第 7 章　一元和 n 元多项式环

一元多项式由于其形式简洁，且有加法和乘法运算，因此在许多领域都有重要应用。譬如，在数学分析中，用多项式函数逼近一般的 n 阶可微函数。在当今信息时代，多项式在计算机科学、现代通信、编码和密码等领域都有应用。

古典代数学研究的中心问题是一元多项式的求根；近世代数学研究的中心问题是各种代数系统的结构及其之间的态射（保持运算的映射）。本章以研究数域 K 上一元多项式环的结构及其态射（一元多项式环的通用性质）为主线，此外还介绍了 n 元多项式环的结构。

7.1　一元多项式环

7.1.1　内容精华

一、一元多项式的概念和运算

1. **数域 K 上一元多项式**的定义包含两点：

（1）数域 K 上的一元多项式是一个形如下述的表达式：

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

其中 x 是一个符号（它不属于 K），n 是非负整数，$a_i \in K(i=0,1,\cdots,n)$，称为**系数**，$a_i x^i$ 称为 **i 次项**（$i=1,2,\cdots,n$），a_0 称为**零次项**或**常数项**。

（2）两个这种形式的表达式相等当且仅当它们含有完全相同的项（除去系数为 0 的项外，系数为 0 的项允许任意删去和添加）。此时，符号 x 称为**不定元**。（这一条意味着一元多项式的表示方法是唯一的。）

系数全为 0 的多项式称为**零多项式**，记作 0。

从定义立即得出：数域 K 上两个一元多项式相等当且仅当它们的同次项的系数都对应相等。

我们常常用 $f(x),g(x),h(x),\cdots$ 或 $f,g,h,\cdots$ 表示一元多项式。

2. 一元多项式的重要特点是它有“次数”的概念。

设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，如果 $a_n\neq 0$，那么称 a_nx^n 是 $f(x)$的**首项**，称 n 是 $f(x)$的**次数**，记作 $\deg f(x)$或 $\deg f$。

零多项式的次数定义为$-\infty$，并且规定：

$$(-\infty)+(-\infty):=-\infty,$$
$$(-\infty)+n:=-\infty,\forall n\in\mathbf{N},$$
$$-\infty<n,\forall n\in\mathbf{N}.$$

其中 $\mathbf{N}$ 表示自然数集(注意：$0\in\mathbf{N}$)。

注意：不要混淆零多项式与零次多项式，零次多项式形如 a，其中 $a\in K^*$。我们用 K^* 表示 K 中所有非零数组成的集合。

3. 数域 K 上所有一元多项式组成的集合记作 $K[x]$。在 $K[x]$中可以定义加法和乘法运算：

设 $f(x)=\sum\limits_{i=0}^{n}a_ix^i$，$g(x)=\sum\limits_{i=0}^{m}b_ix^i$，不妨设 $m\leqslant n$，令

$$f(x)+g(x):=\sum_{i=0}^{n}(a_i+b_i)x^i, \tag{2}$$

$$f(x)g(x):=\sum_{s=0}^{n+m}\Big(\sum_{i+j=s}a_ib_j\Big)x^s. \tag{3}$$

称 $f(x)+g(x)$是 $f(x)$与 $g(x)$的**和**，称 $f(x)g(x)$是 $f(x)$与 $g(x)$的**积**。

容易验证：一元多项式的加法满足交换律、结合律，且

$$f(x)+0=0+f(x)=f(x),\forall f(x)\in K[x];$$
$$f(x)+[-f(x)]=[-f(x)]+f(x)=0,\forall f(x)\in K[x].$$

其中 $-f(x)=\sum\limits_{i=0}^{n}(-a_i)x^i$。

容易验证：一元多项式的乘法满足交换律、结合律，以及对于加法的分配律，且

$$1\cdot f(x)=f(x)\cdot 1=f(x),\forall f(x)\in K[x].$$

$K[x]$中还可定义减法：

$$f(x)-g(x):=f(x)+[-g(x)]. \tag{4}$$

4. 一元多项式的和与积的次数公式：

命题 1 设 $f(x),g(x)\in K[x]$，则

$$\deg(f\pm g)\leqslant\max\{\deg f,\deg g\}, \tag{5}$$
$$\deg(fg)=\deg f+\deg g. \tag{6}$$

从命题 1 的证明过程看出，一元多项式具有下述性质：

$$f(x)\neq 0 \text{ 且 } g(x)\neq 0 \Rightarrow f(x)g(x)\neq 0. \tag{7}$$

由此得出，一元多项式的乘法适合**消去律**，即

$$f(x)g(x)=f(x)h(x),\text{且 } f(x)\neq 0 \quad \Rightarrow \quad g(x)=h(x).$$

从命题 1 的证明过程还可看出：两个非零多项式乘积的首项系数等于这两个多项式的首项系数的乘积。

二、环的基本概念

整数集 $\mathbf{Z}$，偶数集 $2\mathbf{Z}$，$K[x]$，$M_n[K]$的共同性质：都有加法和乘法运算，并且加法满足交换律、结合律，有零元，每个元素有负元，乘法满足结合律和对于加法的左、右分配律，抽象出环的概念。

1. 环的定义包含两点：

(1) 环 R 是具有加法和乘法两种代数运算的非空集合。所谓 R 上的一个**代数运算**，是指 $R\times R$ 到 R 的一个映射。

(2) 环 R 的加法满足交换律、结合律，有一个元素，记作 0，它使得

$$a+0=a,\forall a\in R,$$

称这个元素 0 是 R 的零元；

对于 $a\in R$，有 $d\in R$，使得 $a+d=0$，称 d 是 a 的负元，记作 $-a$。

环 R 的乘法满足结合律，以及对于加法的左、右分配律。

容易证明，环 R 中的零元是唯一的；R 中元素 a 的负元是唯一的；$-(-a)=a$。

环 R 中可以定义减法：

$$a-b:=a+(-b). \tag{8}$$

$\mathbf{Z}$，$2\mathbf{Z}$，$K[x]$，$M_n[K]$都是环，它们分别称为**整数环**，**偶数环**，**数域 K 上一元多项式环**，**数域 K 上 n 级全矩阵环**。任意一个数域 K 也是环。

2. 常见的特殊类型的环：

若环 R 中的乘法还满足交换律，则称 R 为**交换环**。

若环 R 中有一个元素 e 具有性质：

$$ea=ae=a,\forall a\in R,$$

则称 e 是 R 的**单位元**，此时称 R 是**有单位元的环**。容易证明，在有单位元的环 R 中，单位元是唯一的，通常把单位元记成 1。

如果环 R 中有元素 a，b，$b\neq 0$，若 $ab=0$ ($ba=0$)则 a 称为一个**左零因子**(**右零因子**)。左零因子和右零因子都简称为**零因子**。根据本节例 7，$0a=a0=0$，$\forall a\in R$，因此，0 既是左零因子，又是右零因子，称 0 是**平凡的零因子**；其余的零因子称为**非平凡的零因子**。

如果环 R 没有非平凡的零因子，那么称 R 是**无零因子环**。有单位元 $1(\neq 0)$ 的无零因子的交换环称为**整环**。$\mathbf{Z}, K, K[x]$ 都是整环。$M_n(K)$ 不是整环，因为它不满足乘法交换律，且它有非平凡的零因子。$2\mathbf{Z}$ 不是整环，因为它没有单位元。

3. 子环的定义如下：

如果环 R 的一个非空子集 R_1 对于 R 的加法和乘法也成为一个环，那么称 R_1 是 R 的一个**子环**。由子环的定义立即得出：子环 R_1 对于 R 的加法和乘法都封闭，即

$$a, b \in R_1 \quad \Rightarrow \quad a+b \in R_1, ab \in R_1.$$

反过来，需要把 R_1“对加法封闭”改成“对减法封闭”，R_1 才能成为 R 的一个子环。见下面的命题：

命题 2 环 R 的一个非空子集 R_1 为一个子环的充分必要条件是 R_1 对于 R 的减法与乘法都封闭，即

$$a, b \in R_1 \quad \Rightarrow \quad a-b \in R_1, ab \in R_1.$$

证明 必要性。由于 R_1 是环，因此 R_1 有零元 $0'$，从而 $0'+0'=0'$，两边加上 $0'$ 在 R 中的负元 $-0'$，得 $0'+0=0$。于是 $0'=0$，即 R 的零元 0 是 R' 的零元。任给 $b\in R_1$，设 b 在 R_1 中的负元为 b'，则 $b+b'=0$。在 R 中看此式得 $b'=-b$，因此 $-b\in R_1$。任给 $a, b\in R_1$，有 $a-b=a+(-b)\in R_1, ab\in R_1$。

充分性。由于 R_1 非空集，因此存在 $c\in R_1$。由已知条件得，$c-c\in R_1$，于是 $0\in R_1$。

任给 $b\in R_1$，由已知条件得，$0-b\in R_1$，于是 $-b\in R_1$。

任给 $a, b\in R_1$，则 $-b\in R_1$，由已知条件得

$$a+b=a-(-b)\in R_1, ab\in R_1.$$

因此 R 的加法和乘法限制到 R_1 上是 R_1 的加法和乘法，显然 R_1 的加法满足交换律、结合律，上面已证 $0\in R_1$；对于任意 $b\in R_1$，有 $-b\in R_1$。显然 R_1 的乘法满足结合律，以及对于加法的左、右分配律，所以 R_1 成为一个环，从而 R_1 是 R 的一个子环。 ■

$K[x]$ 中所有零次多项式添上零多项式组成的集合 S，对于一元多项式的减法与乘法封闭，因此 S 是 $K[x]$ 的一个子环。显然 $K[x]$ 中的单位元 $1\in S$。数域 K 到 S 有一个对应法则 τ：非零数 a 对应到零次多项式 a，数 0 对应到零多项式 0。显然 τ 是双射，且 τ 保持加法与乘法运算，即

$$\tau(a+b)=\tau(a)+\tau(b), \forall\, a, b\in K;$$

$$\tau(ab)=\tau(a)\tau(b), \forall\, a, b\in K.$$

给定 $A\in M_n(K)$，形如下述的表达式称为数域 K 上矩阵 A 的多项式：

$$a_m A^m + a_{m-1}A^{m-1} + \cdots + a_1 A + a_0 I,$$

其中 $m\in\mathbf{N}, a_i\in K, i=0, 1, \cdots, m$。把数域 K 上矩阵 A 的所有多项式组成的集合记作

$K[A]$。易证 $K[A]$对于矩阵的减法和乘法封闭，因此 $K[A]$是 $M_n(K)$的一个子环，显然 $I\in K[A]$，易看出 $K[A]$是交换环。

$K[A]$中所有数量矩阵组成的集合 W，对于矩阵的减法和乘法封闭，因此 W 是 $K[A]$的一个子环，显然 $I\in W$。数域 K 到 W 有一个对应法则 $\tau: a\longmapsto aI$，显然 τ 是双射，且 τ 保持加法与乘法运算。

由上面的例子抽象出下述概念：

设 R 是有单位元 $1'$的交换环，如果 R 有一个子环 R_1 满足下列条件：

(i) $1'\in R_1$；

(ii) 数域 K 到 R_1 有一个双射 τ，且 τ 保持加法与乘法运算，

那么 ***R* 可看成是 *K* 的一个扩环**。

如果有单位元 $1'$的交换环 R 可看成是数域 K 的扩环，那么 K 到子环 R_1 的上述双射 τ 具有性质：$\tau(1)=1'$。理由如下：

任取 $b\in R_1$，由于 τ 是满射，因此存在 $k\in K$，使得 $\tau(k)=b$。于是

$$\tau(1)b=\tau(1)\tau(k)=\tau(1k)=\tau(k)=b.$$

从而 $\tau(1)$是交换环 R_1 的单位元。由于 R 的单位元 $1'\in R_1$，因此 $\tau(1)=1'$。

三、一元多项式环 $K[x]$的通用性质

在 $K[x]$中有完全平方公式：

$$(x+a)^2=x^2+2ax+a^2.$$

利用完全平方公式(当 $a=1$)可以简便地计算 101^2：

$$101^2=(100+1)^2=100^2+2\times 1\times 100+1^2=10201.$$

这是在完全平方公式(当 $a=1$)中，x 用 100 代入，而左右两边仍保持相等。

设 A 是数域 K 上的 n 级矩阵，利用矩阵乘法的分配律，得

$$\begin{aligned}(A+aI)^2&=(A+aI)(A+aI)=A^2+A(aI)+(aI)A+(aI)(aI)\\&=A^2+2aA+a^2I.\end{aligned}$$

从这发现，在完全平方公式中，x 可以用矩阵 A 代入(此时 a 换成 aI)，左右两边保持相等。由此猜测，$K[x]$中有关加法和乘法的等式，x 可以用矩阵 A 代入，左右两边保持相等。由此抽象出一元多项式环 $K[x]$的通用性质：在数域 K 上一元多项式的有关加法和乘法的等式中，不定元 x 可以用环 R(它可以看成是 K 的一个扩环)中任一元素代入，从而得到环 R 中相应的等式，即下面的定理 1。

定理 1 设 K 是一个数域，R 是一个有单位元 $1'$的交换环，它可以看成是 K 的一个扩环，其中 K 到 R 的子环 R_1 的保持加法和乘法运算的双射记作 τ。任意给定 $t\in R$，令

$$\sigma_t : K[x] \longrightarrow R$$

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \longmapsto \quad \sum_{i=0}^{n} \tau(a_i) t^i =: f(t),$$

则 σ_t 是 $K[x]$到 R 的一个映射，且 σ_t 保持加法和乘法运算，即如果在 $K[x]$中，有

$$f(x) + g(x) = h(x), f(x)g(x) = p(x),$$

那么在 R 中，有

$$f(t) + g(t) = h(t), f(t)g(t) = p(t);$$

还有，$\sigma_t(x) = t$。映射 σ_t 称为 ***x* 用 *t* 代入**。

证明 由于 $K[x]$中每个元素 $f(x)$ 写成 $\sum_{i=0}^{n} a_i x^i$ 的表法唯一(除了系数为 0 的项以外)，并且 τ 是 K 到 R_1 的双射，因此 σ_t 是 $K[x]$ 到 R 的一个映射。

据 σ_t 的定义，得

$$\sigma_t(x) = \sigma_t(1x) = \tau(1)t = 1't = t$$

设 $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i$，不妨设 $n \geqslant m$。则

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

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

据 σ_t 的定义，得

$$\begin{aligned}
h(t) &= \sum_{i=0}^{n} \tau(a_i + b_i) t^i = \sum_{i=0}^{n} [\tau(a_i) + \tau(b_i)] t^i \\
&= \sum_{i=0}^{n} \tau(a_i) t^i + \sum_{i=0}^{n} \tau(b_i) t^i = f(t) + g(t); \\
p(t) &= \sum_{s=0}^{n+m} \tau\Big(\sum_{i+j=s} a_i b_j \Big) t^s = \sum_{s=0}^{n+m} \Big[\sum_{i+j=s} \tau(a_i)\tau(b_j) j \Big] t^s; \\
f(t)g(t) &= \Big[\sum_{i=0}^{n} \tau(a_i) t^i \Big] \Big[\sum_{j=0}^{m} \tau(b_j) t^j \Big] \\
&= \sum_{i=0}^{n} \sum_{j=0}^{m} \tau(a_i)\tau(b_j) t^{i+j} \\
&= \sum_{s=0}^{n+m} \Big[\sum_{i+j=s} \tau(a_i)\tau(b_j) j \Big] t^s \\
&= p(t).
\end{aligned}$$

因此 σ_t 保持加法与乘法运算。 ■

定理 1 证明的关键是:一元多项式 $f(x)$的表法唯一,从而 σ_t 是 $K[x]$到 R 的一个映射。至于 σ_t 保持加法和乘法运算,这是自然的,因为 $K[x]$和 R 都是交换环,都遵从交换环的运算法则。

定理 1 表明:只要把一元多项式环 $K[x]$中有关加法与乘法的等式研究清楚了,那么对于可看成是 K 的扩环的任一交换环 R,通过把不定元 x 用 R 的任一元素代入,就可以得到 R 中有关加法和乘法的相应等式。

从前面的讨论知道,$K[x]$,$K[A]$(其中 A 是 K 上任意给定的一个 n 级矩阵)都可看成是 K 的扩环,因此不定元 x 既可以用 $K[x]$中任一多项式代入,又可以用矩阵 A 的任一多项式代入,还可以用可看成 K 的扩环的任一交换环 R 的任一元素代入。这就是为什么把符号 x 叫做不定元的缘由,并且由此看到 x 的确不属于 K。

综上所述,本章的主要任务是探讨一元多项式环 $K[x]$中有关加法与乘法的若干重要等式。这些等式在本章及后续几章中将发挥重要作用。探讨 $K[x]$中有关加法和乘法的等式本质上就是研究一元多项式环 $K[x]$的结构,这是本章的主线。

学习高等代数一定要抓住研究结构这条主线。在本套书上册中,研究了数域 K 上 n 元齐次线性方程组的解集的结构,非齐次线性方程组的解集的结构;数域 K 上 n 元有序数组形成的 n 维向量空间 K^n 及其子空间的结构,n 维欧几里得空间 $\mathbf{R}^n$ 的结构;以及通过建立等价关系(相抵、相似、合同)研究了数域 K 上 $s\times n$ 矩阵的集合 $M_{s\times n}(K)$的相抵分类,n 级矩阵的集合 $M_n(K)$的相似分类和合同分类,继而解决了实(复)数域上 n 元二次型的分类,这些都是在研究结构。在本套书下册中,我们将继续贯穿研究结构这条主线。

7.1.2 典型例题

例 1 证明:在 $K[x]$中,如果 $f(x)=c\,g(x)$,$c\in K^*$,那么

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

证明 若 $g(x)=0$,则 $f(x)=c\cdot 0=0$,从而

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

下面设 $g(x)\neq 0$,由于 $f(x)=c\,g(x)$,$c\in K^*$,因此 $f(x)\neq 0$,并且

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

例 2 证明:在 $K[x]$中,如果 $f(x)=h(x)g(x)$,且 $f(x)\neq 0$,那么

$$\deg g(x) \leqslant \deg f(x).$$

证明 由于 $f(x)=h(x)g(x)$,且 $f(x)\neq 0$,因此 $h(x)\neq 0$,$g(x)\neq 0$;并且

$$\deg f(x) = \deg h(x) + \deg g(x) \geqslant \deg g(x).$$ ■

例 3 证明：在 $K[x]$ 中，如果 $c \in K^*$ 且 $c = f(x)g(x)$，那么 $\deg f(x) = \deg g(x) = 0$。

证明 由于 $c = f(x)g(x)$，且 $c \in K^*$，因此

$$0 = \deg c = \deg f(x) + \deg g(x).$$

由此推出，$\deg f(x) = \deg g(x) = 0$。 ■

例 4 设 R 是一个有单位元 $1(\neq 0)$ 的环。对于 $a \in R$，如果存在 $b \in R$，使得

$$ab = ba = 1,$$

那么称 a 是**可逆元**(或**单位**)，称 b 是 a 的**逆元**，记作 a^{-1}。证明：如果 a 是可逆元，那么 a 的逆元唯一。

证明 假设 b_1, b_2 都是 a 的逆元，则

$$b_1 a b_2 = (b_1 a) b_2 = 1 b_2 = b_2,$$

$$b_1 a b_2 = b_1 (a b_2) = b_1 1 = b_1,$$

因此

$$b_1 = b_2.$$ ■

例 5 证明：在整数环 $\mathbf{Z}$ 中，a 为可逆元当且仅当 $a = \pm 1$。

证明 必要性。设 a 是可逆元，则存在 $b \in \mathbf{Z}$，使得

$$ab = 1.$$

从而 $a \neq 0$，假如 $a \neq \pm 1$，则 $|a| > 1$，从而在整数环 $\mathbf{Z}$ 中有带余除法：

$$1 = 0a + 1, 0 \leqslant 1 < |a|.$$

又有

$$1 = ba + 0,$$

比较上面两个式子，据带余除法中余数的唯一性，得

$$1 = 0,$$

矛盾，因此 $a = \pm 1$。

充分性。由于 $1 \cdot 1 = 1, (-1)(-1) = 1$，因此 1 和 -1 都是 $\mathbf{Z}$ 中的可逆元。 ■

例 6 证明：在 $K[x]$ 中，$f(x)$ 是可逆元当且仅当 $f(x)$ 是零次多项式，即它是 K 中非零数。

证明 必要性。在 $K[x]$ 中，

$f(x)$ 是可逆元

$\Leftrightarrow$ 存在 $g(x) \in K[x]$，使得 $f(x)g(x) = 1$

$\Rightarrow$ $\deg f(x) = \deg g(x) = 0$。

充分性。对于任意 $c \in K^*$，都有 $cc^{-1} = 1$，因此 c 是可逆元。 ■

例 7 设 R 是任意一个环，证明：

(1) $0a = a0 = 0, \forall a \in R$；

(2) $\forall a,b\in R$,有 $a(-b)=-ab,(-a)b=-ab,(-a)(-b)=ab$。

证明 (1)对任意 $a\in R$,有

$$0a=(0+0)a=0a+0a.$$

上式两边加上$(-0a)$,得

$$0a+(-0a)=(0a+0a)+(-0a),$$

从而 $$0=0a+0,$$

于是 $$0=0a.$$

同理可证 $$a0=0.$$

(2) 任取 $a,b\in R$,由于

$$ab+a(-b)=a[b+(-b)]=a0=0,$$

因此 $$a(-b)=-ab.$$

同理可证 $$(-a)b=-ab.$$

从而

$$(-a)(-b)=-[a(-b)]=-(-ab)=ab.$$ ■

例 8 设 R 是环,对于 $a\in R,n\in\mathbf{N}^*$,其中 $\mathbf{N}^*$ 表示正整数集。令

$$na:=\underbrace{a+a+\cdots+a}_{n\text{ 个}}.$$

对于 $0\in\mathbf{N}$,令 $0a:=0$,其中等号右边的 $0\in R$。证明:对任意 $a,b\in R$,任意 $m,n\in\mathbf{N}$,有

$$(m+n)a=ma+na,$$

$$(mn)a=m(na),$$

$$n(a+b)=na+nb,$$

$$n(ab)=(na)b=a(nb).$$

证明 若 m,n 中有一个为 0,则第一、二式显然成立;若 $n=0$,则第三、四式显然成立。

下面设 $m\neq0$ 且 $n\neq0$。由定义立即得到第一、二式。由定义及环的加法的交换律、结合律立即得到第三式。

$$n(ab)=\underbrace{ab+ab+\cdots+ab}_{n\text{ 个}}=(\underbrace{a+a+\cdots+a}_{n\text{ 个}})b$$

$$=(na)b.$$

同理可证 $$n(ab)=a(nb).$$ ■

在环 R 中,对于 $a\in R,n\in\mathbf{N}^*$,令

$$(-n)a:=n(-a).$$

可以证明例 8 中的四个等式对于任意 $m,n\in\mathbf{Z}$ 仍然成立。

例 9 设 R 是环，对于 $a\in R,n\in\mathbf{N}^*$，令

$$a^n := \underbrace{a\,a\cdots a}_{n\text{ 个}}.$$

证明：对于任意 $m,n\in\mathbf{N}^*$，有

$$a^m a^n = a^{m+n},$$
$$(a^m)^n = a^{mn}.$$

证明 由定义和环的乘法结合律立即得到。 ■

例 10 设数域 K 上的 n 级矩阵 A 为

$$A=\begin{pmatrix} k & c & 0 & 0 & \cdots & 0 & 0\\ 0 & k & c & 0 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \cdots & k & c\\ 0 & 0 & 0 & 0 & \cdots & 0 & k \end{pmatrix},$$

其中 $k,c\in K^*$，说明 A 可逆，并且求 A^{-1}。

解 令

$$H=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0\\ 0 & 0 & 1 & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 0 & 1 & 0\\ 0 & 0 & 0 & \cdots & 0 & 0 & 1\\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix},$$

则 $A=kI+cH$。我们知道 $H^n=0$。

在 $K[x]$ 中直接计算可得

$$(1-x)(1+x+\cdots+x^{n-1}) = 1-x^n. \tag{9}$$

$K[H]$ 可看成是 K 的一个扩环。于是 x 用 $-\frac{c}{k}H$ 代入，从(9)式得

$$\left[I-\left(-\frac{c}{k}H\right)\right]\left[I+\left(-\frac{c}{k}H\right)+\left(-\frac{c}{k}H\right)^2+\cdots+\left(-\frac{c}{k}H\right)^{n-1}\right]$$
$$= I-\left(-\frac{c}{k}H\right)^n. \tag{10}$$

由于 $H^n=0$，因此(10)式可写成

$$\left(I+\frac{c}{k}H\right)\left(I-\frac{c}{k}H+\frac{c^2}{k^2}H^2+\cdots+(-1)^{n-1}\frac{c^{n-1}}{k^{n-1}}H^{n-1}\right)=I.$$

从而

$$(kI+cH)\left(\frac{1}{k}I-\frac{c}{k^2}H+\frac{c^2}{k^3}H^2+\cdots+(-1)^{n-1}\frac{c^{n-1}}{k^n}H^{n-1}\right)=I.$$

这表明 $A=kI+cH$ 是可逆矩阵，并且

$$A^{-1}=\frac{1}{k}I-\frac{c}{k^2}H+\frac{c^2}{k^3}H^2+\cdots+(-1)^{n-1}\frac{c^{n-1}}{k^n}H^{n-1}.$$

点评 在例 10 中，利用一元多项式环 $K[x]$ 的通用性质，求出了 n 级矩阵 A 的逆矩阵，这比用初等变换法求逆矩阵更为简便，这是求逆矩阵的第 6 种方法。其他 5 种方法在本套书上册讲过，它们分别是：伴随矩阵法，“凑”矩阵法，初等变换法，转化为解线性方程组的方法，分块求逆法。

例 11 设 $A\in M_n(K)$，并且设 A 的特征多项式为

$$|\lambda I-A|=(\lambda-\lambda_1)^{l_1}(\lambda-\lambda_2)^{l_2}\cdots(\lambda-\lambda_s)^{l_s},$$

其中 $\lambda_1,\lambda_2,\cdots,\lambda_s$ 是两两不等的复数，$l_1+l_2+\cdots+l_s=n$。证明：对于 $k\in K^*$，矩阵 kA 的特征多项式为

$$|\lambda I-kA|=(\lambda-k\lambda_1)^{l_1}(\lambda-k\lambda_2)^{l_2}\cdots(\lambda-k\lambda_s)^{l_s}.$$

由此得出，如果 λ_i 是 A 的 l_i 重特征值，那么 $k\lambda_i$ 是 kA 的 l_i 重特征值。

证明 设 $A=(a_{ij})$，则

$$\begin{aligned}|\lambda I-A|&=\begin{vmatrix}\lambda-a_{11}&-a_{12}&\cdots&-a_{1n}\\-a_{21}&\lambda-a_{22}&\cdots&-a_{2n}\\\vdots&\vdots&&\vdots\\-a_{n1}&-a_{n2}&\cdots&\lambda-a_{nn}\end{vmatrix}\\&=\sum_{j_1j_2\cdots j_n}(-1)^{\tau(j_1j_2\cdots j_n)}(\lambda\delta_{1j_1}-a_{1j_1})\cdots(\lambda\delta_{nj_n}-a_{nj_n}).\end{aligned}$$

其中 δ_{ij} 是 Kronecker 记号，由已知条件得

$$\begin{aligned}&\sum_{j_1j_2\cdots j_n}(-1)^{\tau(j_1j_2\cdots j_n)}(\lambda\delta_{1j_1}-a_{1j_1})\cdots(\lambda\delta_{nj_n}-a_{nj_n})\\&=(\lambda-\lambda_1)^{l_1}(\lambda-\lambda_2)^{l_2}\cdots(\lambda-\lambda_s)^{l_s}.\end{aligned}\tag{11}$$

由于 $K[\lambda]$ 可看成是 K 的一个扩环，因此不定元 λ 用 $\frac{\lambda}{k}$ 代入，从(11)式得

$$\begin{aligned}&\sum_{j_1j_2\cdots j_n}(-1)^{\tau(j_1j_2\cdots j_n)}\left(\frac{\lambda}{k}\delta_{1j_1}-a_{1j_1}\right)\cdots\left(\frac{\lambda}{k}\delta_{nj_n}-a_{nj_n}\right)\\&=\left(\frac{\lambda}{k}-\lambda_1\right)^{l_1}\left(\frac{\lambda}{k}-\lambda_2\right)^{l_2}\cdots\left(\frac{\lambda}{k}-\lambda_s\right)^{l_s}.\end{aligned}\tag{12}$$

据行列式的定义，(12)式左端是$\frac{\lambda}{k}I-A$ 的行列式，于是(12)式可写成

$$\left|\frac{\lambda}{k}I-A\right|=\left(\frac{\lambda}{k}-\lambda_1\right)^{l_1}\left(\frac{\lambda}{k}-\lambda_2\right)^{l_2}\cdots\left(\frac{\lambda}{k}-\lambda_s\right)^{l_s}. \tag{13}$$

(13)式两边同乘以 k^n，得

$$|\lambda I-kA|=(\lambda-k\lambda_1)^{l_1}(\lambda-k\lambda_2)^{l_2}\cdots(\lambda-k\lambda_s)^{l_s}. \tag{14}$$

若 λ_i 是 A 的 l_i 重特征值，则从(14)式看出，$k\lambda_i$ 是 kA 的 l_i 重特征值。 ■

例 12 设数域 K 上 n 级矩阵 A 的特征多项式为

$$|\lambda I-A|=(\lambda-\lambda_1)^{l_1}(\lambda-\lambda_2)^{l_2}\cdots(\lambda-\lambda_s)^{l_s}. \tag{15}$$

其中 $\lambda_1,\lambda_2,\cdots,\lambda_s$ 是两两不等的复数，证明：A^2 的特征多项式为

$$|\lambda I-A^2|=(\lambda-\lambda_1^2)^{l_1}(\lambda-\lambda_2^2)^{l_2}\cdots(\lambda-\lambda_s^2)^{l_s}.$$

由此得出，如果 λ_i 是 A 的 l_i 重特征值，那么 λ_i^2 是 A^2 的至少 l_i 重特征值。

证明 在例 11 中取 $k=-1$，得 $-A$ 的特征多项式为

$$|\lambda I-(-A)|=[\lambda-(-1)\lambda_1]^{l_1}[\lambda-(-1)\lambda_2]^{l_2}\cdots[\lambda-(-1)\lambda_s]^{l_s},$$

即

$$|\lambda I+A|=(\lambda+\lambda_1)^{l_1}(\lambda+\lambda_2)^{l_2}\cdots(\lambda+\lambda_s)^{l_s}. \tag{16}$$

把(15)式与(16)式相乘，得

$$|\lambda^2 I-A^2|=(\lambda^2-\lambda_1^2)^{l_1}(\lambda^2-\lambda_2^2)^{l_2}\cdots(\lambda^2-\lambda_s^2)^{l_s}. \tag{17}$$

据行列式的定义，(17)式左端完全展开后是 λ^2 的多项式，因此(17)式是 $K[\lambda^2]$ 中的一个等式。由于 $K[\lambda]$ 可看成是 K 的一个扩环，因此 $K[\lambda^2]$ 的不定元 λ^2 可用 $K[\lambda]$ 中元素 λ 代入，把(17)式左端展开成 λ^2 的多项式后，从此式得到

$$|\lambda I-A^2|=(\lambda-\lambda_1^2)^{l_1}(\lambda-\lambda_2^2)^{l_2}\cdots(\lambda-\lambda_s^2)^{l_s}. \tag{18}$$

若 λ_i 是 A 的 l_i 重特征值，则从(18)式看出，λ_i^2 是 A^2 的至少 l_i 重特征值(注意，当$i\neq j$，有可能 $\lambda_i^2=\lambda_j^2$)。 ■

点评 在例 11 和例 12 中，分别要先把行列式$|\lambda I-A|$或$|\lambda^2 I-A^2|$完全展开成 λ 的多项式或λ^2 的多项式后，才能运用一元多项式环 $K[\lambda]$或 $K[\lambda^2]$的通用性质。这一点要特别注意。

习题 7.1

1. 在 $K[x]$中，如果 $f(x)$与 $g(x)$的次数都是 3，试问：$f(x)+g(x)$的次数一定是 3 吗？请举例说明。

2. 设 R 是有单位元 $1(\neq 0)$的环，证明：R 中的可逆元不可能是零因子。

3. 设数域 K 上 n 级矩阵 A 为

$$A=\begin{pmatrix}1 & b & b^2 & \cdots & b^{n-2} & b^{n-1}\\ 0 & 1 & b & \cdots & b^{n-3} & b^{n-2}\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1 & b\\ 0 & 0 & 0 & \cdots & 0 & 1\end{pmatrix}.$$

说明 A 可逆,并且求 A^{-1}。

4. 设 B 是数域 K 上的 n 级幂零矩阵,其幂零指数为 l,令 $A=aI+kB,a,k\in K^*$。说明 A 可逆,并且求 A^{-1}。

5. 设 A 是数域 K 上的 n 级矩阵。证明:对任意 $m\in\mathbf{N}^*$,有

$$(I+A)^m=I+\mathrm{C}_m^1A+\mathrm{C}_m^2A^2+\cdots+\mathrm{C}_m^mA^m.$$

6. 设数域 K 上的 n 级矩阵 A 的特征多项式为

$$|\lambda I-A|=(\lambda-\lambda_1)^{l_1}(\lambda-\lambda_2)^{l_2}\cdots(\lambda-\lambda_s)^{l_s},$$

其中 $\lambda_1,\lambda_2,\cdots,\lambda_s$ 是两两不等的复数。证明:A^3 的特征多项式为

$$|\lambda I-A^3|=(\lambda-\lambda_1^3)^{l_1}(\lambda-\lambda_2^3)^{l_2}\cdots(\lambda-\lambda_s^3)^{l_s}.$$

由此得出,如果 λ_i 是 A 的 l_i 重特征值,那么 λ_i^3 是 A^3 的至少 l_i 重特征值。

7. 设数域 K 上的 n 级矩阵 A 的特征多项式同第 6 题所给出的,对于任一正整数 m,证明:A^m 的特征多项式为

$$|\lambda I-A^m|=(\lambda-\lambda_1^m)^{l_1}(\lambda-\lambda_2^m)^{l_2}\cdots(\lambda-\lambda_s^m)^{l_s}.$$

由此得出,如果 λ_i 是 A 的 l_i 重特征值,那么 λ_i^m 是 A^m 的至少 l_i 重特征值。

7.2 整除关系,带余除法

7.2.1 内容精华

为了研究一元多项式环 $K[x]$的结构,我们从乘法运算入手,首先从乘法运算引出整除的概念,然后对于没有整除关系的两个多项式,探索带余除法。

一、整除关系

定义 1 设 $f(x),g(x)\in K[x]$,如果存在 $h(x)\in K[x]$,使得 $f(x)=h(x)g(x)$,那么称 $g(x)$**整除** $f(x)$,记作 $g(x)\mid f(x)$;否则,称 $g(x)$不能整除 $f(x)$,记作 $g(x)\nmid f(x)$。

在定义 1 中要注意 $h(x)\in K[x]$这个条件。

当 $g(x)$整除 $f(x)$时，称 $g(x)$是 $f(x)$的一个**因式**，称 $f(x)$是 $g(x)$的一个**倍式**。

从整除的定义容易推导出下列事实：

(1) $0|f(x) \Leftrightarrow f(x)=0$；

(2) $f(x)|0, \forall f(x)\in K[x]$；

(3) $b|f(x), \forall b\in K^*, \forall f(x)\in K[x]$。

整除是集合 $K[x]$中的一个二元关系，它具有：

(1) 反身性，即 $f(x)|f(x), \forall f(x)\in K[x]$；

(2) 传递性，即若 $f(x)|g(x)$，且 $g(x)|h(x)$，则 $f(x)|h(x)$。

注意整除关系不具有对称性，即从 $g(x)|f(x)$不能推出 $f(x)|g(x)$。

定义 2 在 $K[x]$中，如果 $g(x)|f(x)$且 $f(x)|g(x)$，那么称 $f(x)$与 $g(x)$**相伴**，记作 $f(x)\sim g(x)$。

命题 1 在 $K[x]$中，$f(x)\sim g(x)$当且仅当存在 $c\in K^*$，使得

$$f(x) = c\,g(x).$$

命题 2 在 $K[x]$中，如果 $g(x)|f_i(x), i=1,2,\cdots,s$，那么对于任意 $u_1(x),\cdots,u_s(x)\in K[x]$，都有

$$g(x)|[u_1(x)f_1(x)+\cdots+u_s(x)f_s(x)].$$

二、带余除法

在 $K[x]$中，如果 $g(x)$不能整除 $f(x)$，那么能有什么样的结论呢？例如，设 $f(x)=x^2, g(x)=x-1$，则

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

由此受到启发，猜测有下述结论：

定理 1(带余除法) 设 $f(x), g(x)\in K[x]$，且 $g(x)\neq 0$，则在 $K[x]$中存在唯一的一对多项式 $h(x), r(x)$，使得

$$f(x) = h(x)g(x)+r(x), \deg r(x) < \deg g(x), \tag{1}$$

其中 $f(x)$、$g(x)$分别叫做**被除式**、**除式**，$h(x)$、$r(x)$分别叫做**商式**、**余式**。(1)式称为**除法算式**。

定理 1 表明，数域 K 上的一元多项式环 $K[x]$是具有除法算式的环。除法算式是 $K[x]$中有关加法和乘法的第一个重要等式，它非常有用。

利用带余除法可以证明：

推论 1 设 $f(x), g(x)\in K[x]$，且 $g(x)\neq 0$，则 $g(x)|f(x)$当且仅当 $g(x)$除 $f(x)$的余式为 0。

命题 3 设 $f(x),g(x)\in K[x]$，数域 $F\supseteq K$，则

在 $K[x]$ 中，$g(x)\mid f(x)$ $\Leftrightarrow$ 在 $F(x)$ 中，$g(x)\mid f(x)$。

命题 3 表明，整除性不随数域的扩大而改变。

利用带余除法还可以得到用一次多项式 $x-c$ 去除一个多项式的**综合除法**：

设 $f(x)=\sum_{i=0}^{n}a_ix^i$，$a_n\neq 0$，$n\geqslant 1$，则由带余除法得

$$f(x)=h(x)(x-c)+r,r\in K. \tag{2}$$

从(2)式得

$$1\leqslant \deg f(x)\leqslant \max\{\deg h(x)(x-c),\deg r\},$$

由此得出，
$$\begin{aligned}\deg f(x)&=\deg h(x)(x-c)\\&=\deg h(x)+\deg (x-c)\\&=\deg h(x)+1.\end{aligned}$$

因此 $\deg h(x)=n-1$，从而可设 $h(x)=\sum_{i=0}^{n-1}b_ix^i$。

比较(2)式两边的首项系数，得

$$a_n=b_{n-1}. \tag{3}$$

比较(2)式两边的 s 次项的系数($s=1,2,\cdots,n-1$)，得

$$a_s=-cb_s+b_{s-1},$$

从而
$$a_s+cb_s=b_{s-1},s=1,2,\cdots,n-1. \tag{4}$$

比较(2)式两边的常数项，得

$$a_0=-cb_0+r.$$

从而
$$a_0+cb_0=r. \tag{5}$$

从(3)、(4)、(5)式得

a_n	a_{n-1}	$\cdots$	a_1	a_0	c
	$b_{n-1}c$	$\cdots$	b_1c	b_0c	
a_n	$a_{n-1}+b_{n-1}c$	$\cdots$	a_1+b_1c	a_0+b_0c	
$\|\|$	$\|\|$		$\|\|$	$\|\|$	
b_{n-1}	b_{n-2}	$\cdots$	b_0	r	

于是求出了商式 $h(x)=b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+\cdots+b_0$，余式 r。

整数环 $\mathbf{Z}$ 中也有带余除法：

定理 2 任给 $a,b\in\mathbf{Z},b\neq0$,则存在唯一的一对整数 q,r,使得

$$a=qb+r,0\leqslant r<|b|. \tag{6}$$

关于整数环 $\mathbf{Z}$ 中的整除关系及其性质,我们把它们放在本节习题的第 5 题中。

* 三、带余除法的应用之一:λ-矩阵的相抵标准形

本套书上册中,我们讲了数域 K 上的矩阵,现在我们把它推广成整环 R 上的矩阵。

定义 3 设 R 是一个整环,由 R 中 $s\times n$ 个元素排成的 s 行 n 列的一张表称为 R 上的一个 $s\times n$ **矩阵**。

可以像数域 K 上的矩阵那样,定义 R 上矩阵的加法、纯量乘法(用 R 中元素乘矩阵)、乘法这三种运算,这些运算满足与数域 K 上矩阵一样的运算法则;还可以定义 R 上矩阵的三种初等行(列)变换(其中,3°型初等行(列)变换应当是用 R 中的可逆元乘某一行(列))。可以像数域 K 上 n 级矩阵的行列式那样,定义 R 上 n 级矩阵的行列式,而且同样有行列式的 7 条性质以及行列式按一行(列)展开定理。对于整环 R 上的 n 级矩阵 A,同样可以有可逆矩阵的概念。但是要注意:R 上 n 级矩阵 A 可逆的充分必要条件是 $|A|$ 为 R 中的可逆元。整环 R 上的矩阵的秩的概念通过子式来定义:

定义 4 设 A 是整环 R 上的一个非零矩阵,如果 A 有一个 r 阶子式不为 0,而所有 $r+1$ 阶子式(如果有的话)全为 0,那么称 A 的**秩**为 r。零矩阵的秩规定为 0。

设 K 是数域,整环 $K[\lambda]$ 上的矩阵称为 λ-矩阵。用 $A(\lambda),B(\lambda),\cdots$ 来记 λ-矩阵。注意 $K[\lambda]$ 中的可逆元都是 K 中非零数,因此 λ-矩阵的 3°型初等行(列)变换可叙述成:用 K 中一个非零数乘某一行(列)。

对于 λ-矩阵 $A(\lambda),B(\lambda)$,如果可以通过一系列的初等行(列)变换把 $A(\lambda)$ 变成 $B(\lambda)$,那么称 $A(\lambda)$ 与 $B(\lambda)$ **相抵**。

利用 $K[\lambda]$ 中的带余除法可以证明下述关于 λ-矩阵的相抵标准形的定理。

定理 3 任意一个非零的 n 级 λ-矩阵 $A(\lambda)$ 一定相抵于对角 λ-矩阵:

$$\mathrm{diag}\{d_1(\lambda),d_2(\lambda),\cdots,d_n(\lambda)\}, \tag{7}$$

其中 $d_i(\lambda)|d_{i+1}(\lambda),i=1,2,\cdots,n-1$,并且对于非零的 $d_i(\lambda)$,其首项系数为 1。满足这些要求的 λ-矩阵(7)称为 $A(\lambda)$ 的一个**相抵标准形**或 **Smith 标准形**。

关于 λ-矩阵 $A(\lambda)$ 的相抵标准形的唯一性问题,我们把它留在下一节讨论。

定理 3 是对于 λ-矩阵来叙述并且证明的。我们可以把它的叙述略加修改,并且类似地证明整数环 $\mathbf{Z}$ 上的 n 级矩阵的相应定理。

定理 4 整数环 $\mathbf{Z}$ 上任一非零的 n 级矩阵 A 一定相抵于 $\mathbf{Z}$ 上的对角矩阵:

$$\mathrm{diag}\{d_1,d_2,\cdots,d_n\}, \tag{8}$$

其中 $d_j \in \mathbf{N}(j=1,2,\cdots,n)$，并且 $d_i \mid d_{i+1}, i=1,2,\cdots,n-1$，满足这些要求的矩阵(8)称为 A 的一个**相抵标准形**或 **Smith 标准形**。

定理 4 的证明与定理 3 类似，只要把“首项系数为 1”改成“正整数”，把“次数”改成“绝对值”即可。

7.2.2　典型例题

例 1　证明整除关系具有传递性，即在 $K[x]$ 中，如果 $f(x) \mid g(x)$ 且 $g(x) \mid h(x)$，那么 $f(x) \mid h(x)$。

证明　由已知条件得，存在 $u(x), v(x) \in K[x]$，使得

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

从而　　$$h(x) = v(x)u(x)f(x).$$

因此　　$$f(x) \mid h(x).$$ ■

例 2　证明：在 $K[x]$ 中，如果 $g(x) \mid f_i(x), i=1,2,\cdots,s$，那么对于任意 $u_1(x),\cdots,u_s(x) \in K[x]$，有

$$g(x) \mid [u_1(x)f_1(x) + \cdots + u_s(x)f_s(x)].$$

证明　由已知条件得，存在 $h_i(x) \in K[x]$，使得

$$f_i(x) = h_i(x)g(x), i = 1,2,\cdots,s.$$

从而

$$\begin{aligned} & u_1(x)f_1(x) + \cdots + u_s(x)f_s(x) \\ = & u_1(x)h_1(x)g(x) + \cdots + u_s(x)h_s(x)g(x) \\ = & [u_1(x)h_1(x) + \cdots + u_s(x)h_s(x)]g(x). \end{aligned}$$

因此　　$$g(x) \mid [u_1(x)f_1(x) + \cdots + u_s(x)f_s(x)].$$ ■

例 3　设 $f(x) = x^4 + 2x^3 - 5x + 7, g(x) = x^2 - 3x + 1$。用 $g(x)$ 去除 $f(x)$，求商式和余式。

解

x^2-3x+1	x^4+2x^3-5x+7	$x^2+5x+14$
	$x^4-3x^3+x^2$	
	$5x^3-x^2-5x+7$	
	$5x^3-15x^2+5x$	
	$14x^2-10x+7$	
	$14x^2-42x+14$	
	$32x-7$	

因此，商式为 $x^2+5x+14$，余式为 $32x-7$。即

$$f(x)=(x^2+5x+14)g(x)+(32x-7).$$

例 4 设 $f(x)=x^4-x^3+4x^2+a_1x+a_0$，$g(x)=x^2+2x-3$。求 $g(x)$整除 $f(x)$的充分必要条件。

解

x^2+2x-3	$x^4-x^3+4x^2+a_1x+a_0$	$x^2-3x+13$
	$x^4+2x^3-3x^2$	
	$-3x^3+7x^2+a_1x+a_0$	
	$-3x^3-6x^2+9x$	
	$13x^2+(a_1-9)x+a_0$	
	$13x^2+26x-39$	
	$(a_1-35)x+(a_0+39)$	

因此，$g(x)\mid f(x)$ $\Leftrightarrow$ $(a_1-35)x+(a_0+39)=0$

$\Leftrightarrow$ $a_1-35=0$ 且 $a_0+39=0$

$\Leftrightarrow$ $a_1=35$ 且 $a_0=-39$.

例 5 用综合除法求 $x+3$ 除 $f(x)=2x^4-x^3+5x-3$ 所得的商式与余式。

解

2	−1	0	5	−3	−3
	−6	21	−63	174	
2	−7	21	−58	171	

因此，商式为 $2x^3-7x^2+21x-58$，余式为 171。

例 6 在例 5 中，用 $x+3$ 除 $f(x)$所得的商式记作 $h_1(x)$，接着用 $x+3$ 除 $h_1(x)$所得的商式记作 $h_2(x)$，…，如此进行下去，得到 $f(x)$的一个表达式，称它为 $x+3$ 的幂和。把 $f(x)$表示成 $x+3$ 的幂和。

解 在例 5 中已求出 $h_1(x)=2x^3-7x^2+21x-58$，余式为 171。

2	−7	21	−58	−3
	−6	39	−180	
2	−13	60	−238	

于是商式为 $h_2(x)=2x^2-13x+60$，余式为 −238。

$$\begin{array}{c|ccc|c} & 2 & -13 & 60 & -3 \\ & & -6 & 57 & \\ \hline & 2 & -19 & 117 & \end{array}$$

于是商式为 $h_3(x)=2x-19$，余式为 117。

$$\begin{array}{c|cc|c} & 2 & -19 & -3 \\ & & -6 & \\ \hline & 2 & -25 & \end{array}$$

于是商式为 $h_4(x)=2$，余式为 -25，从而

$$\begin{aligned} f(x) &= h_1(x)(x+3)+171 \\ &= [h_2(x)(x+3)-238](x+3)+171 \\ &= [(2x-19)(x+3)+117](x+3)^2-238(x+3)+171 \\ &= [2(x+3)-25](x+3)^3+117(x+3)^2-238(x+3)+171 \\ &= 2(x+3)^4-25(x+3)^3+117(x+3)^2-238(x+3)+171. \end{aligned}$$

点评　例 6 利用综合除法把 $f(x)$表示成了 $x+3$ 的幂和的形式，从而给出了多项式函数 $f(x)$在 $x=-3$ 处的展开式，这与数学分析课中用泰勒级数公式求出的 $f(x)$在 $x=-3$ 处的展开式一致。

例 7　证明：设 $d,n\in\mathbf{N}^*$，则在 $K[x]$中，$x^d-1\mid x^n-1\Leftrightarrow d\mid n$。

证明　充分性。设 $d\mid n$，则 $n=sd,s\in\mathbf{N}^*$。显然有

$$x^s-1=(x-1)(x^{s-1}+x^{s-2}+\cdots+x+1).$$

由于 $K[x]$可看成是 K 的一个扩环，因此不定元 x 可用 x^d 代入，从上式得

$$(x^d)^s-1=(x^d-1)(x^{d(s-1)}+x^{d(s-2)}+\cdots+x^d+1).$$

由此得出，

$$x^d-1\mid x^n-1.$$

必要性。在整数环 $\mathbf{Z}$ 中，作带余除法：

$$n=sd+r,0\leqslant r<d,$$

假如 $r\neq0$，则

$$\begin{aligned} x^n-1 &= x^{sd+r}-1 \\ &= x^{sd}\cdot x^r-x^r+x^r-1 \\ &= x^r(x^{sd}-1)+(x^r-1). \end{aligned} \tag{9}$$

由充分性所证的结论得，$x^d-1\mid x^{sd}-1$.

又由已知条件得，$x^d-1\mid x^n-1$.

因此从(9)式得，$x^d-1\mid x^r-1$.

由此推出 $d\leqslant r$.

这与 $r<d$ 矛盾。因此 $r=0$。从而 $d\mid n$。 ■

例 8 证明：设 d,n 都是正整数，则对任一不等于 ±1 的整数 a，有 $a^d-1\mid a^n-1\Leftrightarrow d\mid n$。

证明 充分性。设 $d\mid n$，则 $n=sd,s\in\mathbf{N}^*$。在 $K[x]$ 中显然有

$$x^s-1=(x-1)(x^{s-1}+s^{s-2}+\cdots+x+1).$$

x 用 a^d 代入，从上式得

$$a^{ds}-1=(a^d-1)(a^{d(s-1)}+a^{d(s-2)}+\cdots+a^d+1).$$

由此得出，$a^d-1\mid a^n-1$.

