 如果 $\varphi(x) \in P[x]$，满足 $\varphi(x) \mid f(x)$，$\varphi(x) \mid g(x)$，则 $\varphi(x) \mid d(x)$，即 $f(x)$与 $g(x)$的公因式均是 $d(x)$的因式

则称 $d(x)$为 $f(x)$与 $g(x)$的最大公因式。

例 1.3.4 设 $f(x)$，$g(x)$为实数域 $\mathbf{R}$ 上的多项式，即 $f(x)$，$g(x) \in \mathbf{R}[x]$，$f(x) = x^2 - 1$，$g(x) = (x+1)^2$，于是 $f(x)$与 $g(x)$的最大公因式为 $x+1$。□

定理 1.3.1 设 $f(x)$，$g(x) \in P[x]$，在 P 上存在一个 $f(x)$与 $g(x)$的最大公因式 $d(x)$，并且 $d(x)$可表示成 $f(x)$，$g(x)$的一个组合，即存在 $u(x)$，$v(x) \in P[x]$，使

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

证 (1) 如果 $f(x) = g(x) = 0$，则 $f(x)$与 $g(x)$的最大公因式为零；

(2) 如果 $f(x)$，$g(x)$不都为零，不妨设 $g(x) \neq 0$。用 $g(x)$除 $f(x)$，得商式 $q_1(x)$，余式 $r_1(x)$。若 $r_1(x) \neq 0$，再用 $r_1(x)$除 $g(x)$，得商式 $q_2(x)$，余式 $r_2(x)$。若 $r_2(x) \neq 0$，再用 $r_2(x)$除 $r_1(x)$，得商式 $q_3(x)$，余式 $r_3(x)$，如此继续下去(这种方法，称为辗转相除法)。显然，所得余式的次数不断降低，这样经有限次辗转相除，必有一个余式 $r_k(x)$，它能整除前一个余式 $r_{k-1}(x)$，即

$$\left.\begin{aligned} f(x) &= q_1(x)g(x) + r_1(x) \\ g(x) &= q_2(x)r_1(x) + r_2(x) \\ r_1(x) &= q_3(x)r_2(x) + r_3(x) \\ &\vdots \\ r_{k-3}(x) &= q_{k-1}(x)r_{k-2}(x) + r_{k-1}(x) \\ r_{k-2}(x) &= q_k(x)r_{k-1}(x) + r_k(x) \\ r_{k-1}(x) &= q_{k+1}(x)r_k(x) + 0 \end{aligned}\right\} \tag{1.3.1}$$

对于式(1.3.1)的各式，由下往上，从 $r_{k-1}(x) = q_{k+1}(x)r_k(x)$，可得 $r_k(x)$是 $r_{k-1}(x)$与 $r_k(x)$的最大公因式；再由 $r_{k-2}(x) = q_k(x)r_{k-1}(x) + r_k(x)$，可得 $r_k(x)$是 $r_{k-2}(x)$与 $r_{k-1}(x)$的最大公因式；继续逐步往上，可得 $r_k(x)$是 $f(x)$与 $g(x)$的最大公因式。

对于式(1.3.1)的各式，由下往上，从 $r_{k-2}(x) = q_k(x)r_{k-1}(x) + r_k(x)$，得

$$r_k(x) = r_{k-2}(x) - q_k(x)r_{k-1}(x) \tag{1.3.2}$$

再由 $r_{k-3}(x) = q_{k-1}(x)r_{k-2}(x) + r_{k-1}(x)$，得 $r_{k-1}(x) = r_{k-3}(x) - q_{k-1}(x)r_{k-2}(x)$，代入式(1.3.2)，得

$$r_k(x) = [1 + q_k(x)q_{k-1}(x)]r_{k-2}(x) - q_k(x)r_{k-3}(x)$$

用同样的方法，逐个消去 $r_{k-2}(x)$，$r_{k-3}(x)$，…，$r_1(x)$，最后得到

$$r_k(x) = u(x)f(x) + v(x)g(x)$$

从最大公因式的定义可看出：数域 P 上的两个不全为零的多项式的最大公因式不是唯一的。例如，在有理数域 $\mathbf{Q}$ 上的多项式 $f(x) = x^2 - 1$，$g(x) = x + 1$，$f(x)$与 $g(x)$的最大公因式是 $x+1$，也可以是 $2(x+1)$或 $c(x+1)$，其中 c 是不为零的有理数。

数域 P 上的两个多项式的最大公因式，在可相差 P 上非零常数倍的意义下是唯一确定的。我们约定：不全为零的多项式 $f(x)$与 $g(x)$的最高次项系数为 1 的那个最大公因式，记为 $(f(x), g(x))$。

定义 1.3.3 设数域 P 上的两个多项式 $f(x),g(x)$，若 $(f(x),g(x))=1$，则称 $f(x)$ 与 $g(x)$ 互素或互质。

例 1.3.5 设数域 P 上的多项式

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

求 $(f(x),g(x))$，并求 $u(x),v(x)\in P[x]$，使

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

解

$$
\begin{array}{c|r|r|c}
x-1 & x^3-x^2-x-2 & x^4-2x^3+x^2-x-2 & x-1 \\
 & x^3\quad -4x & x^4-x^3-x^2-2x & \\
\cline{2-3}
 & -x^2+3x-2 & -x^3+2x^2+x-2 & \\
 & -x^2\quad +4 & -x^3+x^2+x+2 & \\
\cline{2-3}
 & 3x-6 & x^2\quad -4 & \frac{1}{3}x+\frac{2}{3} \\
 & & x^2-2x & \\
\cline{3-3}
 & & 2x-4 & \\
 & & 2x-4 & \\
\cline{3-3}
 & & 0 &
\end{array}
$$

用等式写出来可得

$$f(x)=(x-1)g(x)+x^2-4$$
$$g(x)=(x-1)(x^2-4)+3x-6$$
$$x^2-4=\left(\frac{1}{3}x+\frac{2}{3}\right)(3x-6)$$

于是

$$(f(x),g(x))=x-2$$

$$
\begin{aligned}
3x-6&=g(x)-(x-1)(x^2-4)\\
&=g(x)-(x-1)[f(x)-(x-1)g(x)]\\
&=-(x-1)f(x)+(x^2-2x+2)g(x)
\end{aligned}
$$

$$x-2=\frac{-1}{3}(x-1)f(x)+\frac{1}{3}(x^2-2x+2)g(x)$$

所以

$$u(x)=-\frac{1}{3}(x-1),\ v(x)=\frac{1}{3}(x^2-2x+2)\quad \square$$

推论 1.3.1 设 $f(x),g(x)\in P[x]$，$f(x)$ 与 $g(x)$ 互素的充分必要条件为可求得 P 上多项式 $u(x),v(x)$，使 $u(x)f(x)+v(x)g(x)=1$。

例 1.3.6 判定在有理数域 $\mathbf{Q}$ 上的多项式 $f(x)$ 与 $g(x)$ 是否互素，并求出 $\mathbf{Q}$ 上的多项式 $u(x),v(x)$，使

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

其中

$$f(x)=2x^3-4x^2-8x+1$$
$$g(x)=2x^3-5x^2-5x+2$$

解

$$
\begin{array}{r|c|c|l}
2x+1 & 2x^3-5x^2-5x+2 & 2x^3-4x^2-8x+1 & 1 \\
 & 2x^3-6x^2-2x & 2x^3-5x^2-5x+2 & \\
\hline
 & x^2-3x+2 & x^2-3x-1 & \\
 & x^2-3x-1 & & \\
\cline{2-2}
 & 3 & & \\
\end{array}
$$

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

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

于是，$(f(x),g(x))=1$，即 $f(x)$与 $g(x)$互素

$$
\begin{aligned}
3 &= g(x)-(2x+1)(x^2-3x-1)\\
&= g(x)-(2x+1)[f(x)-g(x)]\\
&= -(2x+1)f(x)+(2x+2)g(x)
\end{aligned}
$$

于是

$$(f(x),g(x))=\frac{-(2x+1)}{3}f(x)+\frac{2(x+1)}{3}g(x)$$

因此

$$u(x)=\frac{-(2x+1)}{3},\quad v(x)=\frac{2(x+1)}{3}\quad \square$$

定义 1.3.4 设 $f_1(x),f_2(x),\cdots,f_k(x)(k\geqslant 2)$为数域 P 上的 k 个多项式，P 上的多项式 $d(x)$满足：

(1) $d(x)\mid f_i(x),\quad i=1,2,\cdots,k$；

(2) 如果 $\varphi(x)\mid f_i(x)\quad (i=1,2,\cdots,k)$，有 $\varphi(x)\mid d(x)$，则称 $d(x)$为 $f_1(x),f_2(x),\cdots,f_k(x)$的最大公因式。

$f_1(x),f_2(x),\cdots,f_k(x)$的最高次项系数为 1 的那个最大公因式，记为$(f_1(x),f_2(x),\cdots,f_k(x))$。

如果$(f_1(x),f_2(x),\cdots,f_k(x))=1$ 时，则称 $f_1(x),f_2(x),\cdots,f_k(x)$为互素的多项式。

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

例 1.3.7 在有理数域 **Q** 上，$f(x)=x^3-1$，$g(x)=x^2-1$，$h(x)=(x-1)^2$，求$(f(x),g(x),h(x))$。

解

$$(f(x),g(x),h(x))=((f(x),g(x)),h(x))=(x-1,h(x))=x-1\quad \square$$

定义 1.3.5 设 $p(x)$为数域 P 上的次数大于零的多项式，如果它不能表示成 $P[x]$中两个次数比 $p(x)$低的多项式的乘积，则称 $p(x)$为 P 上的不可约多项式，或称既约多项式，否则称为可约多项式。