必要性的证明与例 7 的必要性证明类似。 ■

* **例 9** 求下述 λ-矩阵的一个相抵标准形。

$$A(\lambda)=\begin{pmatrix}\lambda-1 & 3 & -4\\ -4 & \lambda+7 & -8\\ -6 & 7 & \lambda-7\end{pmatrix}.$$

解 首先要使 λ-矩阵的(1,1)元变成能整除该矩阵的所有元素，从而可把第 1 行和第 1 列的其他元素变成 0。然后把右下角矩阵的(1,1)元也变成能整除该矩阵的所有元素，依次进行下去。

$$A(\lambda)\xrightarrow[③+②]{}\begin{pmatrix}\lambda-1 & 3 & -1\\ -4 & \lambda+7 & \lambda-1\\ -6 & 7 & \lambda\end{pmatrix}\xrightarrow{(①,③)}\begin{pmatrix}-1 & 3 & \lambda-1\\ \lambda-1 & \lambda+7 & -4\\ \lambda & 7 & -6\end{pmatrix}$$

$$\xrightarrow[③+①\lambda]{②+①\cdot(\lambda-1)}\begin{pmatrix}-1 & 3 & \lambda-1\\ 0 & 4\lambda+4 & \lambda^2-2\lambda-3\\ 0 & 3\lambda+7 & \lambda^2-\lambda-6\end{pmatrix}\longrightarrow\begin{pmatrix}-1 & 0 & 0\\ 0 & \lambda+1 & \frac{1}{4}(\lambda-3)(\lambda+1)\\ 0 & 3\lambda+7 & \lambda^2-\lambda-6\end{pmatrix}$$

$$\xrightarrow[③+②\left[-\frac{1}{4}(\lambda-3)\right]]{}\begin{pmatrix}1 & 0 & 0\\ 0 & \lambda+1 & 0\\ 0 & 3\lambda+7 & \frac{1}{4}(\lambda-3)(\lambda+1)\end{pmatrix}$$

$$\xrightarrow{③+②(-3)}\begin{pmatrix}1 & 0 & 0\\ 0 & \lambda+1 & 0\\ 0 & 4 & \frac{1}{4}(\lambda-3)(\lambda+1)\end{pmatrix}\longrightarrow\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & (\lambda-3)(\lambda+1)\\ 0 & \lambda+1 & 0\end{pmatrix}$$

$$\longrightarrow\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & (\lambda-3)(\lambda+1)\\ 0 & 0 & -(\lambda-3)(\lambda+1)^2\end{pmatrix}\longrightarrow\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & (\lambda-3)(\lambda+1)^2\end{pmatrix}.$$

最后一个 λ-矩阵就是 $A(\lambda)$的一个相抵标准形。其中，$d_1(\lambda)=1$，$d_2(\lambda)=1$，$d_3(\lambda)=(\lambda-3)(\lambda+1)^2$。

* **例 10**　一元多项式环 $K[x]$的一个非空子集 J 如果对减法封闭，并且满足

$$f(x)\in K[x]\text{ 且 }g(x)\in J\quad\Rightarrow\quad f(x)g(x)\in J,$$

那么称 J 是 $K[x]$的一个**理想子环**，简称为**理想**。证明：$K[x]$的任一理想 J 是由某一个多项式的倍式组成的集合。

证明　若 $J=\{0\}$，则 J 是由 0 的倍式组成的集合。

下设 $J\neq\{0\}$。在 J 的所有非零多项式中取一个次数最低的多项式 $m(x)$，任取 $f(x)\in J$。作带余除法：

$$f(x)=h(x)m(x)+r(x),\deg r(x)<\deg m(x).$$

由于 J 是理想，因此

$$r(x)=f(x)-h(x)m(x)\in J.$$

假如 $r(x)\neq0$，则这与 $m(x)$的取法矛盾。因此 $r(x)=0$，从而 $f(x)=h(x)m(x)$。又显然 $m(x)$的任一倍式属于 J。因此 J 是由 $m(x)$的所有倍式组成的集合。

点评　从例 10 的证明看出，带余除法起了关键作用。

习题 7.2

1. 用 $g(x)$除 $f(x)$，求商式与余式：

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

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

2. 设 $f(x)=x^4-3x^3+a_1x+a_0$，$g(x)=x^2-3x+1$，求 $g(x)$整除 $f(x)$的充分必要条件。

3. 用综合除法求一次多项式 $g(x)$除 $f(x)$所得的商式与余式。

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

(2) $f(x)=5x^3-3x+4, g(x)=x+2$。

4. 把第 3 题的第(2)小题中的 $f(x)$表示成 $x+2$ 的幂和。

5. 设 $a,b\in\mathbf{Z}$,如果有 $h\in\mathbf{Z}$,使得 $a=hb$,那么称 b 整除 a,记作 $b|a$。此时称 b 是 a 的因数(或因子),称 a 是 b 的倍数。证明:

(1) 如果 $a|b$ 且 $b|a$(此时称 a 与 b 相伴),那么 $a=\pm b$,反之也成立;

(2) 如果 $a|b$ 且 $b|c$,那么 $a|c$;

(3) 如果 $b|a_i, i=1,2,\cdots,s$,那么对任意 $u_1,\cdots,u_s\in\mathbf{Z}$,有 $b|u_1a_1+u_2a_2+\cdots+u_sa_s$;

(4) 如果 $b|a$ 且 $a\neq0$,那么 $|b|\leqslant|a|$。

6. 设 A 是数域 K 上的 n 级矩阵,

$$f(A)=A^3-4A^2+7A-I, g(A)=A-2I.$$

求 $h(A), r(A)$,使得 $f(A)=h(A)g(A)+r(A)$。

* 7. 求下列 λ-矩阵的相抵标准形:

(1) $\begin{pmatrix}\lambda & -1 & 0\\ 4 & \lambda-4 & 0\\ 2 & -1 & \lambda-2\end{pmatrix}$; (2) $\begin{pmatrix}\lambda-4 & 5 & -2\\ -5 & \lambda+7 & -3\\ -6 & 9 & \lambda-4\end{pmatrix}$。

8. 设 $m\in\mathbf{N}^*, a\in K^*$,证明:在 $K[x]$中,$x-a|x^m-a^m$,并且求商式。

9. 设 $m\in\mathbf{N}^*, a\in K^*$,证明:在 $K[x]$中,$x+a|x^{2m+1}+a^{2m+1}$,并且求商式。

7.3 最大公因式

7.3.1 内容精华

利用带余除法和整除的性质,本节要推导出一元多项式环 $K[x]$中有关加法和乘法的又一些重要等式。

一、最大公因式

定义 1 $K[x]$中多项式 $f(x)$与 $g(x)$的一个公因式 $d(x)$如果满足下述条件:对于 $f(x)$与 $g(x)$的任一公因式 $c(x)$,都有 $c(x)|d(x)$,那么称 $d(x)$是 $f(x)$与 $g(x)$的一个**最大公因式**。

定义 1 中的条件刻画了 $d(x)$是 $f(x)$与 $g(x)$的公因式中的“最大者”。另一种自然的想法是把 $f(x)$与 $g(x)$的公因式组成的集合中,次数最高的多项式定义为 $f(x)$与 $g(x)$的最大公因式。但是这样定义最大公因式就不容易求两个多项式的最大公因式,也无法确定 0 与 0 的最大公因式(因为任一多项式都是 0 与 0 的公因式)。而采用定义 1 所述的条件就比较容易求出两个多项式的最大公因式。例如,用定义 1 立即得到:$f(x)$是 $f(x)$与 0 的一个最大公因式。特别地,0 是 0 与 0 的最大公因式。从定义 1 还可看出,对于不全为 0 的两个多项式 $f(x)$与 $g(x)$,它们的最大公因式是次数最高的公因式。

由最大公因式的定义容易看出:如果 $f(x)$与 $g(x)$的最大公因式存在,那么 $f(x)$与 $g(x)$的任意两个最大公因式 $d_1(x)$与 $d_2(x)$是相伴的,即它们相差一个非零数因子(由于 $d_1(x)$是 $f(x)$与 $g(x)$的一个最大公因式,因此 $d_2(x)\mid d_1(x)$;同理 $d_1(x)\mid d_2(x)$,从而 $d_1(x)$与 $d_2(x)$相伴)。如果 $f(x)$与 $g(x)$不全为 0,那么它们的最大公因式不是 0,于是我们用$(f(x),g(x))$(或者 $g.c.d(f(x),g(x))$)表示首项系数为 1 的最大公因式,简称为 $f(x)$与 $g(x)$的**首一最大公因式**。

在 $K[x]$中,如果

$$\{f(x)\text{ 与 }g(x)\text{ 的公因式}\}=\{p(x)\text{ 与 }q(x)\text{ 的公因式}\},$$

那么$\{f(x)$与 $g(x)$的最大公因式$\}=\{p(x)$与 $q(x)$的最大公因式$\}$.

由此结论立即得到:若 $a,b\in K^*$,则

$$\{f(x)\text{与 }g(x)\text{的最大公因式}\}=\{af(x)\text{与 }bg(x)\text{的最大公因式}\}.$$

还可得到:

引理 1 在 $K[x]$中,如果有等式

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

成立,那么

$$\{f(x)\text{ 与 }g(x)\text{ 的最大公因式}\}=\{g(x)\text{ 与 }r(x)\text{ 的最大公因式}\}.$$

由于 $K[x]$中有除法算式,因此根据引理可以用**辗转相除法**求出 $f(x)$与 $g(x)$的最大公因式,其中 $g(x)\neq 0$。即,我们可以证明:

定理 1 对于 $K[x]$中任意两个多项式 $f(x)$与 $g(x)$,存在它们的一个最大公因式 $d(x)$,并且存在 $u(x),v(x)\in K[x]$,使得

$$d(x)=u(x)f(x)+v(x)g(x). \tag{1}$$

定理 1 的证明中给出了求 $f(x)$与 $g(x)$的最大公因式的方法,称它为**辗转相除法**。它是求任意两个多项式的最大公因式的统一的、机械的方法,非常有用。

(1)式是 $K[x]$中关于加法和乘法的第二个重要等式,很有用。

二、互素

定义 2 设 $f(x),g(x)\in K[x]$，如果$(f(x),g(x))=1$，那么称 $f(x)$与 $g(x)$**互素**。

由定义 2 立即得出，$K[x]$中 $f(x)$与 $g(x)$互素当且仅当它们的公因式都是 K 中非零数。

由定义 2 和定理 1 以及上述结论可以推导出：

定理 2 $K[x]$中两个多项式 $f(x)$与 $g(x)$互素的充分必要条件是，存在 $u(x),v(x)\in K[x]$，使得

$$u(x)f(x)+v(x)g(x)=1. \tag{2}$$

定理 2 是十分重要的结论，(2)式是 $K[x]$中关于加法与乘法的第三个重要等式。

利用辗转相除法可以证明：

命题 1 设 $f(x)$与 $g(x)\in K[x]$，数域 $F\supseteq K$，则 $f(x)$与 $g(x)$在 $K[x]$中的首一最大公因式等于它们在 $F(x)$中的首一最大公因式，即 $f(x)$与 $g(x)$的首一最大公因式不随数域的扩大而改变。

由命题 1 立即得到：

推论 1 设 $f(x),g(x)\in K[x]$，数域 $F\supseteq K$，则 $f(x)$与 $g(x)$在 $K[x]$中互素当且仅当 $f(x)$与 $g(x)$在 $F[x]$中互素，即互素性不随数域的扩大而改变。

在 $K[x]$中，两个多项式互素当且仅当它们的公因式都是 K 中非零数。由此可以直观地猜测并且可以证明有关互素的一些性质：

性质 1 在 $K[x]$中，如果

$$f(x)\mid g(x)h(x),\text{且}(f(x),g(x))=1,$$

那么

$$f(x)\mid h(x).$$

性质 2 在 $K[x]$中，如果 $f(x)\mid h(x)$，$g(x)\mid h(x)$，且$(f(x),g(x))=1$，那么 $f(x)g(x)\mid h(x)$。

性质 3 在 $K[x]$中，如果

$$(f(x),h(x))=1,(g(x),h(x))=1,$$

那么

$$(f(x)g(x),h(x))=1.$$

性质 3 可以用定理 2 证明。性质 3 可以推广成：若$(f_i(x),h(x))=1,i=1,2,\cdots,s$，则$(f_1(x)f_2(x)\cdots f_s(x),h(x))=1$。

三、多个多项式的最大公因式和互素

在 $K[x]$中，多个多项式的最大公因式的概念与两个多项式的最大公因式类似。在

$K[x]$中，$f_1(x),f_2(x),\cdots,f_s(x)$的一个公因式$d(x)$如果满足下述条件：$f_1(x),f_2(x),\cdots,f_s(x)$的任一公因式$c(x)$都能整除$d(x)$，那么$d(x)$称为$f_1(x),f_2(x),\cdots,f_s(x)$的**一个最大公因式**。

从多个多项式的最大公因式的定义立即得到：在$K[x]$中，s个多项式$f_1(x),f_2(x),\cdots,f_s(x)$的最大公因式如果存在，那么它在相伴的意义下是唯一的。对于s个不全为0的多项式$f_1(x),\cdots,f_s(x)$，它们的最大公因式不是0，从而我们用$(f_1(x),\cdots,f_s(x))$表示首项系数为1的最大公因式，简称为首一最大公因式。

用数学归纳法可以证明：在$K[x]$中，任意s个($s\geqslant 2$)多项式$f_1(x),f_2(x),\cdots,f_s(x)$的最大公因式存在。

从上述结论的证明立即得出：对于s个不全为0的多项式$f_1(x),f_2(x),\cdots,f_s(x)$，有

$$(f_1(x),f_2(x),\cdots,f_s(x))=((f_1(x),\cdots,f_{s-1}(x)),f_s(x)). \tag{3}$$

从而有$K[x]$中多项式$u_i(x),i=1,2,\cdots,s$，使得

$$\begin{aligned}&u_1(x)f_1(x)+u_2(x)f_2(x)+\cdots+u_s(x)f_s(x)\\&=(f_1(x),f_2(x),\cdots,f_s(x)).\end{aligned} \tag{4}$$

定义3 在$K[x]$中，s个多项式$f_1(x),f_2(x),\cdots,f_s(x)$如果满足$(f_1(x),f_2(x),\cdots,f_s(x))=1$，那么称$f_1(x),f_2(x),\cdots,f_s(x)$**互素**。

定理3 在$K[x]$中，$f_1(x),f_2(x),\cdots,f_s(x)$互素的充分必要条件是，存在$u_1(x),u_2(x),\cdots,u_s(x)\in K[x]$，使得

$$u_1(x)f_1(x)+u_2(x)f_2(x)+\cdots+u_s(x)f_s(x)=1. \tag{5}$$

注意：$s(s\geqslant 3)$个多项式互素时，它们不一定两两互素。

在整数环$\mathbf{Z}$中，类似地可讨论最大公因数和互素的概念，以及它们的性质。下面把它们列举出来，证明留给读者。

定义4 整数a与b的一个公因数d如果满足下述条件：a与b的任一公因数c都能整除d，那么称d是a与b的一个**最大公因数**。

定理4 任给两个整数a与b，都存在它们的一个最大公因数d，并且存在整数u,v，使得

$$ua+vb=d. \tag{6}$$

从定义4得出，若d_1,d_2都是整数a与b的最大公因数，则$d_1=\pm d_2$。若a与b不全为0，则a与b的最大公因数恰有两个，它们互为相反数。用(a,b)表示正的那个最大公因数，或者记作$g.c.d(a,b)$。

定义5 设$a,b\in\mathbf{Z}$，如果$(a,b)=1$，那么a与b**互素**。

定理5 两个整数a与b互素当且仅当存在$u,v\in\mathbf{Z}$，使得

$$ua+vb=1. \tag{7}$$

互素的整数的性质：在 $\mathbf{Z}$ 中，

(1) 若 $a|bc$，且 $(a,b)=1$，则 $a|c$；

(2) 若 $a|c, b|c$，且 $(a,b)=1$，则 $ab|c$；

(3) 若 $(a,c)=1, (b,c)=1$，则 $(ab,c)=1$。

性质 3 可以推广成：若 $(a_i,c)=1, i=1,2,\cdots,s$，则 $(a_1a_2\cdots a_s,c)=1$。

在 $\mathbf{Z}$ 中，$a_1,a_2,\cdots,a_s$ 的一个公因数 d 如果满足下述条件：$a_1,a_2,\cdots,a_s$ 的任一公因数 c 能整除 d，那么称 d 是 $a_1,a_2,\cdots,a_s$ 的一个**最大公因数**。

从多个整数的最大公因数的定义得出，不全为 0 的整数 $a_1,a_2,\cdots,a_s$ 的最大公因数恰有两个，它们互为相反数。我们约定用 $(a_1,a_2,\cdots,a_s)$ 表示正的那个最大公因数，或者记作 $g.c.d(a_1,a_2,\cdots,a_s)$。

用数学归纳法可以证明，任意 $s(s\geqslant 2)$ 个整数都有最大公因数。由此得出，对于不全为 0 的整数 $a_1,a_2,\cdots,a_s$，有

$$(a_1,a_2,\cdots,a_s)=((a_1,a_2,\cdots,a_{s-1}),a_s).$$

从而存在 $u_1,u_2,\cdots,u_s\in\mathbf{Z}$，使得

$$u_1a_1+u_2a_2+\cdots+u_sa_s=(a_1,a_2,\cdots,a_s).$$

对于 s 个整数 $a_1,a_2,\cdots,a_s$，如果 $(a_1,a_2,\cdots,a_s)=1$，那么称 $a_1,a_2,\cdots,a_s$ **互素**。

$a_1,a_2,\cdots,a_s$ 互素当且仅当存在 $u_1,u_2,\cdots,u_s\in\mathbf{Z}$，使得

$$u_1a_1+u_2a_2+\cdots+u_sa_s=1.$$

整数 m 称为整数 a 与 b 的**最小公倍数**，如果

1° $a|m, b|m$；

2° 从 $a|l, b|l$ 可推出 $m|l$。

可以证明，任意两个整数都有最小公倍数，若 a 与 b 全不为 0，则 a 与 b 的最小公倍数恰有两个，且它们互为相反数。用 $[a,b]$ 表示正的那个最小公倍数，若 $a>0, b>0$，则

$$[a,b]=\frac{ab}{(a,b)}.$$

* 四、最大公因式的应用之一：λ-矩阵的行列式因子

定义 6 设 $A(\lambda)$ 是一个 $s\times n$ λ-矩阵，对于正整数 $k(1\leqslant k\leqslant\min\{s,n\})$，$A(\lambda)$ 的所有 k 阶子式的首一最大公因式 $D_k(\lambda)$ 称为 $A(\lambda)$ 的 k 阶**行列式因子**。

定理 6 相抵的 λ-矩阵，它们的秩相等，并且各阶行列式因子也对应相等。

据 7.2 节的内容精华中的定理 3 得，任一非零的 n 级 λ-矩阵 $A(\lambda)$ 相抵于下述对角 λ-矩阵：

$$\operatorname{diag}\{d_1(\lambda),d_2(\lambda),\cdots,d_n(\lambda)\},\tag{8}$$

其中 $d_i(\lambda)|d_{i+1}(\lambda), i=1,2,\cdots,n-1$，并且非零的 $d_i(\lambda)$ 的首项系数为 1。现在来计算 λ-矩

阵(8)的各阶行列式因子。设

$$d_i(\lambda)\neq 0, i=1,2,\cdots,r; d_{r+1}(\lambda)=\cdots=d_n(\lambda)=0.$$

则

$$\begin{aligned}
&D_1(\lambda)=(d_1(\lambda),d_2(\lambda),\cdots,d_r(\lambda),0,\cdots,0)=d_1(\lambda),\\
&D_2(\lambda)=(d_1(\lambda)d_2(\lambda),d_1(\lambda)d_3(\lambda),\cdots,d_{r-1}(\lambda)d_r(\lambda),0,\cdots,0)\\
&\quad=d_1(\lambda)d_2(\lambda),\\
&\cdots\\
&D_r(\lambda)=d_1(\lambda)d_2(\lambda)\cdots d_r(\lambda),\qquad (9)\\
&D_{r+1}(\lambda)=\cdots=D_n(\lambda)=0.
\end{aligned}$$

根据定理 6,$D_1(\lambda),D_2(\lambda),\cdots,D_n(\lambda)$也是 $A(\lambda)$的各阶行列式因子。由上述式子得到

$$d_1(\lambda)=D_1(\lambda), d_2(\lambda)=\frac{D_2(\lambda)}{D_1(\lambda)},\cdots,d_r(\lambda)=\frac{D_r(\lambda)}{D_{r-1}(\lambda)}. \qquad (10)$$

这表明 $A(\lambda)$的相抵标准形中主对角线上的非零元可以用 $A(\lambda)$的行列式因子计算出,因此 $A(\lambda)$的相抵标准形中主对角线上的非零元是唯一确定的,其个数等于 $A(\lambda)$的秩。这样我们证明了下面的定理:

定理 7 n 级 λ-矩阵 $A(\lambda)$的相抵标准形是唯一的。 ■

定义 7 n 级 λ-矩阵 $A(\lambda)$的相抵标准形中主对角线上的非零元 $d_1(\lambda),d_2(\lambda),\cdots,d_r(\lambda)$称为 $A(\lambda)$的**不变因子**。

定理 8 两个 n 级 λ-矩阵相抵的充分必要条件是它们有相同的不变因子,或者有相同的各阶行列式因子。

从(9)式立即得出,$D_i(\lambda)\mid D_{i+1}(\lambda), i=1,2,\cdots,n-1$。因此在求 $A(\lambda)$的各阶行列式因子时,往往先求出最高阶的行列式因子,较为简便。

设 A 是数域 K 上的 n 阶矩阵,$\lambda I-A$ 称为 A 的**特征矩阵**,由于$|\lambda I-A|$是 λ 的 n 次多项式,因此 $\lambda I-A$ 的 n 阶行列式因子 $D_n(\lambda)=|\lambda I-A|\neq 0$。由于 $D_n(\lambda)=d_1(\lambda)d_2(\lambda)\cdots d_n(\lambda)$,因此 $\lambda I-A$ 的不变因子有 n 个,并且

$$d_1(\lambda)d_2(\lambda)\cdots d_n(\lambda)=D_n(\lambda)=|\lambda I-A|.$$

即 $\lambda I-A$ 的 n 个不变因子的乘积等于 A 的特征多项式。

设 $A(\lambda)$是 n 级可逆的 λ-矩阵,则$|A(\lambda)|$是 K 中非零数。于是 $D_n(\lambda)=1$,从而

$$D_i(\lambda)=1, i=1,2,\cdots,n.$$

因此

$$d_i(\lambda)=1, i=1,2,\cdots,n.$$

这证明了:n 级可逆的 λ-矩阵的相抵标准形为单位矩阵 I。于是 n 级可逆的 λ-矩阵经过一系列初等行(列)变换能变成单位矩阵 I。

由单位矩阵 I 经过一次 λ-矩阵的初等行(列)变换得到的矩阵称为初等 λ-矩阵。容易

看出,初等 λ-矩阵都是可逆的。对 λ-矩阵 $A(\lambda)$ 作一次初等行(列)变换就相当于用一个相应的初等 λ-矩阵左(右)乘 $A(\lambda)$。于是容易推出下列结论:

n 级 λ-矩阵可逆当且仅当它可以表示成一系列初等 λ-矩阵的乘积。

两个 n 级 λ-矩阵 $A(\lambda)$ 与 $B(\lambda)$ 相抵当且仅当存在可逆的 λ-矩阵 $P(\lambda)$ 和 $Q(\lambda)$,使得 $B(\lambda)=P(\lambda)A(\lambda)Q(\lambda)$。

7.3.2　典型例题

例 1　求 $f(x)$ 与 $g(x)$ 的首一最大公因式,并且把它表示成 $f(x)$ 与 $g(x)$ 的倍式和:

$$f(x)=x^4+3x-2,g(x)=3x^3-x^2-7x+4.$$

解

	$g(x)$	$3f(x)$	
$3x-4$	$3x^3-x^2-7x+4$	$3x^4\qquad+9x-6$	$x+\frac{1}{3}$
	$3x^3+3x^2-3x$	$3x^4-x^3-7x^2+4x$	
	$-4x^2-4x+4$	x^3+7x^2+5x-6	
	$-4x^2-4x+4$	$x^3-\frac{1}{3}x^2-\frac{7}{3}x+\frac{4}{3}$	
	0		
		$r_1(x)=\frac{22}{3}x^2+\frac{22}{3}x-\frac{22}{3}$	
		$\frac{3}{22}r_1(x)=x^2+x-1$	

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

由于

$$3f(x)=\left(x+\frac{1}{3}\right)g(x)+r_1(x),$$

$$g(x)=(3x-4)\left[\frac{3}{22}r_1(x)\right]+0,$$

因此

$$\begin{aligned}(f(x),g(x))&=\frac{3}{22}r_1(x)=\frac{3}{22}\left[3f(x)-\left(x+\frac{1}{3}\right)g(x)\right]\\&=\frac{9}{22}f(x)-\left(\frac{3}{22}x+\frac{1}{22}\right)g(x).\end{aligned}$$

例 2　证明:在 $K[x]$ 中,如果 $f(x)$ 与 $g(x)$ 不全为 0,那么

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

证明 设 $f(x)=f_1(x)(f(x),g(x)),g(x)=g_1(x)(f(x),g(x))$.

据定理 1,存在 $u(x),v(x)\in K[x]$,使得

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

即 $u(x)f_1(x)(f(x),g(x))+v(x)g_1(x)(f(x),g(x))=(f(x),g(x))$.

由消去律,得

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

因此 $(f_1(x),g_1(x))=1$. ■

例 3 设 $f(x),g(x)\in K[x],a,b,c,d\in K$,使得 $ad-bc\neq 0$。证明:

$$(af(x)+bg(x),cf(x)+dg(x))=(f(x),g(x)).$$

证明 若 $c(x)\mid f(x)$且 $c(x)\mid g(x)$,则

$$c(x)\mid af(x)+bg(x),c(x)\mid cf(x)+dg(x).$$

设 $p(x)=af(x)+bg(x),q(x)=cf(x)+dg(x)$,

由于 $ad-bc\neq 0$,因此可解得

$$f(x)=\frac{d}{ad-bc}p(x)-\frac{b}{ad-bc}q(x),$$

$$g(x)=-\frac{c}{ad-bc}p(x)+\frac{a}{ad-bc}q(x).$$

若 $h(x)\mid p(x)$且 $h(x)\mid q(x)$,则 $h(x)\mid f(x)$且 $h(x)\mid g(x)$。

因此 $\{p(x)$与 $q(x)$的公因式$\}=\{f(x)$与 $g(x)$的公因式$\}$.

由此得出,$(af(x)+bg(x),cf(x)+dg(x))=(f(x),g(x))$。 ■

例 4 证明:在 $K[x]$中,如果$(f,g)=1$,那么

(1) $(f,f+g)=1,(g,f+g)=1$;

(2) $(fg,f+g)=1$。

证明 (1) 据例 3 的结论得

$$(f,f+g)=(1f+0g,1f+1g)=(f,g)=1,$$

$$(g,f+g)=(0f+1g,1f+1g)=(f,g)=1.$$

(2) 由第(1)小题结论和性质 3 立即得到

$$(fg,f+g)=1.$$ ■

例 5 证明:在 $K[x]$中,如果$(f(x),g(x))=1$,那么对任意正整数 m,有

$$(f(x^m),g(x^m))=1.$$

证明 由于$(f(x),g(x))=1$,因此存在 $u(x),v(x)\in K[x]$,使得

$$u(x)f(x)+v(x)g(x)=1. \tag{11}$$

由于 $K[x]$可看成是 K 的一个扩环,因此不定元 x 可用 x^m 代入,从(11)式得

$$u(x^m)f(x^m)+v(x^m)g(x^m)=1. \tag{12}$$

由于 $u(x^m),v(x^m)\in K[x]$,因此由(12)式得

$$(f(x^m),g(x^m))=1. \quad \blacksquare$$

点评 在例 5 中,运用一元多项式环 $K[x]$的通用性质很容易地证明了$(f(x^m),g(x^m))=1$,并且把道理讲清楚了。如果没有讲一元多项式环的通用性质,那么例 5 的证明或者比较繁琐,或者没有把(11)式中用 x^m 代替 x 的道理讲清楚。

例 6 设 $A\in M_n(K),f(x),g(x)\in K[x]$。证明:如果 $d(x)$是 $f(x)$与 $g(x)$的一个最大公因式,那么齐次线性方程组 $d(A)\boldsymbol{X}=\boldsymbol{0}$ 的解空间 W_3 等于 $f(A)\boldsymbol{X}=\boldsymbol{0}$ 的解空间 W_1 与 $g(A)\boldsymbol{X}=\boldsymbol{0}$ 的解空间 W_2 的交。

证明 由定理 1,存在 $u(x),v(x)\in K[x]$,使得

$$d(x)=u(x)f(x)+v(x)g(x). \tag{13}$$

由于 $K[A]$可看成是 K 的一个扩环,因此 x 可用 A 代入,从(13)式得

$$d(A)=u(A)f(A)+v(A)g(A). \tag{14}$$

任取 $\boldsymbol{\eta}\in W_1\cap W_2$,则 $f(A)\boldsymbol{\eta}=\boldsymbol{0}$ 且 $g(A)\boldsymbol{\eta}=\boldsymbol{0}$。于是

$$d(A)\boldsymbol{\eta}=u(A)f(A)\boldsymbol{\eta}+v(A)g(A)\boldsymbol{\eta}=\boldsymbol{0}.$$

因此 $\boldsymbol{\eta}\in W_3$,从而 $W_1\cap W_2\subseteq W_3$。

设 $$f(x)=f_1(x)d(x),g(x)=g_1(x)d(x),$$

则 x 用 A 代入,从上面两式得,

$$f(A)=f_1(A)d(A),g(A)=g_1(A)d(A).$$

任取 $\boldsymbol{\delta}\in W_3$,则 $d(A)\boldsymbol{\delta}=\boldsymbol{0}$,从而

$$f(A)\boldsymbol{\delta}=f_1(A)d(A)\boldsymbol{\delta}=\boldsymbol{0},g(A)\boldsymbol{\delta}=g_1(A)d(A)\boldsymbol{\delta}=\boldsymbol{0}.$$

因此 $\boldsymbol{\delta}\in W_1\cap W_2$,从而 $W_3\subseteq W_1\cap W_2$。

综上所述得, $$W_3=W_1\cap W_2. \quad \blacksquare$$

例 7 设 $A\in M_n(K),f_1(x),f_2(x)\in K[x]$,记 $f(x)=f_1(x)f_2(x)$。证明:如果 $(f_1(x),f_2(x))=1$,那么 $f(A)\boldsymbol{X}=\boldsymbol{0}$ 的任一个解可以唯一地表示成 $f_1(A)\boldsymbol{X}=\boldsymbol{0}$ 的一个解与 $f_2(A)\boldsymbol{X}=\boldsymbol{0}$ 的一个解的和。

证明 可表性。由于$(f_1(x),f_2(x))=1$,因此存在 $u(x),v(x)\in K[x]$,使得

$$u(x)f_1(x)+v(x)f_2(x)=1. \tag{15}$$

不定元 x 用 A 代入,从(15)式得

$$u(A)f_1(A)+v(A)f_2(A)=I. \tag{16}$$

任取 $f(A)\boldsymbol{X}=\boldsymbol{0}$ 的一个解 $\boldsymbol{\eta}$，则 $f(A)\boldsymbol{\eta}=\boldsymbol{0}$，从(16)式得

$$\boldsymbol{\eta}=I\boldsymbol{\eta}=u(A)f_1(A)\boldsymbol{\eta}+v(A)f_2(A)\boldsymbol{\eta}.$$

记 $\boldsymbol{\eta}_1=v(A)f_2(A)\boldsymbol{\eta}$，$\boldsymbol{\eta}_2=u(A)f_1(A)\boldsymbol{\eta}$，则 $\boldsymbol{\eta}=\boldsymbol{\eta}_2+\boldsymbol{\eta}_1$。

由于 $f(x)=f_1(x)f_2(x)$，因此 $f(A)=f_1(A)f_2(A)$，从而

$$\begin{aligned}f_1(A)\boldsymbol{\eta}_1&=f_1(A)v(A)f_2(A)\boldsymbol{\eta}\\&=v(A)f_1(A)f_2(A)\boldsymbol{\eta}\\&=v(A)f(A)\boldsymbol{\eta}\\&=v(A)\boldsymbol{0}\\&=\boldsymbol{0},\\f_2(A)\boldsymbol{\eta}_2&=f_2(A)u(A)f_1(A)\boldsymbol{\eta}\\&=u(A)f(A)\boldsymbol{\eta}\\&=\boldsymbol{0}.\end{aligned}$$

因此 $\boldsymbol{\eta}_1,\boldsymbol{\eta}_2$ 分别是 $f_1(A)\boldsymbol{X}=\boldsymbol{0}$，$f_2(A)\boldsymbol{X}=\boldsymbol{0}$的一个解。

唯一性。任取 $f(A)\boldsymbol{X}=\boldsymbol{0}$ 的一个解 $\boldsymbol{\eta}$，设

$$\boldsymbol{\eta}=\boldsymbol{\eta}_1+\boldsymbol{\eta}_2,\boldsymbol{\eta}=\boldsymbol{\delta}_1+\boldsymbol{\delta}_2,$$

其中 $\boldsymbol{\eta}_i,\boldsymbol{\delta}_i$ 是 $f_i(A)\boldsymbol{X}=\boldsymbol{0}$ 的解，$i=1,2$，则

$$\boldsymbol{\eta}_1-\boldsymbol{\delta}_1=\boldsymbol{\delta}_2-\boldsymbol{\eta}_2.$$

用 W_i 表示 $f_i(A)\boldsymbol{X}=\boldsymbol{0}$ 的解空间，$i=1,2$，则 $\boldsymbol{\eta}_1-\boldsymbol{\delta}_1\in W_1\cap W_2$。

由于$(f_1(x),f_2(x))=1$，因此用例 6 的结论得，$I\boldsymbol{X}=\boldsymbol{0}$ 的解空间 $W_3=W_1\cap W_2$。显然 $W_3=\{\boldsymbol{0}\}$。因此 $W_1\cap W_2=\{\boldsymbol{0}\}$。从而 $\boldsymbol{\eta}_1-\boldsymbol{\delta}_1=\boldsymbol{0}$，即 $\boldsymbol{\eta}_1=\boldsymbol{\delta}_1$。于是 $\boldsymbol{\eta}_2=\boldsymbol{\delta}_2$。 ■

点评 从例 6 和例 7 的证明中看到：运用一元多项式环 $K[x]$的通用性质，把 x 用矩阵 A 代入，从 $K[x]$中关于最大公因式的等式和关于互素的多项式的等式，便得到关于矩阵 A 的多项式的等式，而这些等式在证明中起了关键作用。例如，在例 7 中，把 $f(A)\boldsymbol{X}=\boldsymbol{0}$ 的一个解 $\boldsymbol{\eta}$ 表示成 $f_1(A)\boldsymbol{X}=\boldsymbol{0}$ 的一个解 $\boldsymbol{\eta}_1$ 与 $f_2(A)\boldsymbol{X}=\boldsymbol{0}$ 的一个解 $\boldsymbol{\eta}_2$ 的和，等式(16)起了关键作用。

例 8 证明：在 $K[x]$中，如果$(f(x),g(x))=1$，并且 $\deg f(x)>0$，$\deg g(x)>0$，那么在 $K[x]$中存在唯一的一对多项式 $u(x),v(x)$，使得

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

且 $\deg u(x)<\deg g(x)$，$\deg v(x)<\deg f(x)$。

证明 由于$(f(x),g(x))=1$，因此存在 $p(x),q(x)\in K[x]$，使得

$$p(x)f(x)+q(x)g(x)=1. \tag{17}$$

用 $g(x)$去除 $p(x)$，有 $h(x),r(x)\in K[x]$，使得

$$p(x)=h(x)g(x)+r(x),\deg r(x)<\deg g(x). \tag{18}$$

把(18)式代入(17)式,得

$$r(x)f(x)+[h(x)f(x)+q(x)]g(x)=1. \tag{19}$$

令 $u(x)=r(x)$,$v(x)=h(x)f(x)+q(x)$,则(19)式成为

$$u(x)f(x)+v(x)g(x)=1, \tag{20}$$

其中 $\deg u(x)=\deg r(x)<\deg g(x)$。由于 $\deg g(x)>0$,因此从(20)式看出 $u(x)\neq 0$。

假如 $\deg v(x)\geqslant\deg f(x)$,则

$$\begin{aligned}\deg[v(x)g(x)]&=\deg v(x)+\deg g(x)\geqslant\deg f(x)+\deg g(x)\\&>\deg f(x)+\deg u(x)=\deg[u(x)f(x)].\end{aligned}$$

从而

$$\begin{aligned}\deg[u(x)f(x)+v(x)g(x)]&=\deg[v(x)g(x)]\\&\geqslant\deg f(x)+\deg g(x)>0.\end{aligned}$$

这与(20)式矛盾,因此 $\deg v(x)<\deg f(x)$。存在性得证。

唯一性。假设 $K[x]$ 中还有一对多项式 $u_1(x)$,$v_1(x)$,使得

$$u_1(x)f(x)+v_1(x)g(x)=1,$$

且 $\deg u_1(x)<\deg g(x)$,$\deg v_1(x)<\deg f(x)$,则

$$[u_1(x)-u(x)]f(x)=[v(x)-v_1(x)]g(x). \tag{21}$$

由于 $(f(x),g(x))=1$,因此从(21)式得

$$g(x)\mid[u_1(x)-u(x)].$$

假如 $u_1(x)-u(x)\neq 0$,则 $\deg g(x)\leqslant\deg[u_1(x)-u(x)]<\deg g(x)$。矛盾,因此 $u_1(x)-u(x)=0$,从而 $v(x)-v_1(x)=0$。即

$$u(x)=u_1(x),v(x)=v_1(x). \qquad \blacksquare$$

例 9 设 $m,n\in\mathbf{N}^*$,证明:在 $K[x]$ 中,

$$(x^m-1,x^n-1)=x^{(m,n)}-1. \tag{22}$$

证明 当 $m=n$ 时,$(m,n)=m$,显然有

$$(x^m-1,x^m-1)=x^m-1.$$

下面设 $m>n$,对幂指数 m 和 n 的最大值作第二数学归纳法。

当 $\max\{m,n\}=2$ 时,$m=2,n=1$,$(m,n)=1$。

显然有 $(x^2-1,x-1)=x-1$.

假设幂指数的最大值小于 m 时,命题为真,现在来看 $\max\{m,n\}=m$ 的情形。

$$\begin{aligned}(x^m-1,x^n-1)&=(x^m-x^{m-n}+x^{m-n}-1,x^n-1)\\&=(x^{m-n}(x^n-1)+x^{m-n}-1,x^n-1).\end{aligned}$$

由于 $\{x^{m-n}(x^n-1)+x^{m-n}-1$ 与 x^n-1 的公因式$\}$

$=\{x^n-1$ 与 $x^{m-n}-1$ 的公因式$\}$,

因此 $(x^{m-n}(x^n-1)+x^{m-n}-1,x^n-1)=(x^n-1,x^{m-n}-1)$.

由于 $\max\{n,m-n\}<m$,且$(n,m-n)=(m,n)$,因此据归纳假设得

$$(x^n-1,x^{m-n}-1)=x^{(n,m-n)}-1=x^{(m,n)}-1.$$

从而 $$(x^m-1,x^n-1)=x^{(m,n)}-1.$$

据数学归纳法原理,对一切正整数 m,n,命题为真。 ■

例 10 给定一个正整数 m,对于 $a,b\in\mathbf{Z}$,如果 m 能整除 $a-b$,那么称 a 与 b **模 m 同余**,记作

$$a\equiv b \pmod m.$$

设 $a_i,b_i\in\mathbf{Z},i=1,2$。证明:如果 $a_i\equiv b_i \pmod m,i=1,2$,那么

$$a_1+a_2\equiv b_1+b_2 \pmod m,a_1a_2\equiv b_1b_2 \pmod m.$$

证明 由已知条件得,$m\mid a_i-b_i,i=1,2$。由于

$$(a_1+a_2)-(b_1+b_2)=(a_1-b_1)+(a_2-b_2),$$

因此 $m\mid(a_1+a_2)-(b_1+b_2)$,从而 $a_1+a_2\equiv b_1+b_2 \pmod m$。

$$\begin{aligned}a_1a_2-b_1b_2&=a_1a_2-b_1a_2+b_1a_2-b_1b_2\\&=(a_1-b_1)a_2+b_1(a_2-b_2).\end{aligned}$$

于是 $m\mid a_1a_2-b_1b_2$。因此 $a_1a_2\equiv b_1b_2 \pmod m$。 ■

例 11 设 $a,n\in\mathbf{N}^*$,且 $a\geqslant 2$,证明:

$$(a^n+a^{n-1}+\cdots+a+1,a-1)=(n+1,a-1). \tag{23}$$

证明

$$\begin{aligned}&a^n+a^{n-1}+\cdots+a+1\\&=(a-1+1)^n+(a-1+1)^{n-1}+\cdots+(a-1+1)+1\\&\equiv n+1 \pmod{a-1}.\end{aligned}$$

因此 $$a-1\mid(a^n+a^{n-1}+\cdots+a+1)-(n+1).$$

从而 $$a^n+a^{n-1}+\cdots+a+1=l(a-1)+(n+1),$$

其中 l 是某个整数,根据整数环中类似于 7.3.1 节引理的结论,得

$$(a^n+a^{n-1}+\cdots+a+1,a-1)=(a-1,n+1).$$ ■

例 12 设 $a,n\in\mathbf{N}^*$,且 $a\geqslant 2,n\geqslant 2$。令

$$M=a^{n-2}+a^{n-3}+\cdots+a+1,$$

证明: $$(a^n-1,M)=(a-1,n-1). \tag{24}$$

证明 据例 11 的结论,得

$$(M,a-1)=(n-1,a-1).$$

由于

$$\begin{aligned} a^n-1&=(a-1)(a^{n-1}+a^{n-2}+\cdots+a+1)\\ &=(a-1)(a^{n-1}+M)\\ &=(a-1)a^{n-1}+(a-1)M. \end{aligned}$$

因此，若 c 是 $a-1$ 与 M 的公因数，则 c 也是 a^n-1 与 M 的公因数；反之，若 e 是 a^n-1 与 M 的公因数，则 $e|a^n-1$。从而 $a^n-1=be$，对于某个整数 b，即

$$aa^{n-1}-be=1.$$

因此 $(a^{n-1},e)=1$。由于 $e|(a-1)a^{n-1}$，因此 $e|a-1$。从而 e 是 $a-1$ 与 M 的公因数。所以

$$(a-1,M)=(a^n-1,M).$$

综上所述，得

$$(a^n-1,M)=(n-1,a-1).$$ ■

例 13 设 $f(x),g(x)\in K[x]$，$K[x]$ 中一个多项式 $m(x)$ 称为 $f(x)$ 与 $g(x)$ 的一个最小公倍式，如果

1° $f(x)|m(x),g(x)|m(x)$；

2° $f(x)|u(x),g(x)|u(x)\Rightarrow m(x)|u(x)$。

(1) 证明：$K[x]$ 中任意两个多项式都有最小公倍式，并且 $f(x)$ 与 $g(x)$ 的最小公倍式在相伴的意义下是唯一的；

(2) 用 $[f(x),g(x)]$ 表示首项系数是 1 的最小公倍式，证明：如果 $f(x),g(x)$ 的首项系数都是 1，那么

$$[f(x),g(x)]=\frac{f(x)g(x)}{(f(x),g(x))}.$$

证明 (1) 由于 0 的倍式只有 0，因此任一多项式 $f(x)$ 与 0 的最小公倍式是 0。

设 $f(x),g(x)$ 是 $K[x]$ 中全不为 0 的多项式，则

$$f(x)=f_1(x)(f(x),g(x)),g(x)=g_1(x)(f(x),g(x)).$$

令 $$m(x)=f_1(x)g_1(x)(f(x),g(x)),$$

则 $$f(x)|m(x),g(x)|m(x).$$

假设 $f(x)|u(x),g(x)|u(x)$，则存在 $p(x),q(x)\in K[x]$，使得

$$u(x)=p(x)f(x),u(x)=q(x)g(x).$$

从而 $$p(x)f(x)=q(x)g(x).$$

于是 $$p(x)f_1(x)(f(x),g(x))=q(x)g_1(x)(f(x),g(x)).$$

因此 $$p(x)f_1(x)=q(x)g_1(x).$$

由于 $(f_1(x),g_1(x))=1$，因此 $f_1(x)|q(x)$。

从而存在 $h(x)\in K[x]$，使得 $q(x)=h(x)f_1(x)$。

于是 $$u(x)=h(x)f_1(x)g(x)=h(x)m(x).$$

因此 $m(x)|u(x)$。从而 $m(x)$ 是 $f(x)$ 与 $g(x)$ 的最小公倍式。

设 $m_1(x),m_2(x)$ 都是 $f(x)$ 与 $g(x)$ 的最小公倍式，则

$$m_1(x)\mid m_2(x),m_2(x)\mid m_1(x).$$

因此 $$m_1(x)\sim m_2(x).$$

(2) 设 $f(x)$ 与 $g(x)$ 都是首项系数为 1 的多项式，则从第(1)小题的证明看出

$$\begin{aligned}[f(x),g(x)] &= f_1(x)g_1(x)(f(x)g(x))\\ &= \frac{f(x)g(x)}{(f(x),g(x))}.\end{aligned}$$

■

习题 7.3

1. 求 $f(x)$ 与 $g(x)$ 的首一最大公因式，并且把它表示成 $f(x)$ 与 $g(x)$ 的倍式和：

(1) $f(x)=x^4+3x^3-x^2-4x-3$，

$g(x)=3x^3+10x^2+2x-3$；

(2) $f(x)=x^4+6x^3-6x^2+6x-7$，

$g(x)=x^3+x^2-7x+5$。

2. 证明：在 $K[x]$ 中，如果 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的倍式和，并且 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个公因式，那么 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式。

3. 证明：在 $K[x]$ 中，$(f(x),g(x))h(x)$ 是 $f(x)h(x)$ 与 $g(x)h(x)$ 的一个最大公因式；特别地，若 $h(x)$ 的首项系数为 1，则

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

4. 证明：在 $K[x]$ 中，如果 $f(x),g(x)$ 不全为零，并且

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

那么 $$(u(x),v(x))=1.$$

5. 设 $f_i(x),g_j(x)\in K[x]$，$i=1,2,\cdots,s;j=1,2,\cdots,m$。证明：如果 $(f_i(x),g_j(x))=1$，$i=1,2,\cdots,s;j=1,2,\cdots,m$，那么

$$(f_1(x)f_2(x)\cdots f_s(x),g_1(x)g_2(x)\cdots g_m(x))=1.$$

6. 证明：在 $K[x]$ 中两个非零多项式 $f(x)$ 与 $g(x)$ 不互素的充分必要条件是，存在两个非零多项式 $u(x),v(x)$，使得 $u(x)f(x)=v(x)g(x)$，$\deg u(x)<\deg g(x)$，$\deg v(x)<\deg f(x)$。

7. 证明：在 $K[x]$ 中，设 $f(x)$ 与 $g(x)$ 不全为零。如果 $f(x)|h(x)$，$g(x)|h(x)$，那么

$$f(x)g(x) \mid h(x)(f(x),g(x)).$$

8. 在 $K[x]$ 中，给定一个多项式 $h(x)$，对于 $f(x)$，$g(x)\in K[x]$，如果 $h(x)|f(x)-g(x)$，那么称 $f(x)$ 与 $g(x)$ 模 $h(x)$ **同余**，记作 $f(x)\equiv g(x) \pmod{h(x)}$。设 $f_i(x)$，$g_1(x)\in K[x]$，$i=1,2$。证明：如果

$$f_i(x) \equiv g_i(x) \pmod{h(x)}, i = 1,2,$$

那么

$$f_1(x)+f_2(x)\equiv g_1(x)+g_2(x) \pmod{h(x)},$$

$$f_1(x)f_2(x)\equiv g_1(x)g_2(x) \pmod{h(x)}.$$

9. 在 $K[x]$ 中，设 $f_1(x)$，$f_2(x)$，$\cdots$，$f_s(x)$ 两两互素，任意给定 $r_1(x)$，$r_2(x)$，$\cdots$，$r_s(x)\in K[x]$，则同余方程组

$$\begin{cases} g(x) \equiv r_1(x) \pmod{f_1(x)} \\ g(x) \equiv r_2(x) \pmod{f_2(x)} \\ \cdots \\ g(x) \equiv r_s(x) \pmod{f_s(x)} \end{cases}$$

在 $K[x]$ 中必有解，并且如果 $c(x)$ 和 $d(x)$ 都是这个同余方程组的解，那么

$$c(x) \equiv d(x) \pmod{f_1(x)f_2(x)\cdots f_s(x)}.$$

* 10. 求下述 λ-矩阵的行列式因子和不变因子：

(1) $A(\lambda)=\begin{pmatrix} \lambda-2 & 0 & 0 \\ 0 & \lambda-2 & -1 \\ 0 & 0 & \lambda-2 \end{pmatrix}$；

(2) $B(\lambda)=\begin{pmatrix} \lambda-1 & 0 & 0 \\ 0 & \lambda-5 & -1 \\ 0 & 0 & \lambda-5 \end{pmatrix}$。

11. 在 $K[x]$ 中，设 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式，证明：在 $K[x]$ 中存在唯一的一对多项式 $u(x)$，$v(x)$ 使得

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

其中，$\deg u(x)<\deg g(x)-\deg d(x)$，$\deg v(x)<\deg f(x)-\deg d(x)$。

7.4 不可约多项式,唯一因式分解定理

7.4.1 内容精华

本节要利用最大公因式和互素的知识揭示数域 K 上一元多项式环 $K[x]$的结构。

从直觉判断,一个多项式,如果它的因式最少,那么它是最简单的多项式,从而它在研究 $K[x]$的结构中将起基本建筑块的作用。由于 $K[x]$中零次多项式是任一多项式的因式,又 $f(x)$的相伴元是 $f(x)$的因式,因此因式最少的多项式应当是因式只有零次多项式和相伴元这样的多项式,即下面要研究的不可约多项式。

一、不可约多项式

定义 1 $K[x]$中一个次数大于 0 的多项式 $f(x)$,如果它在 $K[x]$中的因式只有零次多项式和 $f(x)$的相伴元,那么称 $f(x)$是数域 K 上的一个**不可约多项式**;否则称 $f(x)$是**可约的**。

不可约多项式在研究数域 K 上一元多项式环 $K[x]$的结构中起着基本建筑块的作用。

定理 1 设 $p(x)$是 $K[x]$中一个次数大于 0 的多项式,则下列命题等价:

(1)$p(x)$是不可约多项式;

(2)$\forall f(x)\in K[x]$,有 $p(x)\mid f(x)$或$(p(x),f(x))=1$;

(3)在 $K[x]$中,从 $p(x)\mid f(x)g(x)$可推出

$$p(x)\mid f(x) \text{ 或 } p(x)\mid g(x);$$

(4)$p(x)$不能分解成两个次数较 $p(x)$的次数低的多项式的乘积。

上述是分别从因式的角度,从与任一多项式的关系的角度,从整除关系的角度,以及从因式分解的角度对不可约多项式的刻画。

从上述的命题(3)与不可约多项式的定义等价,运用数学归纳法可证得:在 $K[x]$中,如果 $p(x)$不可约,且

$$p(x)\mid f_1(x)f_2(x)\cdots f_s(x),$$

那么 $p(x)\mid f_j(x)$,对于某个 $j\in\{1,2,\cdots,s\}$。

从上述的命题(4)与不可约多项式的定义等价,立即得出,$K[x]$中一次多项式都是不可约的。

二、唯一因式分解定理

从不可约多项式的等价条件(4)猜测有下述定理 2,它揭示了数域 K 上一元多项式环 $K[x]$的结构。

定理 2(唯一因式分解定理) $K[x]$中任一次数大于 0 的多项式 $f(x)$能够唯一地分解成数域 K 上有限多个不可约多项式的乘积。所谓唯一性是指,如果 $f(x)$有两个这样的分解式:

$$f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)\cdots q_t(x), \tag{1}$$

那么一定有 $s=t$,且适当排列因式的次序后有

$$p_i(x) \sim q_i(x), i = 1,2,\cdots,s.$$

从唯一性的证明中可以看出,$f(x)$的任一不可约因式一定与 $f(x)$的分解式中某一个不可约因式相伴,因此 $f(x)$的分解式给出了它的全部不可约因式(在相伴意义下)。

研究 $K[x]$的结构的途径如图 7-1 所示。

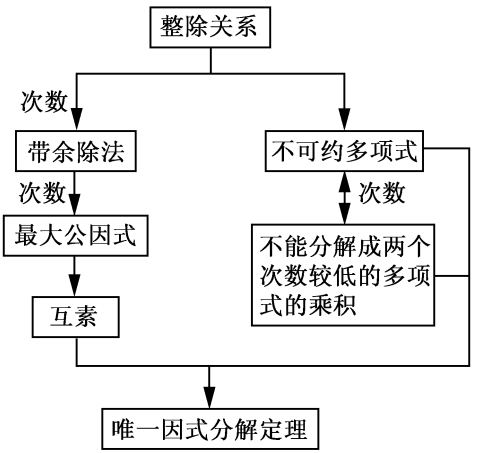

图 7-1

$K[x]$中次数大于 0 的多项式 $f(x)$的标准分解式为

$$f(x) = ap_1^{l_1}(x)p_2^{l_2}(x)\cdots p_s^{l_s}(x), \tag{2}$$

其中 a 是 $f(x)$的首项系数,$p_1(x),p_2(x),\cdots,p_s(x)$是 K 上两两不等的首一不可约多项式,$l_i>0,i=1,2,\cdots,s$。$f(x)$的标准分解式是 $K[x]$中有关乘法的第四个重要等式,它有许多用处。

如果知道 $K[x]$中两个次数大于 0 的多项式 $f(x),g(x)$的标准分解式:

$$f(x) = ap_1^{l_1}(x)p_2^{l_2}(x)\cdots p_s^{l_s}(x),$$

$$g(x) = bp_1^{r_1}(x)p_2^{r_2}(x)\cdots p_m^{r_m}(x)q_1^{t_1}(x)\cdots q_n^{t_n}(x), m \leqslant s,$$

那么

$$(f(x),g(x)) = p_1^{\min\{l_1,r_1\}}(x)\cdots p_m^{\min\{l_m,r_m\}}(x); \tag{3}$$

$$[f(x),g(x)] = p_1^{\max\{l_1,r_1\}}(x)\cdots p_m^{\max\{l_m,r_m\}}(x)p_{m+1}^{l_{m+1}}(x)\cdots p_s^{l_s}(x)q_1^{t_1}(x)\cdots q_n^{t_n}(x). \tag{4}$$

在整数环 **Z** 中也有唯一因子分解定理，下面列举出有关概念和结论。证明留给读者。

定义 2　一个大于 1 的整数 m，如果它的正因数只有 1 和它自身，那么称 m 是一个**素数**；否则称 m 是**合数**。

素数在整数环 **Z** 的结构中起着基本建筑块的作用。

定理 3　设 p 是大于 1 的整数，则下列命题等价：

(1) p 是素数；

(2) 对任意整数 a，都有 $p\mid a$ 或 $(p,a)=1$；

(3) 在 **Z** 中，从 $p\mid ab$ 可推出 $p\mid a$ 或 $p\mid b$；

(4) p 不能分解成两个较小的正整数的乘积。

素数的等价条件(3)可推广为：若素数 p 能整除一些整数 $a_1,a_2,\cdots,a_s$ 的乘积，则 p 能整除其中的一个。

定理 4(算术基本定理)　任一大于 1 的整数 a 都能唯一地分解成有限多个素数的乘积。所谓唯一性是指，如果 a 有两个这样的分解式：

$$a = p_1p_2\cdots p_s = q_1q_2\cdots q_t,$$

那么 $s=t$，且适当排列因数的次序后，有

$$p_i = q_i, i = 1,2,\cdots,s.$$

算术基本定理揭示了整数环 **Z** 的结构。

任一大于 1 的整数 a 的标准分解式为：

$$a = p_1^{r_1}p_2^{r_2}\cdots p_m^{r_m},$$

其中 $p_1,p_2,\cdots,p_m$ 是两两不等的素数，r_i 是正整数，$i=1,2,\cdots,m$。

在 **Z** 中，设

$$a = p_1^{r_1}p_2^{r_2}\cdots p_t^{r_t}p_{t+1}^{r_{t+1}}\cdots p_m^{r_m},$$
$$b = p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}q_{t+1}^{k_{t+1}}\cdots q_s^{k_s},$$

则

$$(a,b) = p_1^{\min\{r_1,k_1\}}p_2^{\min\{r_2,k_2\}}\cdots p_t^{\min\{r_t,k_t\}},$$
$$[a,b] = p_1^{\max\{r_1,k_1\}}p_2^{\max\{r_2,k_2\}}\cdots p_t^{\max\{r_t,k_t\}}p_{t+1}^{r_{t+1}}\cdots p_m^{r_m}q_{t+1}^{k_{t+1}}\cdots q_s^{k_s}.$$

7.4.2　典型例题

例 1　设 $f(x)\in K[x]$，且 $\deg f(x)>0$。证明下列命题等价：

(1) $f(x)$与 $K[x]$中某一个不可约多项式的方幂相伴；

(2) $\forall g(x)\in K[x]$,有$(f(x),g(x))=1$,或者 $f(x)\mid g^m(x)$对于某一个正整数 m；

(3) $\forall g(x),h(x)\in K[x]$,从 $f(x)\mid g(x)h(x)$可以推出 $f(x)\mid g(x)$或者 $f(x)\mid h^m(x)$对于某一个正整数 m。

证明 (1) ⇒(2) 设 $f(x)\sim p^l(x)$,其中 $p(x)$不可约,$l\in\mathbf{N}^*$,则 $f(x)=ap^l(x)$,对某个 $a\in K^*$。任取 $g(x)\in K[x]$,有$(p(x),g(x))=1$ 或 $p(x)\mid g(x)$,于是$(p^l(x),g(x))=1$ 或 $p^l(x)\mid g^l(x)$。从而$(f(x),g(x))=1$ 或 $f(x)\mid g^l(x)$。

(2)⇒(3) 设 $f(x)\mid g(x)h(x)$,如果 $\forall m\in\mathbf{N}^*$ 都有 $f(x)\nmid h^m(x)$,那么据命题(2)得,$(f(x),h(x))=1$。从而 $f(x)\mid g(x)$。

(3)⇒(1) 假如 $f(x)$不与某一个不可约多项式的方幂相伴,则 $f(x)$的标准分解式为

$$f(x)=ap_1^{l_1}(x)p_2^{l_2}(x)\cdots p_s^{l_s}(x),$$

其中 $s\geqslant 2$。取 $g(x)=ap_1^{l_1}(x)$,$h(x)=p_2^{l_2}(x)\cdots p_s^{l_s}(x)$,则 $f(x)=g(x)h(x)$。从而 $f(x)\mid g(x)h(x)$。据命题(3)得,$f(x)\mid g(x)$或者 $f(x)\mid h^m(x)$对于某一个正整数 m,从而

$$\deg f(x)\leqslant \deg g(x) \text{ 或 } p_1(x)\mid p_2^{l_2m}(x)\cdots p_s^{l_sm}(x).$$

前者是不可能的。后者推出 $p_1(x)\mid p_j(x)$对某个 $j\in\{2,\cdots,s\}$。由于 $p_j(x)$不可约,因此$p_1(x)\sim p_j(x)$。由于它们的首项系数都为 1,因此 $p_1(x)=p_j(x)$。矛盾,所以 $f(x)=ap_1^{l_1}(x)$,即 $f(x)$与某一个不可约多项式的方幂相伴。 ■

例 2 在 $K[x]$中,设$(f,g_i)=1,i=1,2$,证明:

$$(fg_1,g_2)=(g_1,g_2).$$

证法一 设 $g_1(x),g_2(x)$的标准分解式为

$$g_1(x)=b_1q_1^{r_1}(x)\cdots q_m^{r_m}(x)q_{m+1}^{r_{m+1}}(x)\cdots q_t^{r_t}(x),$$
$$g_2(x)=b_2q_1^{k_1}(x)\cdots q_m^{k_m}(x)u_1^{e_1}(x)\cdots u_n^{e_n}(x).$$

由于$(f,g_i)=1,i=1,2$,因此 $f(x)$的标准分解式为

$$f(x)=ap_1^{l_1}(x)p_2^{l_2}(x)\cdots p_s^{l_s}(x).$$

其中 $p_i(x)(i=1,2,\cdots,s)$在 $g_1(x),g_2(x)$的标准分解式中不出现。

于是

$$(fg_1,g_2)=q_1^{\min\{r_1,k_1\}}(x)\cdots q_m^{\min\{r_m,k_m\}}=(g_1,g_2).$$ ■

证法二 显然,若 $c_1(x)\mid g_1(x)$且 $c_1(x)\mid g_2(x)$,则 $c_1(x)\mid f(x)g_1(x)$且 $c_1(x)\mid g_2(x)$。

反之,若 $c_2(x)\mid f(x)g_1(x)$且 $c_2(x)\mid g_2(x)$,由于$(f,g_i)=1,i=1,2$,因此$(f,g_1g_2)=1$。于是存在 $u(x),v(x)\in K[x]$,使得 $u(x)f(x)+v(x)g_1(x)g_2(x)=1$。从而

$$u(x)f(x)g_1(x)+v(x)g_1^2(x)g_2(x)=g_1(x).$$

因此 $c_2(x)\mid g_1(x)$。由上述推出,$(fg_1,g_2)=(g_1,g_2)$。 ■

例 3　设 $f(x),g(x)\in K[x]$，其中 $g(x)=kx+b,k\neq 0$。证明：对任意给定的正整数 m，有

$$g(x)\mid f^m(x)\quad\Leftrightarrow\quad g(x)\mid f(x).$$

证明　充分性是显然的。下面证必要性。由于一次多项式 $g(x)=kx+b,k\neq 0$ 是不可约的，因此从 $g(x)\mid f^m(x)$ 可推出 $g(x)\mid f(x)$。 ■

点评　从证明过程看出，只要 $g(x)$ 是 K 上不可约多项式，就有 $g(x)\mid f^m(x)\Leftrightarrow g(x)\mid f(x)$。

例 4　在 $K[\lambda]$ 中，设 $f(\lambda)=\lambda^n+a_{n-1}\lambda^{n-1}+\cdots+a_1\lambda+a_0$。令

$$A=\begin{pmatrix}0&0&\cdots&0&0&-a_0\\1&0&\cdots&0&0&-a_1\\0&1&\cdots&0&0&-a_2\\\vdots&\vdots&&\vdots&\vdots&\vdots\\0&0&\cdots&1&0&-a_{n-2}\\0&0&\cdots&0&1&-a_{n-1}\end{pmatrix},$$

称 A 是 $f(\lambda)$ 的**友矩阵**。

(1) 求 $f(\lambda)$ 的友矩阵 A 的特征多项式；

*(2) 如果 $f(\lambda)$ 不可约，求 $f(\lambda)$ 的友矩阵 A 的特征矩阵 $\lambda I-A$ 的行列式因子和不变因子，以及相抵标准形。

解　(1)

$$|\lambda I-A|=\begin{vmatrix}\lambda&0&\cdots&0&0&a_0\\-1&\lambda&\cdots&0&0&a_1\\\vdots&\vdots&&\vdots&\vdots&\vdots\\0&0&\cdots&-1&\lambda&a_{n-2}\\0&0&\cdots&0&-1&\lambda+a_{n-1}\end{vmatrix}.$$

按最后一行展开，然后对于 $(n,n-1)$ 元的余子式也按最后一行展开，依次下去，可得

$$\begin{aligned}|\lambda I-A|&=(\lambda+a_{n-1})\lambda^{n-1}+(-1)(-1)^{n+(n-1)}[a_{n-2}\lambda^{n-2}+\cdots]\\&=\lambda^n+a_{n-1}\lambda^{n-1}+a_{n-2}\lambda^{n-2}+\cdots+a_1\lambda+a_0.\end{aligned}$$

于是得出，$f(\lambda)$ 的友矩阵 A 的特征多项式等于 $f(\lambda)$。

(2) $f(\lambda)$ 的友矩阵 A 的特征矩阵 $\lambda I-A$ 的 n 阶行列式因子 $D_n(\lambda)=|\lambda I-A|=f(\lambda)$。由于 $D_{n-1}(\lambda)\mid D_n(\lambda)$，且 $f(\lambda)$ 不可约，因此 $D_{n-1}(\lambda)=1$ 或 $D_{n-1}(\lambda)=D_n(\lambda)$。由于 $\lambda I-A$ 的 $n-1$ 阶子式至多是 $n-1$ 次多项式，因此 $D_{n-1}(\lambda)$ 至多是 $n-1$ 次多项式，从而 $D_{n-1}(\lambda)\neq D_n(\lambda)$。于是 $D_{n-1}(\lambda)=1$，由此推出 $D_{n-2}(\lambda)=\cdots=D_1(\lambda)=1$。于是

$$d_1(\lambda)=d_2(\lambda)=\cdots=d_{n-1}(\lambda)=1,$$

$$d_n(\lambda)=\frac{D_n(\lambda)}{D_{n-1}(\lambda)}=f(\lambda).$$

因此,$\lambda I-A$ 的相抵标准形为

$$\mathrm{diag}\{1,\cdots,1,f(\lambda)\}.$$

* **例 5** 已知条件同例 4,如果 $f(\lambda)=p^3(\lambda)$,其中 $p(\lambda)$是 K 上首一不可约多项式,且 $n\geqslant 3$,求 $f(\lambda)$的友矩阵 A 的特征矩阵$\lambda I-A$ 的行列式因子和不变因子;并且求 $\lambda I-A$ 的相抵标准形。

解 $f(\lambda)$的友矩阵 A 的特征矩阵$\lambda I-A$ 的 n 阶行列式因子 $D_n(\lambda)=|\lambda I-A|=f(\lambda)=p^3(\lambda)$。由于 $D_{n-1}(\lambda)|D_n(\lambda)$,$\deg D_{n-1}(\lambda)\leqslant n-1$,且 $p(\lambda)$不可约,因此 $D_{n-1}(\lambda)$有且只有三种可能:$1,p(\lambda),p^2(\lambda)$。

情形 1 $D_{n-1}(\lambda)=1$。此时 $D_{n-2}(\lambda)=\cdots=D_1(\lambda)=1$。

从而 $d_1(\lambda)=d_2(\lambda)=\cdots=d_{n-1}(\lambda)=1$,$d_n(\lambda)=D_n(\lambda)=p^3(\lambda)$。此时 $\lambda I-A$ 的相抵标准形为

$$\mathrm{diag}\{1,\cdots,1,p^3(\lambda)\}.$$

情形 2 $D_{n-1}(\lambda)=p(\lambda)$,此时 $d_n(\lambda)=\dfrac{D_n(\lambda)}{D_{n-1}(\lambda)}=p^2(\lambda)$。

由于 $d_i(\lambda)|d_{i+1}(\lambda)$,$i=1,2,\cdots,n-1$,且

$$d_1(\lambda)d_2(\lambda)\cdots d_n(\lambda)=|\lambda I-A|=p^3(\lambda),$$

因此 $d_{n-1}(\lambda)=p(\lambda)$。从而 $d_{n-2}(\lambda)=\cdots=d_1(\lambda)=1$。

此时,$\lambda I-A$ 的相抵标准形为

$$\mathrm{diag}\{1,\cdots,1,p(\lambda),p^2(\lambda)\}.$$

$$D_{n-2}(\lambda)=\frac{D_{n-1}(\lambda)}{d_{n-1}(\lambda)}=1,D_{n-3}(\lambda)=\cdots=D_1(\lambda)=1.$$

情形 3 $D_{n-1}(\lambda)=p^2(\lambda)$,此时 $d_n(\lambda)=\dfrac{D_n(\lambda)}{D_{n-1}(\lambda)}=p(\lambda)$。

由于 $d_i(\lambda)|d_{i+1}(\lambda)$,$i=1,2,\cdots,n-1$,且

$$d_1(\lambda)d_2(\lambda)\cdots d_n(\lambda)=|\lambda I-A|=p^3(\lambda),$$

因此 $d_{n-1}(\lambda)=p(\lambda)$,$d_{n-2}(\lambda)=p(\lambda)$,$d_{n-3}(\lambda)=\cdots=d_1(\lambda)=1$,此时 $\lambda I-A$ 的相抵标准形为

$$\mathrm{diag}\{1,\cdots,1,p(\lambda),p(\lambda),p(\lambda)\}.$$

$$D_{n-2}(\lambda)=\frac{D_{n-1}(\lambda)}{d_{n-1}(\lambda)}=p(\lambda),D_{n-3}(\lambda)=\frac{D_{n-2}(\lambda)}{d_{n-2}(\lambda)}=1,$$

$$D_{n-4}(\lambda)=\cdots=D_1(\lambda)=1.$$

习题 7.4

1. 证明下列多项式在实数域和有理数域上都不可约：

(1) x^2+1；

(2) x^2+x+1。

2. 分别在复数域、实数域和有理数域上分解下列多项式为不可约因式的乘积：

(1) x^4+1；

(2) x^4+4。

3. 证明：在 $K[x]$ 中，$g^2(x)\mid f^2(x)$ 当且仅当 $g(x)\mid f(x)$。

4. 证明：在 $K[x]$ 中，对任意正整数 m 有

$$(f^m(x),g^m(x))=(f(x),g(x))^m.$$

5. 设 m 为正整数，

(1) 在 $\mathbf{R}[x]$ 中，x^4+m 是否可约？如果可约，请写出它的标准分解式；

(2) 在 $\mathbf{Q}[x]$ 中，求出 x^4+m 可约的充分必要条件；当 x^4+m 在 $\mathbf{Q}$ 上可约时，写出它的标准分解式。

*6. $K[\lambda]$ 中，$f(\lambda)=p^4(\lambda)$，其中 $p(\lambda)$ 是 K 上首一不可约多项式，$\deg f(\lambda)=n\geqslant 4$。$f(\lambda)$ 的友矩阵记作 A，求 $\lambda I-A$ 的行列式因子和不变因子，并且求 $\lambda I-A$ 的相抵标准形。

7.5 重 因 式

7.5.1 内容精华

唯一因式分解定理揭示了数域 K 上一元多项式环的结构：每一个次数大于 0 的多项式 $f(x)$ 都可以唯一地分解成有限多个不可约多项式的乘积。在 $f(x)$ 的标准分解式中，如果一个不可约因式 $p_j(x)$ 的幂指数为 l_j，那么自然可以把 $p_j(x)$ 叫做 $f(x)$ 的 l_j 重因式。此时 $p_j^{l_j}(x)\mid f(x)$，但是 $p_j^{l_j+1}(x)\nmid f(x)$。由此引出下述定义：

定义 1 $K[x]$ 中，不可约多项式 $p(x)$ 称为 $f(x)$ 的 **k 重因式**，如果 $p^k(x)\mid f(x)$，而 $p^{k+1}(x)\nmid f(x)$。

在上述定义中，如果 $k=0$，那么 $p(x)$ 不是 $f(x)$ 的因式；如果 $k=1$，那么称 $p(x)$ 是 $f(x)$ 的**单因式**；如果 $k>1$，那么称 $p(x)$ 是 $f(x)$ 的**重因式**。

显然，如果 $f(x)$ 的标准分解式为

$$f(x) = ap_1^{l_1}(x)p_2^{l_2}(x)\cdots p_s^{l_s}(x), \tag{1}$$

那么 $p_i(x)$ 是 $f(x)$ 的 l_i 重因式，$i=1,2,\cdots,s$。在(1)式中如果 $l_1=l_2=\cdots=l_s=1$，那么称 $f(x)$ 没有重因式。

如何判别一个多项式有没有重因式呢？由于没有一般的方法求一个多项式的标准分解式，因此我们必须寻找别的方法来判断一个多项式有没有重因式。下面先看一个简单的例子，以便从中受到启发。

设 $f(x)=(x+1)^3\in\mathbf{R}[x]$。显然 $f(x)$ 有重因式 $x+1$。如果把 $f(x)$ 看成多项式函数，那么对 $f(x)$ 可以求导数，得 $f'(x)=3(x+1)^2$。于是

$$(f(x),f'(x)) = (x+1)^2.$$

由此受到启发，有可能运用导数概念以及求最大公因式的方法来讨论一个多项式有没有重因式的问题。我们模仿实变量多项式函数的求导公式，对于任意数域 K 上的一元多项式给出导数的定义：

定义 2 对于 $K[x]$ 中的多项式

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

我们把多项式

$$n\,a_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

称为 $f(x)$ 的**导数**(或**一阶导数**)，记作 $f'(x)$。

$f'(x)$ 的导数叫做 $f(x)$ 的二阶导数，记作 $f''(x)$；$f''(x)$ 的导数叫做 $f(x)$ 的三阶导数，记作 $f'''(x)$，等等。$f(x)$ 的 k 阶导数记作 $f^{(k)}(x)$。

从定义 2 立即得出，一个 n 次多项式的导数是一个 $n-1$ 次多项式；它的 n 阶导数是 K 中一个非零数；它的 $n+1$ 阶导数是零多项式。零多项式的导数是零多项式。

根据定义 2，通过直接验证，得

$$[f(x)+g(x)]' = f'(x)+g'(x),$$
$$[c\,f(x)]' = c\,f'(x), c\in K,$$
$$[f(x)g(x)]' = f'(x)g(x)+f(x)g'(x),$$
$$[f^m(x)]' = m\,f^{m-1}(x)f'(x), m\in\mathbf{N}^*$$

从前面的例子，$f(x)=(x+1)^3$，$f'(x)=3(x+1)^2$，受到启发，猜测且可证明有下述结论：

定理 1 设 K 是数域，在 $K[x]$ 中，如果不可约多项式 $p(x)$ 是 $f(x)$ 的一个 $k(k\geqslant 1)$ 重因式，那么 $p(x)$ 是 $f'(x)$ 的一个 $k-1$ 重因式。特别地，$f(x)$ 的单因式不是 $f'(x)$ 的因式。

推论 1 设 K 是数域，在 $K[x]$ 中，不可约多项式 $p(x)$ 是 $f(x)$ 的一个重因式，当且仅当 $p(x)$ 是 $f(x)$ 与 $f'(x)$ 的一个公因式。

从推论 1 立即得到：

推论 2 设 K 是数域，在 $K[x]$中，次数大于 0 的多项式 $f(x)$有重因式当且仅当 $f(x)$与 $f'(x)$有次数大于 0 的公因式。 ■

从推论 2 立即得到：

推论 3 设 K 是数域，在 $K[x]$中，次数大于 0 的多项式 $f(x)$没有重因式当且仅当 $f(x)$与 $f'(x)$互素。 ■

推论 3 表明，判断数域 K 上一个次数大于 0 的多项式 $f(x)$有没有重因式，只要计算 $(f(x),f'(x))$，而求最大公因式有统一的方法——辗转相除法。所以我们有统一的方法——辗转相除法判断一个多项式有没有重因式。

由于在数域扩大时，两个多项式的互素性不改变，一个多项式的导数也不改变，因此从推论 3 立即得到：

推论 4 设数域 F 包含数域 K，对于 $K[x]$中次数大于 0 的多项式 $f(x)$，$f(x)$在 $K[x]$中没有重因式当且仅当 $f(x)$在 $F[x]$中没有重因式。即 $f(x)$有无重因式不会随数域的扩大而改变。 ■

一个多项式如果没有重因式，那么它的结构比较简单，便于研究它的性质。如果数域 K 上次数大于 0 的多项式 $f(x)$有重因式，我们可以想办法求出一个多项式 $g(x)$，它与 $f(x)$含有完全相同的不可约因式(不计重数)，但是 $g(x)$没有重因式。如何求这个多项式 $g(x)$呢？设

$$f(x) = ap_1^{l_1}(x)p_2^{l_2}(x)\cdots p_s^{l_s}(x),$$

其中 $p_1(x),p_2(x),\cdots,p_s(x)$是两两不等的首一不可约多项式。据定理 1 得

$$f'(x) = p_1^{l_1-1}(x)p_2^{l_2-1}(x)\cdots p_s^{l_s-1}(x)h(x),$$

其中 $h(x)$不能被任何 $p_i(x)$整除，$i=1,2,\cdots,s$。于是

$$(f(x),f'(x)) = p_1^{l_1-1}(x)p_2^{l_2-1}(x)\cdots p_s^{l_s-1}(x).$$

因此用 $(f(x),f'(x))$去除 $f(x)$所得商式是

$$a\,p_1(x)p_2(x)\cdots p_s(x),$$

这就是我们要求的 $g(x)$，它没有重因式，且与 $f(x)$含有完全相同的不可约因式(不计重数)。这表明去掉 $f(x)$的不可约因式的重数的方法是：先用辗转相除法求出 $f(x)$与 $f'(x)$的首一最大公因式 $(f(x),f'(x))$，然后对 $f(x)$与 $(f(x),f'(x))$作带余除法，所得商式 $g(x)$即为所求的没有重因式的多项式。

7.5.2 典型例题

例 1 判断下述有理系数多项式有无重因式。如果有重因式，试求出一个多项式与它有完全相同的不可约因式(不计重数)，且这个多项式没有重因式。

$$f(x) = x^3 + x^2 - 16x + 20.$$

解 $f'(x)=3x^2+2x-16$

用辗转相除法求出$(f(x),f'(x))=x-2$。因此 $f(x)$有重因式。

用$(f(x),f'(x))$去除 $f(x)$得商式为 $x^2+3x-10$,它没有重因式,且它与 $f(x)$有完全相同的不可约因式(不计重数)。

例 2 求例 1 中的多项式 $f(x)$在 $\mathbf{Q}[x]$中的标准分解式。

解 例 1 中已求出用 $x-2$ 去除 $f(x)$所得商式为 $x^2+3x-10$,余式为 0,因此

$$\begin{aligned} f(x) &= (x^2 + 3x - 10)(x - 2) \\ &= (x + 5)(x - 2)^2. \end{aligned}$$

例 3 设 K 是数域,在 $K(x)$中,$f(x)=x^3+ax+b$,求 $f(x)$有重因式的充分必要条件。

解 $f'(x)=3x^2+a$

设 $a\neq 0$,用辗转相除法求 $f(x)$与 $f'(x)$的最大公因式:

$h_2(x)=3x-\frac{9b}{2a}$	$f'(x)$ $3x^2 \quad +a$ $3x^2+\frac{9b}{2a}x$	$3f(x)$ $3x^3 \quad +3ax+3b$ $3x^3 \quad +ax$	$h_1(x)$ x
	$-\frac{9b}{2a}x+a$ $-\frac{9b}{2a}x-\frac{27b^2}{4a^2}$	$r_1(x)=2ax+3b$ $\frac{1}{2a}r_1(x)=x+\frac{3b}{2a}$	
	$r_2(x)=\frac{4a^3+27b^2}{4a^2}$		

$f(x)$有重因式

$\Leftrightarrow$ $(f(x),f'(x))\neq 1$

$\Leftrightarrow$ $4a^3+27b^2=0$。

当 $a=0$ 时,上述结论仍然成立。

例 4 $K[x]$中,$f(x)$的次数大于 0,令

$$g(x) := f(x+b), b \in K.$$

证明:$f(x)$在 K 上不可约当且仅当 $g(x)$在 K 上不可约。

证明 充分性。易知 $\deg g(x)=\deg f(x)$。假如 $f(x)$在 K 上可约,则在 $K[x]$中,有

$$f(x) = f_1(x)f_2(x), \deg f_i(x) < \deg f(x), i = 1,2.$$

x 用 $x+b$ 代入,从上式得

$$f(x+b) = f_1(x+b)f_2(x+b).$$

令 $g_i(x):=f_i(x+b)$，显然 $\deg g_i(x)=\deg f_i(x)$，$i=1,2$. 于是在 $K[x]$ 中，有

$$g(x)=g_1(x)g_2(x),\deg g_i(x)<\deg g(x),i=1,2.$$

这与 $g(x)$ 在 K 上不可约矛盾，因此 $f(x)$ 在 K 上不可约。

必要性。x 用 $x-b$ 代入，则从 $g(x)=f(x+b)$ 得 $g(x-b)=f(x)$，从充分性证得的结论知，如果 $f(x)$ 在 K 上不可约，那么 $g(x)$ 在 K 上不可约。 ■

例 5 $K[x]$ 中，$f(x)$ 的次数大于 0，令

$$g(x):=f(x+b).$$

证明：$f(x)$ 有重因式当且仅当 $g(x)$ 有重因式。

证明 设 $f(x)$ 在 $K[x]$ 中的标准分解式为

$$f(x)=ap_1^{l_1}(x)p_2^{l_2}(x)\cdots p_s^{l_s}(x). \tag{2}$$

x 用 $x+b$ 代入，从上式得

$$f(x+b)=ap_1^{l_1}(x+b)p_2^{l_2}(x+b)\cdots p_s^{l_s}(x+b).$$

令 $q_i(x)=p_i(x+b)$，$i=1,2,\cdots,s$，由于 $p_i(x)$ 在 K 上不可约，因此据例 4 得，$q_i(x)$ 在 K 上也不可约，$i=1,2,\cdots,s$。于是 $g(x)$ 在 $K[x]$ 中的标准分解式为

$$g(x)=aq_1^{l_1}(x)q_2^{l_2}(x)\cdots q_s^{l_s}(x). \tag{3}$$

$f(x)$ 有重因式 $\Leftrightarrow$ (2) 式中有某个 $l_j>1$

$\Leftrightarrow$ (3) 式中有某个 $l_j>1$

$\Leftrightarrow$ $g(x)$ 有重因式。 ■

例 6 设 K 是数域，在 $K[x]$ 中，

$$f(x)=x^3+a_2x^2+a_1x+a_0.$$

求 $f(x)$ 有重因式的充分必要条件。

解 令 $g(x):=f\left(x-\dfrac{a_2}{3}\right)$

$$=\left(x-\frac{a_2}{3}\right)^3+a_2\left(x-\frac{a_2}{3}\right)^2+a_1\left(x-\frac{a_2}{3}\right)+a_0$$

$$=x^3+\left(a_1-\frac{1}{3}a_2^2\right)x+\frac{2}{27}a_2^3-\frac{a_1a_2}{3}+a_0$$

运用例 5 和例 3 的结论得，$f(x)$ 有重因式当且仅当

$$0=4\left(a_1-\frac{1}{3}a_2^2\right)^3+27\left(\frac{2}{27}a_2^3-\frac{a_1a_2}{3}+a_0\right)^2$$

$$=4a_2^3a_0-a_2^2a_1^2-18a_2a_1a_0+4a_1^3+27a_0^2.$$

点评 研究数域 K 上的 3 次多项式没有重因式的充分必要条件是有实际应用的。例如，在密码学中，可以利用平面上的下述曲线：

$$y^2 = x^3 + ax + b,$$

其中 $4a^3+27b^2\neq 0$，来建立公钥密码体系。据例 3 的结论知道，这里关于 a,b 的条件正是 3 次多项式 $f(x)=x^3+ax+b$ 没有重因式的充分必要条件。

例 7 设 K 是数域，在 $K[x]$ 中，$f(x)$ 是 4 次多项式。如果 $x-2$ 是 $f(x)+5$ 的三重因式，$x+3$ 是 $f(x)-2$ 的二重因式，求 $f(x)$。

解 由已知条件得，$x-2$ 是 $(f(x)+5)'=f'(x)$ 的二重因式，$x+3$ 是 $(f(x)-2)'=f'(x)$ 的单因式。

由于 $\deg f(x)=4$，因此 $\deg f'(x)=3$。从而 $f'(x)$ 的标准分解式为

$$f'(x) = a(x-2)^2(x+3).$$

于是

$$f'(x)=a(x^3-x^2-8x+12).$$

根据 $K[x]$ 中多项式的导数的定义，得

$$f(x) = a\left(\frac{1}{4}x^4 - \frac{1}{3}x^3 - 4x^2 + 12x\right) + b.$$

由于 $x-2$ 整除 $f(x)+5$，用综合除法得

$$\frac{28}{3}a + b + 5 = 0. \tag{4}$$

由于 $x+3$ 整除 $f(x)-2$，用综合除法得

$$-\frac{171}{4}a + b - 2 = 0. \tag{5}$$

联立(4)和(5)式，解得

$$a = -\frac{84}{625}, b = -\frac{2341}{625}.$$

因此

$$f(x)=-\frac{21}{625}x^4+\frac{28}{625}x^3+\frac{336}{625}x^2-\frac{1008}{625}x-\frac{2341}{625}.$$

例 8 设 K 是数域，证明：$K[x]$ 中一个 n 次($n\geqslant 1$)多项式 $f(x)$ 能被它的导数整除的充分必要条件是它与一个一次因式的 n 次幂相伴。

证明 充分性。设 $f(x)=a(cx+b)^n$，则

$$f'(x) = na(cx+b)^{n-1}c.$$

从而

$$f'(x) \mid f(x).$$

必要性。设 $f'(x)\mid f(x)$，则 $(f(x),f'(x))=cf'(x)$，其中 c^{-1} 是 $f'(x)$ 的首项系数。由于用 $(f(x),f'(x))$ 去除 $f(x)$ 所得的商式 $g(x)$ 与 $f(x)$ 有完全相同的不可约因式(不计重数)，且 $g(x)$ 没有重因式，因此

$$f(x) = cg(x)f'(x).$$

由于 $\deg f(x)=n,\deg f'(x)=n-1$,因此 $g(x)=a(x+b)$.

从而 $$f(x)=a(x+b)^n.$$ ■

习题 7.5

1. 判别下列有理系数多项式有无重因式? 如果有重因式,试求出一个多项式与它有完全相同的不可约因式(不计重数),且这个多项式没有重因式。

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

(2) $f(x)=x^3+2x^2-11x-12$。

2. 对于第 1 题中有重因式的多项式 $f(x)$,求出它在 $\mathbf{Q}[x]$中的标准分解式。

3. 在 $\mathbf{Q}[x]$中,$f(x)=x^5-3x^4+2x^3+2x^2-3x+1$。

(1) 求一个没有重因式的多项式 $g(x)$,使它与 $f(x)$含有完全相同的不可约因式(不计重数);

(2) 求 $f(x)$的标准分解式。

4. 举例说明:在数域 K 上的一元多项式环 $K[x]$中,一个不可约多项式 $p(x)$是 $f(x)$的导数 $f'(x)$的 $k-1$ 重因式($k\geqslant 2$),但是 $p(x)$不是 $f(x)$的 k 重因式。

5. 设 K 是数域,证明:在 $K[x]$中,若不可约多项式 $p(x)$是 $f(x)$的导数 $f'(x)$的 $k-1$ 重因式($k\geqslant 1$),并且 $p(x)$是 $f(x)$的因式,则 $p(x)$是 $f(x)$的 k 重因式。

6. 设 K 是数域,证明:在 $K[x]$中,不可约多项式 $p(x)$是 $f(x)$的 k 重因式($k\geqslant 1$)的充分必要条件为:$p(x)$是 $f(x),f'(x),\cdots,f^{(k-1)}(x)$的因式,但不是 $f^{(k)}(x)$的因式。

7. 设 K 是数域,$K[x]$中,$f(x)$如下所述,求 $f(x)$有重因式的充分必要条件。

(1) $f(x)=x^4+ax^2+b$;

(2) $f(x)=x^4+cx+d$;

(3) $f(x)=x^4+cx^3+d$。

7.6 一元多项式的根,复数域上的不可约多项式

7.6.1 内容精华

唯一因式分解定理揭示了数域 K 上一元多项式环 $K[x]$的结构:每一个次数大于 0 的多项式都可以唯一地分解成有限多个不可约多项式的乘积。下一步的任务就是要决定

$K[x]$中的所有不可约多项式。由于一次因式都是不可约的,因此我们要进一步在次数大于 1 的多项式中寻找不可约多项式。次数大于 1 的多项式如果有一次因式,那么它是可约的;如果没有一次因式,那么它可能是不可约的,也可能是可约的。于是次数大于 1 的多项式不可约的必要条件是它没有一次因式,但这不是充分条件。为此要研究 $K[x]$中的多项式 $f(x)$有一次因式的充分必要条件,首先研究用一次多项式 $x-a$ 去除 $f(x)$得到的余式是什么样子。

定理 1(余数定理) 在 $K[x]$中,用 $x-a$ 去除 $f(x)$所得的余式是 $f(a)$。

由定理 1 立即得到:

推论 1 在 $K[x]$中,$x-a \mid f(x) \Leftrightarrow f(a)=0$。 ■

从推论 1 看出,需要引进多项式的根的概念:

定义 1 设 K 是数域,R 是一个有单位元的交换环,且 R 可看成是 K 的一个扩环。对于 $f(x)\in K[x]$,如果有 $c\in R$,使得 $f(c)=0$,那么称 c 是 $f(x)$在 R 中的一个**根**。

$f(x)$在复数域和实数域中的根分别称为复根和实根。若 $f(x)\in \mathbf{Q}[x]$,则 $f(x)$在 $\mathbf{Q}$ 中的根(如果有的话)称为有理根。

从定义 1 和推论 1 立即得出:

定理 2(Bezout 定理) 在 $K[x]$中,$x-a$ 是 $f(x)$的一次因式当且仅当 a 是 $f(x)$在 K 中的一个根。 ■

于是 $K[x]$中的多项式 $f(x)$有一次因式的充分必要条件是它在 K 中有根。如果 $x-a$ 是 $f(x)$的 k 重因式($k\geqslant 0$),那么称 a 是 $f(x)$的 ***k* 重根**。当 $k\geqslant 2$ 时,a 称为重根;当 $k=1$ 时,a 称为单根;当 $k=0$ 时,a 不是根。

对于 $K[x]$中的 n 次($n>0$)多项式 $f(x)$,设

$$f(x)=a(x-c_1)^{r_1}(x-c_2)^{r_2}\cdots(x-c_m)^{r_m}p_{m+1}^{r_{m+1}}(x)\cdots p_s^{r_s}(x),$$

其中 $c_1,c_2,\cdots,c_m$ 是 K 中两两不等的数,$p_{m+1}(x),\cdots,p_s(x)$是次数大于 1 的首一不可约多项式,它们两两不等,$r_i\geqslant 0,i=1,2,\cdots,s$。由于 $r_1+r_2+\cdots+r_m\leqslant n$,因此有:

定理 3 $K[x]$中 n 次($n>0$)多项式 $f(x)$在 K 中至多有 n 个根(重根按重数计算)。 ■

显然,当 $n=0$ 时,定理 3 也成立。

从定理 3 得出:如果一个次数不超过 n 的多项式在 K 中有 $n+1$ 个根,那么它必为零多项式,由此立即得出:

定理 4 在 $K[x]$中,设 $f(x)$与 $g(x)$的次数都不超过 n,如果 K 中有 $n+1$ 个不同的数 $c_1,c_2,\cdots,c_{n+1}$,使得

$$f(c_i)=g(c_i),i=1,2,\cdots,n+1, \tag{1}$$

那么 $f(x)=g(x)$。

定理4使我们可以把数域 K 上的一元多项式 $f(x)$ 与一元多项式函数 f 等同看待。理由如下：

任意给定 $f(x)\in K[x]$，可以得到 K 到自身的一个映射 $f: a\longmapsto f(a), \forall a\in K$。这个映射 f 称为由多项式 $f(x)$ 诱导的**多项式函数**，也称为 K **上的一元多项式函数**。

把数域 K 上的所有一元多项式函数组成的集合记作 K_{pol}，在此集合中规定

$$(f+g)(a) := f(a)+g(a), \forall a \in K, \tag{2}$$

$$(fg)(a) := f(a)g(a) \forall a \in K. \tag{3}$$

从(2)、(3)式看出，$f+g$，fg 分别是由多项式

$$h(x) = f(x)+g(x), p(x) = f(x)g(x)$$

诱导的多项式函数，因此(2)、(3)式定义了集合 K_{pol} 上的加法运算和乘法运算。易看出，零函数是 K_{pol} 中的零元，常值函数1是 K_{pol} 中的单位元；易验证 K_{pol} 是一个有单位元的交换环，称它为 K 上的**一元多项式函数环**。

定理5 数域 K 上的两个多项式 $f(x)$ 与 $g(x)$ 如果不相等，那么它们诱导的多项式函数 f 与 g 也不相等。

证明 设 $f(x)\neq g(x)$。假如 $f=g$，则 $\forall a\in K$，有 $f(a)=g(a)$。由于 K 是数域，它有无穷多个元素，于是根据定理4得，$f(x)=g(x)$，矛盾。因此 $f\neq g$。 ■

注意，定理5证明中的关键是 K 中有无穷多个元素。

设 K 是数域，把多项式 $f(x)$ 对应到它诱导的多项式函数 f，这是 $K[x]$ 到 K_{pol} 的一个映射，显然它是满射；从定理5得出，这个映射是单射，从而它是双射。由于多项式 $f(x)+g(x)$ 对应的多项式函数是 $f+g$，多项式 $f(x)g(x)$ 对应的多项式函数是 fg，因此这个映射保持加法运算和乘法运算。

定义2 设 R 和 R' 是两个环，如果存在从 R 到 R' 的一个双射 σ，它保持加法和乘法运算，即对 $\forall a,b\in R$，有

$$\sigma(a+b) = \sigma(a)+\sigma(b),$$

$$\sigma(ab) = \sigma(a)\sigma(b),$$

那么称 σ 是环 R 到 R' 的一个**同构映射**，此时称环 R 与 R' 是**同构**的，记作 $R\cong R'$。

从上面的讨论立即得到：设 K 是数域，则

$$K[x] \cong K_{\text{pol}}.$$

从而可以把数域 K 上的一元多项式 $f(x)$（这是一个表达式）与数域 K 上的一元多项式函数 f（这是一个映射）等同起来。

由 Bezout 定理立即得到：在 $K[x]$ 中，$x-a$ 是 $f(x)$ 的一次因式当且仅当多项式函数 f 在 a 处的函数值 $f(a)=0$。这使得我们可以运用函数论的知识来研究数域 K 上的不可约多项式。

现在来研究复数域上的不可约多项式有哪些。设

$$f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbf{C}[x]$$

且 $\deg f(x)=n>0$。假如 $f(x)$没有复根，则$\forall z\in\mathbf{C}$，有 $f(z)\neq0$。于是函数

$$\Phi(z)=\frac{1}{f(z)}$$

的定义域为 $\mathbf{C}$。类似于实变量函数，复变量的多项式函数有导数，且复变量函数的导数与四则运算的关系，以及复合函数的求导法则，都像实变量函数那样，因此，$\Phi(z)$在复平面 $\mathbf{C}$ 的每一个点处都有导数，此时称 $\Phi(z)$在复平面 $\mathbf{C}$ 上**解析**。

当$|z|\to+\infty$时，$|\Phi(z)|$的变化趋势如何？我们有

$$\begin{aligned}|f(z)|&=|a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0|\\&\geqslant|a_nz^n|-|a_{n-1}z^{n-1}+\cdots+a_1z+a_0|\\&\geqslant|a_n||z|^n-(|a_{n-1}||z|^{n-1}+\cdots+|a_1||z|+|a_0|).\end{aligned}$$

直觉猜测：当$|z|$充分大时，有

$$|a_n||z|^n-(|a_{n-1}||z|^{n-1}+\cdots+|a_1||z|+|a_0|)>0.$$

为了论证这一猜测是真的，令

$$M=\max\{|a_{n-1}|,\cdots,|a_1|,|a_0|\}.$$

于是当$|z|-1>0$时，有

$$\begin{aligned}&|a_{n-1}||z|^{n-1}+\cdots+|a_1||z|+|a_0|\\\leqslant&M(|z|^{n-1}+\cdots+|z|+1)\\=&M\frac{1-|z|^n}{1-|z|}=M\frac{|z|^n-1}{|z|-1}<M\frac{|z|^n}{|z|-1}.\end{aligned}$$

又当$|z|-1>0$时，有

$$\frac{M|z|^n}{|z|-1}\leqslant|a_n||z|^n\quad\Leftrightarrow\quad|z|\geqslant1+\frac{M}{|a_n|}.$$

因此，当$|z|\geqslant1+\frac{M}{|a_n|}$时，有

$$\begin{aligned}|f(z)|&\geqslant|a_n||z|^n-(|a_{n-1}||z|^{n-1}+\cdots+|a_1||z|+|a_0|)\\&>|a_n||z|^n-M\frac{|z|^n}{|z|-1}\geqslant0.\end{aligned}$$

于是，当$|z|\geqslant1+\frac{M}{|a_n|}$时，有

$$|\Phi(z)|=\frac{1}{|f(z)|}\leqslant\frac{1}{|a_n||z|^n-(|a_{n-1}||z|^{n-1}+\cdots+|a_1||z|+|a_0|)}$$

$$= \frac{\frac{1}{|z|^n}}{|a_n| - \left(|a_{n-1}| \frac{1}{|z|} + \cdots + |a_1| \frac{1}{|z|^{n-1}} + |a_0| \frac{1}{|z|^n}\right)}$$

$\to 0$，当 $|z| \to +\infty$.