注：数域 P 上的不可约多项式$p(x)$的因式，只有 P 中的非零元素 c 或 $cp(x)$。

数域 P 上的一次多项式都是不可约多项式。

例 1.3.8 x^2+1 在实数域上是不可约多项式，但在复数域上是可约多项式，因为 $x^2+1=(x+\mathrm{i})(x-\mathrm{i})$。$\square$

定理 1.3.2 唯一因式分解定理 数域 P 上的任一个次数大于零的多项式$f(x)$，都可表示成 $P[x]$中的一些不可约多项式的乘积。并且，如果

$$f(x)=p_1(x)p_2(x)\cdots p_r(x)$$
$$=q_1(x)q_2(x)\cdots q_s(x)$$
是 $f(x)$的两种分解式，则 $r=s$，且适当重排因式次序之后，有
$$p_i(x)=c_iq_i(x)$$
其中 $c_i(i=1,\cdots,r)$是 P 中一些不为零的数。

例 1.3.9

$$\begin{aligned} x^4-4&=(x^2-2)(x^2+2) && \text{在 } \mathbf{Q} \text{ 中}\\ &=(x-\sqrt{2})(x+\sqrt{2})(x^2+2) && \text{在 } \mathbf{R} \text{ 中}\\ &=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}\mathrm{i})(x+\sqrt{2}\mathrm{i}) && \text{在 } \mathbf{C} \text{ 中} \quad \square \end{aligned}$$

注：唯一因式分解定理，只是理论上的重要结果。对于一般的多项式来说，不存在统一有效的分解方法。

§1.4 复数域与实数域上的多项式

设数域 P 上的多项式
$$f(x)=a_nx^n+\cdots+a_1x+a_0$$
又设 $\alpha\in P$
$$f(\alpha)=a_n\alpha^n+\cdots+a_1\alpha+a_0$$
是 $f(x)$在 α 的值。$f(x)$是在数域 P 上的一个函数，称 $f(x)$为 P 上的多项式函数。

定义 1.4.1 如果 $f(x)$是数域 P 上的一个多项式，α 是 P 中的数，当 $x=\alpha$ 时，$f(\alpha)=0$，则称 α 是$f(x)$在 P 中的一个根或零点。

显然，α 是$f(x)$的根的充分必要条件为 $x-\alpha$ 是$f(x)$的因式。

定义 1.4.2 如果 $f(x)$是数域 P 上的一个多项式，α 是 P 中的数，k 为正整数。若$(x-\alpha)^k\mid f(x)$，且$(x-\alpha)^{k+1}\nmid f(x)$，则称 α 为$f(x)$的 k 重根，$x-\alpha$ 称为$f(x)$的 k 重因式。当 $k=1$ 时，称 α 为$f(x)$的单根。

例 1.4.1 设有理数域上多项式 $f(x)=(x-1)^3(x+1/2)$，则 1 是 $f(x)$的 3 重根，$-1/2$ 是 $f(x)$的单根。□

定理 1.4.1 数域 P 上每一个 n 次多项式，在 P 中至多有 n 个根(重根按重数计算)。

证 当 $n=0$ 时，即多项式 $f(x)$为零次多项式，多项式没根，于是定理成立；

当 $n>0$ 时，假定 n 次多项式$f(x)$有 $n+1$ 个根，$\alpha_1,\alpha_2,\cdots,\alpha_{n+1}$，于是 $f(x)$有因式$(x-\alpha_1)$，$(x-\alpha_2)$，$\cdots$，$(x-\alpha_n)$，$(x-\alpha_{n+1})$。由于$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)(x-\alpha_{n+1})$是 $n+1$ 次的，所以这是不可能的。因此，定理成立。

例 1.4.2 多项式 $f(x)=x^2-2$ 在有理数域中没有根；在实数域中有两个根：$\sqrt{2}$与 $-\sqrt{2}$；在复数域中也有两个根：$\sqrt{2}$与 $-\sqrt{2}$。可见无论在哪个数域中，二次多项式 $f(x)$根的个数都不超过 2。□

推论 1.4.1 如果 $f(x)$，$g(x)$是数域 P 上的两个次数$\leqslant n$ 的多项式，且 P 中有$n+1$ 个不同的数 $\alpha_1,\alpha_2,\cdots,\alpha_{n+1}$，使 $f(\alpha_i)=g(\alpha_i)$ $(i=1,2,\cdots,n+1)$，则 $f(x)=g(x)$。

证 由于 $f(\alpha_i)=g(\alpha_i)$ $(i=1,2,\cdots,n+1)$，所以 $f(\alpha_i)-g(\alpha_i)=0$。从而多项式 $f(x)$