所以 $$\lim_{|z| \to +\infty} |\Phi(z)| = 0.$$

于是存在 $r>0, M_1>0$，使得当 $|z|>r$ 时，有

$$|\Phi(z)| \leqslant M_1.$$

显然 $\Phi(z)$ 在圆盘 $|z| \leqslant r$ 上连续。根据“有界闭集上的连续函数必有界(指它的模)”，因此 $\Phi(z)$ 在 $|z| \leqslant r$ 上有界，即存在 $M_2>0$，使得当 $|z| \leqslant r$ 时，有

$$|\Phi(z)| \leqslant M_2$$

综上所述得，$\forall z \in \mathbf{C}$，有

$$|\Phi(z)| \leqslant \max\{M_1, M_2\}.$$

这表明 $\Phi(z)$ 在复平面 $\mathbf{C}$ 上有界。

根据复变函数论的 Liouvill 定理：在复平面 $\mathbf{C}$ 上解析且有界的函数必为常值函数，得

$$\Phi(z) = b, \forall z \in \mathbf{C},$$

其中 b 是某个非零复数，从而

$$f(z) = \frac{1}{b}, \forall z \in \mathbf{C}.$$

由此得出，$f(x) = \frac{1}{b}$。这与 $\deg f(x) = n > 0$ 矛盾。因此 $f(x)$ 必有复根。于是我们证明了：

定理 6(代数基本定理) 每一个次数大于 0 的复系数多项式至少有一个复根。 ■

定理 6 被称为“代数基本定理”是因为在 19 世纪以前求代数方程的根是代数学的最重要课题，这个定理的第一个严格证明是高斯(Gauss)于 1799 年给出的，后来他又给出了四个证明；Jordan，Weyl 等人也给过证明。

由定理 6 立即得到：每一个次数大于 0 的复系数多项式都有一次因式，从而次数大于 1 的复系数多项式都是可约的。于是得到：

推论 2 复数域上的不可约多项式只有一次多项式。 ■

定理 7(复系数多项式唯一因式分解定理) 每一个次数大于 0 的复系数多项式在复数域上都可以唯一地分解成一次因式的乘积。 ■

因此次数大于 0 的复系数多项式 $f(x)$ 的标准分解式为

$$f(x) = a(x-c_1)^{l_1}(x-c_2)^{l_2}\cdots(x-c_s)^{l_s}. \tag{4}$$

于是立即得出：

推论 3 每一个 n 次($n>0$)复系数多项式恰有 n 个复根(重根按重数计算)。 ■

显然,当 $n=0$ 时,推论 3 也成立。

至此我们完全决定了复数域上的不可约多项式(见推论 2),从而细化了复系数多项式的唯一因式分解定理。

利用复系数多项式唯一因式分解定理,可以得出数域 K 上的 n 次($n>0$)多项式 $f(x)$ 的复根与它的系数之间的关系:

设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in K[x]$,$n>0$。把 $f(x)$ 看成复系数多项式,设它的 n 个复根为 $c_1,c_2,\cdots,c_n$(它们可能有相同的),则 $f(x)$ 在复数域上有因式分解:

$$f(x)=(x-c_1)(x-c_2)\cdots(x-c_n). \tag{5}$$

把(5)式的右端展开,并且比较各项系数得

$$\begin{aligned}
&a_{n-1}=-(c_1+c_2+\cdots+c_n),\\
&\cdots\\
&a_{n-k}=(-1)^k\sum_{1\leqslant i_1<\cdots<i_k\leqslant n}c_{i_1}c_{i_2}\cdots c_{i_k},\\
&\cdots\\
&a_0=(-1)^nc_1c_2\cdots c_n.
\end{aligned} \tag{6}$$

公式(6)称为 **Vieta 公式**。

* 复系数多项式唯一因式分解定理在 λ-矩阵相抵的判定上也有应用。

定义 3 设 $A(\lambda)$ 是 $\mathbf{C}[\lambda]$ 上的 n 级非零矩阵,$A(\lambda)$ 的每个次数大于 0 的不变因子的标准分解式中,出现的所有一次因式的方幂(相同的必须按出现的次数计算)称为 $A(\lambda)$ 的**初等因子**。

从定义 3 看出,如果知道了 $A(\lambda)$ 的不变因子,那么可以唯一确定出 $A(\lambda)$ 的初等因子;反之,如果知道了 $A(\lambda)$ 的初等因子,也可以唯一确定出 $A(\lambda)$ 的不变因子。考虑到以后的应用,假定 $A(\lambda)$ 的秩为 n。于是 $A(\lambda)$ 的不变因子有 n 个。我们把 $A(\lambda)$ 的初等因子中同一个一次因式的方幂按降幂排列,并且当同一个一次因式的方幂不到 n 个时,就在后面补上适当个数的 1,以便凑齐 n 个方幂。于是有

$$\begin{array}{cccc}
(\lambda-\lambda_1)^{k_{11}}, & (\lambda-\lambda_1)^{k_{12}}, & \cdots, & (\lambda-\lambda_1)^{k_{1n}}\\
(\lambda-\lambda_2)^{k_{21}}, & (\lambda-\lambda_2)^{k_{22}}, & \cdots, & (\lambda-\lambda_2)^{k_{2n}}\\
\vdots & \vdots & & \vdots\\
(\lambda-\lambda_s)^{k_{s1}}, & (\lambda-\lambda_s)^{k_{s2}}, & \cdots, & (\lambda-\lambda_s)^{k_{sn}}.
\end{array} \tag{7}$$

由于(7)式中出现的一次因式的方幂(除去零次幂以外)就是 $A(\lambda)$ 的全部次数大于 0 的不变因子的标准分解式中的一次因式方幂,因此(7)式中的一次因式方幂应当分别属于 $A(\lambda)$

的各个不变因子。注意到 $A(\lambda)$ 的不变因子具有性质：

$$d_i(\lambda) \mid d_{i+1}(\lambda), i = 1,2,\cdots,n-1.$$

因此 $d_n(\lambda)$ 应当包含(7)式中每个一次因式的最高方幂，$d_{n-1}(\lambda)$ 应当包含(7)式中每个一次因式的次高方幂。如此下去，换句话说，(7)式中第 1 列的一次因式方幂的乘积就是 $d_n(\lambda)$，第 2 列的一次因式方幂的乘积就是 $d_{n-1}(\lambda)$，…，第 n 列的一次因式方幂(可能是零次幂)的乘积就是 $d_1(\lambda)$。这样从 $A(\lambda)$ 的初等因子便唯一确定出了 $A(\lambda)$ 的不变因子。由此立即得出：

定理 8 $\mathbf{C}[\lambda]$ 上两个满秩 n 级矩阵相抵的充分必要条件是它们有相同的初等因子。 ■

对于数域 K 上的 n 级矩阵 A，它的特征矩阵 $\lambda I-A$ 是满秩的 n 级 λ-矩阵(因为 $|\lambda I-A| \neq 0$)。由于 $\lambda I-A$ 的 n 个不变因子的乘积等于 $|\lambda I-A|$，因此如果 $|\lambda I-A|$ 在 $K[\lambda]$ 中的标准分解式是一次因式方幂的乘积，那么 $\lambda I-A$ 的每个不变因子在 $K[\lambda]$ 中的标准分解式也都是一次因式方幂的乘积，这时所有这些一次因式的方幂(相同的必须按出现的次数计算)是 $\lambda I-A$ 的初等因子。按照上面一段的议论，$\lambda I-A$ 的不变因子与初等因子互相唯一确定。因此与定理 8 一样，有下述结论：

定理 9 设 A,B 是数域 K 上的 n 级矩阵，如果它们的特征多项式在 $K[\lambda]$ 中都能分解成一次因式方幂的乘积，那么 $\lambda I-A$ 与 $\lambda I-B$ 相抵的充分必要条件是它们有相同的初等因子。

今后我们把数域 K 上 n 级矩阵 A 的特征矩阵 $\lambda I-A$ 的不变因子叫做 A 的**不变因子**。如果 A 的特征多项式 $|\lambda I-A|$ 在 $K[\lambda]$ 中能分解成一次因式方幂的乘积，那么我们把 $\lambda I-A$ 的初等因子叫做 A 的**初等因子**。

设 $A(\lambda)$ 是 $\mathbf{C}[\lambda]$ 上的 n 级满秩矩阵，$A(\lambda)$ 的初等因子比起不变因子较容易求出。

定理 10 设 $A(\lambda)$ 是 $\mathbf{C}[\lambda]$ 上的 n 级满秩矩阵，通过初等变换把 $A(\lambda)$ 化成对角矩阵，然后把主对角线上每个次数大于 0 的多项式分解成互不相同的一次因式方幂的乘积，那么所有这些一次因式的方幂(相同的按出现的次数计算)就是 $A(\lambda)$ 的初等因子。

设 A 是数域 K 上的 n 级矩阵，如果它的特征多项式 $|\lambda I-A|$ 在 $K[\lambda]$ 中能分解成一次因式的方幂的乘积，那么可以按照定理 10 所讲的方法求出 A 的特征矩阵 $\lambda I-A$ 的初等因子。

前面指出，可以把数域 K 上的一元多项式与一元多项式函数等同看待。从而我们利用函数论的知识证明了代数基本定理，进而决定了复数域上的所有不可约多项式。现在我们反过来要运用多项式的理论来解决函数论中的一些问题。定理 4 表明：数域 K 上一个次数不超过 n 的多项式，被它在 K 的 $n+1$ 个不同元素的值所唯一确定。于是在实际问题中，如果变量 y 与变量 x 之间有确定的依赖关系(即函数关系)，并且通过观测得到当 x 取 $n+1$ 个不同的值 $c_0,c_1,\cdots,c_n$ 时，y 的对应值为 $d_0,d_1,\cdots,d_n$。那么我们可以找一个次数不

超过 n 的多项式 $f(x)$，满足 $f(c_i)=d_i, i=0,1,\cdots,n$，用多项式函数 $y=f(x)$ 来近似地描述 y 与 x 的函数关系。此时把这个多项式函数 $y=f(x)$ 称为原来函数的**插值函数**，或**插值多项式**。求插值函数的问题称为插值问题。下面介绍求插值多项式的一些方法。

定理 11 设 $c_0,c_1,\cdots,c_n$ 是数域 K 中 $n+1$ 个不同的数 $d_0,d_1,\cdots,d_n\in K$，则 $K[x]$ 中存在唯一的一个次数不超过 n 的多项式 $f(x)$，使得

$$f(c_i)=d_i, i=0,1,2,\cdots,n. \tag{8}$$

证明 据定理 4 得，满足(8)式的次数不超过 n 的多项式 $f(x)$ 如果存在，那么它是唯一的。现在来证存在性。

先看一个特殊情形：任意取定 $i\in\{0,1,\cdots,n\}$，设

$$d_0=\cdots=d_{i-1}=d_{i+1}=\cdots=d_n=0.$$

如果存在一个次数不超过 n 的多项式 $f_i(x)$，使得

$$f_i(c_j)=d_j=0, j\neq i; f_i(c_i)=d_i. \tag{9}$$

那么 $f_i(x)$ 有 n 个不同的根 $c_0,\cdots,c_{i-1},c_{i+1},\cdots,c_n$。由于 $\deg f_i(x)\leqslant n$，因此

$$f_i(x)=a_i(x-c_0)\cdots(x-c_{i-1})(x-c_{i+1})\cdots(x-c_n). \tag{10}$$

由于 $f_i(c_i)=d_i$，因此由(10)式得

$$a_i=\frac{d_i}{(c_i-c_0)\cdots(c_i-c_{i-1})(c_i-c_{i+1})\cdots(c_i-c_n)}. \tag{11}$$

把(11)式代入(10)式得

$$f_i(x)=d_i\frac{(x-c_0)\cdots(x-c_{i-1})(x-c_{i+1})\cdots(x-c_n)}{(c_i-c_0)\cdots(c_i-c_{i+1})(c_i-c_{i+1})\cdots(c_i-c_n)}. \tag{12}$$

显然(12)式给出的 $f_i(x)$ 是次数不超过 n 的多项式，且满足(9)式。

现在看一般情形。令

$$f(x)=\sum_{i=0}^{n}d_i\frac{(x-c_0)\cdots(x-c_{i-1})(x-c_{i+1})\cdots(x-c_n)}{(c_i-c_0)\cdots(c_i-c_{i-1})(c_i-c_{i+1})\cdots(c_i-c_n)}. \tag{13}$$

则 $\deg f(x)\leqslant n$，且满足

$$\begin{aligned}f(c_j)&=\sum_{i=0}^{n}d_i\frac{(c_j-c_0)\cdots(c_j-c_{i-1})(c_j-c_{i+1})\cdots(c_j-c_n)}{(c_i-c_0)\cdots(c_i-c_{i-1})(c_i-c_{i+1})\cdots(c_i-c_n)}\\&=d_j.\end{aligned}$$

■

(13)式给出的多项式称为**拉格朗日(Lagrange)插值公式**。

定理 11 中求插值多项式 $f(x)$ 还可以用**牛顿(Newton)插值公式**：

$$\begin{aligned}f(x)=u_0+u_1(x-c_0)+u_2(x-c_0)(x-c_1)+\cdots\\+u_n(x-c_0)(x-c_1)\cdots(x-c_{n-1}).\end{aligned} \tag{14}$$

其中系数 $u_0,u_1,\cdots,u_n$ 可以通过把 x 逐次用 $c_0,c_1,\cdots,c_n$ 代入而从(14)式求出。

定理 11 中求插值多项式 $f(x)$还可以用**待定系数法**，设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, \tag{15}$$

由于要求 $f(c_i)=d_i, i=0,1,\cdots,n$，因此可以得到一个含未知数 $a_n,a_{n-1},\cdots,a_0$ 的 $n+1$ 个方程组成的线性方程组，它的系数行列式是范德蒙行列式，这个行列式不等于 0，因此方程组有唯一解。

7.6.2 典型例题

例 1 在 $\mathbf{Q}[x]$中，$f(x)=x^3-3x^2+ax+4$。求 a 的值，使 $f(x)$在 $\mathbf{Q}$ 中有重根，并且求出相应的重根及其重数。

解法一 $c\in\mathbf{Q}$ 是 $f(x)$的重根

$\Leftrightarrow$ $x-c$ 是 $f(x)$的重因式

$\Leftrightarrow$ $x-c$ 是$(f(x),f'(x))$的因式。

用辗转相除法求$(f(x),f'(x))$，当 $a\neq 3$ 时，

c 是 $f(x)$在 $\mathbf{Q}$ 中的重根

$\Leftrightarrow$ $4a^3-9a^2+216a=0(a\in\mathbf{Q})$且 $x-c$ 是 $x+\dfrac{12+a}{2a-6}$的因式

$\Leftrightarrow$ $a=0$ 且 $c=2$。

当 $a=3$ 时，$(f(x),f'(x))=1$，从而 $f(x)$没有重因式，因此 $f(x)$在 $\mathbf{Q}$ 中没有重根。

综上所述，$f(x)$在 $\mathbf{Q}$ 中有重根当且仅当 $a=0$，此时 2 是 $f(x)$的重根。用 $x-2$ 去除 $f(x)$，采用综合除法，易求出 2 是 $f(x)$的二重根。

解法二 $f(x)$在 $\mathbf{Q}$ 中有重根

$\Rightarrow$ $f(x)$在 $\mathbf{Q}[x]$中有重因式

$\Leftrightarrow$ $4\cdot(-3)^3\cdot 4-(-3)^2a^2-18\cdot(-3)\cdot a\cdot 4+4a^3+27\cdot 4^2=0$

$\Leftrightarrow$ $4\cdot a^3-9a^2+216a=0$

$\Leftrightarrow$ $a=0$ 或 $4a^2-9a+216=0$(舍去)。

因此 $f(x)$在 $\mathbf{Q}$ 中有重根的必要条件是 $a=0$，再看它是否为充分条件。当 $a=0$ 时，

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

因此 $f(x)$在 $\mathbf{Q}$ 中有重根当且仅当 $a=0$,此时 2 是 $f(x)$的二重根。

点评 解法一具有普遍性,解法二针对 $f(x)$是 3 次多项式,利用了 7.5 节例 6 中关于 3 次多项式有重因式的充分必要条件,从而变得比较简捷。

需要注意:$K[x]$中的多项式 $f(x)$在 K 中有重根的必要条件是 $f(x)$在 $K[x]$中有重因式,但这不是充分条件。即,可能 $f(x)$在 $K[x]$中有重因式,但是 $f(x)$在 K 中没有重根。例如,$\mathbf{Q}[x]$中,$f(x)=(x^2-2)^2$ 有二重因式 x^2-2,但是 $f(x)$在 $\mathbf{Q}$ 中没有根,当然也就没有重根。当 K 是复数域时,$\mathbf{C}[x]$中的多项式 $f(x)$在 $\mathbf{C}$ 中有重根当且仅当 $f(x)$有重因式。

例 2 设 K 是数域,证明:$K[x]$中两个次数大于 0 的多项式没有公共复根的充分必要条件是它们互素。

证明 设 $f(x),g(x)\in K[x]$,则

$f(x)$与 $g(x)$有公共复根

$\Leftrightarrow$ $f(x)$与 $g(x)$在 $\mathbf{C}[x]$中有公共的一次因式

$\Leftrightarrow$ $f(x)$与 $g(x)$在 $\mathbf{C}[x]$中不互素

$\Leftrightarrow$ $f(x)$与 $g(x)$在 $K[x]$中不互素。

从而 $f(x)$与 $g(x)$没有公共复根当且仅当 $f(x)$与 $g(x)$在 $K[x]$中互素。 ■

点评 在例 2 证明过程的第二步的充分性利用了复数域上每一个次数大于 0 的多项式都可以分解成一次因式的乘积。例 2 的结论使我们可以利用辗转相除法判断 $K[x]$中两个多项式有无公共复根,并且如果有的话,把公共复根求出来:c 是 $f(x)$与 $g(x)$的公共复根当且仅当 $x-c$ 是$(f(x),g(x))$的因式。

例 3 $\mathbf{Q}[x]$中,$f(x)=x^3-3x^2+x-3$,$g(x)=x^4-x^3+2x^2-x+1$。$f(x)$与 $g(x)$有无公共复根?如果有,试把它求出来。

解法一 用辗转相除法求出:

$$(f(x),g(x))=x^2+1=(x-\mathrm{i})(x+\mathrm{i}).$$

因此 i 和 $-$i 是 $f(x)$与 $g(x)$的公共复根。

解法二

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

于是 $$(f(x),g(x))=x^2+1=(x-\mathrm{i})(x+\mathrm{i}).$$

因此 i 和 $-\mathrm{i}$ 是 $f(x)$ 与 $g(x)$ 的公共复根。

点评 例 3 的解法一用辗转相除法求 $(f(x),g(x))$ 是普遍适用的方法。解法二通过因式分解来求 $(f(x),g(x))$，只对一些特殊的多项式适用，因为没有一个通法来把 $K[x]$ 中任意一个次数大于 0 的多项式分解成不可约多项式的乘积。

例 4 证明：在 $K[x]$ 中，如果 $x-a\mid f(x^m)$，其中 m 是任一正整数，那么

$$x^m-a^m \mid f(x^m).$$

证明 令 $g(x)=f(x^m)$，由于 $x-a\mid f(x^m)$，即 $x-a\mid g(x)$，因此 a 是 $g(x)$ 在 K 中的根，从而 $g(a)=0$，于是 $f(a^m)=g(a)=0$。这表明 a^m 是 $f(x)$ 在 K 中的根。因此 $x-a^m\mid f(x)$。从而有 $h(x)\in K[x]$，使得 $f(x)=h(x)(x-a^m)$。不定元 x 用 x^m 代入，从上式得 $f(x^m)=h(x^m)(x^m-a^m)$，于是 $x^m-a^m\mid f(x^m)$。 ■

点评 例 4 的证明主要是利用了根与一次因式的关系，以及一元多项式环的通用性质。如果不用一元多项式环的通用性质，就很难把道理讲清楚。

例 5 证明：在 $\mathbf{Q}[x]$ 中，有

$$x^2+x+1\mid x^{3m}+x^{3n+1}+x^{3l+2},$$

其中 $m,n,l\in\mathbf{N}^*$。

证明 把上述多项式看成复数域上的多项式，记 $w=\dfrac{-1+\sqrt{3}\,\mathrm{i}}{2}$。由于 $w^3=1$，因此有

$$1+w+w^2=0,$$

$$w^{3m}+w^{3n+1}+w^{3l+2}=1+w+w^2=0.$$

从而 w 是 x^2+x+1 与 $x^{3m}+x^{3n+1}+x^{3l+2}$ 的公共复根。据 Bezout 定理得，$x-w$ 是它们的公因式，从而它们不互素。由于互素性不随数域的扩大而改变，因此 x^2+x+1 与 $x^{3m}+x^{3n+1}+x^{3l+2}$ 在 $\mathbf{Q}[x]$ 中也不互素。又由于二次多项式 x^2+x+1 在 $\mathbf{Q}[x]$ 中没有一次因式，因此它在 $\mathbf{Q}$ 上不可约。于是在 $\mathbf{Q}[x]$ 中，有

$$x^2+x+1\mid x^{3m}+x^{3n+1}+x^{3l+2}.$$ ■

点评 例 5 的证明充分显示了掌握理论的重要性。利用根与一次因式的关系，互素性不随数域的扩大而改变，$\mathbf{Q}[x]$ 中不可约多项式与任一多项式的关系要么互素，要么能整除它，就证明了结论。几乎不用什么计算，也不需要什么特殊技巧。

例 6 证明：在 $\mathbf{Q}[x]$ 中，如果

$$x^2+x+1\mid f_1(x^3)+xf_2(x^3),$$

那么 1 是 $f_i(x)$ 的根，$i=1,2$。

证明 由已知条件得，存在 $h(x)\in\mathbf{Q}[x]$，使得

$$f_1(x^3)+xf_2(x^3)=h(x)(x^2+x+1). \tag{16}$$

记 $w=\dfrac{-1+\sqrt{3}\,\mathrm{i}}{2}$，则 $w^2+w+1=0$，$(w^2)^2+w^2+1=w+w^2+1=0$。

x 分别用 w，w^2 代入，从(1)式得

$$f_1(1)+wf_2(1)=0,$$
$$f_1(1)+w^2f_2(1)=0.$$

联立解得，$f_1(1)=0$，$f_2(1)=0$。

因此 1 是 $f_i(x)$的根，$i=1,2$。 ■

点评 例 6 的证题思路是为了求 $f_1(1)$、$f_2(1)$，需要列出两个方程，利用已知的整除关系可写出关于整除的等式(16)。从(16)式的具体情形看出，应当把 x 用三次单位根 w，w^2 代入，才能得到关于 $f_1(1)$、$f_2(1)$的两个方程。

例 7 设 K 是一个数域，$f(x)\in K[x]$且 $f(x)$的次数 n 大于 0。证明：如果在 $K[x]$中，$f(x)\mid f(x^m)$，m 是一个大于 1 的整数，那么 $f(x)$的复根只能是 0 或单位根。

证明 任取 $f(x)$的一个复根 c，则 $f(c)=0$。

由于在 $K[x]$中，$f(x)\mid f(x^m)$，因此存在 $h(x)\in K[x]$，使得

$$f(x^m)=h(x)f(x). \tag{17}$$

x 用 c 代入，从(17)式得 $f(c^m)=h(c)f(c)=0$。于是 c^m 是 $f(x)$的一个复根。

x 用 c^m 代入，从(17)式得 $f(c^{m^2})=h(c^m)f(c^m)=0$。于是 c^{m^2} 也是 $f(x)$的一个复根。依次下去可得，c，c^m，c^{m^2}，c^{m^3}，…都是 $f(x)$的复根。把 $f(x)$看成 $\mathbf{C}[x]$中的多项式，由于 $\deg f(x)=n$，因此 $f(x)$恰有 n 个复根(重根按重数计算)。于是必存在正整数 j，使得 $c^{m^j}=c^{m^i}$ 对于某个正整数 $i<j$。由此得出 $c^{m^i}(c^{m^j-m^i}-1)=0$。因此 $c^{m^i}=0$ 或 $c^{m^j-m^i}=1$。从而 $c=0$ 或 c 是单位根。 ■

点评 从例 7 的证明过程看出，运用一元多项式环的通用性质才能把从 c 是 $f(x)$的复根推导出 c^m，c^{m^2}，c^{m^3}，…都是 $f(x)$的复根的道理讲清楚。否则，不仅道理说不清楚，而且容易产生差错。

例 8 设 K 是一个数域，$f(x)\in K[x]$且 $\deg f(x)=n>0$。证明：c 是 $f(x)$的 k 重复根($k\geqslant 1$)的充分必要条件是：

$$f(c)=f'(c)=\cdots=f^{(k-1)}(c)=0,\ f^{(k)}(c)\neq 0. \tag{18}$$

证明 必要性。设 c 是 $f(x)$的 k 重复根($k\geqslant 1$)，则在 $\mathbf{C}[x]$中，$x-c$ 是 $f(x)$的 k 重因式，从而 $x-c$ 是 $f'(x)$的 $k-1$ 重因式，于是 $x-c$ 是 $f''(x)$的 $(k-1)-1=k-2$ 重因式。依次下去可得，$x-c$ 是 $f'''(x)$的 $k-3$ 重因式，…，$x-c$ 是 $f^{(k-1)}(x)$的 1 重因式，$x-c$ 不是 $f^{(k)}(x)$的因式，因此

$$f(c)=f'(c)=\cdots=f^{(k-1)}(c)=0, f^{(k)}(c)\neq 0.$$

充分性。设复数 c 使得(18)式成立，则 c 是 $f(x), f'(x), \cdots, f^{(k-1)}(x)$ 的复根，c 不是 $f^{(k)}(x)$ 的复根。从而在 $\mathbf{C}[x]$ 中，$x-c$ 是 $f^{(k-1)}(x)$ 的单因式。于是 $x-c$ 是 $f^{(k-2)}(x)$ 的 2 重因式。依此类推可得，$x-c$ 分别是 $f^{(k-3)}(x), \cdots, f'(x), f(x)$ 的 3 重，…，$k-1$ 重，k 重因式，因此 c 是 $f(x)$ 的 k 重复根。 ■

例 9 设 $f(x)=x^4+5x^3+ax^2+bx+c\in\mathbf{Q}[x]$，如果 -2 是 $f(x)$ 的 3 重根，求 a,b,c。

解 据例 8 的结论，-2 是 $f(x)$ 的 3 重根当且仅当

$$f(-2)=f'(-2)=f''(-2)=0, f'''(-2)\neq 0$$

$$f'(x)=4x^3+15x^2+2ax+b,$$

$$f''(x)=12x^2+30x+2a,$$

$$f'''(x)=24x+30.$$

解关于 a,b,c 的方程组

$$\begin{cases}(-2)^4+5\times(-2)^3+a(-2)^2+b(-2)+c=0,\\ 4\times(-2)^3+15\times(-2)^2+2a(-2)+b=0,\\ 12\times(-2)^2+30\times(-2)+2a=0,\end{cases}$$

得，$a=6, b=-4, c=-8$。

例 10 证明：数域 K 上任意一个不可约多项式在复数域内没有重根。

证明 设 $p(x)$ 是 $K[x]$ 中的不可约多项式，它在 $K[x]$ 中的标准分解式为 $p(x)=a\cdot\frac{1}{a}p(x)$，其中 a 是 $p(x)$ 的首项系数。由此看出 $p(x)$ 在 $K[x]$ 中没有重因式。从而 $p(x)$ 在 $\mathbf{C}[x]$ 中没有重因式，于是 $p(x)$ 在复数域内没有重根。 ■

点评 例 10 的证明的关键是利用了“有无重因式不随数域的扩大而改变”这个结论。

例 11 证明：在 $K[x]$ 中，如果 $f(x)$ 与一个不可约多项式 $p(x)$ 有公共复根，那么 $p(x)\mid f(x)$。

证明 由已知条件得，$f(x)$ 与 $p(x)$ 在 $\mathbf{C}[x]$ 中有公共的一次因式，因此在 $\mathbf{C}[x]$ 中，$(f(x),p(x))\neq 1$。从而在 $K[x]$ 中，$(f(x),p(x))\neq 1$。由于 $p(x)$ 是 K 上不可约多项式，因此 $p(x)\mid f(x)$。 ■

点评 例 11 证明的关键有两点：第一，互素性不随数域的扩大而改变；第二，$K[x]$ 中，不可约多项式 $p(x)$ 与任一多项式 $f(x)$ 的关系或者互素，或者 $p(x)\mid f(x)$。

从例 5、例 6、例 7、例 10、例 11 等题目看出，掌握一元多项式环的通用性质，掌握“整除关系，首一最大公因式，互素性，有无重因式都不随数域的扩大而改变”，掌握 $K[x]$ 中不可约多项式与任一多项式的关系等理论，可以比较容易找到解题思路，而且能把解题过程写

得清楚明白,不至于含糊不清。

例 12 在 $\mathbf{C}[x]$中,求 x^n-1 的标准分解式。

解 c 是 x^n-1 的复根 $\Leftrightarrow$ $c^n-1=0$

$\Leftrightarrow$ c 是 n 次单位根。

由于恰有 n 个两两不等的 n 次单位根:$1,\xi,\xi^2,\cdots,\xi^{n-1}$,其中 $\xi=\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$,因此 x^n-1 在 $\mathbf{C}[x]$中的标准分解式为

$$x^n-1=(x-1)(x-\xi)(x-\xi^2)\cdots(x-\xi^{n-1}). \tag{19}$$

例 13 设 x^n-a^n 是数域 K 上的多项式($a\neq 0$),求 x^n-a^n 在 $\mathbf{C}[x]$中的标准分解式。

解 $x^n-a^n=a^n\left[\left(\frac{x}{a}\right)^n-1\right]$.

x 用$\frac{x}{a}$代入,从例 12 的 x^n-1 的标准分解式(19)得

$$\left(\frac{x}{a}\right)^n-1=\left(\frac{x}{a}-1\right)\left(\frac{x}{a}-\xi\right)\left(\frac{x}{a}-\xi^2\right)\cdots\left(\frac{x}{a}-\xi^{n-1}\right).$$

从而

$$x^n-a^n=(x-a)(x-a\xi)(x-a\xi^2)\cdots(x-a\xi^{n-1}). \tag{20}$$

例 14 设 K 是一个数域,R 是一个有单位元的交换环,且 R 可看成是 K 的一个扩环,设$a\in R$,令

$$J_a=\{f(x)\in K[x]\mid f(a)=0\}, \tag{21}$$

设 $J_a\neq\{0\}$,证明:

(1) J_a 中存在唯一的首一多项式 $m(x)$,使得

$$J_a=\{h(x)m(x)\mid h(x)\in K[x]\}; \tag{22}$$

(2) 如果 R 是无零因子环,那么第(1)小题中的 $m(x)$在 $K[x]$中不可约。

证明 (1) 在 J_a 中取一个次数最低的首一多项式,记作 $m(x)$,任取 $f(x)\in J_a$,在 $K[x]$中,用 $m(x)$去除 $f(x)$,作带余除法:

$$f(x)=h(x)m(x)+r(x),\deg r(x)<\deg m(x).$$

假如 $r(x)\neq 0$,x 用 a 代入,从上式得

$$f(a)=h(a)m(a)+r(a).$$

由此得出,$r(a)=0$,从而 $r(x)\in J_a$,这与 $m(x)$的取法矛盾,因此 $r(x)=0$。即 $f(x)=h(x)m(x)$,从而(22)式成立。

设首一多项式 $m_1(x)$也使得

$$J_a=\{h(x)m_1(x)\mid h(x)\in K[x]\},$$

则 $m(x)\mid m_1(x)$且 $m_1(x)\mid m(x)$。从而 $m(x)\sim m_1(x)$。又由于它们首一,因此 $m(x)=m_1(x)$。

(2) 假如 $m(x)$ 在 $K[x]$ 中可约，则在 $K[x]$ 中有

$$m(x)=m_1(x)m_2(x),\deg m_i(x)<\deg m(x),i=1,2.$$

x 用 a 代入，从上式得

$$m(a)=m_1(a)m_2(a).$$

由于 $m(a)=0$，且 R 是无零因子环，因此 $m_1(a)=0$ 或者 $m_2(a)=0$。从而 $m_1(x)\in J_a$ 或者 $m_2(x)\in J_a$，这与 $m(x)$ 是 J_a 中次数最低的多项式矛盾。所以 $m(x)$ 在 $K[x]$ 中不可约。■

例 15 在例 14 中，取 K 为复数域 $\mathbf{C}$，取 R 为 $\mathbf{C}[A]$，其中

$$A=\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}.$$

求 J_A 中次数最低的首一多项式 $m(x)$。

解 $$A^2=\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}0 & -2\\ 2 & 0\end{pmatrix}$$

$$=2\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}=2(A-I).$$

因此 $$A^2-2A+2I=0.$$

令 $$f(x)=x^2-2x+2,$$

则 $$f(A)=A^2-2A+2I=0.$$

从而 $f(x)\in J_A$。由例 14 的第(1)小题知道，$m(x)\mid f(x)$。在 $\mathbf{C}[x]$ 中，

$$f(x)=[x-(1+\mathrm{i})][x-(1-\mathrm{i})].$$

显然，$x-(1\pm\mathrm{i})\notin J_A$，因此 $m(x)=f(x)$。即

$$m(x)=x^2-2x+2.$$

点评 例 15 的 J_A 中次数最低的首一多项式 $m(x)$ 在 $\mathbf{C}[x]$ 中可约，这是因为 $\mathbf{C}[A]$ 是有零因子的环。例如，$A-(1+\mathrm{i})I\neq 0$，$A-(1-\mathrm{i})I\neq 0$，但是

$$[A-(1+\mathrm{i})I][A-(1-\mathrm{i})I]=A^2-2A+2I=0.$$

因此 $A-(1\pm\mathrm{i})I$ 都是 $\mathbf{C}[A]$ 中非平凡的零因子。

例 16 设 A 是数域 K 上的 n 级矩阵，证明：A 的特征多项式的 n 个复根的和等于 $\mathrm{tr}(A)$，n 个复根的乘积等于 $|A|$。

证明 A 的特征多项式 $f(\lambda)$ 为

$$f(\lambda)=|\lambda I-A|=\lambda^n-\mathrm{tr}(A)\lambda^{n-1}+\cdots+(-1)^n|A|.$$

设 $f(\lambda)$ 的 n 个复根为 $c_1,c_2,\cdots,c_n$，据 Vieta 公式得

$$-\mathrm{tr}(A)=-(c_1+c_2+\cdots+c_n),$$

$$(-1)^n|A|=(-1)^n c_1c_2\cdots c_n.$$

因此 $$c_1+c_2+\cdots+c_n=\mathrm{tr}(A),c_1c_2\cdots c_n=|A|.$$ ■

例 17 设 $\xi=\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$,其中 n 是大于 1 的正整数,证明:对于 $0<k<n$,有

$$\sum_{0\leqslant j_1<j_2<\cdots<j_k<n}\xi^{j_1}\xi^{j_2}\cdots\xi^{j_k}=0. \tag{23}$$

证明 在 $\mathbf{C}[x]$中,

$$x^n-1=(x-1)(x-\xi)(x-\xi^2)\cdots(x-\xi^{n-1}).$$

当 $0<k<n$ 时,x^n-1 中 x^{n-k}的系数 $a_{n-k}=0$。由 Vieta 公式得,(23)式成立。 ■

* **例 18** 设 A 是有理数域上的 3 级矩阵:

$$A=\begin{pmatrix}2&3&2\\1&8&2\\-2&-14&-3\end{pmatrix},$$

A 有无初等因子? 如果有,试求出 A 的初等因子。

解

$$\lambda I-A=\begin{pmatrix}\lambda-2&-3&-2\\-1&\lambda-8&-2\\2&14&\lambda+3\end{pmatrix}\longrightarrow\begin{pmatrix}-1&\lambda-8&-2\\0&\lambda^2-10\lambda+13&-2\lambda+2\\0&2\lambda-2&\lambda-1\end{pmatrix}$$

$$\longrightarrow\begin{pmatrix}1&0&0\\0&\lambda^2-10\lambda+13&-2(\lambda-1)\\0&2(\lambda-1)&\lambda-1\end{pmatrix}\longrightarrow\begin{pmatrix}1&0&0\\0&\lambda^2-6\lambda+9&0\\0&2(\lambda-1)&\lambda-1\end{pmatrix}$$

$$\longrightarrow\begin{pmatrix}1&0&0\\0&(\lambda-3)^2&0\\0&0&\lambda-1\end{pmatrix}.$$

因此 A 的初等因子为 $\lambda-1,(\lambda-3)^2$。

例 19 求一个次数不超过 3 的多项式 $f(x)\in\mathbf{Q}[x]$,使得 $f(0)=5,f(1)=7,f(-1)=9,f(-2)=13$。

解法一 用拉格朗日插值公式,得

$$\begin{aligned}f(x)=&5\frac{(x-1)(x+1)(x+2)}{(0-1)(0+1)(0+2)}+7\frac{(x-0)(x+1)(x+2)}{(1-0)(1+1)(1+2)}\\&+9\frac{(x-0)(x-1)(x+2)}{(-1-0)(-1-1)(-1+2)}+13\frac{(x-0)(x-1)(x+1)}{(-2-0)(-2-1)(-2+1)}\\=&x^3+3x^2-2x+5.\end{aligned}$$

解法二　用牛顿插值公式，得

$$f(x) = u_0 + u_1x + u_2x(x-1) + u_3x(x-1)(x+1).$$

因为 $f(0)=5$，所以 $u_0=5$。因为 $f(1)=7$，所以

$$7 = 5 + u_1 \cdot 1.$$

从而 $u_1=2$。因为 $f(-1)=9$，所以

$$9 = 5 + 2(-1) + u_2(-1)(-1-1).$$

从而 $u_2=3$。因为 $f(-2)=13$，所以

$$13 = 5 + 2(-2) + 3(-2)(-2-1) + u_3(-2)(-2-1)(-2+1).$$

从而 $u_3=1$。因此

$$\begin{aligned} f(x) &= 5 + 2x + 3x(x-1) + x(x-1)(x+1) \\ &= x^3 + 3x^2 - 2x + 5. \end{aligned}$$

解法三　设 $f(x)=a_3x^3+a_2x^2+a_1x+a_0$。

用待定系数法求出 $a_3=1, a_2=3, a_1=-2, a_0=5$。细节留给读者自己做。

例 20　设 $c_0, c_1, \cdots, c_n$ 是数域 K 的 $n+1$ 个两两不等的元素，令

$$F(x) = (x-c_0)(x-c_1)\cdots(x-c_n).$$

把拉格朗日插值公式用 $F(x)$ 以及 $F'(c_i)(i=0,1,\cdots,n)$ 来表示。

解　$F'(x) = \prod\limits_{j=1}^{n}(x-c_j) + \prod\limits_{j\neq 1}(x-c_j) + \cdots + \prod\limits_{j\neq n}(x-c_j)$

于是 $F'(c_i) = \prod\limits_{j\neq i}(c_i-c_j)$。从而拉格朗日插值公式可写成

$$f(x) = \sum_{i=0}^{n} d_i \frac{F(x)}{F'(c_i)(x-c_i)}.$$

例 21　求所有 4 次多项式，使它在任意自然数上的值都是整数。

解　设 $f(x)=u_0+u_1x+u_2x(x-1)+u_3x(x-1)(x-2)+u_4x(x-1)(x-2)(x-3)$，$u_4\neq 0$，如果 $f(x)$ 在任意自然数上的值都是整数，那么

(1) $u_0=f(0)\in\mathbf{Z}, u_1=f(1)-u_0\in\mathbf{Z}$；

(2) $2!u_2=f(2)-u_0-2u_1\in\mathbf{Z}$；

(3) $3!u_3=f(3)-u_0-3u_1-6u_2\in\mathbf{Z}$；

(4) $4!u_4=f(4)-u_0-4u_1-12u_2-24u_3\in\mathbf{Z}$。

记 $a_0=u_0, a_1=u_1, a_2=2!u_2, a_3=3!u_3, a_4=4!u_4$，则

$$\begin{aligned} f(x) =& a_0 + a_1x + \frac{1}{2!}a_2x(x-1) + \frac{1}{3!}a_3x(x-1)(x-2) \\ &+ \frac{1}{4!}a_4x(x-1)(x-2)(x-3). \end{aligned} \tag{24}$$

其中 $a_0,a_1,a_2,a_3,a_4\in\mathbf{Z}$,且 $a_4\neq0$。

任取正整数 n,有

$$\begin{aligned}f(n)&=a_0+a_1n+\frac{a_2}{2!}n(n-1)+\frac{a_3}{3!}n(n-1)(n-2)+\frac{a_4}{4!}n(n-1)(n-2)(n-3)\\&=a_0+a_1n+\mathrm{C}_n^2a_2+\mathrm{C}_n^3a_3+\mathrm{C}_n^4a_4\in\mathbf{Z}.\end{aligned}$$

因此所求的所有 4 次多项式都是形如(24)式,其中 $a_i\in\mathbf{Z},i=0,1,2,3,4$ 且 $a_4\neq0$。

例 22 设 $f(x),g(x)\in\mathbf{C}[x]$,证明:如果 $f^{-1}(0)=g^{-1}(0)$,且 $f^{-1}(1)=g^{-1}(1)$,那么 $f(x)=g(x)$。

证明 设 $\max\{\deg\ f(x),\deg\ g(x)\}=n$,不妨设 $f(x)$ 的次数为 n,显然 $f^{-1}(0)\cap f^{-1}(1)=\varnothing$,如果能证明

$$|f^{-1}(0)\cup f^{-1}(1)|\geqslant n+1.$$

那么由于 $f^{-1}(0)=g^{-1}(0)$且 $f^{-1}(1)=g^{-1}(1)$,因此 $f(x)=g(x)$。

设 $f(x),f(x)-1$ 的标准分解式分别为

$$f(x)=a\prod_{i=1}^{m}(x-c_i)^{r_i},$$

$$f(x)-1=a\prod_{j=1}^{s}(x-d_j)^{t_j}.$$

其中 $\sum\limits_{i=1}^{m}r_i=n=\sum\limits_{j=1}^{s}t_j$。显然

$$f^{-1}(0)=\{c_1,c_2,\cdots,c_m\},f^{-1}(1)=\{d_1,d_2,\cdots,d_s\}.$$

因此

$$|f^{-1}(0)\cup f^{-1}(1)|=m+s.$$

根据 7.5 节的定理 1,有

$$\begin{aligned}f'(x)&=(f(x)-1)'\\&=\prod_{i=1}^{m}(x-c_i)^{r_i-1}\cdot\prod_{j=1}^{s}(x-d_j)^{t_j-1}\cdot h(x),\end{aligned}$$

其中 $h(x)$不能被 $x-c_i$ 整除,$i=1,2,\cdots,m$;也不能被 $x-d_j$ 整除,$j=1,2,\cdots,s$。于是

$$\sum_{i=1}^{m}(r_i-1)+\sum_{j=1}^{s}(t_j-1)\leqslant\deg\ f'(x)=n-1.$$

另一方面,有

$$\begin{aligned}\sum_{i=1}^{m}(r_i-1)+\sum_{j=1}^{s}(t_j-1)&=\sum_{i=1}^{m}r_i-m+\sum_{j=1}^{s}t_j-s\\&=2n-(m+s).\end{aligned}$$

因此 $2n-(m+s)\leqslant n-1$。由此得出 $m+s\geqslant n+1$。即

$$|f^{-1}(0)\cup f^{-1}(1)|\geqslant n+1.$$

从而　　$f(x)=g(x)$. ■

例 23　求复系数 2 次多项式 $ax^2+bx+c(a\neq 0)$的全部复根。

解　$ax^2+bx+c=a\left[\left(x+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a^2}\right]$.

$x^2-(b^2-4ac)$恰有两个复根(重根按重数计算)，其中一个记作 $\sqrt{b^2-4ac}$，则$(\sqrt{b^2-4ac})^2=b^2-4ac$。从而

$$x^2-\frac{b^2-4ac}{4a^2}=x^2-\left(\frac{\sqrt{b^2-4ac}}{2a}\right)^2=\left(x+\frac{\sqrt{b^2-4ac}}{2a}\right)\left(x-\frac{\sqrt{b^2-4ac}}{2a}\right).$$

x 用 $x+\frac{b}{2a}$ 代入，从上式得

$$\left(x+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a^2}=\left(x+\frac{b}{2a}+\frac{\sqrt{b^2-4ac}}{2a}\right)\left(x+\frac{b}{2a}-\frac{\sqrt{b^2-4ac}}{2a}\right).$$

于是$\left(x+\frac{b}{2a}\right)^2-\frac{\sqrt{b^2-4ac}}{4a^2}$的全部复根是$\frac{-b\pm\sqrt{b^2-4ac}}{2a}$，这也就是 ax^2+bx+c 的全部复根。

习题 7.6

1. 设 $f(x)=x^5+7x^4+19x^3+26x^2+20x+8\in\mathbf{Q}[x]$，判断 -2 是不是 $f(x)$的根，如果是，它是几重根？

2. 在 $\mathbf{Q}[x]$中，$f(x)=2x^3-7x^2+4x+a$，求 a 的值，使 $f(x)$在 $\mathbf{Q}$ 中有重根，并且求出相应的重根及其重数。

3. $\mathbf{Q}[x]$中，$f(x)=x^3-x^2-x-2$，$g(x)=x^4-2x^3+2x^2-3x-2$。$f(x)$与 $g(x)$有无公共复根？如果有，试把它求出来。

4. 设 $f(x)=x^4-5x^3+ax^2+bx+9\in\mathbf{Q}[x]$，如果 3 是 $f(x)$的二重根，求 a,b。

5. 证明：在 $K[x]$中，如果 $x+1\mid f(x^{2k+1})$，那么 $x^{2k+1}+1\mid f(x^{2k+1})$，其中 k 是任意自然数。

6. 证明：在 $\mathbf{Q}[x]$中，如果 $x^2+1\mid f_1(x^4)+xf_2(x^4)$，那么 1 是 $f_i(x)$的根，$i=1,2$。

7. 证明：如果数域 K 上两个首一不可约多项式 $f(x)$与 $g(x)$有一个公共复根，那么 $f(x)=g(x)$。

8. 设 $K[x]$中 n 次多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

的 n 个复根是 $c_1,c_2,\cdots,c_n$，对于 $b\in K$，求数域 K 上以 $bc_1,bc_2,\cdots,bc_n$ 为复根的多项式。

9. 设 $A\in M_n(K)$，A 的不等于零的主子式的最高阶数称为 A 的**主秩**，记作 $\mathrm{pr}(A)$。证明：A 的非零特征值的个数（重根按重数计算）不超过 $\mathrm{pr}(A)$，也不超过 $\mathrm{rank}(A)$。

10. 证明：如果 n 级实矩阵 A 的主对角元全为正数，那么 A 的特征多项式的复根中至少有一个其实部为正数。

* 11. 下列有理数域上的矩阵 A 有无初等因子？如果有，试求出 A 的初等因子。

(1) $A=\begin{pmatrix}0&1&0\\-4&4&0\\-2&1&2\end{pmatrix}$；　(2) $A=\begin{pmatrix}1&-3&3\\-2&-6&13\\-1&-4&8\end{pmatrix}$。

12. 求有理数域上一个次数不超过 3 的多项式 $f(x)$，使得

$$f(1)=2,f(2)=-3,f(3)=1,f(4)=3.$$

13. 求有理数域上一个次数尽可能低的多项式 $f(x)$，使得

$$f(0)=3,f(1)=4,f(2)=9,f(3)=18.$$

7.7 实数域上的不可约多项式，实系数多项式的实根

7.7.1 内容精华

由于把实数域扩充成复数域比较容易实现，因此找出实数域上的所有不可约多项式，可以利用复数域上多项式的信息。

定理 1 设 $f(x)$是实系数多项式，如果 $\bar{c}$ 是 $f(x)$的一个复根，那么 $\bar{c}$ 也是 $f(x)$的一个复根。

定理 2 实数域上的不可约多项式只有一次多项式和判别式小于 0 的二次多项式。

从定理 2 和唯一因式分解定理立即得出：

定理 3（实系数多项式唯一因式分解定理） 每一个次数大于 0 的实系数多项式 $f(x)$在实数域上都可以唯一地分解成一次因式与判别式小于 0 的二次因式的乘积。即

$$f(x)=a(x-c_1)^{r_1}\cdots(x-c_s)^{r_s}(x^2+p_1x+q_1)^{k_1}\cdots(x^2+p_tx+q_t)^{k_t}. \tag{1}$$

其中 a 是 $f(x)$的首项系数；$c_1,\cdots,c_s$ 是两两不等的实数；$(p_1,q_1),(p_2,q_2),\cdots,(p_t,q_t)$是不同的实数对，且满足 $p_i^2-4q_i<0,i=1,2,\cdots,t;r_1,\cdots,r_s,k_1,\cdots,k_t$ 都是非负整数。 ■

从实系数多项式的分解式看出，如果虚数 z 是 $f(x)$ 的一个复根，那么 $\bar{z}$ 也是 $f(x)$ 的一个复根，且它们的重数相同。因此通常我们说："实系数多项式的虚根共轭成对出现。"由此立即得到：

推论 1　实系数的奇次多项式至少有一个实根。 ■

下面我们来研究：一个实系数多项式 $f(x)$ 有多少个不同的实根？$f(x)$ 的所有实根在哪个区间内？（即实根的界的问题）。对每一个实根能否找一个区间包含这个根而不包含其他根？（即把实根分离开），然后我们再去求每个实根的近似值。

先看实系数多项式 $f(x)$ 的实根的界的问题，我们可以更一般地讨论复系数多项式的复根的范围，再由此得出实系数多项式的实根的界。

定理 4　设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个复系数多项式，其次数 $n\geqslant 1$。令

$$M=\max\{|a_{n-1}|,|a_{n-2}|,\cdots,|a_0|\},\tag{2}$$

则当 $|z|\geqslant 1+\dfrac{M}{|a_n|}$ 时，有

$$|a_nz^n|>|a_{n-1}z^{n-1}+\cdots+a_1z+a_0|.\tag{3}$$

证明　当 $M=0$ 时，结论显然成立。下设 $M\neq 0$。当 $|z|\geqslant 1+\dfrac{M}{|a_n|}$ 时，有 $|z|>1$ 且 $|a_n|\geqslant\dfrac{M}{|z|-1}$。从而有

$$\begin{aligned}|a_nz^n|&=|a_n||z|^n\geqslant\frac{M|z|^n}{|z|-1}>\frac{M(|z|^n-1)}{|z|-1}\\&=M(|z|^{n-1}+\cdots+|z|+1)\\&\geqslant|a_{n-1}||z|^{n-1}+\cdots+|a_1||z|+|a_0|\\&=|a_{n-1}z^{n-1}|+\cdots+|a_1z|+|a_0|\\&\geqslant|a_{n-1}z^{n-1}+\cdots+a_1z+a_0|.\end{aligned}$$ ■

从定理 4 得出，当 $|z|\geqslant 1+\dfrac{M}{|a_n|}$ 时，有

$$\begin{aligned}|f(z)|&=|a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0|\\&\geqslant|a_nz^n|-|a_{n-1}z^{n-1}+\cdots+a_1z+a_0|>0.\end{aligned}$$

因此 $f(x)$ 的复根全都在以原点为圆心，以 $1+\dfrac{M}{|a_n|}$ 为半径的圆内。把这一结论用到实系数多项式上，便得到：

推论 2 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个实系数多项式，其次数 $n\geqslant 1$。令

$$M=\max\{|a_{n-1}|,|a_{n-2}|,\cdots,|a_1|,|a_0|\},$$

则 $f(x)$的实根全都在区间$\left(-1-\frac{M}{|a_n|},1+\frac{M}{|a_n|}\right)$内。 ■

从定理 4 还可以得到：

推论 3 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个次数大于 0 的实系数多项式，则对一切充分大的正数 r，$f(r)$的符号与 a_nr^n 的符号一样。 ■

例如，设 $f(x)=x^3-x+1$，我们有 $M=1$，$1+\frac{M}{|a_n|}=2$。因此 $f(x)$的实根全都在区间 $(-2,2)$内。

注意：求出了一个实系数多项式 $f(x)$的实根的界只是表明：如果 $f(x)$有实根，那么它的所有实根都在这个区间内，但是不能肯定 $f(x)$一定有实根。

如何知道 $f(x)$有没有实根？如果有，实根的个数(不计重数)是多少？如何把实根分离开？对这些问题的第一个令人满意的回答是在 1829 年由 Sturm 给出的。下面我们介绍 Sturm 的方法。先给出一个概念：

定义 1 设 $c_1,c_2,\cdots,c_m$ 是一个非零实数的有限序列。如果 $c_ic_{i+1}<0$，那么我们说，在第 $i+1$ 项有一个**变号**。这个序列中变号的总数称为它的**变号数**。一个有限的实数序列的变号数定义为去掉这个序列中的 0 以后得到的序列的变号数。

例如，序列 $-2,0,1,0,0,3,-4,5$ 的变号数是 3。

定理 5(Sturm 定理) 设 $f(x)$是一个次数大于 0 的实系数多项式，对 $f(x)$与 $f'(x)$作下述略微修改的辗转相除法：

$$\begin{aligned}
&f(x)=q_1(x)f'(x)-f_2(x),\ \deg f_2(x)<\deg f'(x),\\
&f'(x)=q_2(x)f_2(x)-f_3(x),\deg f_3(x)<\deg f_2(x),\\
&\cdots\\
&f_{s-1}(x)=q_s(x)f_s(x).
\end{aligned}\tag{4}$$

由此得到一个多项式序列：

$$f_0=f,f_1=f',f_2,\cdots,f_s.\tag{5}$$

称序列(5)是 $f(x)$的**标准序列**。假设区间$[a,b]$使得 $f(a)\neq 0$，$f(b)\neq 0$，则 $f(x)$在区间(a,b)内的不同实根的个数等于 V_a-V_b，其中 V_c 表示序列 $f_0(c),f_1(c),\cdots,f_s(c)$的变号数。

Sturm 定理既能求出一个实系数多项式 $f(x)$ 的不同的实根的个数，又能把实根分离开（见本节典型例题的例 8、例 9 和例 10）。当我们把实根分离开后，如果想进一步求出实根的近似值，那么可以用计算机来计算。有关求实根近似值的算法在计算数学的书中可以找到，这里就不赘述了。

7.7.2　典型例题

例 1　求多项式 x^n-1 在实数域上的标准分解式。

解　记 $\xi=\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$。据 7.6 节的例 12，在 $\mathbf{C}[x]$ 中，有

$$x^n-1=(x-1)(x-\xi)(x-\xi^2)\cdots(x-\xi^{n-1}). \tag{6}$$

当 $0<k<n$ 时，有 $\xi^k\xi^{n-k}=1$，由于 $\xi^k\,\overline{\xi^k}=|\xi^k|^2=1$，因此 $\overline{\xi^k}=\xi^{n-k}$。从而 $\xi^k+\xi^{n-k}=2\cos\dfrac{2k\pi}{n}$。

情形 1　$n=2m+1$。此时有

$$\begin{aligned}x^{2m+1}-1&=(x-1)(x-\xi)(x-\xi^{2m})\cdots(x-\xi^m)(x-\xi^{m+1})\\&=(x-1)\left(x^2-2x\cos\frac{2\pi}{2m+1}+1\right)\cdots\left(x^2-2x\cos\frac{2m\pi}{2m+1}+1\right)\\&=(x-1)\prod_{k=1}^{m}\left(x^2-2x\cos\frac{2k\pi}{2m+1}+1\right).\end{aligned} \tag{7}$$

情形 2　$n=2m$。此时有 $\xi^m=\mathrm{e}^{\mathrm{i}\frac{2m\pi}{2m}}=\mathrm{e}^{\mathrm{i}\pi}=-1$。从而

$$\begin{aligned}x^{2m}-1&=(x-1)(x-\xi)(x-\xi^{2m-1})\cdots(x-\xi^{m-1})(x-\xi^{m+1})(x-\xi^m)\\&=(x-1)\left(x^2-2x\cos\frac{2\pi}{2m}+1\right)\cdots\left(x^2-2x\cos\frac{2(m-1)\pi}{2m}+1\right)(x+1)\\&=(x-1)(x+1)\prod_{k=1}^{m-1}\left(x^2-2x\cos\frac{k\pi}{m}+1\right).\end{aligned} \tag{8}$$

例 2　求多项式 x^n+1 分别在复数域和实数域上的标准分解式。

解　先求 x^n+1 的全部复根。

$z=r(\cos\theta+\mathrm{i}\sin\theta)$ 是 x^n+1 的复根

$\Leftrightarrow$　$r^n(\cos n\theta+\mathrm{i}\sin n\theta)=\cos\pi+\mathrm{i}\sin\pi$，

$\Leftrightarrow$　$r^n=1$ 且 $n\theta=\pi+2k\pi$，$k\in\mathbf{Z}$

$\Leftrightarrow$　$r=1$ 且 $\theta=\dfrac{(2k+1)\pi}{n}$，$k\in\mathbf{Z}$。

$$\Leftrightarrow \quad z=\cos\frac{(2k+1)\pi}{n}+\mathrm{i}\sin\frac{(2k+1)\pi}{n},k\in\mathbf{Z}.$$

令

$$w_k=\mathrm{e}^{\mathrm{i}\frac{(2k+1)\pi}{n}},k=0,1,2,\cdots,n-1.$$

易证 $w_0,w_1,\cdots,w_{n-1}$ 两两不等,从而它们是 x^n+1 的全部复根,因此 x^n+1 在 $\mathbf{C}[x]$ 中的标准分解式为

$$x^n+1=(x-w_0)(x-w_1)\cdots(x-w_{n-1}). \tag{9}$$

当 $0\leqslant k<n$ 时,有

$$w_kw_{n-k-1}=\mathrm{e}^{\mathrm{i}\frac{(2k+1)\pi+[2(n-k-1)+1]\pi}{n}}=1.$$

从而 $\overline{w_k}=w_{n-k-1}$。于是

$$w_k+w_{n-k-1}=2\cos\frac{(2k+1)\pi}{n}.$$

情形 1 $n=2m+1$。此时有

$$w_m=\mathrm{e}^{\mathrm{i}\frac{(2m+1)\pi}{2m+1}}=-1.$$

从而在 $\mathbf{R}[x]$ 中 $x^{2m+1}+1$ 的标准分解式为

$$\begin{aligned}x^{2m+1}+1&=(x-w_0)(x-w_{2m})\cdots(x-w_{m-1})(x-w_{m+1})(x-w_m)\\&=\left(x^2-2x\cos\frac{\pi}{2m+1}+1\right)\cdots\left(x^2-2x\cos\frac{(2m-1)\pi}{2m+1}+1\right)(x+1)\\&=(x+1)\prod_{k=1}^{m}\left(x^2-2x\cos\frac{(2k-1)\pi}{2m+1}+1\right).\end{aligned} \tag{10}$$

情形 2 $n=2m$。此时在 $\mathbf{R}[x]$ 中 $x^{2m}+1$ 的标准分解式为

$$\begin{aligned}x^{2m}+1&=(x-w_0)(x-w_{2m-1})\cdots(x-w_{m-2})(x-w_{m+1})(x-w_{m-1})(x-w_m)\\&=\left(x^2-2x\cos\frac{\pi}{2m}+1\right)\cdots\left(x^2-2x\cos\frac{(2m-3)\pi}{2m}+1\right)\\&\quad\cdot\left(x^2-2x\cos\frac{(2m-1)\pi}{2m}+1\right)\\&=\prod_{k=1}^{m}\left(x^2-2x\cos\frac{(2k-1)\pi}{2m}+1\right).\end{aligned} \tag{11}$$

例 3 证明:

$$\cos\frac{\pi}{2m+1}\cos\frac{2\pi}{2m+1}\cdots\cos\frac{m\pi}{2m+1}=\frac{1}{2^m}. \tag{12}$$

证明　在例 1 的公式(7)中,x 用 -1 代入,得

$$-2=-2\prod_{k=1}^{m}\left(2+2\cos\frac{2k\pi}{2m+1}\right).$$

从而

$$\frac{1}{2^m}=\prod_{k=1}^{m}\left(1+\cos\frac{2k\pi}{2m+1}\right)$$

$$=\prod_{k=1}^{m}2\cos^2\frac{k\pi}{2m+1}$$

由此得出

$$\frac{1}{2^m}=\prod_{k=1}^{m}\cos\frac{k\pi}{2m+1}.$$ ■

例 4　证明:

$$\sin\frac{\pi}{2m}\sin\frac{2\pi}{2m}\cdots\sin\frac{(m-1)\pi}{2m}=\frac{\sqrt{m}}{2^{m-1}}.\tag{13}$$

证明　从例 1 的公式(8)以及下式

$$x^{2m}-1=(x^2-1)(x^{2(m-1)}+x^{2(m-2)}+\cdots+x^4+x^2+1)$$

得

$$x^{2(m-1)}+x^{2(m-2)}+\cdots+x^4+x^2+1=\prod_{k=1}^{m-1}\left(x^2-2x\cos\frac{k\pi}{m}+1\right).$$

x 用 1 代入,从上式得

$$m=\prod_{k=1}^{m-1}\left(2-2\cos\frac{k\pi}{m}\right).$$

于是

$$\frac{m}{2^{m-1}}=\prod_{k=1}^{m-1}\left(1-\cos\frac{k\pi}{m}\right)$$

$$=\prod_{k=1}^{m-1}2\sin^2\frac{k\pi}{2m}.$$

由此得出

$$\frac{\sqrt{m}}{2^{m-1}}=\prod_{k=1}^{m-1}\sin\frac{k\pi}{2m}.$$ ■

例 5 设 A 是实数域上的 n 级斜对称矩阵，证明：如果 A 可逆，那么 A 的特征多项式 $f(\lambda)$的不可约因式都是二次的。

证明 根据《高等代数学习指导书(上册)》第 5 章 5.7 节的例 7，$f(\lambda)$的复根是 0 或纯虚数。如果 A 可逆，那么 $f(\lambda)$的复根都是纯虚数。因此 $f(\lambda)$的不可约因式都是二次的。 ■

例 6 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbf{R}[x]$，证明：

(1) 若 $a_i(i=0,1,\cdots,n)$全是正数或全是负数，则 $f(x)$没有正实根；

(2) 若$(-1)^ia_i(i=0,1,\cdots,n)$全是正数或全是负数，则 $f(x)$没有负实根。

证明 (1) 设 $a_i(i=0,1,\cdots,n)$全是正数。假如 c 是 $f(x)$的正实根，则

$$f(c)=a_nc^n+a_{n-1}c^{n-1}+\cdots+a_1c+a_0>0.$$

这与 c 是 $f(x)$的根矛盾。因此 $f(x)$没有正实根。

设 $a_i(i=0,1,\cdots,n)$全是负数。假如 c 是 $f(x)$的正实根，则 $f(c)=a_nc^n+a_{n-1}c^{n-1}+\cdots+a_1c+a_0<0$，矛盾。因此 $f(x)$没有正实根。

(2) 类似于(1)的证法，请读者自己写出。 ■

例 7 设实系数多项式 $f(x)=x^3+a_2x^2+a_1x+a_0$ 的 3 个复根都是实数，证明：$a_2^2\geqslant 3a_1$。

证明 设 $f(x)$的 3 个复根为实数 c_1,c_2,c_3，则

$$\begin{aligned}0&\leqslant(c_1-c_2)^2+(c_2-c_3)^2+(c_3-c_1)^2\\&=2(c_1^2+c_2^2+c_3^2)-2(c_1c_2+c_2c_3+c_3c_1)\\&=2[(c_1+c_2+c_3)^2-2c_1c_2-2c_1c_3-2c_2c_3]-2(c_1c_2+c_2c_3+c_3c_1)\\&=2(c_1+c_2+c_3)^2-6(c_1c_2+c_1c_3+c_2c_3)\\&=2(-a_2)^2-6a_1.\end{aligned}$$

从而 $a_2^2\geqslant 3a_1$。 ■

例 8 求 $f(x)=x^3-x+1$ 的不同的实根的个数。

解 在 7.7.1 节推论 3 后面，我们已求出了 $f(x)$的实根都在区间$(-2,2)$内。因此只要去求 $f(x)$在$(-2,2)$内有多少个不同的实根即可。

对 $f(x)$和 $f'(x)=3x^2-1$ 作略微修改的辗转相除法，即把每次得到的余式反号以后去除除式：

	$f'(x)$	$f(x)$	
$\frac{9}{2}x+\frac{27}{4}$	$3x^2$　　-1 $3x^2-\frac{9}{2}x$	x^3　　$-x+1$ x^3　　$-\frac{1}{3}x$	$\frac{1}{3}x$
	$\frac{9}{2}x-1$ $\frac{9}{2}x-\frac{27}{4}$	$-\frac{2}{3}x+1$ $f_2(x)=\frac{2}{3}x-1$	
	$\frac{23}{4}$ $f_3(x)=-\frac{23}{4}$		

于是 $f(x)$的标准序列为

$$f_0=x^3-x+1, f_1=3x^2-1, f_2=\frac{2}{3}x-1, f_3=-\frac{23}{4}.$$

从 $f_3=-\frac{23}{4}$知道，$(f(x),f'(x))=1$。因此 $f(x)$没有重根。现在来计算 $f(x)$的标准序列在-2 与 2 处的变号数：

	f_0	f_1	f_2	f_3
-2	$-$	$+$	$-$	$-$
2	$+$	$+$	$+$	$-$

于是 $V_{-2}=2, V_2=1$，从而 $f(x)$在$(-2,2)$内的不同的实根的个数为 $V_{-2}-V_2=1$。由于 $f(x)$没有重根，因此 $f(x)$的实根的总数为 1。

例 9　对于例 8 的 $f(x)$，求出它的实根所在的区间，使区间的长度小于$\frac{1}{2}$。

解　从例 8 知道，$f(x)$的唯一的实根在$(-2,2)$内。先求 $f(x)$的标准序列在此区间的中点处的变号数：$V_0=1$。于是 $f(x)$的实根在$(-2,0)$内，接着求 $f(x)$的标准序列在$(-2,0)$的中点处的变号数：$V_{-1}=1$。于是 $f(x)$的实根在$(-2,-1)$内，再求 $f(x)$的标准序列在区间$(-2,-1)$的中点处的变号数：$V_{-\frac{3}{2}}=2$，因此 $f(x)$的唯一实根在$\left(-\frac{3}{2},-1\right)$内。

例 10　求 $f(x)=x^3-7x-7$ 的不同的实根的个数，并且把这些实根分离开，使得每个

实根所在的区间的长度小于$\frac{1}{2}$。

解 $M=\max\{0,7,7\}=7,-1-\frac{M}{|a_3|}=-8,1+\frac{M}{|a_3|}=8$。于是 $f(x)$的实根都在区间$(-8,8)$内。

对 $f(x)$和 $f'(x)=3x^2-7$ 作略加修改的辗转相除法,得到 $f(x)$的标准序列:

$$f_0=x^3-7x-7,f_1=3x^2-7,f_2=\frac{14}{3}x+7,f_3=\frac{1}{4}.$$

从 $f_3=\frac{1}{4}$知道,$(f(x),f'(x))=1$。因此 $f(x)$没有重根。

	f_0	f_1	f_2	f_3	变号数
-8	$-$	$+$	$-$	$+$	3
8	$+$	$+$	$+$	$+$	0

于是 $V_{-8}=3,V_8=0$,从而 $f(x)$有 3 个不同的实根。

为了把 $f(x)$的 3 个实根分离开,我们相继求 $f(x)$的标准序列在区间中点处的变号数,每求一次,都要选择合适的小区间。

	f_0	f_1	f_2	f_3	变号数
0	$-$	$-$	$+$	$+$	1
4	$+$	$+$	$+$	$+$	0
2	$-$	$+$	$+$	$+$	1
3	$-$	$+$	$+$	$+$	1
$\frac{7}{2}$	$+$	$+$	$+$	$+$	0

于是在$(3,\frac{7}{2})$有 $f(x)$的一个实根。

	f_0	f_1	f_2	f_3	变号数
-4	$-$	$+$	$-$	$+$	3
-2	$-$	$+$	$-$	$+$	3
-1	$-$	$-$	$+$	$+$	1

$-\frac{3}{2}$	−	−	0	+	1
$-\frac{7}{4}$	−	+	−	+	3
$-\frac{13}{8}$	+	+	−	+	2

于是 $f(x)$的另外两个实根分别在$\left(-\frac{7}{4},-\frac{13}{8}\right),\left(-\frac{13}{8},-\frac{3}{2}\right)$内。

例 11　设 $f(x)$是实系数多项式，它的次数 $n\geqslant 2$，证明：如果对任意 $t\in\mathbf{R}$ 都有 $f(t)\geqslant 0$，那么存在两个实系数多项式 $g(x),h(x)$，使得

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

证明　把 $f(x)$因式分解，得

$$f(x)=a(x-c_1)^{r_1}\cdots(x-c_s)^{r_s}(x^2+p_1x+q_1)^{k_1}\cdots(x^2+p_mx+q_m)^{k_m}. \tag{14}$$

其中 $c_1,\cdots,c_s$ 是两两不等的实数，$(p_1,q_1),\cdots,(p_m,q_m)$是不同的实数对，且满足 $p_i^2-4q_i<0$，$i=1,2,\cdots,m$；$r_1,\cdots,r_s,k_1,\cdots,k_m$ 都是非负整数。由于 $f(t)\geqslant 0,\forall t\in\mathbf{R}$，因此 $a>0$，且 $r_1,\cdots,r_s$ 都是偶数（假如有 r_j 是奇数，则可以找到 t 使得 $f(t)<0$ 矛盾）。设 $r_i=2r_i'$，则

$$f(x)=a(x^2-2c_1x+c_1^2)^{r_1'}\cdots(x^2-2c_sx+c_s^2)^{r_s'}\cdot (x^2+p_1x+q_1)^{k_1}\cdots(x^2+p_mx+q_m)^{k_m}. \tag{15}$$

则(15)式中出现的二次多项式都形如 x^2+bx+c，其中 $b^2-4c\leqslant 0$。用待定系数法可以证明这种二次多项式可以表示成

$$x^2+bx+c=(d_1x+e_1)^2+(d_2x+e_2)^2. \tag{16}$$

分别比较二次项、一次项的系数以及常数项，得

$$1=d_1^2+d_2^2, \tag{17}$$

$$b=2d_1e_1+2d_2e_2, \tag{18}$$

$$c=e_1^2+e_2^2. \tag{19}$$

取 $d_1=\frac{1}{2},d_2=\frac{\sqrt{3}}{2}$，则 $d_1^2+d_2^2=1$，代入(18)式，得

$$b=e_1+\sqrt{3}e_2. \tag{20}$$

从(20)式得，$e_1=b-\sqrt{3}e_2$，代入(19)式得

$$c=b^2-2\sqrt{3}be_2+4e_2^2. \tag{21}$$

从(21)式看出，e_2 应当是二次方程

$$4y^2-2\sqrt{3}by+b^2-c=0 \tag{22}$$

的实根，由于二次方程(22)的判别式

$$\begin{aligned}\Delta &= (-2\sqrt{3}b)^2 - 4 \cdot 4(b^2 - c)\\ &= 4(3b^2 - 4b^2 + 4c)\\ &= 4(4c - b^2) \geqslant 0,\end{aligned}$$

因此方程(22)有实根，从而可解得 e_2，进而可求出 e_1。所以(16)式的确成立。

设 $f_1(x)=g_1^2(x)+h_1^2(x)$，$f_2(x)=g_2^2(x)+h_2^2(x)$，则

$$\begin{aligned}f_1(x)f_2(x) &= [g_1^2(x)+h_1^2(x)][g_2^2(x)+h_2^2(x)]\\ &= \begin{vmatrix} g_1(x) & -h_1(x) \\ h_1(x) & g_1(x) \end{vmatrix} \cdot \begin{vmatrix} g_2(x) & -h_2(x) \\ h_2(x) & g_2(x) \end{vmatrix}\\ &= \begin{vmatrix} g_1(x)g_2(x)-h_1(x)h_2(x) & -g_1(x)h_2(x)-h_1(x)g_2(x) \\ h_1(x)g_2(x)+g_1(x)h_2(x) & -h_1(x)h_2(x)+g_1(x)g_2(x) \end{vmatrix}\\ &= [g_1(x)g_2(x)-h_1(x)h_2(x)]^2 + [g_1(x)h_2(x)+h_1(x)g_2(x)]^2.\end{aligned}$$

用数学归纳法可以证明：若 $f_i(x)=g_i^2(x)+h_i^2(x)$，$i=1,2,\cdots,v$，则存在 $g(x),h(x)\in \mathbf{R}[x]$，使得

$$f_1(x)f_2(x)\cdots f_v(x) = g^2(x)+h^2(x).$$

于是由(15)式和(16)式得，存在 $g(x),h(x)\in\mathbf{R}[x]$，使得

$$f(x) = g^2(x)+h^2(x).$$ ■

点评 证明例 11 的关键想法是把 $f(x)$分解成实系数不可约多项式的乘积，并且从已知条件可推出 $f(x)$的一次因式的幂指数应当都是偶数，从而 $f(x)$可分解成二次多项式的方幂的乘积，其中每个二次因式都形如 x^2+bx+c，且满足 $b^2-4c\leqslant 0$。然后对 x^2+bx+c(其中$b^2-4c\leqslant 0$)容易用待定系数法证明它可以表示成两个一次多项式的平方和，最后可证得所要求的结论。

习题 7.7

1. 设 $a\in\mathbf{R}^*$，求多项式 x^n-a^n 在实数域上的标准分解式。
2. 设 $a\in\mathbf{R}^*$，求多项式 x^n+a^n 在实数域上的标准分解式。
3. 证明：$\prod\limits_{k=1}^{m-1}\cos\dfrac{k\pi}{2m}=\dfrac{\sqrt{m}}{2^{m-1}}$。
4. 证明：$\prod\limits_{k=1}^{m}\sin\dfrac{(2k-1)\pi}{2(2m+1)}=\dfrac{1}{2^m}$。

5. 证明：$\prod_{k=1}^{m}\sin\frac{k\pi}{2m+1}=\frac{\sqrt{2m+1}}{2^m}$。

6. 证明：$\prod_{k=1}^{m}\cos\frac{(2k-1)\pi}{2(2m+1)}=\frac{\sqrt{2m+1}}{2^m}$。

7. 证明：$\prod_{k=1}^{m}\sin\frac{(2k-1)\pi}{4m}=\frac{\sqrt{2}}{2^m}$。

8. 证明：$\prod_{k=1}^{m}\cos\frac{(2k-1)\pi}{4m}=\frac{\sqrt{2}}{2^m}$。

9. 求 $f(x)=x^4+12x^2+5x-9$ 的不同的实根的个数，并且把这些实根分离开，使得每个实根所在的区间的长度小于 1。

10. 求 $f(x)=x^3-5x^2+8x-8$ 的不同的实根的个数，以及这些根在哪些相邻的整数之间。

11. 证明：如果实数域上的 n 级矩阵 A 与 B 不相似，那么把它们看成复数域上的矩阵后仍然不相似。

12. $f(x)=x^5+20x+16$ 在 $\mathbf{C}$ 中有无重根？求 $f(x)$的不同的实根的个数。

13. 构造次数最小的实系数多项式，它有

(1) 2 重根 1，单根 2 和 $1+\mathrm{i}$；

(2) 2 重根 i，单根 $-1-\mathrm{i}$。

7.8 有理数域上的不可约多项式

7.8.1 内容精华

有理数域上的不可约多项式有哪些？如何判别一个有理系数多项式是否不可约？本节将对此予以讨论。

设 $f(x)\in\mathbf{Q}[x]$，由于 $f(x)$与它的相伴元只相差一个非零有理数因子，因此 $f(x)$与它的相伴元在有理数域上有相同的因式，从而 $f(x)$在 $\mathbf{Q}$ 上不可约当且仅当它的相伴元在 $\mathbf{Q}$ 上不可约。这样我们可以从 $f(x)$的相伴元中选择一个最简单的多项式作为代表研究它的不可约性。这个代表很自然地可以如下选取：例如，$f(x)=\frac{1}{2}x^3+\frac{1}{3}x^2-2x+1=\frac{1}{6}(3x^3+2x^2-12x+6)$，显然，$3x^3+2x^2-12x+6$ 就是与 $f(x)$相伴的最简单的多项式。一般地，设 $f(x)$的各项系数的分母的最小公倍数为 m，则 $f(x)=\frac{1}{m}mf(x)$，其中 $mf(x)$的各项系

数都为整数。设 $mf(x)$的各项系数的最大公因数为 d,则 $mf(x)=d\,\frac{m}{d}f(x)$,其中$\frac{m}{d}f(x)$的各项系数的最大公因数为±1。于是$\frac{m}{d}f(x)$就是与 $f(x)$相伴的最简单的多项式。由此抽象出本原多项式的概念。

一、本原多项式

定义 1 一个非零的整系数多项式 $g(x)$,如果它的各项系数的最大公因数只有±1,那么称 $g(x)$是一个**本原多项式**。

从前面一段知道,任何一个非零的有理系数多项式 $f(x)$都与一个本原多项式相伴($\frac{m}{d}f(x)$就是一个本原多项式)。进一步可以证明:与 $f(x)$相伴的本原多项式在相差一个正负号下是唯一的。证明如下:

设 $f(x)=rg(x)=sh(x)$,其中 $g(x)$,$h(x)$都是本原多项式,$r,s\in\mathbf{Q}^*$,则 $g(x)=\frac{s}{r}h(x)$。设$\frac{s}{r}=\frac{q}{p}$,其中 $p,q\in\mathbf{Z}$,且$(p,q)=1$。

则 $$pg(x)=qh(x).$$

设 $$g(x)=\sum_{i=0}^{n}b_ix^i,h(x)=\sum_{i=0}^{n}c_ix^i,$$

则 $$p\sum_{i=0}^{n}b_ix^i=q\sum_{i=0}^{n}c_ix^i.$$

从而 $$pb_i=qc_i,i=0,1,\cdots,n,$$

于是 $$q\mid pb_i,i=0,1,\cdots,n,$$

由于$(q,p)=1$,因此 $$q\mid b_i,i=0,1,\cdots,n.$$

由于 $g(x)$本原,因此 $q=\pm1$。同理可证 $p=\pm1$。于是 $g(x)=\pm h(x)$。

从上述结论立即得到本原多项式的第一条性质:

性质 1 两个本原多项式 $g(x)$与 $h(x)$在 $\mathbf{Q}[x]$中相伴当且仅当 $g(x)=\pm h(x)$。

由于任何一个次数大于 0 的有理系数多项式都与一个本原多项式相伴,因此我们只需要去研究本原多项式是否不可约。由于因式分解涉及乘法,因此自然要问:两个本原多项式的乘积是否还是本原多项式?下面的性质 2 回答了这个问题。

性质 2(高斯(Gauss)引理) 两个本原多项式的乘积还是本原多项式。

我们想寻找本原多项式不可约的充分条件,这不容易直接找出。我们可以反过来思考:从一个本原多项式可约能够推出什么样的结论?从不可约多项式的等价条件得出,如果一个次数大于 0 的本原多项式可约,那么它可以分解成两个次数较低的有理系数多项式

的乘积。从高斯引理可以进一步直觉判断它可以分解成两个次数较低的本原多项式的乘积。于是我们猜测并且可以证明有下述性质 3：

性质 3 一个次数大于 0 的本原多项式 $g(x)$在 **Q** 上可约当且仅当 $g(x)$能分解成两个次数较低的本原多项式的乘积。

下述性质 4 给出了本原多项式组成的集合的结构。

性质 4 每一个次数大于 0 的本原多项式 $g(x)$可以唯一地分解成 **Q** 上不可约的本原多项式的乘积。唯一性是指，假如 $g(x)$有两个这样的分解式：

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

则 $s=t$，且适当排列因式的次序后，有

$$p_i(x) = \pm q_i(x), i = 1,2,\cdots,s.$$

可分解性由性质 3 得到。唯一性由 $\mathbf{Q}[x]$中的唯一因式分解定理的唯一性以及性质 1 立即得到。

利用性质 3 可以得到整系数多项式在 **Q** 上可约的充分必要条件：

推论 1 一个次数大于 0 的整系数多项式 $f(x)$在 **Q** 上可约当且仅当 $f(x)$能分解成两个次数较低的整系数多项式的乘积。

二、整系数多项式的有理根

一个次数大于 1 的整系数多项式 $f(x)$如果有一次因式，那么 $f(x)$可约。因此次数大于 1 的整系数多项式 $f(x)$在 $\mathbf{Q}[x]$上不可约的必要条件是 $f(x)$没有一次因式，而 $f(x)$有一次因式当且仅当 $f(x)$在 **Q** 中有根。于是我们先来研究一个整系数多项式在 **Q** 中有根的必要条件。

定理 1 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个次数 n 大于 0 的整系数多项式，如果 $\frac{q}{p}$是 $f(x)$的一个有理根，其中 p,q 是互素的整数，那么 $p|a_n, q|a_0$。

从定理 1 的证明过程看到，如果 $\frac{q}{p}$是 $f(x)$的一个有理根，且 $(p,q)=1$，那么存在一个整系数多项式 $g(x)$，使得 $f(x)=(px-q)g(x)$。当 ±1 不是 $f(x)$的根时，可推出

$$\frac{f(1)}{p-q} \in \mathbf{Z}, \frac{f(-1)}{p+q} \in \mathbf{Z}.$$

因此如果计算出 $\frac{f(1)}{p-q} \notin \mathbf{Z}$ 或 $\frac{f(-1)}{p+q} \notin \mathbf{Z}$，那么 $\frac{q}{p}$不是 $f(x)$的根，这个判断方法在求整系数多项式的有理根时有用。

三、整系数多项式在 Q 上不可约的判别方法

利用定理 1 可以判断一个二次或三次整系数多项式是否在 **Q** 上不可约：二次或三次整系数多项式在 **Q** 上不可约当且仅当它没有有理根。

注意：对于四次或四次以上的整系数多项式 $f(x)$，如果它没有有理根，那么只能说明 $f(x)$ 没有一次因式，还不能说明 $f(x)$ 在 **Q** 上不可约，因为 $f(x)$ 可能有二次因式或次数大于 2 的因式。这表明，对于四次或四次以上的整系数多项式 $f(x)$，没有有理根只是 $f(x)$ 在 **Q** 上不可约的必要条件，但不是充分条件。

下面来探索本原多项式 $f(x)$ 在 **Q** 上不可约的充分条件。

设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个次数 n 大于 0 的本原多项式，为了探索 $f(x)$ 在 **Q** 上不可约的充分条件，我们来分析如果 $f(x)$ 可约，那么能推导出什么结论。由于本原多项式的各项系数的最大公因数只有 ±1，因此任何一个素数都不能整除它的各项系数。我们考虑这样一类的本原多项式：存在一个素数 p 能整除首项系数以外的一切系数，但是 p 不能整除首项系数。即 $p\mid a_i, i=0,1,\cdots,n-1$；而 $p\nmid a_n$。假如 $f(x)$ 在 **Q** 上可约，据性质 3 得

$$f(x)=(b_mx^m+\cdots+b_1x+b_0)(c_lx^l+\cdots+c_1x+c_0). \tag{1}$$

其中 $b_i(i=0,1,\cdots,m)$，$c_j(j=0,1,\cdots,l)$ 都是整数，且 $b_m\neq0$，$c_l\neq0$，$m<n$，$l<n$，$m+l=n$。由(1)式得

$$a_n=b_mc_l, a_0=b_0c_0.$$

已知 $p\mid a_0$，因此 $p\mid b_0$ 或 $p\mid c_0$。不妨设 $p\mid b_0$。又已知 $p\nmid a_n$，因此 $p\nmid b_m$ 且 $p\nmid c_l$。于是存在 $k(0<k\leqslant m)$ 使得

$$p\mid b_0, p\mid b_1,\cdots,p\mid b_{k-1}, p\nmid b_k.$$

由于 $a_k=b_0c_k+b_1c_{k-1}+\cdots+b_{k-1}c_1+b_kc_0$，且 $p\mid a_k$，因此 $p\mid b_kc_0$。由于 $p\nmid b_k$，因此 $p\mid c_0$，又 $p\mid b_0$，从而 $p^2\mid a_0$。于是只要 $p^2\nmid a_0$，那么 $f(x)$ 在 **Q** 上不可约。这样我们探索出了 $f(x)$ 在 **Q** 上不可约的充分条件，这就是著名的 Eisenstein 判别法：

定理 2(Eisenstein 判别法) 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

是一个次数 n 大于 0 的本原多项式。如果存在一个素数 p，使得

(1) $p\mid a_i, i=0,1,\cdots,n-1$；

(2) $p\nmid a_n$；

(3) $p^2\nmid a_0$。

那么 $f(x)$ 在 **Q** 上不可约。 ■

注:定理 2 中的 $f(x)$是一个次数大于 0 的整系数多项式时,利用推论 1,从 $f(x)$可约得出(1)式,因此在定理 2 中,把“$f(x)$是本原多项式”换成“$f(x)$是整系数多项式”仍然成立。

利用定理 2 可以证明:

推论 2 在 $\mathbf{Q}[x]$中存在任意次数的不可约多项式。

证明 任取正整数 n,设 $f(x)=x^n+3$。素数 3 符合定理 2 的所有条件,因此 $f(x)$在 $\mathbf{Q}$ 上不可约。 ■

有时直接用 Eisenstein 判别法无法判断 $f(x)$在 $\mathbf{Q}$ 上是否不可约,这时可尝试利用 7.5 节的例 4,选择一个有理数 b(通常取 $b=1$,或 -1),如果用 Eisenstein 判别法能判断 $g(x)=f(x+b)$在 $\mathbf{Q}$ 上不可约,那么 $f(x)$在 $\mathbf{Q}$ 上不可约。

对于 Eisenstein 判别法中的 3 个条件,很自然地会想:如果改成存在素数 p,使得

$$p \mid a_i, i=1,2,\cdots,n, \quad p \nmid a_0, p^2 \nmid a_n,$$

那么 $f(x)$是否在 $\mathbf{Q}$ 上不可约?为了回答这个问题,我们考虑由数域 K 上的分式组成的集合 $K(x)$,它有加法和乘法运算,成为一个有单位元的交换环(我们将在本章 7.12 节详细讨论这个环)。显然,$K(x)$可以看成 K 的一个扩环。利用数域 K 上一元多项式环的通用性质可以证明下述结论:

* **定理 3** 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个次数 n 大于 0 的整系数多项式,如果存在一个素数 p,使得

$$p \mid a_i, i=1,2,\cdots,n, \quad p \nmid a_0, p^2 \nmid a_n,$$

那么 $f(x)$在 $\mathbf{Q}$ 上不可约。

证明 假如 $f(x)$在 $\mathbf{Q}$ 上可约,则存在两个次数分别为 n_1, n_2($n_i<n, i=1,2$)的整系数多项式 $f_1(x), f_2(x)$,使得

$$f(x)=f_1(x)f_2(x). \tag{2}$$

不定元 x 用 $\mathbf{Q}(x)$中的元素 $\frac{1}{x}$ 代入,从(2)式得

$$f\left(\frac{1}{x}\right)=f_1\left(\frac{1}{x}\right)f_2\left(\frac{1}{x}\right). \tag{3}$$

在(3)式两边乘以 x^n,得

$$x^nf\left(\frac{1}{x}\right)=x^{n_1}f_1\left(\frac{1}{x}\right)x^{n_2}f_2\left(\frac{1}{x}\right). \tag{4}$$

显然 $x^{n_i}f_i(\frac{1}{x})$是整系数多项式,且次数为 n_i,$i=1,2$。

$$x^nf\left(\frac{1}{x}\right)=a_n+a_{n-1}x+\cdots+a_1x^{n-1}+a_0x^n.$$

由已知条件，据 Eisenstein 判别法得，$x^n f(\frac{1}{x})$ 在 **Q** 上不可约，这与(4)式矛盾。因此 $f(x)$ 在 **Q** 上不可约。 ■

定理 3 的证明很简洁，这得益于利用了数域 K 上一元多项式环的通用性质。

在本章 7.12 节的典型例题中，我们将介绍判断整系数多项式在 **Q** 上不可约的又一种方法。

7.8.2 典型例题

例 1 求 $f(x)=3x^4+8x^3+6x^2+3x-2$ 的全部有理根。

解 $a_4=3$ 的因子只有 $\pm1,\pm3$；$a_0=-2$ 的因子只有 $\pm1,\pm2$。于是 $f(x)$ 的有理根只可能是：

$$\pm1,\pm2,\pm\frac{1}{3},\pm\frac{2}{3}.$$

因为 $f(1)=18\neq0$，$f(-1)=-4\neq0$，所以 ±1 不是 $f(x)$ 的根。

考虑 2，因为

$$\frac{f(-1)}{p+q}=\frac{-4}{1+2}=-\frac{4}{3}\notin\mathbf{Z},$$

所以 2 不是 $f(x)$ 的根。

考虑 -2，因为

$$\frac{f(1)}{p-q}=\frac{18}{3}=6,\frac{f(-1)}{p+q}=\frac{-4}{-1}=4,$$

所以需要进一步用综合除法来判断 -2 是不是 $f(x)$ 的根。

3	8	6	3	−2	−2
	−6	−4	−4	2	
3	2	2	−1	0	
	−6	8	−20		
3	−4	10	−21		

这表明 -2 是 $f(x)$ 的单根。于是

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

考虑 $\frac{1}{3}$，因为

$$\frac{f(1)}{p-q}=\frac{18}{3-1}=9,\frac{f(-1)}{p+q}=\frac{-4}{3+1}=-1,$$

所以需要作综合除法。用 $x-\frac{1}{3}$ 去除 $3x^3+2x^2+2x-1$，可得出 $\frac{1}{3}$ 是 $f(x)$ 的单根，且得出

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

显然 x^2+x+1 没有有理根(因为 ±1 都不是它的根)，因此 $f(x)$ 的全部有理根是 -2 和 $\frac{1}{3}$，它们都是单根。

例 2 判断 $f(x)=x^3+2x^2-x+1$ 在 **Q** 上是否不可约。

解 $f(x)$ 的有理根只可能是 ±1。由于

$$f(1)=1+2-1+1\neq0,f(-1)=-1+2+1+1\neq0,$$

因此 $f(x)$ 没有有理根，又由于 $\deg f(x)=3$，因此 $f(x)$ 在 **Q** 上不可约。

例 3 判断 $f(x)=4x^5-27x^4+12x^3-15x+21$ 在 **Q** 上是否不可约。

解 素数 3 能整除首项系数以外的一切系数，但不能整除首项系数 4，且 $3^2\nmid21$，因此 $f(x)$ 在 **Q** 上不可约。

例 4 判断 $f(x)=x^4+2x-1$ 在 **Q** 上是否不可约。

解 x 用 $x+1$ 代入，得

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

素数 2 能整除 $g(x)$ 的首项系数以外的一切系数，但不能整除首项系数 1，且 $2^2\nmid2$，因此 $g(x)$ 在 **Q** 上不可约，从而 $f(x)$ 在 **Q** 上不可约。

例 5 设 p 是一个素数，多项式

$$f_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$$

称为 p 阶**分圆多项式**。证明 $f_p(x)$ 在 **Q** 上不可约。

证明 我们有

$$(x-1)f_p(x)=x^p-1.$$

x 用 $x+1$ 代入，从上式得

$$\begin{aligned}x\,f_p(x+1)&=(x+1)^p-1\\&=x^p+px^{p-1}+\cdots+\mathrm{C}_p^kx^{p-k}+\cdots+px.\end{aligned}$$

于是 $$g(x):=f_p(x+1)=x^{p-1}+px^{p-2}+\cdots+\mathrm{C}_p^kx^{p-k-1}+\cdots+p.$$

我们知道

$$C_p^k = \frac{p(p-1)\cdots(p-k+1)}{k!}, 1 \leqslant k < p.$$

由于$(p,k!)=1$,因此

$$k! \mid (p-1)\cdots(p-k+1).$$

从而 $p \mid C_p^k, 1 \leqslant k < p$,又 $p \nmid 1, p^2 \nmid p$,因此 $g(x)$在 $\mathbf{Q}$ 上不可约,从而 $f_p(x)$在 $\mathbf{Q}$ 上不可约。 ■

点评 据 7.6 节的例 12 以及 $x^p-1=(x-1)(x^{p-1}+\cdots+x+1)$,可得 $x^{p-1}+x^{p-2}+\cdots+x+1=(x-\xi)(x-\xi^2)\cdots(x-\xi^{p-1})$,其中 $\xi=e^{i\frac{2\pi}{p}}$。由于 p 是素数,因此对任意 $j(1\leqslant j<p)$,都有$(\xi^j)^l \neq 1$,其中 $1\leqslant l<p$,即 $\xi,\xi^2,\cdots,\xi^{p-1}$ 都是本原 p 次单位根,显然它们是全部本原 p 次单位根,因此 $x^{p-1}+x^{p-2}+\cdots+x+1$ 是分圆多项式。(关于本原 n 次单位根和分圆多项式的定义可参看《高等代数(下册)——大学高等代数课程创新教材》(丘维声著)第 57 页例 14 和第 78 页的倒数第 4 行至倒数第 2 行。)

例 6 判断 $f(x)=x^4+3x+1$ 在 $\mathbf{Q}$ 上是否不可约。

解 $f(x)$的有理根只可能是± 1,由于 $f(1)=5\neq 0, f(-1)=1-3+1\neq 0$,因此 $f(x)$没有有理根,从而 $f(x)$没有一次因式。假如 $f(x)$在 $\mathbf{Q}$ 上可约,则

$$f(x) = (a_2x^2+a_1x+a_0)(b_2x^2+b_1x+b_0). \tag{5}$$

其中 $a_i(i=0,1,2), b_j(j=0,1,2)$都是整数,比较(5)式的首项系数得,$a_2b_2=1$。于是 a_2 与 b_2 同为 1,或同为-1。不妨设 $a_2=b_2=1$。比较(5)式的其他系数得

$$\begin{cases} a_1+b_1 = 0, \\ a_0+a_1b_1+b_0 = 0, \\ a_0b_1+a_1b_0 = 3, \\ a_0b_0 = 1. \end{cases}$$

由第一式得,$b_1=-a_1$,代入第三式得,$a_1(b_0-a_0)=3$。由第四式得,a_0 与 b_0 同为 1,或同为-1。从而 $b_0-a_0=0$,这与 $a_1(b_0-a_0)=3$ 矛盾,因此 $f(x)$在 $\mathbf{Q}$ 上不可约。

例 7 证明:如果 $p_1,p_2,\cdots,p_t$ 是两两不等的素数$(t\geqslant 1)$,那么对于任意大于 1 的整数 n,都有 $\sqrt[n]{p_1p_2\cdots p_t}$是无理数。

证明 由于$(\sqrt[n]{p_1p_2\cdots p_t})^n=p_1p_2\cdots p_t$,因此 $\sqrt[n]{p_1p_2\cdots p_t}$ 是多项式 $x^n-p_1p_2\cdots p_t$ 的一个实根。假如 $\sqrt[n]{p_1p_2\cdots p_t}$ 是有理数,那么 $x^n-p_1p_2\cdots p_t$ 在 $\mathbf{Q}[x]$ 中有一次因式。由于 $n>1$,因此 $x^n-p_1p_2\cdots p_t$ 在 $\mathbf{Q}$ 上可约。又由于素数 p_1 能整除 $x^n-p_1p_2\cdots p_t$ 的首项系数以外的所有系数,但是 p_1 不能整除首项系数 1,且 $p_1^2 \nmid p_1p_2\cdots p_t$,因此 $x^n-p_1p_2\cdots p_t$ 在 $\mathbf{Q}$ 上不可约,矛盾。所以 $\sqrt[n]{p_1p_2\cdots p_t}$是无理数。 ■

例 8 设 m,n 都是正整数，且 $m<n$，证明：如果 $f(x)$ 是 $\mathbf{Q}$ 上的 m 次多项式，那么对任意素数 p，都有 $\sqrt[n]{p}$ 不是 $f(x)$ 的实根。

证明 假如 $\sqrt[n]{p}$ 是 $f(x)$ 的实根，则 $f(x)$ 作为实数域上的多项式有一次因式 $x-\sqrt[n]{p}$。由于 $(\sqrt[n]{p})^n=p$，因此 $\sqrt[n]{p}$ 是多项式 $g(x)=x^n-p$ 的一个实根。从而 $g(x)$ 作为实数域上的多项式有一次因式 $x-\sqrt[n]{p}$。于是在 $\mathbf{R}[x]$ 中，$f(x)$ 与 $g(x)$ 不互素。由于互素性不随数域的扩大而改变，因此在 $\mathbf{Q}[x]$ 中，$f(x)$ 与 $g(x)$ 也不互素。又由于素数 p 能整除 $g(x)$ 的首项系数以外的一切系数，但不能整除首项系数 1，且 $p^2\nmid p$，因此 $g(x)$ 在 $\mathbf{Q}$ 上不可约。从而 $g(x)$ 能整除 $f(x)$。由此得出，$n\leqslant m$。这与 $m<n$ 矛盾。因此 $\sqrt[n]{p}$ 不是 $f(x)$ 的实根。 ■

点评 在例 8 的证明中，关键是要考虑多项式 $g(x)$，以及利用互素性不随数域的扩大而改变，利用 $\mathbf{Q}[x]$ 中不可约多项式与任一多项式的关系的结论。由此体会到掌握理论的重要性，要善于运用理论去解决问题。

例 9 设 c 是某个首一整系数多项式的复根，$f(x)$ 是以 c 为复根的次数最低的首一整系数多项式，证明 $f(x)$ 在 $\mathbf{Q}$ 上不可约。

证明 假如 $f(x)$ 在 $\mathbf{Q}$ 上可约，则 $f(x)=f_1(x)f_2(x)$，其中 $f_i(x)$ 是首一整系数多项式，且 $\deg f_i(x)<\deg f(x)$，$i=1,2$。由于 $0=f(c)=f_1(c)f_2(c)$，因此 c 是 $f_1(x)$ 的复根或者 c 是 $f_2(x)$ 的复根。这与 $f(x)$ 是以 c 为复根的次数最低的首一整系数多项式矛盾。因此 $f(x)$ 在 $\mathbf{Q}$ 上不可约。 ■

例 10 设 $p(x)$ 是首一整系数多项式，且 $p(x)$ 在 $\mathbf{Q}$ 上不可约。证明：如果首一整系数多项式 $f(x)$ 与 $p(x)$ 有公共复根，那么存在首一整系数多项式 $g(x)$，使得

$$f(x)=g(x)p(x).$$

证明 由于 $f(x)$ 与 $p(x)$ 有公共复根，因此在 $\mathbf{C}[x]$ 中，$f(x)$ 与 $p(x)$ 有公共的一次因式，从而在 $\mathbf{C}[x]$ 中，$f(x)$ 与 $p(x)$ 不互素。于是在 $\mathbf{Q}[x]$ 中，$f(x)$ 与 $p(x)$ 也不互素。由于 $p(x)$ 在 $\mathbf{Q}$ 上不可约，因此 $p(x)\mid f(x)$，即 $p(x)$ 是 $f(x)$ 的一个不可约因式。又由于 $f(x)$ 与 $p(x)$ 的首项系数都为 1，因此 $f(x)$ 与 $p(x)$ 都是本原多项式。据本原多项式在 $\mathbf{Q}[x]$ 中的唯一因式分解定理得，存在整系数多项式 $g(x)$，使得

$$f(x)=p(x)g(x).$$

由于 $f(x)$ 与 $p(x)$ 的首项系数为 1，因此 $g(x)$ 的首项系数为 1。 ■

例 11 设 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是一个次数大于 0 的整系数多项式。证明：如果 $a_n+a_{n-1}+\cdots+a_1+a_0$ 是一个奇数，那么 1 和 -1 都不是 $f(x)$ 的根。

证明 由于 $f(1)=a_n+a_{n-1}+\cdots+a_1+a_0$ 是奇数，因此 1 不是 $f(x)$ 的根，设 $f(x)=mg(x)$，其中 $g(x)$ 是本原多项式，$m\in\mathbf{Z}^*$。假如 -1 是 $f(x)$ 的根，则 $0=f(-1)=$

$mg(-1)$,从而 $g(-1)=0$。于是 $g(x)$有一次因式 $x+1$。据本原多项式在 $\mathbf{Q}[x]$中的唯一因式分解定理得,存在整系数多项式 $h(x)$,使得 $g(x)=(x+1)h(x)$,于是有

$$f(x) = m(x+1)h(x).$$

x 用 1 代入,从上式得,$f(1)=2m\,h(1)$。这与 $f(1)$是奇数矛盾。因此 -1 不是 $f(x)$的根。

■

点评 例 11 的证明由于运用了本原多项式在 $\mathbf{Q}[x]$中的唯一因式分解定理,因此不需要什么计算就证明了 -1 不是 $f(x)$的根。也可以采用下述方法证明这一结论:假如 -1 是 $f(x)$的根,则

$$0 = f(-1) = a_n(-1)^n + a_{n-1}(-1)^{n-1} + \cdots + a_1(-1) + a_0.$$

当 n 是奇数时,从上式得

$$a_n + a_{n-2} + \cdots + a_1 = a_{n-1} + a_{n-3} + \cdots + a_2 + a_0.$$

于是

$$a_n + a_{n-1} + \cdots + a_1 + a_0 = 2(a_n + a_{n-2} + \cdots + a_1).$$

这与已知条件矛盾。当 n 是偶数时,类似的计算可得出与已知条件矛盾。因此 -1 不是 $f(x)$的根。

例 12 设 $f(x)$是一个次数大于 0 的首一整系数多项式,证明:如果 $f(0)$与 $f(1)$都是奇数,那么 $f(x)$没有有理根。

证明 假如 $f(x)$有一个有理根 b,由于 $f(x)$的首项系数为 1,因此 b 必为整数。于是 $x-b$ 是本原多项式,且 $x-b$ 是 $f(x)$的一个因式。又由于 $f(x)$也是本原多项式,因此据本原多项式在 $\mathbf{Q}[x]$中的唯一因式分解定理得,存在整系数多项式 $h(x)$,使得

$$f(x) = (x-b)h(x).$$

x 分别用 0 和 1 代入,从上式得

$$f(0) = (-b)h(0), f(1) = (1-b)h(1).$$

由于 $-b$ 和 $-b+1$ 必有一个是偶数,因此 $f(0)$和 $f(1)$必有一个是偶数。这与已知条件矛盾,所以 $f(x)$没有有理根。 ■

例 13 设 $f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)-1$,其中 $a_1, a_2, \cdots, a_n$ 是两两不等的整数。证明 $f(x)$在 $\mathbf{Q}$ 上不可约。

证明 假如 $f(x)$在 $\mathbf{Q}$ 上可约,则

$$f(x) = g_1(x)g_2(x), \deg g_i(x) < n, g_i(x) \in \mathbf{Z}[x], i = 1,2.$$

x 用 a_j 代入,从上式得

$$-1 = f(a_j) = g_1(a_j)g_2(a_j), j = 1,2,\cdots,n.$$

从而 $g_1(a_j)$与 $g_2(a_j)$一个为 1,另一个为 -1。于是 $g_1(a_j)+g_2(a_j)=0$,$j=1,2,\cdots,n$。这表明多项式 $g_1(x)+g_2(x)$有 n 个不同的根 $a_1, a_2, \cdots, a_n$。但是 $g_1(x)+g_2(x)$的次数小于

n,因此,$g_1(x)+g_2(x)=0$,从而 $f(x)=-g_1^2(x)$。$f(x)$的首项系数为 1,这与$-g_1^2(x)$的首项系数为负数矛盾。因此 $f(x)$在 $\mathbf{Q}$ 上不可约。 ■

例 14 设 $f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)+1$,其中 $a_1,a_2,\cdots,a_n$ 是两两不等的整数。

(1) 证明:当 n 是奇数时,$f(x)$在 $\mathbf{Q}$ 上不可约;

(2) 证明:当 n 是偶数且 $n\geqslant 6$ 时,$f(x)$在 $\mathbf{Q}$ 上不可约;

(3) 当 $n=2$ 或 4 时,$f(x)$在 $\mathbf{Q}$ 上是否不可约?

(1) **证明** 假如 $f(x)$在 $\mathbf{Q}$ 上可约,则

$$f(x)=g_1(x)g_2(x),\deg g_i(x)<n,g_i(x)\in\mathbf{Z}[x],i=1,2.$$

x 用 a_j 代入,从上式得

$$1=f(a_j)=g_1(a_j)g_2(a_j),j=1,2,\cdots,n.$$

于是 $g_1(a_j)$与 $g_2(a_j)$同为 1,或同为-1。从而

$$g_1(a_j)-g_2(a_j)=0,j=1,2,\cdots,n.$$

这表明多项式 $g_1(x)-g_2(x)$有 n 个不同的根 $a_1,a_2,\cdots,a_n$。但是 $g_1(x)-g_2(x)$的次数小于 n,因此 $g_1(x)-g_2(x)=0$。从而 $f(x)=g_1^2(x)$,于是 $\deg f(x)=2\deg g_1(x)$。这与已知 n 是奇数矛盾,因此 $f(x)$在 $\mathbf{Q}$ 上不可约。 ■

(2) **证明** 假如 $f(x)$在 $\mathbf{Q}$ 上可约,由第(1)小题的证明过程得,$f(x)=g_1^2(x)$。从而对一切 $t\in\mathbf{R}$,有 $f(t)=g_1^2(t)\geqslant 0$。不妨设

$$a_1<a_2<a_3<a_4<a_5<a_6<\cdots<a_n.$$

x 用 $a_1+\frac{1}{2}$代入,由 $f(x)$的表达式得

$$\begin{aligned}f\left(a_1+\frac{1}{2}\right)&=\frac{1}{2}\left(a_1+\frac{1}{2}-a_2\right)\cdots\left(a_1+\frac{1}{2}-a_n\right)+1\\&=(-1)^{n-1}\frac{1}{2}\left(a_2-a_1-\frac{1}{2}\right)\cdots\left(a_n-a_1-\frac{1}{2}\right)+1.\end{aligned}$$

由于

$$a_2-a_1-\frac{1}{2}\geqslant 1-\frac{1}{2}=\frac{1}{2},\cdots,$$

$$a_j-a_1-\frac{1}{2}\geqslant(j-1)-\frac{1}{2}=\frac{2j-3}{2},\cdots,$$

$$a_n-a_1-\frac{1}{2}\geqslant(n-1)-\frac{1}{2}=\frac{2n-3}{2},$$

且 $n\geqslant 6$,因此

$$\frac{1}{2}\left(a_2-a_1-\frac{1}{2}\right)\cdots\left(a_n-a_1-\frac{1}{2}\right)\geqslant\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\cdot\frac{7}{2}\cdot\frac{9}{2}\cdot\cdots\cdot\frac{2n-3}{2}$$
$$\geqslant\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\cdot\frac{7}{2}\cdot\frac{9}{2}$$
$$=\frac{15\times63}{64}>1.$$

由于 n 是偶数,因此

$$f\left(a_1+\frac{1}{2}\right)=-\frac{1}{2}\left(a_2-a_1-\frac{1}{2}\right)\cdots\left(a_n-a_1-\frac{1}{2}\right)+1<-1+1=0,$$

矛盾,因此当 n 为偶数且 $n\geqslant6$ 时,$f(x)$在 $\mathbf{Q}$ 上不可约。 ■

(3) **解** 当 $n=2$ 或 4 时,$f(x)$有可能在 $\mathbf{Q}$ 上可约。例如,$(x-1)(x+1)+1=x^2$,

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

例 15 设 $f(x)=(x-a_1)^2(x-a_2)^2\cdots(x-a_n)^2+1$,其中 $a_1,a_2,\cdots,a_n$ 是两两不等的整数。证明 $f(x)$在 $\mathbf{Q}$ 上不可约。

证明 假如 $f(x)$在 $\mathbf{Q}$ 上可约,则

$$f(x)=g_1(x)g_2(x),\deg g_i(x)<2n,g_i(x)\in\mathbf{Z}[x],i=1,2.$$

x 用 a_j 代入,从上式得

$$1=f(a_j)=g_1(a_j)g_2(a_j),j=1,2,\cdots,n.$$

于是 $g_1(a_j)$与 $g_2(a_j)$同为 1,或同为 -1。

由于 $f(x)$没有实根,因此 $g_1(x)$和 $g_2(x)$都没有实根。从而 $g_i(a_1),g_i(a_2),\cdots,g_i(a_n)$同号,$i=1,2$。于是不妨设 $g_i(a_1)=g_i(a_2)=\cdots=g_i(a_n)=1,i=1,2$。

情形 1 $g_1(x)$与 $g_2(x)$中有一个的次数小于 n。不妨设 $\deg g_1(x)<n$,由于 $g_1(a_j)-1=0,j=1,2,\cdots,n$,因此多项式 $g_1(x)-1$ 有 n 个不同的根。于是 $g_1(x)-1=0$。从而 $f(x)=g_2(x)$,这与 $\deg g_2(x)<2n$ 矛盾。

情形 2 $g_1(x)$与 $g_2(x)$的次数都等于 n。由于 $a_1,a_2,\cdots,a_n$ 都是 $g_i(x)-1$ 的根,且 $g_i(x)-1$的首项系数为 1,因此

$$g_i(x)-1=(x-a_1)(x-a_2)\cdots(x-a_n),i=1,2.$$

从而

$$f(x)=[(x-a_1)(x-a_2)\cdots(x-a_n)+1]^2$$
$$=(x-a_1)^2(x-a_2)^2\cdots(x-a_n)^2+1+2(x-a_1)(x-a_2)\cdots(x-a_n).$$

由此推出,$2(x-a_1)(x-a_2)\cdots(x-a_n)=0$,矛盾。

由于 $\deg g_1(x)+\deg g_2(x)=\deg f(x)=2n$,因此只有上述两种可能的情形。从而

$f(x)$在 **Q** 上不可约。 ■

例 16 有理系数多项式 $f(x)=x^4+ux^2+v$ 何时在 **Q** 上可约?

解 先寻找 $f(x)$在 **Q** 上可约的必要条件,设 $f(x)$在 **Q** 上可约,则 $f(x)$有一次因式或者有两个二次因式。

情形 1 $f(x)$有一次因式。此时 $f(x)$有一个有理根 t,从而 t^2 是二次多项式 x^2+ux+v 的有理根。于是判别式 u^2-4v 是一个有理数的平方。

情形 2 $f(x)$有两个二次因式。此时

$$f(x)=(a_2x^2+a_1x+a_0)(b_2x^2+b_1x+b_0),a_2\neq 0,b_2\neq 0.$$

比较系数,得

$$\begin{cases}1=a_2b_2,\\0=a_2b_1+a_1b_2,\\u=a_2b_0+a_1b_1+a_0b_2,\\0=a_1b_0+a_0b_1,\\v=a_0b_0.\end{cases}$$

不妨取 $a_2=1,b_2=1$。于是 $b_1=-a_1,u=b_0-a_1^2+a_0,a_1(b_0-a_0)=0,v=a_0b_0$。

若 $a_1=0$,则 $b_1=0,u=b_0+a_0,v=a_0b_0$。于是

$$u^2-4v=(b_0+a_0)^2-4a_0b_0=(b_0-a_0)^2.$$

若 $a_1\neq 0$,则 $b_0=a_0,u=2a_0-a_1^2,v=a_0^2$。于是

$$\pm 2\sqrt{v}-u=a_1^2.$$

综上所述,$f(x)$在 **Q** 上可约的必要条件是:u^2-4v 是一个有理数的平方;或者 v 是一个有理数的平方,且 $\pm 2\sqrt{v}-u$ 是有理数的平方。

下面来证上述条件是 $f(x)$在 **Q** 上可约的充分条件。

若 $u^2-4v=d^2$,则 $4v=u^2-d^2=(u+d)(u-d)$。从而

$$\begin{aligned}f(x)&=x^4+ux^2+\frac{u+d}{2}\cdot\frac{u-d}{2}\\&=\left(x^2+\frac{u+d}{2}\right)\left(x^2+\frac{u-d}{2}\right).\end{aligned}$$

因此 $f(x)$在 **Q** 上可约。

若 $v=a_0^2$,且 $\pm 2\sqrt{v}-u=a_1^2$,则 $2a_0-a_1^2=u$,从而

$$\begin{aligned}(x^2+a_1x+a_0)(x^2-a_1x+a_0)&=x^4+(2a_0-a_1^2)x^2+a_0^2\\&=x^4+ux^2+v.\end{aligned}$$

因此 $f(x)$在 **Q** 上可约。

至此我们得到了 $f(x)$在 $\mathbf{Q}$ 上可约的充分必要条件是：u^2-4v 是一个有理数的平方；或者 v 是一个有理数的平方，且 $\pm 2\sqrt{v}-u$ 是有理数的平方。

例 17 设 $p(x)$是 n 次有理系数多项式，n 为大于 1 的奇数，且 $p(x)$在 $\mathbf{Q}$ 上不可约。证明：如果 c_1 和 c_2 是 $p(x)$的两个不同的复根，那么 c_1+c_2 不是有理数。

证明 记 $c_1+c_2=c$。假设 c 是有理数，由于

$$0 = p(c_2) = p(c-c_1).$$

因此 c_1 是多项式 $g(x):=p(c-x)$的一个复根，由于 c 是有理数，因此 $g(x)$是有理系数多项式。由于 $g(x)$与 $p(x)$有公共复根 c_1，因此它们在 $\mathbf{C}[x]$中有公共的一次因式 $x-c_1$，从而不互素。于是它们在 $\mathbf{Q}[x]$中也不互素，由于 $p(x)$在 $\mathbf{Q}$ 上不可约，因此 $p(x)\mid g(x)$。从而存在有理系数多项式 $h(x)$使得 $g(x)=p(x)h(x)$。由于 $g(x)$与 $p(x)$的次数相等，因此 $h(x)$是非零有理数。由于 n 是奇数，因此 $g(x)$的首项系数是 $p(x)$的首项系数的相反数。从而 $h(x)=-1$，于是 $g(x)=-p(x)$。x 用 $\frac{c}{2}$ 代入得，$g(\frac{c}{2})=-p(\frac{c}{2})$。又 $g(\frac{c}{2})=p(c-\frac{c}{2})=p(\frac{c}{2})$，从而 $p(\frac{c}{2})=0$。于是 $p(x)$在 $\mathbf{Q}[x]$中有一次因式 $x-\frac{c}{2}$。由于 $\deg p(x)=n>1$，因此 $p(x)$在 $\mathbf{Q}$ 上可约，矛盾。所以 c 不是有理数。 ■

点评 例 17 的证明的思路是利用 c_2 是 $p(x)$的复根，得出 $0=p(c_2)=p(c-c_1)$，由此受到启发去考虑多项式 $g(x):=p(c-x)$，使得 c_1 是 $g(x)$的一个复根，从而 c_1 是 $p(x)$与 $g(x)$的一个公共复根。

* **例 18** 用 $\mathbf{Z}[x]$表示所有整系数多项式组成的集合，证明：对于多项式的加法和乘法，$\mathbf{Z}[x]$成为一个环，且它是整环。

证明 $\mathbf{Z}[x]$是 $\mathbf{Q}[x]$的非空子集。显然 $\mathbf{Z}[x]$对于多项式的减法和乘法都封闭，因此$\mathbf{Z}[x]$是 $\mathbf{Q}[x]$的子环。显然 $\mathbf{Q}[x]$的单位元 1 也是 $\mathbf{Z}[x]$的单位元。由于 $\mathbf{Q}[x]$是交换环，且没有非平凡的零因子，因此 $\mathbf{Z}[x]$也是交换环，且没有非平凡的零因子。从而 $\mathbf{Z}[x]$是整环。 ■

* **例 19** 证明：$\mathbf{Z}[x]$的可逆元只有 ± 1。

证明 设 $g(x)$是 $\mathbf{Z}[x]$的可逆元，则存在 $h(x)\in\mathbf{Z}[x]$，使得 $g(x)h(x)=1$。从而$g(x)$是非零整数 a，$h(x)$是非零整数 b。从 $ab=1$ 得出 $a=\pm 1$。 ■

* **例 20** 证明：在 $\mathbf{Z}[x]$中，$f(x)$与 $g(x)$相伴的充分必要条件是 $f(x)=\pm g(x)$。

证明 充分性是显然的。下面证必要性，由于 $f(x)$与 $g(x)$相伴，因此存在 $h_i(x)\in\mathbf{Z}[x]$，$i=1,2$，使得

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

从而有

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

若 $f(x)=0$，则 $g(x)=0$，于是结论成立。

若 $f(x)\neq 0$，则 $1=h_1(x)h_2(x)$。于是 $h_1(x)$ 是 $\mathbf{Z}[x]$ 的可逆元，从而 $h_1(x)=\pm 1$。因此 $f(x)=\pm g(x)$。 ■

* **例 21** 一个整系数多项式 $p(x)$（$p(x)\neq 0$，且 $p(x)\neq\pm 1$），如果在 $\mathbf{Z}[x]$ 中的因式只有 ± 1（即 $\mathbf{Z}[x]$ 的可逆元）和 $\pm p(x)$（即 $p(x)$ 的相伴元），那么称 $p(x)$ 是 $\mathbf{Z}$ 上的**不可约多项式**；否则称它在 $\mathbf{Z}$ 上**可约**。试问：$\mathbf{Z}[x]$ 中的一次多项式是否一定在 $\mathbf{Z}$ 上不可约？

解 不一定。例如，$x-3$ 在 $\mathbf{Z}$ 上是不可约的，而 $2x-6$ 的因式 2 和 $x-3$ 都既不等于 ± 1，也不等于 $\pm(2x-6)$，因此 $2x-6$ 在 $\mathbf{Z}$ 上可约。

点评 从例 21 看到，一次多项式 $2x-6$ 虽然不能分解成两个次数较低的多项式的乘积，但它在 $\mathbf{Z}$ 上是可约的。这表明虽然在数域 K 上的一元多项式环 $K[x]$ 中，$p(x)$ 不可约的充分必要条件是它不能分解成两个次数较低的多项式的乘积，但是不宜把“不能分解成两个次数较低的多项式的乘积”作为不可约多项式的定义，否则很容易误认为 $\mathbf{Z}[x]$ 中的不可约多项式的定义也是不能分解成两个次数较低的多项式的乘积。“因式只有可逆元和相伴元”才是不可约多项式的本质。一般地，在整环 R 中，一个元素 a（$a\neq 0$，且 a 不是可逆元），如果它的因子只有可逆元和 a 的相伴元，那么称 a 是**不可约**的；否则称 a 是**可约**的。这个定义可参看《抽象代数基础（第二版）》（丘维声编著）第 115 页。

* **例 22** 证明：一个次数大于 0 的整系数多项式 $p(x)$ 如果在 $\mathbf{Z}$ 上不可约，那么它在 $\mathbf{Q}$ 上也不可约。

证明 假如 $p(x)$ 在 $\mathbf{Q}$ 上可约，则据本节的推论 1 得，$p(x)=g_1(x)g_2(x)$，$\deg g_i(x)<\deg p(x)$，$g_i(x)\in\mathbf{Z}[x]$，$i=1,2$。$p(x)$ 的因式 $g_1(x)$ 既不等于 $\pm p(x)$，也不等于 ± 1（否则 $g_2(x)$ 等于 $\pm p(x)$，这不可能），于是 $p(x)$ 在 $\mathbf{Z}$ 上可约，矛盾。因此 $p(x)$ 在 $\mathbf{Q}$ 上不可约。 ■

点评 例 22 的逆命题不成立。例如，一次多项式 $2x-6$ 在 $\mathbf{Q}$ 上是不可约的，但它在 $\mathbf{Z}$ 上可约。对于本原多项式，逆命题才成立，见下面的例 23。

* **例 23** 证明：一个次数大于 0 的本原多项式 $p(x)$ 在 $\mathbf{Q}$ 上不可约当且仅当它在 $\mathbf{Z}$ 上不可约。

证明 充分性由例 22 立即得到。下面来证必要性。

假如 $p(x)$ 在 $\mathbf{Z}$ 上可约，则 $p(x)$ 在 $\mathbf{Z}[x]$ 中有因式 $g(x)$，它既不等于 ± 1，也不等于 $\pm p(x)$。设 $p(x)=g(x)h(x)$，其中 $h(x)\in\mathbf{Z}[x]$。由于 $p(x)$ 是本原多项式，因此 $\deg g(x)>0$。从而

$$\deg h(x)<\deg p(x).$$

同理，$\deg h(x)>0$，从而 $\deg g(x)<\deg p(x)$。于是 $p(x)$ 在 $\mathbf{Q}$ 上可约，矛盾。因此 $p(x)$ 在 $\mathbf{Z}$ 上不可约。 ■

* **例 24** 证明：一个次数大于 0 的整系数多项式 $p(x)$ 如果在 $\mathbf{Z}$ 上不可约，那么它一定是本原多项式。

证明 假如 $p(x)$ 不是本原多项式，则它的各项系数有异于 ± 1 的公因数 m，于是 $p(x)=mg(x)$，又由于 $\deg\ p(x)>0$，因此 $m\neq\pm p(x)$。于是 $p(x)$ 在 $\mathbf{Z}$ 上可约，矛盾。因此 $p(x)$ 是本原多项式。 ■

习题 7.8

1. 求下列多项式的全部有理根：

(1) $2x^3+x^2-3x+1$；　　(2) $2x^4-x^3-19x^2+9x+9$。

2. 判断下列整系数多项式在有理数域上是否不可约：

(1) $x^4-6x^3+2x^2+10$；　　(2) x^3-5x^2+4x+3；

(3) x^3+x^2-3x+2；　　(4) $2x^3-x^2+x+1$；

(5) $7x^5+18x^4+6x-6$；　　(6) x^4-2x^3+2x-3；

(7) x^5+5x^3+1；　　(8) x^p+px^2+1，p 为奇素数；

(9) x^p+px^r+1，p 为奇素数，$0\leqslant r\leqslant p$；　　(10) x^4-5x+1。

3. 设 $n>1$，证明：n 个两两不等的素数的几何平均数一定是无理数。

4. 设 m,n 都是正整数，且 $m<n$；$p_1,p_2,\cdots,p_t$ 是两两不等的素数，$t\geqslant 1$。证明：如果 $f(x)$ 是 $\mathbf{Q}$ 上的 m 次多项式，那么 $\sqrt[n]{p_1p_2\cdots p_t}$ 不是 $f(x)$ 的实根。

5. 设 $f(x)=x^3+ax^2+bx+c$ 是整系数多项式，证明：如果 $(a+b)c$ 是奇数，那么 $f(x)$ 在有理数域上不可约。

6. 设 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是一个次数大于 0 的整系数多项式，证明：如果存在一个素数 p，使得

$$p\mid a_0,p\mid a_1,\cdots,p\mid a_{r-1},p\nmid a_r,p\nmid a_n,$$

且 $p^2\nmid a_0$，那么 $f(x)$ 有一个次数大于或等于 r 的在 $\mathbf{Q}$ 上不可约的因式。

* 7. 设 $f(x)=a_{2n+1}x^{2n+1}+\cdots+a_1x+a_0$ 是一个次数为 $2n+1$ 的整系数多项式。证明：如果存在一个素数 p，使得

$$p^2\mid a_0,\cdots,p^2\mid a_n,p\mid a_{n+1},\cdots,p\mid a_{2n},p\nmid a_{2n+1},$$

且 $p^3\nmid a_0$，那么 $f(x)$ 在 $\mathbf{Q}$ 上不可约。

8. 设 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是一个次数为 n 的整系数多项式。证明：如果 a_0，$a_n+\cdots+a_1+a_0$，$(-1)^na_n+\cdots-a_1+a_0$ 都不能被 3 整除，那么 $f(x)$ 没有整数根。

9. 在 $\mathbf{Q}[x]$ 中把 $g(x)=x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$ 因式分解。

10. 设 n 是大于 1 的整数，$g(x)=\sum_{i=0}^{n-1}x^i$。证明：若 n 不是素数，则 $g(x)$ 在 $\mathbf{Q}$ 上可约。

11. 证明：$x^{105}-9$ 在有理数域上不可约。

7.9 n 元多项式环

7.9.1 内容精华

一、n 元多项式的概念

定义 1 设 K 是一个数域，用不属于 K 的 n 个符号 $x_1,x_2,\cdots,x_n$ 作表达式

$$\sum_{i_1,i_2,\cdots,i_n}a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}, \tag{1}$$

其中 $a_{i_1i_2\cdots i_n}\in K$，$i_1,i_2,\cdots,i_n$ 是非负整数，(1)式中的每一项称为一个**单项式**，$a_{i_1i_2\cdots i_n}$ 称为**系数**；如果只有有限多个单项式的系数不为 0，并且两个这种形式的表达式相等当且仅当它们除去系数为 0 的单项式外含有完全相同的单项式，那么称表达式(1)是**数域 K 上的 n 元多项式**，把符号 $x_1,x_2,\cdots,x_n$ 称为 **n 个无关不定元**。

关于 n 元多项式的定义应当把握两点：它是具有形式(1)的表达式；两个 n 元多项式相等当且仅当它们含有完全相同的单项式(除去系数为 0 的单项式)。第二点使得 n 元多项式成为最基本的概念。

在数域 K 上的 n 元多项式中，如果两个单项式的 $x_j(j=1,2,\cdots,n)$ 的幂指数都对应相等，那么这两个单项式称为**同类项**。在 n 元多项式中，我们把同类项合并成一项，从而各个单项式都是不同类的。

数域 K 上有一个 n 元多项式，如果它的所有系数全为 0，那么称它为**零多项式**，记为 0。

n 元多项式的重要特点之一是它有次数的概念。对于单项式，把它的各个不定元的幂指数之和称为这个单项式的**次数**。对于一个 n 元多项式 $f(x_1,x_2,\cdots,x_n)$，把它的系数不为 0 的单项式的次数的最大值称为这个 n 元多项式的**次数**，记作 $\deg f$，零多项式的次数规定为 $-\infty$。

设一个 n 元多项式 $f(x_1,x_2,\cdots,x_n)$ 的次数为 m，有可能有几个单项式的次数都为 m，因此无法利用单项式的次数来给单项式排序。从字典的排序方法受到启发，把每一个单项式的各个不定元的幂指数写成一个 n 元有序数组，对于 n 元有序非负整数组规定一个先后顺序：

$(i_1,i_2,\cdots,i_n)$ **先于** $(j_1,j_2,\cdots,j_n)$ 当且仅当

$$i_1 = j_1, \cdots, i_{s-1} = j_{s-1}, i_s > j_s,$$

记作$(i_1, i_2, \cdots, i_n) > (j_1, j_2, \cdots, j_n)$。

显然，n 元有序非负整数组的先于关系具有传递性。于是利用这个先于关系就可以给一个 n 元多项式的各个单项式排序：

单项式 $a_{i_1 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ 排在单项式 $b_{j_1 \cdots j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$ 的前面当且仅当$(i_1, i_2, \cdots, i_n) > (j_1, j_2, \cdots, j_n)$。这种排序方法称为**字典排列法**。按字典排列法写出来的第一个系数不为 0 的单项式称为 n 元多项式的**首项**。要注意，首项不一定具有最大的次数。

二、n 元多项式的运算

数域 K 上所有 n 元多项式组成的集合记作 $K[x_1, x_2, \cdots, x_n]$。在这个集合中规定加法运算为把同类项的系数相加，规定乘法运算为

$$\Big(\sum_{i_1, i_2, \cdots, i_n} a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}\Big)\Big(\sum_{j_1, j_2, \cdots, j_n} b_{j_1 j_2 \cdots j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}\Big)$$
$$:= \sum_{s_1, s_2, \cdots, s_n} c_{s_1 s_2 \cdots s_n} x_1^{s_1} x_2^{s_2} \cdots x_n^{s_n}, \tag{2}$$

其中
$$c_{s_1 s_2 \cdots s_n} = \sum_{i_1 + j_1 = s_1} \sum_{i_2 + j_2 = s_2} \cdots \sum_{i_n + j_n = s_n} a_{i_1 i_2 \cdots i_n} b_{j_1 j_2 \cdots j_n}.$$

容易验证 $K[x_1, x_2, \cdots, x_n]$成为一个环，它有单位元 1，它是交换环，称它为数域 K 上 n 元多项式环。

n 元多项式的运算与次数有什么关系？显然有

$$\deg(f+g) \leqslant \max\{\deg f, \deg g\}. \tag{3}$$

乘法运算与次数的关系是什么？在数域 K 上的一元多项式环 $K[x]$中，有 $\deg(fg) = \deg f + \deg g$。证明此等式成立的关键是先证明 fg 的首项等于 f 的首项与 g 的首项的乘积。由此受到启发，在 $K[x_1, x_2, \cdots, x_n]$中，先证明下述结论：

定理 1 在 $K[x_1, x_2, \cdots, x_n]$中，两个非零多项式的乘积的首项等于它们的首项的乘积，从而两个非零多项式的乘积仍是非零多项式，即 $K[x_1, x_2, \cdots, x_n]$是无零因子环。

其次我们要引进齐次多项式的概念：

定义 2 如果数域 K 上的 n 元多项式 $g(x_1, x_2, \cdots, x_n)$的每个系数不为 0 的单项式都是 m 次的，则称该多项式为 ***m* 次齐次多项式**。

由定义 2 得，零多项式可以看成是任意次数的齐次多项式。

第 6 章 6.1 节讲的数域 K 上的 n 元二次型就是数域 K 上的 n 元二次齐次多项式。

显然，$K[x_1, x_2, \cdots, x_n]$中两个齐次多项式的乘积仍是齐次多项式，它的次数等于这两个多项式的次数的和。

对于任何一个 n 元多项式 $f(x_1, x_2, \cdots, x_n)$，如果把 f 中次数相同的单项式写在一起，

那么 f 可以唯一地表示成

$$f(x_1,x_2,\cdots,x_n)=\sum_{i=0}^{m}f_i(x_1,x_2,\cdots,x_n). \tag{4}$$

其中 $m=\deg f$，$f_i(x_1,x_2,\cdots,x_n)$ 是 i 次齐次多项式，称它为 $f(x_1,x_2,\cdots,x_n)$ 的 **i 次齐次成分**。

利用(4)式可以证明下述结论：

定理 2 在 $K[x_1,x_2,\cdots,x_n]$ 中，

$$\deg fg=\deg f+\deg g. \tag{5}$$

三、数域 K 上 n 元多项式环 $K[x_1,x_2,\cdots,x_n]$ 的通用性质

n 元多项式之所以成为最基本的概念，是因为 n 元多项式环 $K[x_1,x_2,\cdots,x_n]$ 具有通用性质。即

定理 3 设 K 是一个数域，R 是一个有单位元的交换环，并且 R 可以看成是 K 的一个扩环(即 R 有一个子环 R_1 与 K 同构，且 R 的单位元是 R_1 的单位元)，K 到 R_1 的同构映射记作 τ，设 $t_1,t_2,\cdots,t_n$ 是 R 的元素，令

$$\sigma_{t_1,t_2,\cdots,t_n}:K[x_1,x_2,\cdots,x_n]\longrightarrow R$$

$$f(x_1,x_2,\cdots,x_n)=\sum_{i_1,\cdots,i_n}a_{i_i\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}\longmapsto\sum_{i_1,\cdots,i_n}\tau(a_{i_1\cdots i_n})t_1^{i_1}\cdots t_n^{i_n},$$

则 $\sigma_{t_1,t_2,\cdots,t_n}$ 是 $K[x_1,x_2,\cdots,x_n]$ 到 R 的一个映射，它使得

$$\sigma_{t_1,t_2,\cdots,t_n}(x_i)=t_i,\ i=1,2,\cdots,n;$$

把 $f(x_1,x_2,\cdots,x_n)$ 在此映射下的象记作 $f(t_1,t_2,\cdots,t_n)$，如果

$$f(x_1,x_2,\cdots,x_n)+g(x_1,x_2,\cdots,x_n)=h(x_1,x_2,\cdots,x_n),$$

$$f(x_1,x_2,\cdots,x_n)g(x_1,x_2,\cdots,x_n)=p(x_1,x_2,\cdots,x_n),$$

那么

$$f(t_1,t_2,\cdots,t_n)+g(t_1,t_2,\cdots,t_n)=h(t_1,t_2,\cdots,t_n),$$

$$f(t_1,t_2,\cdots,t_n)g(t_1,t_2,\cdots,t_n)=p(t_1,t_2,\cdots,t_n),$$

即映射 $\sigma_{t_1,t_2,\cdots,t_n}$ 保持加法和乘法运算。映射 $\sigma_{t_1,t_2,\cdots,t_n}$ 称为 $x_1,x_2,\cdots,x_n$ 用 $t_1,t_2,\cdots,t_n$ **代入**。

证明的关键是由于 $K[x_1,x_2,\cdots,x_n]$ 中一个 n 元多项式 $f(x_1,x_2,\cdots,x_n)$ 的表法唯一，因此上述定义的由 $K[x_1,x_2,\cdots,x_n]$ 到 R 的对应法则 $\sigma_{t_1,t_2,\cdots,t_n}$ 是一个映射。定理 3 的其余结论的证明都是很容易的。

定理 3 的意义在于：只要把数域 K 上 n 元多项式环 $K[x_1,x_2,\cdots,x_n]$ 的结构研究清楚了，那么对于任意一个可以看成 K 的扩环的有单位元的交换环 R，从 $K[x_1,x_2,\cdots,x_n]$ 中有关加法与乘法的等式可以得到 R 中许多有关加法与乘法的等式，达到事半功倍的效果。

特别地，$K[x_1,x_2,\cdots,x_n]$ 中所有零次多项式添上零多项式组成的子集 S 是

$K[x_1,x_2,\cdots,x_n]$的一个子环，显然，$\tau:a\longmapsto a$ 是 K 到 S 的一个同构映射，因此 $K[x_1,x_2,\cdots,x_n]$可看成是 K 的一个扩环，从而 $x_1,x_2,\cdots,x_n$ 可以用环 $K[x_1,x_2,\cdots,x_n]$中任意 n 个元素代入，且这种代入是保持加法与乘法运算的。

四、n 元多项式函数

设 $f(x_1,x_2,\cdots,x_n)\in K[x_1,x_2,\cdots,x_n]$，对于数域 K 中任意 n 个元素 $c_1,c_2,\cdots,c_n$，将 $x_1,x_2,\cdots,x_n$ 用 $c_1,c_2,\cdots,c_n$ 代入，得到 $f(c_1,c_2,\cdots,c_n)\in K$。于是 n 元多项式 $f(x_1,x_2,\cdots,x_n)$诱导了集合 K^n 到 K 的一个映射：

$$\begin{aligned} f:K^n &\longrightarrow K\\ (c_1,c_2,\cdots,c_n) &\longmapsto f(c_1,c_2,\cdots,c_n). \end{aligned}\tag{6}$$

把这个映射 f 称为**数域 K 上的一个 n 元多项式函数**。

显然，零多项式确定的函数是零函数，自然要问：非零多项式诱导的函数是否一定不是零函数？这对于数域 K 上的 n 元非零多项式，回答是肯定的。

定理 4 设 $h(x_1,x_2,\cdots,x_n)$是数域 K 上的 n 元非零多项式，则它诱导的 n 元多项式函数 h 不是零函数。

利用定理 4 立即得到：

定理 5 设 K 是数域，在 $K[x_1,x_2,\cdots,x_n]$中，两个 n 元多项式 $f(x_1,x_2,\cdots,x_n)$与 $g(x_1,x_2,\cdots,x_n)$相等，当且仅当它们诱导的多项式函数 f 与 g 相等。

我们把数域 K 上所有 n 元多项式函数组成的集合记作 K_{npol}，在这个集合中规定加法运算是函数的加法，规定乘法运算是函数的乘法，即 $\forall(c_1,c_2,\cdots,c_n)\in K^n$，令

$$\begin{aligned} (f+g)(c_1,c_2,\cdots,c_n) &:= f(c_1,c_2,\cdots,c_n)+g(c_1,c_2,\cdots,c_n),\\ (fg)(c_1,c_2,\cdots,c_n) &:= f(c_1,c_2,\cdots,c_n)g(c_1,c_2,\cdots,c_n), \end{aligned}$$

如果

$$\begin{aligned} f(x_1,x_2,\cdots,x_n)+g(x_1,x_2,\cdots,x_n) &= h(x_1,x_2,\cdots,x_n),\\ f(x_1,x_2,\cdots,x_n)g(x_1,x_2,\cdots,x_n) &= p(x_1,x_2,\cdots,x_n), \end{aligned}$$

那么有

$$\begin{aligned} f(c_1,c_2,\cdots,c_n)+g(c_1,c_2,\cdots,c_n) &= h(c_1,c_2,\cdots,c_n),\\ f(c_1,c_2,\cdots,c_n)g(c_1,c_2,\cdots,c_n) &= p(c_1,c_2,\cdots,c_n), \end{aligned}$$

因此上述定义的 $f+g$ 是由多项式 $h(x_1,x_2,\cdots,x_n)$诱导的 n 元多项式函数，fg 是由多项式 $p(x_1,x_2,\cdots,x_n)$诱导的 n 元多项式函数，从而上述定义的加法和乘法的确是 K_{npol}的两种运算。容易验证，K_{npol}成为一个有单位元的交换环，称它为**数域 K 上的 n 元多项式函数环**。由 n 元多项式 $f(x_1,x_2,\cdots,x_n)$对应到它诱导的 n 元多项式函数 f，这个对应法则 σ 是 $K[x_1,x_2,\cdots,x_n]$到 K_{npol}的一个映射，显然它是满射；由定理 5 得出，σ 也是单射，从而 σ 是双射。由上述内容知道，σ 保持加法与乘法，因此 σ 是一个同构映射，从而环$K[x_1,x_2,\cdots,x_n]$与

环 K_{npol}是同构的。于是我们可以把数域 K 上的 n 元多项式 $f(x_1,x_2,\cdots,x_n)$与 n 元多项式函数 f 等同看待。注意:n 元多项式是指表达式,n 元多项式函数是指映射,只有在证明了数域 K 上的 n 元多项式环 $K[x_1,x_2,\cdots,x_n]$与 K 上的 n 元多项式函数环 K_{npol}同构之后,才能把 n 元多项式 $f(x_1,x_2,\cdots,x_n)$与由它诱导的 n 元多项式函数 f 等同看待。

设 $f(x_1,x_2,\cdots,x_n)\in K[x_1,x_2,\cdots,x_n]$,$K$ 是数域。如果有$(c_1,c_2,\cdots,c_n)\in K^n$ 使得 $f(c_1,c_2,\cdots,c_n)=0$,那么称$(c_1,c_2,\cdots,c_n)$是 n 元多项式$f(x_1,x_2,\cdots,x_n)$的一个**零点**。当 K 取实数域,若 $n=2$,则二元多项式 $f(x,y)$的零点组成的集合就是平面上的一条**代数曲线**,它也就是方程 $f(x,y)=0$ 表示的曲线;若 $n=3$,则三元多项式 $f(x,y,z)$的零点组成的集合是空间中的一个**代数曲面**,它也就是方程 $f(x,y,z)=0$ 表示的曲面。一般地,数域 K 上一组 n 元多项式,它们的公共零点组成的集合称为**代数簇**(algebraic variety)。研究代数簇是代数几何的一个基本内容。

五、数域 K 上 n 元多项式环的结构

研究数域 K 上一元多项式环 $K[x]$的结构,我们是以带余除法为出发点的。利用带余除法证明了 $K[x]$中两个多项式的最大公因式存在(可以用辗转相除法求出),并且最大公因式可以表示成这两个多项式的倍式和,进而得到两个多项式互素的充分必要条件是 1 可以表示成这两个多项式的倍式和,利用这个结论证明了不可约多项式的几个等价条件,最后证明了 $K[x]$中每一个次数大于 0 的多项式都能唯一地分解成有限多个不可约多项式的乘积,即证明了 $K[x]$中有唯一因式分解定理。从而把 $K[x]$的结构搞清楚了。

研究 $K[x]$的结构的上述途径是否适用于研究数域 K 上 n 元多项式环$K[x_1,x_2,\cdots,x_n]$的结构呢? 其中 $n>1$。

对于数域 K 上的一元多项式 $f(x)$,它的首项就是次数最高的项,因此把 $f(x)$的首项消去后,它的次数就降下来了。从而可以对作为被除式的多项式的次数作数学归纳法,证出 $K[x]$中有带余除法。

对于数域 K 上的 n 元多项式 $f(x_1,x_2,\cdots,x_n)$,当 $n>1$ 时,它的首项不一定是次数最高的项,因此把 $f(x_1,x_2,\cdots,x_n)$的首项消去后,它的次数不一定能降下来。从而当$n>1$时,$K[x_1,x_2,\cdots,x_n]$没有带余除法。1964 年,H. Hironaka 引进了 n 元多项式的除法算法。1965 年,B. Buchberger 使用除法算法对于 $K[x_1,x_2,\cdots,x_n]$中由单项式组成的乘法封闭集中,引进了项序的概念,使得多项式相除后所得的余式唯一确定。

由于当 $n>1$ 时,$K[x_1,x_2,\cdots,x_n]$中没有带余除法,因此研究它的结构就不能从带余除法出发。在 $K[x_1,x_2,\cdots,x_n]$中,整除的概念、不可约多项式的概念仍然是有的。

定义 3 在 $K[x_1,x_2,\cdots,x_n]$中,对于 f,g,如果有 h 使得 $f=hg$,那么称 g **整除** f,记

作 $g|f$；否则称 g **不能整除** f，记作 $g\nmid f$。当 g 整除 f 时，称 g 是 f 的一个**因式**，称 f 是 g 的一个**倍式**。

容易看出，在 $K[x_1,x_2,\cdots,x_n]$ 中，整除关系具有反身性、传递性，但是不具有对称性。

定义 4 在 $K[x_1,x_2,\cdots,x_n]$ 中，如果 $f|g$，且 $g|f$，那么称 f 与 g 是**相伴**的，记作 $f\sim g$。

利用 $K[x_1,x_2,\cdots,x_n]$ 中多项式乘积的次数公式容易证明：$f\sim g$ 当且仅当存在 $c\in K^*$ 使得 $f=cg$。

$K[x_1,x_2,\cdots,x_n]$ 中有了因式的概念，当然也就有两个多项式 f 与 g 的**公因式**的概念。类似于 $K[x]$，我们可以在 $K[x_1,x_2,\cdots,x_n]$ 中定义两个多项式 f 与 g 的**最大公因式**的概念，但是由于 $K[x_1,x_2,\cdots,x_n]$ 中没有带余除法，因此不可能有辗转相除法，从而暂时还不知道任意两个多项式是否一定有最大公因式存在，到后面我们再来回答这个问题。$K[x_1,x_2,\cdots,x_n]$ 中两个多项式的最大公因式如果是 K 中的非零数，那么称这两个多项式**互素**。

定义 5 $K[x_1,x_2,\cdots,x_n]$ 中次数大于 0 的 n 元多项式 $p(x_1,x_2,\cdots,x_n)$，如果它的因式只有 K 中的非零数以及它的相伴元，那么称 $p(x_1,x_2,\cdots,x_n)$ 是 ***K* 上的不可约多项式**；否则称 $p(x_1,x_2,\cdots,x_n)$ 是**可约的**。

由定义 5 和乘积多项式的次数公式立即得到：一次多项式都是不可约的。

命题 1 $K[x_1,x_2,\cdots,x_n]$ 中，次数大于 0 的多项式 $p(x_1,x_2,\cdots,x_n)$ 不可约当且仅当它不能分解成两个次数较低的多项式的乘积。

由命题 1 的充分性立即得到，$K[x_1,x_2,\cdots,x_n]$ 中次数大于 0 的多项式 $f(x_1,x_2,\cdots,x_n)$ 如果可约，那么它能分解成两个次数较低的多项式的乘积。如此下去，可得出：$f(x_1,x_2,\cdots,x_n)$ 能分解成有限多个不可约多项式的乘积。进一步可证明这种分解是唯一的，即如果 $f(x_1,x_2,\cdots,x_n)$ 有两种方式分解成不可约多项式的乘积：

$$f(x_1,x_2,\cdots,x_n)=p_1(x_1,x_2,\cdots,x_n)\cdots p_s(x_1,x_2,\cdots,x_n),$$

$$f(x_1,x_2,\cdots,x_n)=q_1(x_1,x_2,\cdots,x_n)\cdots q_t(x_1,x_2,\cdots,x_n),$$

那么 $s=t$，且经过适当排列因式的次序可使得

$$p_i(x_1,x_2,\cdots,x_n)\sim q_i(x_1,x_2,\cdots,x_n),\ i=1,2,\cdots,s.$$

于是在 $K[x_1,x_2,\cdots,x_n]$ 中也有唯一因式分解定理：

定理 6(唯一因式分解定理) $K[x_1,x_2,\cdots,x_n]$ 中每一个次数大于 0 的多项式 $f(x_1,x_2,\cdots,x_n)$ 都能唯一地分解成数域 K 上有限多个不可约多项式的乘积，所谓唯一性如上所述。

定理 6 可以从参考文献 21 的第三章§ 3.2 的推论 4 立即得到。

在 n 元多项式 $f(x_1,x_2,\cdots,x_n)$ 的分解式中，可以把每一个不可约因式的首项系数提出来，使它们成为首项系数为 1 的多项式，再把相同的不可约因式的乘积写成乘幂的形式，

于是 $f(x_1,x_2\cdots,x_n)$的分解式成为

$$f(x_1,\cdots,x_n)=ap_1^{r_1}(x_1,\cdots,x_n)\cdots p_m^{r_m}(x_1,\cdots,x_n). \tag{7}$$

其中 a 是 $f(x_1,\cdots,x_n)$的首项系数,$p_1(x_1,\cdots,x_n),\cdots,p_m(x_1,\cdots,x_n)$是两两不等的首项系数为 1 的不可约多项式,$r_1,\cdots,r_m$ 是正整数。分解式(7)称为 $f(x_1,x_2\cdots,x_n)$的**标准分解式**。

现在设 $f(x_1,\cdots,x_n),g(x_1,\cdots,x_n)$的标准分解式分别为

$$f(x_1,\cdots,x_n)=ap_1^{r_1}(x_1,\cdots,x_n)\cdots p_l^{r_l}(x_1,\cdots,x_n)p_{l+1}^{r_{l+1}}(x_1,\cdots,x_n)\cdots p_m^{r_m}(x_1,\cdots,x_n),$$

$$g(x_1,\cdots,x_n)=bp_1^{t_1}(x_1,\cdots,x_n)\cdots p_l^{t_l}(x_1,\cdots,x_n)q_{l+1}^{t_{l+1}}(x_1,\cdots,x_n)\cdots q_s^{t_s}(x_1,\cdots,x_n).$$

令

$$d(x_1,\cdots,x_n)=p_1^{u_1}(x_1,\cdots,x_n)\cdots p_l^{u_l}(x_1,\cdots,x_n),$$

其中 $u_i=\min\{r_i,t_i\},i=1,2,\cdots,l$。显然 $d(x_1,\cdots,x_n)$是 $f(x_1,\cdots,x_n)$与 $g(x_1,\cdots,x_n)$的一个公因式。任取 f 与 g 的一个次数大于 0 的公因式 $c(x_1,\cdots,x_n)$,在 $c(x_1,\cdots,x_n)$的标准分解式中任取一个不可约因式 $v(x_1,\cdots,x_n)$。由于 $v(x_1,\cdots,x_n)$是 f 与 g 的公共的不可约因式,因此 $v(x_1,\cdots,x_n)$必然等于某个 $p_j(x_1,\cdots,x_n)$,其中 $j\in\{1,2,\cdots,l\}$;并且 $v(x_1,\cdots,x_n)$在 $c(x_1,\cdots,x_n)$的标准分解式中的幂指数不超过 u_j。于是 $c(x_1,\cdots,x_n)\mid d(x_1,\cdots,x_n)$。这证明了 $d(x_1,\cdots,x_n)$是 $f(x_1,\cdots,x_n)$与 $g(x_1,\cdots,x_n)$的一个最大公因式,它的首项系数为 1,把它记作$(f(x_1,\cdots,x_n),g(x_1,\cdots,x_n))$。这也肯定地回答了前面提出的 $K[x_1,\cdots,x_n]$中任意两个多项式都存在最大公因式的问题。

由于把 n 元多项式分解成不可约因式的乘积没有统一的方法,因此求两个 n 元多项式的最大公因式是不容易的。

7.9.2 典型例题

例 1 将下列三元多项式按字典排列法排列各单项式的顺序。

(1) $f(x_1,x_2,x_3)=4x_1x_2^5x_3^2+5x_1^2x_2x_3-x_1^3x_3^4+x_1^3x_2+x_1x_2^4$;

(2) $g(x_1,x_2,x_3)=x_1^2x_2^3+x_2^2x_3^3+x_1^3x_3^2+x_1^4+x_1^2x_2^4+x_3^4$。

解 (1) $f(x_1,x_2,x_3)=x_1^3x_2-x_1^3x_3^4+5x_1^2x_2x_3+4x_1x_2^5x_3^2+x_1x_2^4$;

(2) $g(x_1,x_2,x_3)=x_1^4+x_1^3x_3^2+x_1^2x_2^4+x_1^2x_2^3+x_2^2x_3^3+x_3^4$。

例 2 把下述三元齐次多项式分解成两个三元齐次多项式的乘积。

$$f(x_1,x_2,x_3)=x_1^3+3x_1^2x_2+4x_1^2x_3+3x_1x_2^2+6x_1x_2x_3+4x_1x_3^2+2x_2^3+5x_2^2x_3+5x_2x_3^2+3x_3^3.$$

解 $f(x_1,x_2,x_3)$是三次齐次多项式,把它分解成两个齐次多项式的乘积,必然一个是

一次齐次多项式，另一个是二次齐次多项式。于是可设

$$f(x_1,x_2,x_3)=(x_1+ax_2+bx_3)(x_1^2+cx_2^2+dx_3^2+ex_1x_2+ux_1x_3+vx_2x_3).$$

比较系数得

$$\begin{aligned}&3=e+a, && 4=u+b, && 3=c+ae,\\ &6=v+au+be, && 4=d+bu, && 2=ac,\\ &5=av+bc, && 5=ad+bv, && 3=bd.\end{aligned}$$

取 $c=1$，则 $a=2$；取 $d=1$，则 $b=3$。从而

$$e=1,\ u=1,\ c=1,\ v=1,\ d=1.$$

因此

$$f(x_1,x_2,x_3)=(x_1+2x_2+3x_3)(x_1^2+x_2^2+x_3^2+x_1x_2+x_1x_3+x_2x_3).$$

例 3 设 $f(x_1,x_2,\cdots,x_n)$是数域 K 上一个齐次多项式。证明：

如果在 $K[x_1,x_2,\cdots,x_n]$中有

$$f(x_1,x_2,\cdots,x_n)=g(x_1,x_2,\cdots,x_n)h(x_1,x_2,\cdots,x_n),$$

那么 $g(x_1,x_2,\cdots,x_n)$和 $h(x_1,x_2,\cdots,x_n)$都是齐次多项式。

证明 假如 g 与 h 不全是齐次多项式，则不妨设 g 不是齐次多项式，于是有 $g=g_l+g_{l+1}+\cdots+g_r$，其中 $g_i(i=l,l+1,\cdots,r)$是 g 的 i 次齐次成分，且 $g_l\neq0,g_r\neq0,r>l$。设 $h=h_t+h_{t+1}+\cdots+h_s$，其中 $h_j(j=t,t+1,\cdots,s)$是 h 的 j 次齐次成分，且 $h_t\neq0,h_s\neq0$(有可能$s=t$，此时 h 是 t 次齐次多项式)。由已知条件得

$$f=gh=\Big(\sum_{i=l}^{r}g_i\Big)\Big(\sum_{j=t}^{s}h_j\Big)=\sum_{i=l}^{r}\sum_{j=t}^{s}g_ih_j,$$

其中 $g_lh_t\neq0,g_rh_s\neq0$。由于 g_lh_t 是 gh 的次数最低的齐次成分，因此 g_lh_t 不会与其他 g_ih_j 相消。又由于 g_rh_s 是 gh 的次数最高的齐次成分，因此 g_rh_s 也不会与其他 g_ih_j 相消。由于 $l<r,t\leqslant s$，因此 $l+t<r+s$。于是 gh 至少有两个非零的齐次成分，这与 f 是齐次多项式矛盾。所以 g 与 h 都是齐次多项式。 ■

点评 例 3 表明：在 $K[x_1,x_2,\cdots,x_n]$中，一个齐次多项式如果能分解成两个多项式的乘积，那么这两个多项式也都是齐次多项式。

例 4 证明：在数域 K 上的 n 元多项式环 $K[x_1,x_2,\cdots,x_n]$中，一个非零多项式 $f(x_1,x_2,\cdots,x_n)$是 m 次齐次多项式的充分必要条件为对一切 $t\in K$，有

$$f(tx_1,tx_2,\cdots,tx_n)=t^mf(x_1,x_2,\cdots,x_n). \tag{8}$$

证明 必要性。设 $f(x_1,x_2,\cdots,x_n)$是 m 次齐次多项式，即

$$f(x_1,x_2,\cdots,x_n)=\sum_{i_1,i_2,\cdots,i_n}a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n},$$

其中 $i_1+i_2+\cdots+i_n=m$。任取 $t\in K$，不定元 $x_1,x_2,\cdots,x_n$ 用 $tx_1,tx_2,\cdots,tx_n$ 代入，从上式得

$$f(tx_1,tx_2,\cdots,tx_n)=\sum_{i_1,\cdots,i_n}a_{i_1i_2\cdots i_n}(tx_1)^{i_1}(tx_2)^{i_2}\cdots(tx_n)^{i_n}$$
$$=t^mf(x_1,x_2,\cdots,x_n).$$

充分性。设对一切 $t\in K$,有(8)式成立。将 $f(x_1,\cdots,x_n)$写成 $f=f_0+f_1+\cdots+f_s$,其中 f_i 是 f 的 i 次齐次成分,$i=0,1,\cdots,s$。任取 $t\in K,x_1,x_2,\cdots,x_n$ 用 $tx_1,tx_2,\cdots,tx_n$ 代入,从上式得

$$f(tx_1,\cdots,tx_n)=f_0(tx_1,\cdots,tx_n)+f_1(tx_1,\cdots,tx_n)+\cdots+f_s(tx_1,\cdots,tx_n).$$

根据刚证的必要性以及充分性的假设得

$$t^mf(x_1,\cdots,x_n)=f_0(tx_1,\cdots,tx_n)+tf_1(x_1,\cdots,x_n)+\cdots+t^sf_s(x_1,\cdots,x_n). \tag{9}$$

将 $f=f_0+f_1+\cdots+f_s$ 代入(9)式的左端,并且根据两个 n 元多项式相等的定义,得到

$$t^mf_i(x_1,\cdots,x_n)=t^if_i(x_1,\cdots,x_n),\quad i=0,1,\cdots,s. \tag{10}$$

任取 $i\in\{0,1,\cdots,s\}$,且 $i\neq m$,如果 $f_i\neq0$,那么从(10)式两边消去 f_i 得,$t^m=t^i,\forall t\in K$。由于 K 是数域,因此有 $x^m=x^i$。这与 $i\neq m$ 矛盾。因此当 $i\neq m$ 时,$f_i=0$。从而 $f=f_m$,于是 f 是 m 次齐次多项式。 ■

点评 例 4 给出了数域 K 上 m 次齐次多项式(或 m 次齐次多项式函数)的一个刻画,它很有用。

例 5 设 $f(x,y,z),g(x,y,z)$都是实数域上的三元多项式,且 $g(x,y,z)$不是零多项式,证明:如果 $g(x,y,z)$的任一非零点都是 $f(x,y,z)$的零点,那么 $f(x,y,z)$是零多项式。

证法一 对于 $g(x,y,z)$的任一非零点(b_1,b_2,b_3),有

$$fg(b_1,b_2,b_3)=f(b_1,b_2,b_3)g(b_1,b_2,b_3)=0.$$

对于 $g(x,y,z)$的任一零点(c_1,c_2,c_3),有

$$fg(c_1,c_2,c_3)=f(c_1,c_2,c_3)g(c_1,c_2,c_3)=0.$$

从而对一切$(a_1,a_2,a_3)\in\mathbf{R}^3$,有 $fg(a_1,a_2,a_3)=0$。于是 fg 是零函数,从而$f(x,y,z)g(x,y,z)$是零多项式。由于 $g(x,y,z)$不是零多项式,因此 $f(x,y,z)$是零多项式。 ■

证法二 假如 $f(x,y,z)$不是零多项式,又由已知条件,$g(x,y,z)$不是零多项式,于是 $f(x,y,z)g(x,y,z)$不是零多项式,从而 fg 不是零函数。因此存在$(c_1,c_2,c_3)\in\mathbf{R}^3$,使得 $fg(c_1,c_2,c_3)\neq0$,即 $f(c_1,c_2,c_3)g(c_1,c_2,c_3)\neq0$,由此得出,$f(c_1,c_2,c_3)\neq0$ 且 $g(c_1,c_2,c_3)\neq0$,这与已知条件矛盾。 ■

点评 例 5 的证明主要用到两个结论:数域 K 上的 n 元多项式环是无零因子环;数域 K 上的 n 元多项式环 $K[x_1,x_2,\cdots,x_n]$与数域 K 上的 n 元多项式函数环 K_{npol}是同构的。例 5 的结论从直观上容易猜测到,但是要想讲出道理证明它就需要用到上述两个结论。这又一次表明:只有掌握理论,才能把道理讲清楚。

例 6 证明：在复数域上的二元多项式环中，下述二次多项式是不可约的：

$$f(x,y)=x^2-2xy+y^2+y.$$

证明 假如 $f(x,y)$ 在复数域上可约，则

$$f(x,y)=(x+ay+b)(x+cy+d),$$

其中 $a,b,c,d\in\mathbf{C}$。比较系数得

$$a+c=-2,ac=1,d+b=0,ad+bc=1,bd=0.$$

由 $d+b=0$ 且 $bd=0$ 推出 $b=d=0$，这与 $ad+bc=1$ 矛盾。因此 $f(x,y)=x^2-2xy+y^2+y$ 在 $\mathbf{C}$ 上是不可约的。■

点评 我们已经知道，在复数域上的一元多项式环中，不可约多项式都是一次的。而例 6 表明，在复数域上的二元多项式环中，存在二次的不可约多项式。在数域 K 上的一元多项式环中，$f(x)$ 有一次因式 $x-a$ 当且仅当 $f(x)$ 在 K 中有根 a。而例 6 表明，在复数域上的二元多项式环中，$f(x,y)=x^2-2xy+y^2+y$ 虽然有许多零点，例如 $(0,0),(0,-1),\left(1,\frac{1\pm\sqrt{3}\mathrm{i}}{2}\right)$ 等，但是 $f(x,y)$ 没有一次因式。这些表明，当 $n>1$ 时，数域 K 上的 n 元多项式环有许多与一元多项式环不同的性质。

例 7 探索并且论证实数域上 n 元二次齐次多项式可约的充分必要条件。

解 实数域上 n 元二次齐次多项式 $f(x_1,x_2,\cdots,x_n)$ 可约当且仅当 $f(x_1,x_2,\cdots,x_n)$ 能分解成两个实系数一次多项式的乘积，根据例 3 的结论可知，这两个一次多项式都是齐次的。根据《高等代数学习指导书(上册)》6.2 节的例 5，一个 n 元实二次型可以分解成两个实系数一次齐次多项式的乘积当且仅当它的秩等于 2 且符号差为 0，或者它的秩等于 1。于是这就是实系数 n 元二次齐次多项式可约的充分必要条件。■

例 8 当 $n>1$ 时，在 $K[x_1,x_2,\cdots,x_n]$ 中是否有下述结论：两个多项式互素的充分必要条件为它们有倍式和等于 1？

解 充分性。设数域 K 上的 n 元多项式 $f(x_1,x_2,\cdots,x_n)$ 与 $g(x_1,x_2,\cdots,x_n)$ 具有性质：存在 $u(x_1,\cdots,x_n),v(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]$ 使得

$$u(x_1,\cdots,x_n)f(x_1,\cdots,x_n)+v(x_1,\cdots,x_n)g(x_1,\cdots,x_n)=1.$$

设 $d(x_1,\cdots,x_n)$ 是 $f(x_1,\cdots,x_n)$ 与 $g(x_1,\cdots,x_n)$ 的一个最大公因式，则从上式得，$d(x_1,\cdots,x_n)\mid 1$。由乘积多项式的次数公式得，$d(x_1,\cdots,x_n)$ 的次数为 0，从而它是 K 中一个非零数。因此 $f(x_1,\cdots,x_n)$ 与 $g(x_1,\cdots,x_n)$ 互素，即充分性是成立的。

必要性。从例 6 中知道，复数域上的二元多项式 $f(x,y)=x^2-2xy+y^2+y$ 不可约。从而 $f(x,y)$ 与 $g(x,y)=x$ 的公因式只有 K 中的非零数，因此 $f(x,y)$ 与 $g(x,y)$ 互素。对于 $\mathbf{C}[x,y]$ 中的任意多项式 $u(x,y),v(x,y)$，都有 $u(x,y)f(x,y)$ 没有常数项，

$v(x,y)g(x,y)$也没有常数项,从而

$$u(x,y)f(x,y)+v(x,y)g(x,y)\neq 1.$$

这个例子表明必要性是不成立的。

点评 在数域 K 上的一元多项式环 $K[x]$中,两个多项式互素的充分必要条件是它们有倍式和等于 1。而当 $n>1$ 时,$K[x_1,\cdots,x_n]$中两个多项式互素的充分条件是它们有倍式和等于 1,但这不是必要条件,其根源在于 $K[x]$中有带余除法,从而求两个多项式的最大公因式有辗转相除法;而当 $n>1$ 时,在 $K[x_1,x_2,\cdots,x_n]$中没有带余除法,从而求两个多项式的最大公因式没有辗转相除法,因此两个多项式的最大公因式无法表示成它们的倍式和。

例 9 把下述有理数域上的二元二次多项式因式分解:

$$f(x,y)=2x^2+xy-y^2+5x+2y+3.$$

解法一 $f(x,y)=2\left(x^2+\dfrac{5+y}{2}x+\dfrac{-y^2+2y+3}{2}\right)$

可暂时把 y 看成常数,括号内的 x 的二次三项式的判别式

$$\Delta=\left(\frac{5+y}{2}\right)^2-2(-y^2+2y+3)=\frac{9y^2-6y+1}{4}=\left(\frac{3y-1}{2}\right)^2.$$

从而

$$\begin{aligned}f(x,y)&=2\left(x-\frac{-\frac{1}{2}(5+y)+\frac{1}{2}(3y-1)}{2}\right)\left(x-\frac{-\frac{1}{2}(5+y)-\frac{1}{2}(3y-1)}{2}\right)\\&=(2x-y+3)(x+y+1).\end{aligned}$$

解法二 设 $f(x,y)=(x+ay+b)(2x+cy+d)$,

比较系数得

$$1=c+2a,\ -1=ac,\ 5=d+2b,\ 2=ad+bc,\ 3=bd.$$

解得 $a=1$ 或$-\dfrac{1}{2}$,$c=-1$ 或 2,$b=1$ 或 3,$d=3$ 或 1。

当 $a=1$ 时,$c=-1$,只有 $b=1$,$d=3$才能满足 $2=ad+bc$。当 $a=-\dfrac{1}{2}$时,无法满足 $2=ad+bc$,应当舍去。因此

$$f(x,y)=(x+y+1)(2x-y+3).$$

例 10 求实数域上二元二次多项式可约的充分必要条件。

解 设 $f(x,y)=a_{11}x^2+2a_{12}xy+a_{22}y^2+2a_1x+2a_2y+a_0$,则 $f(x,y)=0$ 是平面上的二次曲线,运用二次曲线的不变量理论(参看《解析几何(第三版)》第 5 章第 2 节),得

实数域上二元二次多项式 $f(x,y)$可约

$\Leftrightarrow$ $f(x,y)=0$ 为两条相交直线或一对平行直线或两条重合直线;

$\Leftrightarrow$ $I_2<0$ 且 $I_3=0$，或 $I_2=I_3=0$ 且 $K_1\leqslant 0$。

例 11 下列实数域上的二元二次多项式是否可约？如果可约，把它因式分解。

(1) $f(x,y)=2x^2+8xy+8y^2-x-2y-1$；

(2) $g(x,y)=x^2-2xy+y^2-2x-4y+3$。

解 (1) $I_2=\begin{vmatrix}2 & 4\\ 4 & 8\end{vmatrix}=0$，

$$I_3=\begin{vmatrix}2 & 4 & -\frac{1}{2}\\ 4 & 8 & -1\\ -\frac{1}{2} & -1 & -1\end{vmatrix}=0,$$

$$K_1=\begin{vmatrix}2 & -\frac{1}{2}\\ -\frac{1}{2} & -1\end{vmatrix}+\begin{vmatrix}8 & -1\\ -1 & -1\end{vmatrix}=\left(-2-\frac{1}{4}\right)+(-8-1)<0.$$

据例 10 的结论得，$f(x,y)$可约。

$$f(x,y)=2\left[x^2+\left(4y-\frac{1}{2}\right)x+4y^2-y-\frac{1}{2}\right].$$

把括号内看成 x 的二次三项式，它的判别式为

$$\Delta=\left(4y-\frac{1}{2}\right)^2-4\left(4y^2-y-\frac{1}{2}\right)=\frac{9}{4}.$$

于是

$$\begin{aligned}f(x,y)&=2\left(x-\frac{\frac{1}{2}-4y+\frac{3}{2}}{2}\right)\left(x-\frac{\frac{1}{2}-4y-\frac{3}{2}}{2}\right)\\&=(x+2y-1)(2x+4y+1).\end{aligned}$$

(2) $I_2=\begin{vmatrix}1 & -1\\ -1 & 1\end{vmatrix}=0$，$I_3=\begin{vmatrix}1 & -1 & -1\\ -1 & 1 & -2\\ -1 & -2 & 3\end{vmatrix}=-9\neq 0.$

据例 10 的结论得，$g(x,y)$不可约。

点评 由于利用了例 10 的结论，在例 11 中判别实数域上二元二次多项式是否可约变得很容易，而例 10 的结论是运用了解析几何中二次曲线的不变量理论推导出来的。由此可见，数学是一个统一的整体，要善于把代数与几何以及数学分析联系起来。

例 12 设 $f(x,y)=y^2-x^3+x-1\in\mathbf{R}[x,y]$，在平面直角坐标系 Oxy 中画出曲线$f(x,y)=0$。

解 由于用 $-y$ 代 y 方程不变，因此曲线 $f(x,y)=0$ 关于 x 轴对称。只要先画出 x 轴上方的曲线以及 x 轴与曲线的交点。

点 $M(x_0,0)$ 是曲线 $f(x,y)=0$ 与 x 轴的交点当且仅当 $x_0^3-x_0+1=0$，即 x_0 是 $g(x)=x^3-x+1$ 的实根，用 Sturm 定理可以求出 $g(x)=x^3-x+1$ 的唯一实根在 $\left(-\frac{3}{2},-1\right)$ 内(参看 7.7 节中典型例题的例 9)，把这个实根记作 x_0。

在 x 轴的上方，$y=\sqrt{x^3-x+1}$，此函数的定义域为不等式 $x^3-x+1\geqslant 0$ 的解集。由于 $g'(x)=3x^2-1$，因此

$$g'(x)=0 \quad\Leftrightarrow\quad 3x^2-1=0 \quad\Leftrightarrow\quad x=\pm\frac{\sqrt{3}}{3};$$

$$g'(x)>0 \quad\Leftrightarrow\quad 3x^2-1>0 \quad\Leftrightarrow\quad x<-\frac{\sqrt{3}}{3} \text{ 或 } x>\frac{\sqrt{3}}{3};$$

$$g'(x)<0 \quad\Leftrightarrow\quad 3x^2-1<0 \quad\Leftrightarrow\quad -\frac{\sqrt{3}}{3}<x<\frac{\sqrt{3}}{3}.$$

从而 $g(x)$ 在 $\left(-\infty,-\frac{\sqrt{3}}{3}\right)$ 内单调上升，在 $\left(-\frac{\sqrt{3}}{3},\frac{\sqrt{3}}{3}\right)$ 内单调下降，在 $\left(\frac{\sqrt{3}}{3},+\infty\right)$ 内单调上升，于是 $g(x)$ 在 $x=-\frac{\sqrt{3}}{3}$ 处达到极大值，在 $x=\frac{\sqrt{3}}{3}$ 处达到极小值；并且 $g(x)\geqslant 0$ 当且仅当 $x\geqslant x_0$。这表明函数 $y=\sqrt{x^3-x+1}$ 的定义域是 $[x_0,+\infty)$。

由于函数 $h(u)=\sqrt{u}$ 在它的定义域 $[0,+\infty)$ 内单调上升，因此从 $g(x)$ 的上述性质可以推出，$y=\sqrt{x^3-x+1}$ 在 $\left[x_0,-\frac{\sqrt{3}}{3}\right)$ 内单调上升，在 $\left(-\frac{\sqrt{3}}{3},\frac{\sqrt{3}}{3}\right)$ 内单调下降，在 $\left(\frac{\sqrt{3}}{3},+\infty\right)$ 内单调上升，在 $x=-\frac{\sqrt{3}}{3}$ 处达到极大值，在 $x=\frac{\sqrt{3}}{3}$ 处达到极小值。现在可以来画曲线 $f(x,y)=0$。先找几个关键点列表和描点，然后用一条光滑曲线把它们连接起来，最后利用对称性画出 x 轴下方的曲线，如表 7-1 和图 7-2 所示。

表 7-1

x	x_0	$-\frac{\sqrt{3}}{3}\approx-0.58$	0	$\frac{\sqrt{3}}{3}\approx 0.58$	1	2
y	0	$\sqrt{\frac{2}{9}\sqrt{3}+1}\approx 1.18$	1	$\sqrt{1-\frac{1}{9}\sqrt{3}}\approx 0.90$	1	$\sqrt{7}\approx 2.65$

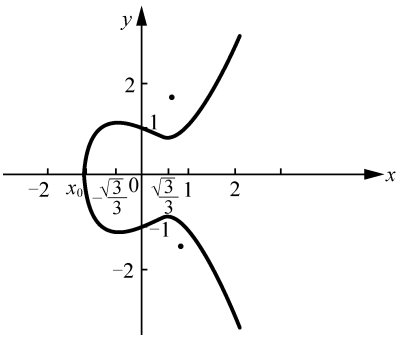

图 7-2

点评 例 12 中的曲线 $y^2=x^3-x+1$ 是一条椭圆曲线,它在公开密钥密码学中有用。

习题 7.9

1. 将下列四元多项式按字典排列法排列各单项式的顺序:

(1) $f(x_1,x_2,x_3,x_4)=x_3^4x_4-x_1^3x_2+5x_2x_3x_4+2x_2^4x_3x_4$;

(2) $f(x_1,x_2,x_3,x_4)=x_1^3+x_3^2+3x_1x_2^2x_4-5x_1^2x_3x_4^2-2x_2^3x_3$。

2. 把三元齐次多项式 $f(x_1,x_2,x_3)=x_1^3+x_2^3+x_3^3-3x_1x_2x_3$ 写成两个三元齐次多项式的乘积。

3. 设 $f(x_1,\cdots,x_n),g(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]$,且 $g(x_1,\cdots,x_n)\neq 0$,其中 K 是数域。证明:如果对于使得 $g(c_1,\cdots,c_n)\neq 0$ 的任意一组元素 $c_1,c_2,\cdots,c_n\in K$,都有 $f(c_1,\cdots,c_n)=0$,那么 $f(x_1,\cdots,x_n)=0$。

4. 证明:在 $K[x_1,\cdots,x_n]$ 中,如果 $g\mid f_i,i=1,2,\cdots,s$,那么对任意 $u_i(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n],i=1,2,\cdots,s$,都有

$$g\mid u_1f_1+u_2f_2+\cdots+u_sf_s.$$

5. 证明:在 $K[x_1,\cdots,x_n]$ 中,f 与 g 相伴当且仅当存在 $c\in K^*$ 使得 $f=cg$。

6. 证明:在 $K[x,y]$ 中,多项式 x^2-y 是不可约的。

7. 证明:在复数域上的二元多项式环中,x^3+y 是不可约的。

8. 下列实数域上的三元二次齐次多项式是否可约? 如果可约,把它因式分解。

(1) $f(x,y,z)=3x^2-2y^2+5xy+3xz-yz$;

(2) $g(x,y,z)=x^2+2y^2+z^2+2xy+2xz$。

9. 下列实数域上的二元二次多项式是否可约? 如果可约,把它因式分解。

(1) $f(x,y)=2x^2+5xy-3y^2+x+10y-3$；

(2) $g(x,y)=17x^2+22xy-23y^2+10x+14y-4$。

10. 设 $p(x_1,\cdots,x_n)$是 $K[x_1,\cdots,x_n]$中的不可约多项式，证明：$p(x_1,\cdots,x_n)$与 $K[x_1,\cdots,x_n]$中任一多项式 $f(x_1,\cdots,x_n)$的关系只有两种可能，即

$p(x_1,\cdots,x_n)\mid f(x_1,\cdots,x_n)$，或者 $p(x_1,\cdots,x_n)$与 $f(x_1,\cdots,x_n)$互素。

11. 在 $\mathbf{R}[x,y]$中，$f(x,y)=x^2-4xy+4y^2-6x+10y-1$ 与 $g(x,y)=3x-y+5$ 是否互素？

7.10　n 元对称多项式

7.10.1　内容精华

观察下述三元多项式 $f(x_1,x_2,x_3)$有什么特点。

$$f(x_1,x_2,x_3)=x_1^3+x_2^3+x_3^3+x_1^2x_2+x_1^2x_3+x_2^2x_3+x_1x_2^2+x_1x_3^2+x_2x_3^2.$$

不定元 x_1,x_2,x_3 的下标分别是 1,2,3。对于自然数 1,2,3 的任意一个三元排列，譬如 231，把不定元 x_1,x_2,x_3 分别用 x_2,x_3,x_1 代入，则上式可写成

$$f(x_2,x_3,x_1)=x_2^3+x_3^3+x_1^3+x_2^2x_3+x_2^2x_1+x_3^2x_1+x_2x_3^2+x_2x_1^2+x_3x_1^2.$$

发现 $f(x_2,x_3,x_1)$的表达式与 $f(x_1,x_2,x_3)$的表达式相等，因此 $f(x_2,x_3,x_1)=f(x_1,x_2,x_3)$。对于自然数 1,2,3 的其他 5 个三元排列，也有类似的结论。这在直观上可以这么说，在三元多项式 $f(x_1,x_2,x_3)$中，不定元 x_1,x_2,x_3 的地位是对称的。于是我们可以把 $f(x_1,x_2,x_3)$称为对称多项式。

一、n 元对称多项式的定义和例子

定义 1　设 $f(x_1,x_2,\cdots,x_n)\in K[x_1,x_2,\cdots,x_n]$，$K$ 是数域，如果对于任意一个 n 元排列 $j_1j_2\cdots j_n$ 都有

$$f(x_{j_1},x_{j_2},\cdots,x_{j_n})=f(x_1,x_2,\cdots,x_n),$$

那么称 $f(x_1,x_2,\cdots,x_n)$是数域 K 上的一个 **n 元对称多项式**。

从定义 1 得出，如果一个 n 元对称多项式 $f(x_1,x_2,\cdots,x_n)$含有一项 $ax_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$，那么它也含有项

$$ax_{j_1}^{i_1}x_{j_2}^{i_2}\cdots x_{j_n}^{i_n},$$

其中 $j_1j_2\cdots j_n$ 是任意一个 n 元排列。（注意：相等的项只写一次。）

例如,若三元对称多项式 $f(x_1,x_2,x_3)$含有一项 $x_1^2x_2$,即 $x_1^2x_2x_3^0$,则它也会有如下 5 项:

$$x_1^2x_3x_2^0,\ x_2^2x_1x_3^0,\ x_2^2x_3x_1^0,\ x_3^2x_1x_2^0,\ x_3^2x_2x_1^0.$$

即会有如下 5 项:

$$x_1^2x_3,\ x_1x_2^2,\ x_2^2x_3,\ x_1x_3^2,\ x_2x_3^2.$$

从定义 1 还得出,零多项式和零次多项式都是对称多项式。

一个 n 元对称多项式如果含有一项 x_1,那么它一定含有项 $x_2,x_3,\cdots,x_n$。因此,$x_1+x_2+\cdots+x_n$是一个 n 元对称多项式,把它用 $\sigma_1(x_1,x_2,\cdots,x_n)$表示。即

$$\sigma_1(x_1,x_2,\cdots,x_n)=x_1+x_2+\cdots+x_n.$$

一个 n 元对称多项式如果含有一项 x_1x_2,那么它一定含有项 x_ix_j,其中 $1\leqslant i<j\leqslant n$。因此下述多项式是一个 n 元对称多项式:

$$\begin{aligned}\sigma_2(x_1,x_2,\cdots,x_n)=&x_1x_2+x_1x_3+\cdots+x_1x_n\\&+x_2x_3+\cdots+x_2x_n\\&+\cdots\\&+x_{n-1}x_n\\=&\sum_{1\leqslant i<j\leqslant n}x_ix_j.\end{aligned}$$

同理,对于任给 $k\in\{2,\cdots,n-1\}$,下述多项式是一个 n 元对称多项式:

$$\sigma_k(x_1,x_2,\cdots,x_n)=\sum_{1\leqslant j_1<j_2<\cdots<j_k\leqslant n}x_{j_1}x_{j_2}\cdots x_{j_k}.$$

显然,下述多项式也是一个 n 元对称多项式:

$$\sigma_n(x_1,x_2,\cdots,x_n)=x_1x_2\cdots x_n.$$

上述 n 个 n 元对称多项式 $\sigma_i(x_1,x_2,\cdots,x_n)$,$i=1,2,\cdots,n$,统称为 ***n* 元初等对称多项式**。

二、数域 K 上 n 元对称多项式组成的集合的结构

数域 K 上所有 n 元对称多项式组成的集合 W 的结构如何?

设 $f(x_1,x_2,\cdots,x_n),g(x_1,x_2,\cdots,x_n)\in W$。如果

$$f(x_1,x_2,\cdots,x_n)+g(x_1,x_2,\cdots,x_n)=h(x_1,x_2,\cdots,x_n),$$

$$f(x_1,x_2,\cdots,x_n)g(x_1,x_2,\cdots,x_n)=p(x_1,x_2,\cdots,x_n).$$

那么对任一 n 元排列 $j_1j_2\cdots j_n$,把不定元 $x_1,x_2,\cdots,x_n$ 分别用 $x_{j_1},x_{j_2},\cdots,x_{j_n}$ 代入,从上两式得

$$f(x_{j_1},x_{j_2},\cdots,x_{j_n})+g(x_{j_1},x_{j_2},\cdots,x_{j_n})=h(x_{j_1},x_{j_2},\cdots,x_{j_n}),$$

$$f(x_{j_1},x_{j_2},\cdots,x_{j_n})g(x_{j_1},x_{j_2},\cdots,x_{j_n})=p(x_{j_1},x_{j_2},\cdots,x_{j_n}).$$

由于 $f(x_1,x_2,\cdots,x_n),g(x_1,x_2,\cdots,x_n)$都是对称多项式,

因此 $$f(x_{j_1},x_{j_2},\cdots,x_{j_n})=f(x_1,x_2,\cdots,x_n),$$

$$g(x_{j_1},x_{j_2},\cdots,x_{j_n})=g(x_1,x_2,\cdots,x_n).$$

由此推出

$$\begin{aligned}h(x_1,x_2,\cdots,x_n)&=f(x_1,x_2,\cdots,x_n)+g(x_1,x_2,\cdots,x_n)\\&=f(x_{j_1},x_{j_2},\cdots,x_{j_n})+g(x_{j_1},x_{j_2},\cdots,x_{j_n})\\&=h(x_{j_1},x_{j_2},\cdots,x_{j_n}).\end{aligned}$$

因此 $h(x_1,x_2,\cdots,x_n)\in W$。同理 $p(x_1,x_2,\cdots,x_n)\in W$。这表明 W 对加法和乘法封闭。又由于 $-g(x_{j_1},x_{j_2},\cdots,x_{j_n})=-g(x_1,x_2,\cdots,x_n)$，因此 W 对减法也封闭。于是我们证明了下述命题：

命题 1 W 是 $K[x_1,x_2,\cdots,x_n]$ 的一个子环。 ■

由命题 1 立即得到：

命题 2 设 $f_1,f_2,\cdots,f_n\in W$，则对于 $K[x_1,x_2,\cdots,x_n]$ 中任意一个多项式 $g(x_1,x_2,\cdots,x_n)=\sum\limits_{i_1,\cdots,i_n}b_{i_1\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$，有

$$g(f_1,f_2,\cdots,f_n)=\sum_{i_1,\cdots,i_n}b_{i_1\cdots i_n}f_1^{i_1}f_2^{i_2}\cdots f_n^{i_n}\in W.$$ ■

特别有

$$g(\sigma_1,\sigma_2,\cdots,\sigma_n)\in W.$$

即初等对称多项式 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 的多项式仍是对称多项式。反之，数域 K 上任一 n 元对称多项式是否都可表示成初等对称多项式 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 的多项式？回答是肯定的，即我们有下述重要定理：

定理 1（对称多项式基本定理） 对于数域 K 上任意一个 n 元对称多项式 $f(x_1,x_2,\cdots,x_n)$，都存在数域 K 上唯一的一个 n 元多项式 $g(x_1,x_2,\cdots,x_n)$，使得

$$f(x_1,x_2,\cdots,x_n)=g(\sigma_1,\sigma_2,\cdots,\sigma_n).$$

三、数域 K 上一元多项式的判别式

对称多项式基本定理的一个重要应用是，研究数域 K 上的一元多项式在复数域中有无重根。

设数域 K 上首项系数为 1 的一元多项式

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

在复数域中的 n 个根为 $c_1,c_2,\cdots,c_n$，则

$f(x)$ 在复数域中有重根 $\Leftrightarrow$ $\prod\limits_{1\leqslant j<i\leqslant n}(c_i-c_j)^2=0.$

据 Vieta 公式

$$-a_{n-1}=c_1+c_2+\cdots+c_n=\sigma_1(c_1,c_2,\cdots,c_n)$$

$$\cdots$$

$$(-1)^k a_{n-k}=\sum_{1\leqslant j_1<\cdots<j_k\leqslant n} c_{j_1}c_{j_2}\cdots c_{j_k}=\sigma_k(c_1,c_2,\cdots,c_n),$$

$$\cdots$$

$$(-1)^n a_0=c_1c_2\cdots c_n=\sigma_n(c_1,c_2,\cdots,c_n).$$

考虑 K 上 n 元多项式：

$$D(x_1,x_2,\cdots,x_n):=\prod_{1\leqslant j<i\leqslant n}(x_i-x_j)^2,$$

显然它是对称多项式。于是存在唯一的 n 元多项式 $g(x_1,x_2,\cdots,x_n)$ 使得

$$D(x_1,x_2,\cdots,x_n)=g(\sigma_1,\sigma_2,\cdots,\sigma_n).$$

$x_1,x_2,\cdots,x_n$ 分别用 $c_1,c_2,\cdots,c_n$ 代入，由上式得

$$D(c_1,c_2,\cdots,c_n)=g(\sigma_1(c_1,\cdots,c_n),\sigma_2(c_1,\cdots,c_n),\cdots,\sigma_n(c_1,\cdots,c_n)).$$

于是

$$\prod_{1\leqslant i<j\leqslant n}(c_i-c_j)^2=g(-a_{n-1},a_{n-2},\cdots,(-1)^n a_0).$$

这样我们证明了下述命题：

命题 3 数域 K 上首项系数为 1 的一元多项式

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

在复数域中有重根的充分必要条件为：$g(-a_{n-1},a_{n-2},\cdots,(-1)^n a_0)=0$. ■

我们把 $f(x)$ 的系数 $a_{n-1},a_{n-2},\cdots,a_0$ 的多项式 $g(-a_{n-1},a_{n-2},\cdots,(-1)^n a_0)$ 称为 $f(x)$ 的**判别式**，记作 $D(f)$。利用它可以判断 $f(x)$ 在复数域中有没有重根：$f(x)$ 有重根当且仅当 $D(f)=0$。

如何求出 $f(x)$ 的判别式 $D(f)$ 呢？

$$\begin{aligned}D(f)&=g(-a_{n-1},a_{n-2},\cdots,(-1)^n a_0)\\&=\prod_{1\leqslant j<i\leqslant n}(c_i-c_j)^2\\&=\begin{vmatrix}1&1&\cdots&1\\c_1&c_2&\cdots&c_n\\c_1^2&c_2^2&\cdots&c_n^2\\\vdots&\vdots&&\vdots\\c_1^{n-1}&c_2^{n-1}&\cdots&c_n^{n-1}\end{vmatrix}\begin{vmatrix}1&c_1&c_1^2&\cdots&c_1^{n-1}\\1&c_2&c_2^2&\cdots&c_2^{n-1}\\\vdots&\vdots&\vdots&&\vdots\\1&c_n&c_n^2&\cdots&c_n^{n-1}\end{vmatrix}\end{aligned}$$

$$= \begin{vmatrix} n & \sum\limits_{i=1}^{n} c_i & \cdots & \sum\limits_{i=1}^{n} c_i^{n-1} \\ \sum\limits_{i=1}^{n} c_i & \sum\limits_{i=1}^{n} c_i^2 & \cdots & \sum\limits_{i=1}^{n} c_i^n \\ \vdots & \vdots & & \vdots \\ \sum\limits_{i=1}^{n} c_i^{n-1} & \sum\limits_{i=1}^{n} c_i^n & \cdots & \sum\limits_{i=1}^{n} c_i^{2n-2} \end{vmatrix}. \tag{1}$$

于是考虑下列 n 元对称多项式：

$$s_k(x_1, x_2, \cdots, x_n) = \sum_{i=0}^{n} x_i^k,\ k = 0, 1, 2, \cdots. \tag{2}$$

称它们为**幂和**。

根据对称多项式基本定理，s_k 能表示成 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 的多项式，从而通过把 $x_1, x_2, \cdots, x_n$ 用 $c_1, c_2, \cdots, c_n$ 代入，可以把(1)的行列式中出现的

$$\sum_{i=1}^{n} c_i^k = s_k(c_1, c_2, \cdots, c_n)$$

用 $\sigma_1(c_1, c_2, \cdots, c_n), \cdots, \sigma_n(c_1, c_2, \cdots, c_n)$ 表示出来，也就是可以通过 $f(x)$ 的系数 $a_{n-1}, \cdots, a_1, a_0$ 计算出来，从而可以求出判别式 $D(f)$。

下述牛顿公式解决了把幂和 s_k 表示成 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 的多项式的问题。

牛顿(Newton)公式　当 $1 \leqslant k \leqslant n$ 时，有

$$s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} + \cdots + (-1)^{k-1}\sigma_{k-1} s_1 + (-1)^k k\sigma_k = 0; \tag{3}$$

当 $k > n$ 时，有

$$s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} + \cdots + (-1)^{n-1}\sigma_{n-1} s_{k-n+1} + (-1)^n \sigma_n s_{k-n} = 0. \tag{4}$$

注意：在上述讨论中，$f(x)$ 的首项系数为 1，如果 $f(x)$ 的首项系数为 a_n，那么可以先对 $a_n^{-1} f(x)$ 运用上述方法求出它的判别式 $D(a_n^{-1} f)$，然后规定 $f(x)$ 的判别式为

$$D(f) := a_n^{2n-2} D(a_n^{-1} f).$$

7.10.2　典型例题

例 1　下述数域 K 上的三元多项式是不是对称多项式？

$$f(x_1, x_2, x_3) = (x_1^2 + x_1 x_2 + x_2^2)(x_2^2 + x_2 x_3 + x_3^2)(x_3^2 + x_3 x_1 + x_1^2).$$

解　对于三元排列 132，213，231，312，321，分别有

$$f(x_1, x_3, x_2) = (x_1^2 + x_1 x_3 + x_3^2)(x_3^2 + x_3 x_2 + x_2^2)(x_2^2 + x_2 x_1 + x_1^2)$$

$$
\begin{aligned}
&= f(x_1,x_2,x_3),\\
f(x_2,x_1,x_3)&= (x_2^2+x_2x_1+x_1^2)(x_1^2+x_1x_3+x_3^2)(x_3^2+x_3x_2+x_2^2)\\
&= f(x_1,x_2,x_3),\\
f(x_2,x_3,x_1)&= (x_2^2+x_2x_3+x_3^2)(x_3^2+x_3x_1+x_1^2)(x_1^2+x_1x_2+x_2^2)\\
&= f(x_1,x_2,x_3),\\
f(x_3,x_1,x_2)&= (x_3^2+x_3x_1+x_1^2)(x_1^2+x_1x_2+x_2^2)(x_2^2+x_2x_3+x_3^2)\\
&= f(x_1,x_2,x_3),\\
f(x_3,x_2,x_1)&= (x_3^2+x_3x_2+x_2^2)(x_2^2+x_2x_1+x_1^2)(x_1^2+x_1x_3+x_3^2)\\
&= f(x_1,x_2,x_3),
\end{aligned}
$$

因此 $f(x_1,x_2,x_3)$是一个对称多项式。

例 2 写出下述三元对称多项式的首项和首项的幂指数组,求它的次数,它是不是齐次多项式?

$$f(x_1,x_2,x_3) = (x_1^2-x_2x_3)(x_2^2-x_3x_1)(x_3^2-x_1x_2).$$

解 由于多项式的乘积的首项等于它们的首项的乘积,因此 $f(x_1,x_2,x_3)$的首项等于 $x_1^2(-x_3x_1)(-x_1x_2)=x_1^4x_2x_3$,从而首项的幂指数组为(4,1,1)。

根据乘积多项式的次数公式得

$$\deg f = 2+2+2 = 6.$$

每个因式是齐次多项式,它们的乘积仍是齐次多项式,因此 $f(x_1,x_2,x_3)$是六次齐次多项式。

例 3 在 $K[x_1,x_2,x_3]$中,用初等对称多项式表出下述对称多项式:

$$f(x_1,x_2,x_3) = x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2.$$

解法一 $f(x_1,x_2,x_3)$的首项为 $x_1^2x_2^2$,首项的幂指数组为(2,2,0),构造对称多项式 $\Phi_1(x_1,x_2,x_3)$如下:

$$\Phi_1(x_1,x_2,x_3) = \sigma_1^{2-2}\sigma_2^{2-0}\sigma_3^0 = \sigma_2^2 = (x_1x_2+x_1x_3+x_2x_3)^2.$$

令

$$
\begin{aligned}
f_1 &= f-\Phi_1\\
&= (x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2)-(x_1x_2+x_1x_3+x_2x_3)^2\\
&= -2(x_1^2x_2x_3+x_1x_2^2x_3+x_1x_2x_3^2)\\
&= -2x_1x_2x_3(x_1+x_2+x_3)\\
&= -2\sigma_3\sigma_1.
\end{aligned}
$$

因此

$$f=\Phi_1+f_1=\sigma_2^2-2\sigma_1\sigma_3.$$

解法二 $f(x_1,x_2,x_3)$是四次齐次对称多项式,其首项为 $x_1^2x_2^2$,首项的幂指数组为(2,2,0),构造的 $\Phi_1(x_1,x_2,x_3)$与 $f(x_1,x_2,x_3)$有相同的首项,因此 $\Phi_1(x_1,x_2,x_3)$也是四次多项式。由于 $\Phi_1(x_1,x_2,x_3)=\sigma_1^{2-2}\sigma_2^{2-0}\sigma_3^0=\sigma_2^2$,因此 $\Phi_1(x_1,x_2,x_3)$也是齐次对称多项式,从而 $f_1=f-\Phi_1$ 也是四次齐次对称多项式。同理,$f_2,\cdots,f_s(s\geqslant 2)$都是四次齐次对称多项式。于是 $f_i(i=1,2,\cdots,s)$如果不是零多项式,那么它的首项幂指数(p_1,p_2,p_3)应当满足 $p_1+p_2+p_3=4$。又由于 f 的首项幂指数组先于 $f_i(i=1,2,\cdots,s)$的首项幂指数组,因此 $2\geqslant p_1\geqslant p_2\geqslant p_3$。满足这些条件的非负整数组只有(2,2,0),(2,1,1)。于是 f_1 的首项为 $ax_1^2x_2x_3$,f_2 为零多项式,从而 $\Phi_2(x_1,x_2,x_3)=a\sigma_1^{2-1}\sigma_2^{1-1}\sigma_3^1=a\sigma_1\sigma_3$。因此

$$f(x_1,x_2,x_3)=f_1+\Phi_1=f_2+\Phi_2+\Phi_1=\Phi_2+\Phi_1=a\sigma_1\sigma_3+\sigma_2^2.$$

为了确定 a 的值,x_1,x_2,x_3 分别用 1,1,1 代入,由上式得

$$3=a\cdot 3\cdot 1+3^2.$$

解得 $a=-2$,因此 $f(x_1,x_2,x_3)=-2\sigma_1\sigma_3+\sigma_2^2$。

例 4 在 $K[x_1,x_2,\cdots,x_n]$中,用初等对称多项式表出下述对称多项式:

$$f(x_1,x_2,\cdots,x_n)=\sum x_1^2x_2^2.$$

这里 $\sum x_1^2x_2^2$ 表示含有项 $x_1^2x_2^2$ 的项数最少的对称多项式。

解 $f(x_1,x_2,\cdots,x_n)$的首项为 $x_1^2x_2^2$,首项的幂指数组为(2,2,0,$\cdots$,0)。$f(x_1,x_2,\cdots,x_n)$是四次齐次对称多项式,$f_i(i=1,2,\cdots,s)$也是四次齐次对称多项式,它们的首项幂指数组$(p_1,p_2,\cdots,p_n)$应当满足:

$$p_1+p_2+\cdots+p_n=4,\ 2\geqslant p_1\geqslant p_2\geqslant\cdots\geqslant p_n.$$

满足这两个条件的非负整数 n 元组$(p_1,p_2,\cdots,p_n)$只可能是

$$(2,2,0,\cdots,0),(2,1,1,0,\cdots 0),(1,1,1,1,0,\cdots,0).$$

它们分别是 f,f_1,f_2 的首项幂指数组,于是 $f_3=0$,且

$$\Phi_1(x_1,\cdots,x_n)=\sigma_1^{2-2}\sigma_2^{2-0}\sigma_3^0\cdots\sigma_n^0=\sigma_2^2,$$

$$\Phi_2(x_1,\cdots,x_n)=a\sigma_1^{2-1}\sigma_2^{1-1}\sigma_3^1\sigma_4^{0-0}\cdots\sigma_n^0=a\sigma_1\sigma_3,$$

$$\Phi_3(x_1,\cdots,x_n)=b\sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^{1-1}\sigma_4^{1-0}\sigma_5^{0-0}\cdots\sigma_n^0=b\sigma_4,$$

于是

$$\begin{aligned}f(x_1,\cdots,x_n)&=f_1+\Phi_1=f_2+\Phi_2+\Phi_1=f_3+\Phi_3+\Phi_2+\Phi_1\\&=\Phi_3+\Phi_2+\Phi_1=b\sigma_4+a\sigma_1\sigma_3+\sigma_2^2.\end{aligned}$$

为了确定 a,b 的值,$x_1,x_2,\cdots,x_n$ 分别用 1,1,1,0,$\cdots$,0 代入,以及用 1,1,1,1,0,$\cdots$,0 代入,得

$$\begin{cases}3=a\cdot 3\cdot 1+3^2,\\6=b\cdot 1+a\cdot 4\cdot 4+6^2.\end{cases}$$

解得 $a=-2,b=2$,因此

$$f(x_1,\cdots,x_n)=-2\sigma_1\sigma_3+\sigma_2^2+2\sigma_4.$$

例 5 在 $K[x_1,x_2,x_3]$中,用初等对称多项式表出下述对称多项式:

$$f(x_1,x_2,x_3)=(2x_1x_2+x_3^2)(2x_2x_3+x_1^2)(2x_3x_1+x_2^2).$$

解 $f(x_1,x_2,x_3)$的首项是 $2x_1x_2\cdot x_1^2\cdot 2x_3x_1=4x_1^4x_2x_3$;首项的幂指数组为 $(4,1,1)$,$f(x_1,x_2,x_3)$是六次齐次对称多项式。满足

$$p_1+p_2+p_3=6,4\geqslant p_1\geqslant p_2\geqslant p_3$$

的非负整数组(p_1,p_2,p_3)只可能是

$$(4,2,0),(4,1,1),(3,3,0),(3,2,1)(2,2,2).$$

除第一组外,后面 4 个分别是 f,f_1,f_2,f_3 的首项幂指数组,于是 $f_4=0$,且

$$\Phi_1=4\sigma_1^{4-1}\sigma_2^{1-1}\sigma_3^1=4\sigma_1^3\sigma_3,\Phi_2=a\sigma_1^{3-3}\sigma_2^{3-0}\sigma_3^0=a\sigma_2^3,$$

$$\Phi_3=b\sigma_1^{3-2}\sigma_2^{2-1}\sigma_3^1=b\sigma_1\sigma_2\sigma_3,\Phi_4=c\sigma_1^{2-2}\sigma_2^{2-2}\sigma_3^2=c\sigma_3^2.$$

因此

$$f(x_1,x_2,x_3)=f_1+\Phi_1=f_2+\Phi_2+\Phi_1=f_3+\Phi_3+\Phi_2+\Phi_1=f_4+\Phi_4+\Phi_3+\Phi_2+\Phi_1$$
$$=\Phi_4+\Phi_3+\Phi_2+\Phi_1=c\sigma_3^2+b\sigma_1\sigma_2\sigma_3+a\sigma_2^3+4\sigma_1^3\sigma_3.$$

为了确定 a,b,c 的值,x_1,x_2,x_3 分别用 1,1,0;1,1,1;1,1,-1 代入,得

$$\begin{cases}2\cdot 1^2\cdot 1^2=a\cdot 1^3,\\(2+1^2)^3=c+b\cdot 3\cdot 3\cdot 1+a\cdot 3^3+4\cdot 3^3\cdot 1,\\[2+(-1)^2](-2+1^2)(-2+1^2)=c+b\cdot 1\cdot(-1)\cdot(-1)+a\cdot(-1)^3+\\\qquad\qquad 4\cdot 1^3\cdot(-1).\end{cases}$$

解得 $a=2,b=-18,c=27$,因此

$$f(x_1,x_2,x_3)=4\sigma_1^3\sigma_3-18\sigma_1\sigma_2\sigma_3+2\sigma_2^3+27\sigma_3^2.$$

例 6 在 $K[x_1,x_2,x_3]$中,用初等对称多项式表出下述对称多项式:

$$f(x_1,x_2,x_3)=(2x_1-x_2-x_3)(2x_2-x_3-x_1)(2x_3-x_1-x_2).$$

解 $f(x_1,x_2,x_3)$的首项是 $2x_1(-x_1)(-x_1)=2x_1^3$,首项的幂指数组为$(3,0,0)$;$f(x_1,x_2,x_3)$是三次齐次对称多项式。满足 $p_1+p_2+p_3=3$ 且 $3\geqslant p_1\geqslant p_2\geqslant p_3$ 的非负整数组(p_1,p_2,p_3)只可能是

$$(3,0,0),(2,1,0),(1,1,1).$$

令

$$\Phi_1=2\sigma_1^{3-0}\sigma_2^{0-0}\sigma_3^0=2\sigma_1^3,\Phi_2=a\sigma_1^{2-1}\sigma_2^{1-0}\sigma_3^0=a\sigma_1\sigma_2,\Phi_3=b\sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^1=b\sigma_3.$$

因此 $$f(x_1,x_2,x_3)=\Phi_1+\Phi_2+\Phi_3=2\sigma_1^3+a\sigma_1\sigma_2+b\sigma_3.$$

把 x_1,x_2,x_3 分别用 1,1,0 和 1,1,1 代入,得

$$\begin{cases}(2-1-0)(2-0-1)(0-1-1)=2\cdot 2^3+a\cdot 2\cdot 1\\(2-1-1)^3=2\cdot 3^3+a\cdot 3\cdot 3+b\cdot 1\end{cases}$$

解得 $a=-9,b=27$,因此

$$f(x_1,x_2,x_3)=2\sigma_1^3-9\sigma_1\sigma_2+27\sigma_3.$$

例 7 证明:数域 K 上三次方程 $x^3+a_2x^2+a_1x+a_0=0$ 的 3 个复根成等差数列的充分必要条件为

$$2a_2^2-9a_1a_2+27a_0=0.$$

证明 设 $x^3+a_2x^2+a_1x+a_0=0$ 的 3 个复根为 c_1,c_2,c_3,则这 3 个复根成等差数列当且仅当下式成立:

$$(2c_1-c_2-c_3)(2c_2-c_1-c_3)(2c_3-c_1-c_2)=0.$$

据例 6 的结论,有

$$(2x_1-x_2-x_3)(2x_2-x_3-x_1)(2x_3-x_1-x_2)=2\sigma_1^3-9\sigma_1\sigma_2+27\sigma_3.$$

x_1,x_2,x_3 分别用 c_1,c_2,c_3 代入,且利用 Vieta 公式,从上式得

$$\begin{aligned}&(2c_1-c_2-c_3)(2c_2-c_3-c_1)(2c_3-c_1-c_2)\\=&2(-a_2)^3-9(-a_2)a_1+27(-a_0)\\=&-2a_2^3+9a_1a_2-27a_0.\end{aligned}$$

因此 $x^3+a_2x^2+a_1x+a_0=0$ 的 3 个复根成等差数列当且仅当

$$2a_2^3-9a_1a_2+27a_0=0.$$ ■

例 8 设数域 K 上三次方程 $x^3+a_2x^2+a_1x+a_0=0$ 的 3 个复根为 c_1,c_2,c_3,求它的某一复根的平方等于其他两个复根的平方和的充分必要条件。

解 上述三次方程的某一复根的平方等于其他两个复根的平方和当且仅当下式成立:

$$(c_1^2-c_2^2-c_3^2)(c_2^2-c_3^2-c_1^2)(c_3^2-c_1^2-c_2^2)=0.$$

由此受到启发,考虑下述对称多项式:

$$f(x_1,x_2,x_3)=(x_1^2-x_2^2-x_3^2)(x_2^2-x_3^2-x_1^2)(x_3^2-x_1^2-x_2^2).$$

它的首项是 $x_1^2(-x_1^2)(-x_1^2)=x_1^6$,首项幂指数组为(6,0,0),它是六次齐次多项式。满足 $p_1+p_2+p_3=6$ 且 $6\geqslant p_1\geqslant p_2\geqslant p_3$ 的非负整数组(p_1,p_2,p_3)只可能是

$$(6,0,0),(5,1,0),(4,2,0),(4,1,1),(3,3,0),(3,2,1),(2,2,2).$$

于是

$$f(x_1,x_2,x_3)=\sigma_1^6+a\sigma_1^4\sigma_2^1+b\sigma_1^2\sigma_2^2+c\sigma_1^3\sigma_3+d\sigma_2^3+e\sigma_1\sigma_2\sigma_3+h\sigma_3^2.$$

把 x_1,x_2,x_3 分别用 1,1,0;1,−1,0;1,2,0;1,1,1;1,1,−1;1,1,2 代入,得

$$0=2^6+a2^4+b2^2+d,\ 0=d(-1)^3,$$

$$
\begin{aligned}
(-3)\cdot 3\cdot(-5) &= 3^6+a\cdot 3^4\cdot 2+b\cdot 3^2\cdot 2^2+d\cdot 2^3,\\
(-1)(-1)(-1) &= 3^6+a\cdot 3^4\cdot 3+b\cdot 3^2\cdot 3^2+c\cdot 3^3\cdot 1,\\
&\quad +d\cdot 3^3+e\cdot 3\cdot 3\cdot 1+h\cdot 1^2,\\
(-1)(-1)(-1) &= 1^6+a\cdot 1^4(-1)+b\cdot 1^2(-1)^2+c\cdot 1^3(-1)\\
&\quad +d(-1)^3+e\cdot 1\cdot(-1)(-1)+h(-1)^2,\\
(-4)(-4)\cdot 2 &= 4^6+a\cdot 4^4\cdot 5+b\cdot 4^2\cdot 5^2+c\cdot 4^3\cdot 2\\
&\quad +d\cdot 5^3+e\cdot 4\cdot 5\cdot 2+h\cdot 2^2,
\end{aligned}
$$

解得 $a=-6, b=8, d=0, c=8, e=-16, h=8$。

因此 $f(x_1,x_2,x_3)=\sigma_1^6-6\sigma_1^4\sigma_2+8\sigma_1^2\sigma_2^2+8\sigma_1^3\sigma_3-16\sigma_1\sigma_2\sigma_3+8\sigma_3^2$.

x_1,x_2,x_3 用 c_1,c_2,c_3 代入，且用 Vieta 公式，得

$$
\begin{aligned}
&(c_1^2-c_2^2-c_3^2)(c_2^2-c_3^2-c_1^2)(c_3^2-c_1^2-c_2^2)\\
=&(-a_2)^6-6(-a_2)^4a_1+8(-a_2)^2a_1^2+8(-a_2)^3(-a_0)\\
&-16(-a_2)a_1(-a_0)+8(-a_2)^2\\
=&a_2^6-6a_2^4a_1+8a_2^2a_1^2+8a_2^3a_0-16a_2a_1a_0+8a_0^2.
\end{aligned}
$$

因此 $x^3+a_2x^2+a_1x+a_0=0$ 的某一复根平方等于其他两个复根的平方和当且仅当

$$a_2^6-6a_2^4a_1+8a_2^2a_1^2+8a_2^3a_0-16a_2a_1a_0+8a_0^2=0.$$

例 9 设 $1\leqslant k\leqslant n$，把幂和 $s_k(x_1,x_2,\cdots,x_n)$ 用初等对称多项式 $\sigma_1(x_1,x_2,\cdots,x_n)$，$\sigma_2(x_1,x_2,\cdots,x_n),\cdots,\sigma_k(x_1,x_2,\cdots,x_n)$ 表示。

解 根据牛顿公式，当 $1\leqslant k\leqslant n$ 时，有

$$s_k-\sigma_1s_{k-1}+\sigma_2s_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}s_1+(-1)^k k\sigma_k=0.$$

于是有

$$
\begin{aligned}
&s_1-\sigma_1=0,\\
&s_2-\sigma_1s_1+2\sigma_2=0,\\
&s_3-\sigma_1s_2+\sigma_2s_1-3\sigma_3=0,\\
&\cdots\\
&s_k-\sigma_1s_{k-1}+\sigma_2s_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}s_1+(-1)^k k\sigma_k=0.
\end{aligned}
$$

由此得出

$$
\begin{aligned}
s_1&=\sigma_1,\\
s_2&=\sigma_1s_1-2\sigma_2=\sigma_1^2-2\sigma_2\\
&=\begin{vmatrix}\sigma_1 & 1\\ 2\sigma_2 & \sigma_1\end{vmatrix},
\end{aligned}
$$

$$s_3=\sigma_1 s_2-\sigma_2 s_1+3\sigma_3$$
$$=\begin{vmatrix}\sigma_1 & 1 & 0\\ 2\sigma_2 & \sigma_1 & 1\\ 3\sigma_3 & \sigma_2 & \sigma_1\end{vmatrix}.$$

由此受到启发,猜想

$$s_k=\begin{vmatrix}\sigma_1 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0\\ 2\sigma_2 & \sigma_1 & 1 & 0 & 0 & 0 & \cdots & 0 & 0\\ 3\sigma_3 & \sigma_2 & \sigma_1 & 1 & 0 & 0 & \cdots & 0 & 0\\ 4\sigma_4 & \sigma_3 & \sigma_2 & \sigma_1 & 1 & 0 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots\\ (k-1)\sigma_{k-1} & \sigma_{k-2} & \sigma_{k-3} & \sigma_{k-4} & \sigma_{k-5} & \sigma_{k-6} & \cdots & \sigma_1 & 1\\ k\sigma_k & \sigma_{k-1} & \sigma_{k-2} & \sigma_{k-3} & \sigma_{k-4} & \sigma_{k-5} & \cdots & \sigma_2 & \sigma_1\end{vmatrix}.$$

先对 $k=4$ 验证一下这个猜想,按第 4 行展开下述行列式:

$$\begin{vmatrix}\sigma_1 & 1 & 0 & 0\\ 2\sigma_2 & \sigma_1 & 1 & 0\\ 3\sigma_3 & \sigma_2 & \sigma_1 & 1\\ 4\sigma_4 & \sigma_3 & \sigma_2 & \sigma_1\end{vmatrix}=-4\sigma_4+\sigma_3\begin{vmatrix}\sigma_1 & 0 & 0\\ 2\sigma_2 & 1 & 0\\ 3\sigma_3 & \sigma_1 & 1\end{vmatrix}-\sigma_2 s_2+\sigma_1 s_3$$
$$=-4\sigma_4+\sigma_3\sigma_1-\sigma_2 s_2+\sigma_1 s_3=s_4.$$

由此受到鼓舞,也促使我们用第二数学归纳法证明上述猜想。

$k=1$ 时,$|\sigma_1|=\sigma_1=s_1$,因此命题成立。

假设当小于 k 时命题成立($1<k\leqslant n$),现在来看 k 的情形。对于上述 k 阶行列式按第 k 行展开,得

$$(-1)^{k+1}k\sigma_k+(-1)^{k+2}\sigma_{k-1}\sigma_1+(-1)^{k+3}\sigma_{k-2}\begin{vmatrix}\sigma_1 & 1 & 0 & 0 & \cdots & 0 & 0\\ 2\sigma_2 & \sigma_1 & 0 & 0 & \cdots & 0 & 0\\ 3\sigma_3 & \sigma_2 & 1 & 0 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots\\ (k-1)\sigma_{k-1} & \sigma_{k-2} & \sigma_{k-4} & \sigma_{k-5} & \cdots & \sigma_1 & 1\end{vmatrix}$$
$$+\cdots+(-1)^{k+(k-1)}\sigma_2 s_{k-2}+(-1)^{k+k}\sigma_1 s_{k-1}$$
$$=(-1)^{k+1}k\sigma_k+(-1)^{k}\sigma_{k-1}s_1+(-1)^{k-1}\sigma_{k-2}s_{k-2}+\cdots+(-1)\sigma_2 s_{k-2}+\sigma_1 s_{k-1}=s_k.$$

由第二数学归纳法原理得,当 $1\leqslant k\leqslant n$ 时有

$$s_k=\begin{vmatrix}\sigma_1 & 1 & 0 & 0 & 0 & \cdots & 0 & 0\\ 2\sigma_2 & \sigma_1 & 1 & 0 & 0 & \cdots & 0 & 0\\ 3\sigma_3 & \sigma_2 & \sigma_1 & 1 & 0 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots\\ k\sigma_k & \sigma_{k-1} & \sigma_{k-2} & \sigma_{k-3} & \sigma_{k-4} & \cdots & \sigma_2 & \sigma_1\end{vmatrix}. \tag{5}$$

例 10 设 $1\leqslant k\leqslant n$,把初等对称多项式 $\sigma_k(x_1,x_2,\cdots,x_n)$ 用幂和 $s_1(x_1,x_2,\cdots,x_n)$,$s_2(x_1,x_2,\cdots,x_n),\cdots,s_k(x_1,x_2,\cdots,x_n)$ 表示。

解 根据牛顿公式,当 $1\leqslant k\leqslant n$ 时,可得

$$\sigma_1=s_1,$$

$$\sigma_2=\frac{1}{2}(\sigma_1 s_1-s_2)=\frac{1}{2}(s_1^2-s_2)=\frac{1}{2}\begin{vmatrix}s_1 & 1\\ s_2 & s_1\end{vmatrix},$$

$$\sigma_3=\frac{1}{3}(s_3-\sigma_1 s_2+\sigma_2 s_1)=\frac{1}{3}\left(s_3-s_1s_2+s_1\frac{1}{2}\begin{vmatrix}s_1 & 1\\ s_2 & s_1\end{vmatrix}\right)$$

$$=\frac{1}{6}\begin{vmatrix}s_1 & 1 & 0\\ s_2 & s_1 & 2\\ s_3 & s_2 & s_1\end{vmatrix}.$$

由此受到启发,猜想

$$\sigma_k=\frac{1}{k!}\begin{vmatrix}s_1 & 1 & 0 & 0 & \cdots & 0 & 0\\ s_2 & s_1 & 2 & 0 & \cdots & 0 & 0\\ s_3 & s_2 & s_1 & 3 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots\\ s_{k-1} & s_{k-2} & s_{k-3} & s_{k-4} & \cdots & s_1 & k-1\\ s_k & s_{k-1} & s_{k-2} & s_{k-3} & \cdots & s_2 & s_1\end{vmatrix}.$$

我们用第二数学归纳法证明这个猜想。

$k=1$ 时,$|s_1|=s_1=\sigma_1$,命题为真。

假设当小于 k 时命题为真($1<k\leqslant n$),现在来看 k 的情形。把上述右端的行列式按最后一行展开,得

$$(-1)^{k+1}s_k(k-1)!+(-1)^{k+2}s_{k-1}\begin{vmatrix}s_1 & 0 & 0 & \cdots & 0 & 0\\ s_2 & 2 & 0 & \cdots & 0 & 0\\ s_3 & s_1 & 3 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ s_{k-1} & s_{k-3} & s_{k-4} & \cdots & s_1 & k-1\end{vmatrix}$$

$$+(-1)^{k+3}s_{k-2}\begin{vmatrix} s_1 & 1 & 0 & \cdots & 0 & 0 \\ s_2 & s_1 & 0 & \cdots & 0 & 0 \\ s_3 & s_2 & 3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ s_{k-1} & s_{k-2} & s_{k-4} & \cdots & s_1 & k-1 \end{vmatrix}$$

$$+\cdots+(-1)^{k+(k-1)}s_2(k-1)(k-2)!\sigma_{k-2}+(-1)^{k+k}s_1(k-1)!\sigma_{k-1}$$

$$=(-1)^{k+1}(k-1)!s_k+(-1)^k s_{k-1}(k-1)!s_1+(-1)^{k-1}s_{k-2}(k-1)!\sigma_2$$

$$+\cdots+(-1)(k-1)!s_2\sigma_{k-2}+(k-1)!s_1\sigma_{k-1}$$

$$=\frac{k!}{k}[(-1)^{k+1}s_k+(-1)^k s_{k-1}\sigma_1+(-1)^{k-1}s_{k-2}\sigma_2+\cdots+(-1)s_2\sigma_{k-2}+s_1\sigma_{k-1}]$$

$$=k!\sigma_k.$$

根据第二数学归纳法原理得，当 $1\leqslant k\leqslant n$ 时，有

$$\sigma_k=\frac{1}{k!}\begin{vmatrix} s_1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ s_2 & s_1 & 2 & 0 & \cdots & 0 & 0 \\ s_3 & s_2 & s_1 & 3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ s_k & s_{k-1} & s_{k-2} & s_{k-3} & \cdots & s_2 & s_1 \end{vmatrix}. \tag{6}$$

点评 例 9 和例 10 分别是把幂和 $s_k(1\leqslant k\leqslant n)$ 用初等对称多项式 $\sigma_1,\sigma_2,\cdots,\sigma_k$ 表示，以及把初等对称多项式 $\sigma_k(1\leqslant k\leqslant n)$ 用幂和 $s_1,s_2,\cdots,s_k$ 表示，所得到公式(5)和(6)都有用。公式(5)可以用来求一元 n 次多项式的判别式。公式(6)在本节例 16 中有用。

例 9 和例 10 的解法体现了数学的思维方式，从观察 $k=1,2,3$ 的情形，猜想对一般的 k 有什么结论，然后给予证明。如果在题目中就把公式(5)和(6)写出来，那么就不知道这两个公式是怎么想出来的。学习数学和搞数学科研一样，关键是想法(idea)。

例 11 求数域 K 上不完全三次方程 $x^3+a_1x+a_0=0$ 的判别式。

解 记 $f(x)=x^3+a_1x+a_0$。三次方程 $x^3+a_1x+a_0$ 的判别式也就是 $f(x)$ 的判别式 $D(f)$，记 $f(x)$ 的 3 个复根为 c_1,c_2,c_3，则

$$D(f)=\begin{vmatrix} 3 & s_1(c_1,c_2,c_3) & s_2(c_1,c_2,c_3) \\ s_1(c_1,c_2,c_3) & s_2(c_1,c_2,c_3) & s_3(c_1,c_2,c_3) \\ s_2(c_1,c_2,c_3) & s_3(c_1,c_2,c_3) & s_4(c_1,c_2,c_3) \end{vmatrix}$$

根据牛顿(Newton)公式得

$$s_1=\sigma_1,\ s_2=\sigma_1s_1-2\sigma_2,\ s_3=\sigma_1s_2-\sigma_2s_1+3\sigma_3.$$

x_1,x_2,x_3 用 c_1,c_2,c_3 代入，结合 Vieta 公式，得 $\sigma_1(c_1,c_2,c_3)=0,\sigma_2(c_1,c_2,c_3)=a_1$，

$\sigma_3(c_1,c_2,c_3)=-a_0$。从而

$$\begin{aligned}
s_1(c_1,c_2,c_3) &=\sigma_1(c_1,c_2,c_3)\\
&=0,\\
s_2(c_1,c_2,c_3) &=\sigma_1(c_1,c_2,c_3)s_1(c_1,c_2,c_3)-2\sigma_2(c_1,c_2,c_3)\\
&=-2a_1,\\
s_3(c_1,c_2,c_3) &=\sigma_1(c_1,c_2,c_3)s_2(c_1,c_2,c_3)-\sigma_2(c_1,c_2,c_3)s_1(c_1,c_2,c_3)\\
&\quad+3\sigma_3(c_1,c_2,c_3)\\
&=3(-a_0)=-3a_0,\\
s_4(c_1,c_2,c_3) &=\sigma_1(c_1,c_2,c_3)s_3(c_1,c_2,c_3)-\sigma_2(c_1,c_2,c_3)s_2(c_1,c_2,c_3)\\
&\quad+\sigma_3(c_1,c_2,c_3)s_1(c_1,c_2,c_3)\\
&=-a_1(-2a_1)=2a_1^2.
\end{aligned}$$

因此

$$\begin{aligned}
D(f)&=\begin{vmatrix} 3 & 0 & -2a_1\\ 0 & -2a_1 & -3a_0\\ -2a_1 & -3a_0 & 2a_1^2 \end{vmatrix}\\
&=3\begin{vmatrix} -2a_1 & -3a_0\\ -3a_0 & 2a_1^2 \end{vmatrix}-2a_1\begin{vmatrix} 0 & -2a_1\\ -2a_1 & -3a_0 \end{vmatrix}\\
&=3(-4a_1^3-9a_0^2)-2a_1(-4a_1^2)\\
&=-4a_1^3-27a_0^2. \qquad (7)
\end{aligned}$$

例 12 设 $f(x)=x^3-x+1$,求 $f(x)$的判别式 $D(f)$,$f(x)$有没有重根?

解 $a_1=-1,a_0=1$。由例 11 的结论得

$$D(f)=-4\cdot(-1)^3-27\cdot 1^2=-23.$$

$D(f)\neq 0$,因此 $f(x)$没有重根。

例 13 设 $f(x)$是实系数三次多项式,讨论 $D(f)=0$,$D(f)>0$,$D(f)<0$ 时,$f(x)$的根的情况。

解 $D(f)=0$ 时,$f(x)$有重根,$D(f)>0$ 或 $D(f)<0$ 时,$f(x)$没有重根,由于 $\deg f(x)=3$,因此 $f(x)$至少有一个实根 c_1,设 $f(x)$的另外两个复根为 c_2,c_3。

当 $D(f)=0$ 时,由于 $f(x)$有重根,因此 $c_1=c_2$(或 c_3),或 $c_2=c_3$。若 $c_1=c_2$(或 c_3),则 $f(x)$有两个实根。由于实系数多项式的虚根共轭成对出现,因此 c_3(或 c_2)也必为实根。从而 $f(x)$有 3 个实根,若 $c_2=c_3$,同理 c_2 与 c_3 都是实根,从而 $f(x)$有 3 个实根。总之,当 $D(f)=0$ 时,$f(x)$有重根,且 3 个复根都是实数。

当 $D(f)>0$ 或 $D(f)<0$ 时,$f(x)$有 3 个不同的复根 c_1,c_2,c_3,其中 c_1 是实根。由于

$$D(f)=(c_1-c_2)^2(c_1-c_3)^2(c_2-c_3)^2,$$

因此当 c_2,c_3 都是实数时，有 $D(f)>0$；当 c_2,c_3 是一对共轭虚数时，设 $c_2=a+b\mathrm{i},c_3=a-b\mathrm{i}$，则

$$\begin{aligned}D(f)&=[c_1^2-c_1(c_3+c_2)+c_2c_3]^2(2b\mathrm{i})^2\\&=(c_1^2-c_1 2a+a^2+b^2)^2(-4b^2)\\&=-4[(c_1-a)^2+b^2]^2b^2<0.\end{aligned}$$

因此当 $D(f)>0$ 时，$f(x)$ 有 3 个互不相同的实根；当 $D(f)<0$ 时，$f(x)$ 有一个实根和一对共轭虚根。

点评 例 12 中的 $f(x)=x^3-x+1$，它的判别式 $D(f)<0$。据例 13 的结论，它有一个实根和一对共轭虚根。在 7.9 节的例 12 中我们用 Sturm 定理已经求出 x^3-x+1 有唯一实根。平面曲线 $y^2=x^3+a_1x+a_0$ 如果满足 $4a_1^3+27a_0^2>0$，那么它是一条椭圆曲线。这也就是多项式 $f(x)=x^3+a_1x+a_0$ 的判别式满足 $D(f)<0$。从而 $f(x)$ 只有一个实根。此时 $y^2=x^3+a_1x+a_0$ 的图形与 7.9 节中例 12 的图 7-2 类似。这样的曲线在公开密钥密码学中有用。

例 14 求数域 K 上完全三次方程

$$f(x)=x^3+a_2x^2+a_1x+a_0=0$$

的判别式。

解 设 $f(x)$ 的 3 个复根为 c_1,c_2,c_3，由 Vieta 公式得

$$\sigma_1(c_1,c_2,c_3)=-a_2,\sigma_2(c_1,c_2,c_3)=a_1,\sigma_3(c_1,c_2,c_3)=-a_0.$$

根据例 9 的公式(5)，x_1,x_2,x_3 分别用 c_1,c_2,c_3 代入，得

$$\begin{aligned}s_1(c_1,c_2,c_3)&=\sigma_1(c_1,c_2,c_3)=-a_2,\\s_2(c_1,c_2,c_3)&=[\sigma_1(c_1,c_2,c_3)]^2-2\sigma_2(c_1,c_2,c_3)\\&=(-a_2)^2-2a_1=a_2^2-2a_1,\\s_3(c_1,c_2,c_3)&=\begin{vmatrix}-a_2&1&0\\2a_1&-a_2&1\\-3a_0&a_1&-a_2\end{vmatrix}\\&=-a_2^3+3a_1a_2-3a_0.\end{aligned}$$

根据牛顿公式，x_1,x_2,x_3 分别用 c_1,c_2,c_3 代入得

$$\begin{aligned}s_4&=(c_1,c_2,c_3)\\&=(-a_2)(-a_2^3+3a_1a_2-3a_0)-a_1(a_2^2-2a_1)+(-a_0)(-a_2)\\&=a_2^4-4a_1a_2^2+4a_2a_0+2a_1^2.\end{aligned}$$

于是

$$
\begin{aligned}
D(f)&=\begin{vmatrix} 3 & -a_2 & a_2^2-2a_1 \\ -a_2 & a_2^2-2a_1 & -a_2^3+3a_1a_2-3a_0 \\ a_2^2-2a_1 & -a_2^3+3a_1a_2-3a_0 & a_2^4-4a_1a_2^2+4a_2a_0+2a_1^2 \end{vmatrix}\\
&=\begin{vmatrix} 3 & -a_2 & a_2^2-2a_1 \\ -a_2 & a_2^2-2a_1 & -a_2^3+3a_1a_2-3a_0 \\ -2a_1 & a_1a_2-3a_0 & -a_2^2a_1+a_2a_0+2a_1^2 \end{vmatrix}\\
&=\begin{vmatrix} 3 & -a_2 & -2a_1 \\ -a_2 & a_2^2-2a_1 & a_1a_2-3a_0 \\ -2a_1 & a_1a_2-3a_0 & -2a_2a_0+2a_1^2 \end{vmatrix}\\
&=\begin{vmatrix} 3 & -a_2 & -2a_1 \\ 0 & \frac{2}{3}a_2^2-2a_1 & \frac{1}{3}a_1a_2-3a_0 \\ 0 & \frac{1}{3}a_1a_2-3a_0 & -2a_2a_0+\frac{2}{3}a_1^2 \end{vmatrix}\\
&=3\left[\left(-\frac{4}{3}a_2^3a_0+\frac{4}{9}a_2^2a_1^2+4a_2a_1a_0-\frac{4}{3}a_1^3\right)-\left(\frac{1}{9}a_1^2a_2^2-2a_2a_1a_0+9a_0^2\right)\right]\\
&=-4a_2^3a_0+a_2^2a_1^2+18a_2a_1a_0-4a_1^3-27a_0^2. \qquad (8)
\end{aligned}
$$

例 15 求数域 K 上 n 次多项式 $f(x)=x^n+a$ 的判别式。

解 设 $f(x)$的 n 个复根为 $c_1,c_2,\cdots,c_n$。由 Vieta 公式,得

$$\sigma_1(c_1,c_2,\cdots,c_n)=\sigma_2(c_1,c_2,\cdots,c_n)=\cdots=\sigma_{n-1}(c_1,c_2,\cdots,c_n)=0,$$

$$\sigma_n(c_1,c_2,\cdots,c_n)=(-1)^n a.$$

当 $1\leqslant k<n$ 时,根据例 9 的公式(5),$x_1,x_2,\cdots,x_n$ 分别用 $c_1,c_2,\cdots,c_n$ 代入,得

$$s_k(c_1,c_2,\cdots,c_n)=\begin{vmatrix} 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 \end{vmatrix}=0.$$

当 $k=n$ 时,有

$$s_n(c_1,c_2,\cdots,c_n)=\begin{vmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ n(-1)^n a & 0 & 0 & \cdots & 0 & 0 \end{vmatrix}$$

$$= (-1)^{n-1}(-1)^n na = -na.$$

当 $n<k<2n$ 时，根据牛顿公式，$x_1, x_2, \cdots, x_n$ 分别用 $c_1, c_2, \cdots, c_n$ 代入，得

$$s_k(c_1, c_2, \cdots, c_n) = 0.$$

于是

$$D(f) = \begin{vmatrix} n & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & -na \\ 0 & 0 & 0 & \cdots & -na & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & -na & 0 & \cdots & 0 & 0 \end{vmatrix}$$

$$= (-1)^{\tau(1n(n-1)\cdots 2)} n(-na)^{n-1}$$

$$= (-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}.$$

例 16　求数域 K 上的 n 次多项式 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$，使得它的 n 个复根的 k 次幂的和等于 0，其中 $1 \leqslant k < n$。

解　设 $f(x)$ 的 n 个复根为 $c_1, c_2, \cdots, c_n$，则由已知条件得

$$s_1(c_1, \cdots, c_n) = s_2(c_1, \cdots, c_n) = \cdots = s_{n-1}(c_1, \cdots, c_n) = 0.$$

为了求 $f(x)$ 的各项系数的值，只要先求 $\sigma_1(c_1, \cdots, c_n), \cdots, \sigma_{n-1}(c_1, \cdots, c_n), \sigma_n(c_1, \cdots, c_n)$。利用例 10 的公式(6)，$x_1, x_2, \cdots, x_n$ 分别用 $c_1, c_2, \cdots, c_n$ 代入，当 $1 \leqslant k \leqslant n-1$ 时，有

$$\sigma_k(c_1, \cdots, c_n) = \frac{1}{k!} \begin{vmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{vmatrix} = 0,$$

而

$$\sigma_n(c_1, \cdots, c_n) = \frac{1}{n!} \begin{vmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 2 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & n-1 \\ b & 0 & 0 & 0 & \cdots & 0 & 0 \end{vmatrix}$$

$$= (-1)^{n+1} \frac{b}{n},$$

其中 $b = s_n(c_1, c_2, \cdots, c_n)$，根据 Vieta 公式得

$$a_{n-1} = a_{n-2} = \cdots = a_1 = 0,\ a_0 = (-1)^n(-1)^{n+1} \frac{b}{n} = -\frac{b}{n}.$$

因此所求的多项式 $f(x)=x^n-\dfrac{b}{n}$。

点评 从例 15 的解题过程和例 16 的结论看出，数域 K 上首项系数为 1 的 n 次多项式 $f(x)$，它的 n 个复根的 k 次幂的和($1\leqslant k<n$)都等于 0 当且仅当 $f(x)=x^n-\dfrac{b}{n}$，其中 b 是 $f(x)$的 n 个复根的 n 次幂的和，这个命题的必要性在 9.7 节的例 4 中有用。

习题 7.10

1. 设 $f(x_1,x_2,x_3)$是数域 K 上的一个三元多项式：

$$f(x_1,x_2,x_3)=x_1^3x_2^2+x_1^3x_3^2+x_1^2x_2^3+x_1^2x_3^3+x_2^3x_3^2+x_2^2x_3^3.$$

证明 $f(x_1,x_2,x_3)$是对称多项式。

2. 在 $K[x_1,x_2,x_3]$的含有项 $x_1^3x_2$ 的对称多项式中，写出项数最少的那个对称多项式。

3. 在 $K[x_1,x_2,x_3]$中，用初等对称多项式表出下列对称多项式：

(1) $x_1^3x_2+x_1^3x_3+x_1x_2^3+x_1x_3^3+x_2^3x_3+x_2x_3^3$；

(2) $x_1^4+x_2^4+x_3^4$；

(3) $(x_1x_2+x_3^2)(x_2x_3+x_1^2)(x_3x_1+x_2^2)$。

4. 在 $K[x_1,x_2,\cdots,x_n]$中，用初等对称多项式表出下列对称多项式($n\geqslant 3$)：

(1) $\sum x_1^3$；

(2) $\sum x_1^2x_2^2x_3$。

5. 证明：数域 K 上三次方程 $x^3+a_2x^2+a_1x+a_0=0$ 的 3 个复根成等比数列的充分必要条件为 $a_2^3a_0-a_1^3=0$。

6. 设 c_1,c_2,c_3 是 $x^3+a_2x^2+a_1x+a_0$ 的 3 个复根，计算

$$(c_1^2+c_1c_2+c_2^2)(c_2^2+c_2c_3+c_3^2)(c_3^2+c_3c_1+c_1^2).$$

7. 在 $K[x_1,x_2,x_3]$中，把幂和 s_2,s_3,s_4 表示成初等对称多项式 $\sigma_1,\sigma_2,\sigma_3$ 的多项式。

8. 求数域 K 上四次多项式 $f(x)=x^4+a_1x+a_0$ 的判别式。

9. 设 $f(x)$是实系数 n 次多项式，其中 $n\geqslant 4$。证明：如果 $D(f)>0$，那么 $f(x)$无重根且有偶数对虚根；如果 $D(f)<0$，那么 $f(x)$无重根且有奇数对虚根。

10. 求数域 K 上的 n 次多项式 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$，使得它的 n 个复根的 k 次幂的和等于 0，其中 $2\leqslant k\leqslant n$。

11. 设 $f(x)$是数域 K 上首项系数为 1 的 n 次多项式，$a\in K$，$g(x)=(x-a)f(x)$。证明：$D(g)=D(f)f(a)^2$。

12. 设 $f(x_1,x_2,\cdots,x_n)\in K[x_1,x_2,\cdots,x_n]$，其中 K 是数域。证明：如果 $f(\sigma_1,\sigma_2,\cdots,\sigma_n)=0$，那么 $f(x_1,x_2,\cdots,x_n)=0$。

* 7.11 结　式

7.11.1 内容精华

7.10 节讨论的求数域 K 上一元 n 次多项式 $f(x)$的判别式 $D(f)$，首先要求出 $f(x)$的 n 个复根 $c_1,c_2,\cdots,c_n$ 的 k 次幂的和 $s_k(c_1,c_2,\cdots,c_n)$，其中 $1\leqslant k\leqslant 2n-2$，然后再计算由这些幂和排成的 n 阶行列式。当 n 较大时，计算量是较大的。有没有其他方法求 $D(f)$呢？引进一元多项式 $f(x)$的判别式 $D(f)$这个概念是为了判断 $f(x)$在复数域中有没有重根。我们知道 $f(x)$在复数域中有重根当且仅当 $f(x)$在 $\mathbf{C}[x]$中有重因式。由于 $f(x)$有无重因式不随数域的扩大而改变，因此 $f(x)$在 $\mathbf{C}[x]$中有重因式当且仅当 $f(x)$在 $K[x]$中有重因式，而 $f(x)$在 $K[x]$中有重因式当且仅当 $f(x)$与 $f'(x)$不互素。于是我们可以用辗转相除法求 $f(x)$与 $f'(x)$的最大公因式。$f(x)$在复数域中有重根当且仅当$(f(x),f'(x))\neq 1$。我们在 7.6 节的典型例题和习题中曾经用辗转相除法讨论过一些多项式在复数域中有重根的充分必要条件。把判别 $f(x)$在复数域中有没有重根的这两种方法结合起来就得出，$f(x)$的判别式 $D(f)=0$ 当且仅当$(f(x),f'(x))\neq 1$，而 $f(x)$与 $f'(x)$不互素当且仅当 $f(x)$与 $f'(x)$在复数域中有公共根。由此受到启发，如果我们能研究出 $K[x]$中两个多项式$f(x)$与 $g(x)$在复数域有没有公共根的新的判别方法，那么就能给出求 $f(x)$的判别式 $D(f)$的又一种方法，而且还可以用来求两个二元多项式的公共零点，进一步可以用来求 n 个 n 元多项式的公共零点，达到一箭三雕的效果。

设

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n,$$
$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m$$

是 $K[x]$中两个非零多项式，其中 $n>0$，$m>0$，并且允许 $a_0=0$ 或 $b_0=0$(包括 $a_0=b_0=0$)这些可能性。

首先我们来求 $f(x)$与 $g(x)$有公共复根(即 $f(x)$与 $g(x)$不互素)的必要条件。设 $f(x)$与 $g(x)$有次数大于 0 的公因式 $d(x)$，则存在 $f_1(x),g_1(x)\in K[x]$，使得

$$f(x)=f_1(x)d(x),\ g(x)=g_1(x)d(x). \tag{1}$$

由于 $\deg d(x)>0$,因此

$$\deg f_1(x)<\deg f(x)\leqslant n,\ \deg g_1(x)<\deg g(x)\leqslant m.$$

从(1)式得

$$g_1(x)f(x)=f_1(x)g(x). \tag{2}$$

设

$$f_1(x)=u_0x^{n-1}+u_1x^{n-2}+\cdots+u_{n-1}, \tag{3}$$

$$g_1(x)=v_0x^{m-1}+v_1x^{m-2}+\cdots+v_{m-1}. \tag{4}$$

比较(2)式两边多项式的各次项的系数,得

$$\begin{cases} a_0v_0 & & & & & & & & & = b_0u_0 \\ a_1v_0+a_0v_1 & & & & & & & & & = b_1u_0+b_0u_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & a_nv_{m-2}+a_{n-1}v_{m-1} & & & & & & & = b_mu_{n-2}+b_{m-1}u_{n-1} \\ & & & & a_nv_{m-1} & & & & & = b_mu_{n-1}. \end{cases} \tag{5}$$

由于 $f(x)\neq0$,$g(x)\neq0$,因此 $f_1(x)\neq0$,$g_1(x)\neq0$,从而

$$(u_0,u_1,\cdots,u_{n-1})\neq0,\ (v_0,v_1,\cdots,v_{m-1})\neq0.$$

于是(5)式表明相应的 $m+n$ 元齐次线性方程组有非零解:

$$(v_0,v_1,\cdots,v_{m-1},-u_0,-u_1,\cdots,-u_{n-1}). \tag{6}$$

因此它的系数矩阵 A 的行列式等于零,从而 $|A'|=0$,即

$$\begin{array}{l} m\text{ 行}\left\{\begin{array}{l}\\\\\\\\\end{array}\right. \\ n\text{ 行}\left\{\begin{array}{l}\\\\\\\\\end{array}\right. \end{array}\left|\begin{array}{ccccccccccc} a_0 & a_1 & \cdots & \cdots & \cdots & \cdots & a_n & & & & \\ & a_0 & a_1 & \cdots & \cdots & \cdots & \cdots & a_n & & & \\ & & & \cdots & \cdots & \cdots & \cdots & \cdots & & & \\ & & & & a_0 & a_1 & \cdots & \cdots & \cdots & \cdots & a_n \\ b_0 & b_1 & \cdots & \cdots & \cdots & b_m & & & & & \\ & b_0 & b_1 & \cdots & \cdots & \cdots & b_m & & & & \\ & & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & \\ & & & & & & b_0 & b_1 & \cdots & \cdots & b_m \end{array}\right|=0. \tag{7}$$

由此受到启发,引进下述概念:

定义 1 设

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,$$

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m$$

是数域 K 上两个多项式，其中 $n>0$，$m>0$，(7)式左端的行列式称为 $f(x)$ 与 $g(x)$ 的**结式**，记作 $\mathrm{Res}(f,g)$。

上面的讨论表明：$K[x]$ 中两个非零多项式 $f(x)$ 与 $g(x)$ 有公共复根的必要条件是它们的结式 $\mathrm{Res}(f,g)=0$。现在来看这是不是充分条件。

设 $\mathrm{Res}(f,g)=0$，则上述与(5)式相应的齐次线性方程组有非零解(6)，从而(5)式成立。令 $f_1(x)$，$g_1(x)$ 分别如(3)、(4)式，则(2)式成立，并且有 $\deg f_1<n$，$\deg g_1<m$。现在我们增加一个条件：a_0 与 b_0 不全为 0，不妨设 $a_0\neq 0$，则 $\deg f=n$。从(2)式得 $f(x)\mid f_1(x)g(x)$。假如 $(f(x),g(x))=1$，则 $f(x)\mid f_1(x)$，从而 $\deg f\leqslant \deg f_1<n$，矛盾。因此 $f(x)$ 与 $g(x)$ 不互素，从而 $f(x)$ 与 $g(x)$ 有公共复根。

综合上述讨论，我们可以得到下面的结论：

定理 1　设

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n,$$
$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m$$

是 $K[x]$ 中两个多项式，其中 $n>0$ 且 $m>0$，则 $f(x)$ 与 $g(x)$ 的结式 $\mathrm{Res}(f,g)=0$ 的充分必要条件是 $a_0=b_0=0$，或者 $f(x)$ 与 $g(x)$ 有公共复根。

证明　如果 $f(x)$ 与 $g(x)$ 都是零多项式，那么命题显然成立。

如果 $f(x)$ 与 $g(x)$ 有且只有一个是零多项式，不妨设 $g(x)=0$，$f(x)\neq 0$，此时 $\mathrm{Res}(f,g)=0$。若 $a_0\neq 0$，则 $f(x)$ 的次数为 $n>0$。此时 $f(x)$ 的 n 个复根都是 $f(x)$ 与 $g(x)$ 的公共复根。

下面设 $f(x)$ 与 $g(x)$ 都是非零多项式，设 $\mathrm{Res}(f,g)=0$，如果 a_0 与 b_0 不全为 0，那么上面已证 $f(x)$ 与 $g(x)$ 有公共复根，因此必要性得证。充分性有一半已证(即从 $f(x)$ 与 $g(x)$ 有公共复根已经推导出 $\mathrm{Res}(f,g)=0$)。现在证另一半：若 $a_0=b_0=0$，则 $\mathrm{Res}(f,g)$ 的第 1 列全为 0，从而 $\mathrm{Res}(f,g)=0$。■

定理 1 的第一个用处是给出了判别数域 K 上两个非零多项式有没有公共复根的新方法：n 次和 m 次多项式 $f(x)$ 与 $g(x)$ 有公共复根当且仅当 $\mathrm{Res}(f,g)=0$。

定理 1 的第二个用处是可以用来求数域 K 上两个二元多项式在 $\mathbf{C}^2$ 中的公共零点。设 $f(x,y),g(x,y)\in K[x,y]$，把它们都按 x 的降幂排列写出：

$$f(x,y)=a_0(y)x^n+a_1(y)x^{n-1}+\cdots+a_n(y),\tag{8}$$
$$g(x,y)=b_0(y)x^m+b_1(y)x^{m-1}+\cdots+b_m(y),\tag{9}$$

其中 $a_i(y),b_j(y),i=0,1,\cdots,n,j=0,1,\cdots,m$，都是 y 的多项式，且 $a_0(y)$ 与 $b_0(y)$ 不全为 0。

如果 (x_0,y_0) 是 $f(x,y)$ 与 $g(x,y)$ 在 $\mathbf{C}^2$ 中的一个公共零点，那么 $f(x_0,y_0)=0$，$g(x_0,y_0)=0$，从而 x_0 是 x 的复系数多项式 $f(x,y_0)$ 与 $g(x,y_0)$ 的一个公共根，据定理 1

得，$f(x,y_0)$与 $g(x,y_0)$的结式 $\mathrm{Res}(f(x,y_0),g(x,y_0))=0$。由此受到启发，我们考虑下述 $m+n$ 阶行列式，并且把它记作 $R_x(f,g)$，即

$$R_x(f,g)=\left|\begin{array}{cccccccccc}
a_0(y) & a_1(y) & \cdots & \cdots & \cdots & \cdots & a_n(y) & & & \\
 & a_0(y) & a_1(y) & \cdots & \cdots & \cdots & \cdots & a_n(y) & & \\
 & & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\
 & & & & a_0(y) & a_1(y) & \cdots & \cdots & a_n(y) & \\
b_0(y) & b_1(y) & \cdots & \cdots & \cdots & \cdots & b_m(y) & & & \\
 & b_0(y) & b_1(y) & \cdots & \cdots & \cdots & \cdots & b_m(y) & & \\
 & & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\
 & & & b_0(y) & b_1(y) & \cdots & \cdots & \cdots & b_m(y) &
\end{array}\right.\begin{array}{l}\left.\begin{array}{l}\\\\\\\end{array}\right\}m\text{ 行}\\ \left.\begin{array}{l}\\\\\\\end{array}\right\}n\text{ 行}\end{array}\tag{10}$$

$R_x(f,g)$是 y 的一个多项式，不定元 y 用 y_0 代入，$R_x(f,g)$的象就是 $\mathrm{Res}(f(x,y_0),g(x,y_0))$。因此如果$(x_0,y_0)$是 $f(x,y)$与 $g(x,y)$在 $\mathbf{C}^2$ 中的一个公共零点，那么 y_0 就是多项式 $R_x(f,g)$的一个复根，而 x_0 是 $f(x,y_0)$与 $g(x,y_0)$的一个公共复根。

反之，如果 y_0 是多项式 $R_x(f,g)$的一个复根，那么

$$\mathrm{Res}(f(x,y_0),g(x,y_0))=0.$$

根据定理 1 得，$f(x,y_0)$与 $g(x,y_0)$有公共复根。任取 $f(x,y_0)$与 $g(x,y_0)$的一个公共复根 x_0，都有(x_0,y_0)是 $f(x,y)$与 $g(x,y)$在 $\mathbf{C}^2$ 中的公共零点。

上述讨论给出了求数域 K 上两个二元多项式 $f(x,y)$与 $g(x,y)$在 $\mathbf{C}^2$ 中的公共零点的方法：第一步，计算 $R_x(f,g)$；第二步，求 $R_x(f,g)$的所有复根；第三步，对于 $R_x(f,g)$的每一个复根 y_0，求 $f(x,y_0)$与 $g(x,y_0)$的所有公共复根；第四步，写出 $f(x,y)$与 $g(x,y)$在 $\mathbf{C}^2$ 中的所有公共零点。

由于 x 与 y 的地位是对称的，因此也可以类似地定义 $R_y(f,g)$，先求 $R_y(f,g)$的所有复根，然后对于 $R_y(f,g)$的每一个复根 x_0，去求 $f(x_0,y)$与 $g(x_0,y)$的所有公共复根，最后就可以写出 $f(x,y)$与 $g(x,y)$在 $\mathbf{C}^2$ 中的所有公共零点。

上述方法也适用于解二元高次方程组：

$$\begin{cases}f(x,y)=0,\\ g(x,y)=0.\end{cases}\tag{11}$$

解方程组(11)就是求 $f(x,y)$与 $g(x,y)$的公共零点。

进一步可以用类似于上述方法求 n 个 n 元多项式在 $\mathbf{C}^n$ 中的所有公共零点。参看本节习题的第 8 题及书末的习题解答。

定理 1 的第三个用处是可以通过计算 $f(x)$与 $f'(x)$的结式 $\mathrm{Res}(f,f')$来求 $f(x)$的判别式 $D(f)$。这个想法是自然的，因为 $\mathrm{Res}(f,f')=0$ 当且仅当 $f(x)$与 $f'(x)$有公共复根，而 $f(x)$与 $f'(x)$有公共复根当且仅当 $D(f)=0$，由此看出 $\mathrm{Res}(f,f')$与 $D(f)$必然有联系。为了找出它们之间的内在联系，我们注意到 $D(f)$是用 $f(x)$的 n 个复根的表达式来定义的，从而探索的思路是去寻找 $\mathrm{Res}(f,f')$与 $f(x)$的复根之间的关系。一般地，就是要去寻找 $\mathrm{Res}(f,g)$与 $f(x)$的复根(或 $g(x)$的复根)之间的关系。

设 $f(x),g(x)$是定义 1 中给出的数域 K 上的两个多项式，且 $a_0\neq 0,b_0\neq 0$，设 $f(x)$的 n 个复根为 $c_1,c_2,\cdots,c_n$；$g(x)$的 m 个复根为 $d_1,d_2,\cdots,d_m$，于是

$$f(x)=a_0(x-c_1)(x-c_2)\cdots(x-c_n), \tag{12}$$

$$g(x)=b_0(x-d_1)(x-d_2)\cdots(x-d_m). \tag{13}$$

根据 Vieta 公式得，$f(x)$的 $n-k$ 次项的系数 a_k 为

$$a_k=(-1)^k a_0\sigma_k(c_1,c_2,\cdots,c_n),k=1,2,\cdots,n. \tag{14}$$

$g(x)$的 $m-k$ 次项的系数 b_k 为

$$b_k=(-1)^k b_0\sigma_k(d_1,d_2,\cdots,d_m),k=1,2,\cdots,m. \tag{15}$$

$f(x)$与 $g(x)$的结式 $\mathrm{Res}(f,g)$是由它们的系数 $a_0,a_1,\cdots,a_n,b_0,b_1,\cdots,b_m$ 排列成的一个 $m+n$ 阶行列式，想研究 $\mathrm{Res}(f,g)$与 $f(x)$的复根(或 $g(x)$的复根)之间的关系，自然要利用(14)式和(15)式。为了能利用多项式的理论来研究这个问题，我们在数域 K 上的$n+m+1$元多项式环

$$K[x,y_1,\cdots,y_n,z_1,\cdots,z_m]$$

中，令

$$\widetilde{f}(x,y_1,\cdots,y_n)=a_0(x-y_1)(x-y_2)\cdots(x-y_n), \tag{16}$$

$$\widetilde{g}(x,z_1,\cdots,z_m)=b_0(x-z_1)(x-z_2)\cdots(x-z_m). \tag{17}$$

把 $\widetilde{f}$ 按 x 的降幂排列，则 x^n 的系数为 a_0，x^{n-k}的系数为

$$a_k(y_1,\cdots,y_n)=(-1)^k a_0\sigma_k(y_1,\cdots,y_n),k=1,2,\cdots,n. \tag{18}$$

同理，把 $\widetilde{g}$ 按 x 的降幂排列，则 x^m 的系数为 b_0，x^{m-k}的系数为

$$b_k(z_1,\cdots,z_m)=(-1)^k b_0\sigma_k(z_1,\cdots,z_m),k=1,2,\cdots,m. \tag{19}$$

仿照定义 1，规定 $\widetilde{f}$ 与 $\widetilde{g}$ 对 x 的结式为

$$\mathrm{Res}_x(\widetilde{f},\widetilde{g})=$$

$$\begin{vmatrix}
a_0 & a_1(y_1,\cdots,y_n) & \cdots & \cdots & a_n(y_1,\cdots,y_n) & & \\
 & a_0 & a_1(y_1,\cdots,y_n) & \cdots & \cdots & a_n(y_1,\cdots,y_n) & \\
 & & \cdots & \cdots & \cdots & \cdots & \\
 & & a_0 & a_1(y_1,\cdots,y_n) & \cdots & \cdots & a_n(y_1,\cdots,y_n)\\
b_0 & b_1(z_1,\cdots,z_m) & \cdots & \cdots & b_m(z_1,\cdots,z_m) & & \\
 & b_0 & b_1(z_1,\cdots,z_m) & \cdots & \cdots & b_m(z_1,\cdots,z_m) & \\
 & & \cdots & \cdots & \cdots & \cdots & \\
 & & b_0 & b_1(z_1,\cdots,z_m) & \cdots & \cdots & b_m(z_1,\cdots,z_m)
\end{vmatrix} \tag{20}$$

显然，$\mathrm{Res}_x(\widetilde{f},\widetilde{g})\in K[y_1,\cdots,y_n,z_1,\cdots,z_m]$。把不定元 $y_1,y_2,\cdots,y_n,z_1,\cdots,z_m$ 分别用 $c_1,c_2,\cdots,c_n,d_1,\cdots,d_m$ 代入，结合(14)、(15)、(18)和(19)式便知道，$\mathrm{Res}_x(\widetilde{f},\widetilde{g})$ 的象就是 $\mathrm{Res}(f,g)$。于是如果我们能求出 $\mathrm{Res}_x(\widetilde{f},\widetilde{g})$ 的一个明显的表达式，那么就能得到 $\mathrm{Res}(f,g)$ 的一个明显的表达式。

从(18)式看出，$a_k(y_1,\cdots,y_n)$ 是 k 次齐次多项式，其中 $k=1,2,\cdots,n$；从(19)式看出，$b_k(z_1,\cdots,z_m)$ 是 k 次齐次多项式，其中 $k=1,2,\cdots,m$。由此受到启发，把(20)式右端的行列式 D 的第 1 行乘 y_1，第 2 行乘 y_1^2，…，第 m 行乘 y_1^m，第 $m+1$ 行乘 y_1，第 $m+2$ 行乘 y_1^2，…，第 $m+n$ 行乘 y_1^n，得到一个行列式 $\widetilde{D}$，则 $\widetilde{D}$ 的第 1 列元素都是一次齐次多项式，第 2 列元素都是二次齐次多项式，…，第 $m+n$ 列元素都是 $m+n$ 次齐次多项式。由于 $\widetilde{D}$ 的每一项是从 $\widetilde{D}$ 的第 $1,2,\cdots,m+n$ 列各取一个元素(它们位于不同行)作成的乘积，因此 $\widetilde{D}$ 的每一个非零项的次数为

$$1+2+\cdots+(n+m)=\frac{1}{2}(n+m+1)(n+m).$$

把 $\widetilde{D}$ 的第 1 行提出 y_1，…，第 m 行提出 y_1^m，第 $m+1$ 行提出 y_1，…，第 $m+n$ 行提出 y_1^n，得

$$\widetilde{D}=y_1y_1^2\cdots y_1^m y_1y_1^2\cdots y_1^n D=y_1^{\frac{m(m+1)+n(n+1)}{2}}D.$$

从而 D 的每一个非零项的次数是

$$\frac{1}{2}(n+m+1)(n+m)-\frac{1}{2}[m(m+1)+n(n+1)]=mn.$$

这证明了 $\mathrm{Res}_x(\widetilde{f},\widetilde{g})$ 是 $y_1,\cdots,y_n,z_1,\cdots,z_m$ 的 mn 次齐次多项式。

从(17)式和(16)式分别得出：

$$\widetilde{g}(x,z_1,\cdots,z_m)=b_0x^m+\cdots+b_k(z_1,\cdots,z_m)x^{m-k}+\cdots+b_m(z_1,\cdots,z_m), \tag{21}$$

$$\widetilde{f}(x,y_1,\cdots,y_n)=a_0x^n+\cdots+a_k(y_1,\cdots,y_n)x^{n-k}+\cdots+a_n(y_1,\cdots,y_n). \tag{22}$$

把 x 用 y_i 代入($i=1,2,\cdots,n$)，从(21)、(16)式分别得到

$$\widetilde{g}(y_i,z_1,\cdots,z_m)=b_0y_i^m+\cdots+b_k(z_1,\cdots,z_m)y_i^{m-k}+\cdots+b_m(z_1,\cdots,z_m),\tag{23}$$

$$\widetilde{f}(y_i,y_1,\cdots,y_n)=0.\tag{24}$$

把(22)式代入(24)式,得

$$a_0y_i^n+\cdots+a_k(y_1,\cdots,y_n)y_i^{n-k}+\cdots+a_n(y_1,\cdots,y_n)=0.\tag{25}$$

由此受到启发,我们把 D 的第 1 列乘 y_i^{n+m-1},第 2 列乘 y_i^{n+m-2},…,第 $n+m-1$ 列乘 y_i,然后把它们都加到第 $n+m$ 列上,得到一个行列式 D^*,则 $D=D^*$。利用(23)式和(25)式可得出 D^* 的第 $n+m$ 列为

$$\begin{pmatrix} y_i^{m-1}\ 0\\ y_i^{m-2}\ 0\\ \vdots\\ 0\\ y_i^{n-1}\widetilde{g}(y_i,z_1,\cdots,z_m)\\ y_i^{n-2}\widetilde{g}(y_i,z_1,\cdots,z_m)\\ \vdots\\ \widetilde{g}(y_i,z_1,\cdots,z_m)\end{pmatrix}.$$

从 D^* 的第 $n+m$ 列提出公因子 $\widetilde{g}(y_i,z_1,\cdots,z_m)$,由此得出

$$\widetilde{g}(y_i,z_1,\cdots,z_m)\mid \mathrm{Res}_x(\widetilde{f},\widetilde{g}),\tag{26}$$

其中 $i=1,2,\cdots,n$。由于

$$\widetilde{g}(y_i,z_1,\cdots,z_m)=b_0(y_i-z_1)(y_i-z_2)\cdots(y_i-z_m),$$

$$\widetilde{g}(y_j,z_1,\cdots,z_m)=b_0(y_j-z_1)(y_j-z_2)\cdots(y_j-z_m),$$

因此当 $i\neq j$ 时,$\widetilde{g}(y_i,z_1,\cdots,z_m)$与 $\widetilde{g}(y_j,z_1,\cdots,z_m)$没有公共的一次因式。据唯一因式分解定理得

$$\prod_{i=1}^{n}\widetilde{g}(y_i,z_1,\cdots,z_m)\ \Big|\ \mathrm{Res}_x(\widetilde{f},\widetilde{g}).\tag{27}$$

由于 $\prod\limits_{i=1}^{n}\widetilde{g}(y_i,z_1,\cdots,z_m)$ 的次数为 mn,与 $\mathrm{Res}_x(\widetilde{f},\widetilde{g})$的次数相等,因此从(27)式得

$$\mathrm{Res}_x(\widetilde{f},\widetilde{g})=r\prod_{i=1}^{n}\widetilde{g}(y_i,z_1,\cdots,z_m).\tag{28}$$

对于某个 $r\in K^*$,为了确定 r 的值,把 $y_1,\cdots,y_n,z_1,\cdots,z_m$ 分别用 $0,\cdots,0,1,\cdots,1$ 代入,从(18)和(19)式得到(20)式右端的行列式为下述下三角形行列式:

$$\begin{vmatrix} a_0 & & & & & & & & \\ & a_0 & & & & & & & \\ & & \cdots & \cdots & \cdots & \cdots & \cdots & & \\ & & & a_0 & & & & & \\ b_0 & -b_0 m & \cdots & (-1)^{m-1} b_0 m & (-1)^m b_0 & & & & \\ & b_0 & \cdots & \cdots & \cdots & (-1)^{m-1} b_0 m & (-1)^m b_0 & & \\ & & \cdots & \cdots & \cdots & \cdots & \cdots & & \\ & & & b_0 & -b_0 m & \cdots & (-1)^{m-1} b_0 m & (-1)^m b_0 \end{vmatrix}$$

$$= a_0^m (-1)^{mn} b_0^n. \tag{29}$$

由(23)和(19)式得

$$\widetilde{g}(0,1,\cdots,1) = b_m(1,\cdots,1) = (-1)^m b_0. \tag{30}$$

由(28)、(29)和(30)式得

$$(-1)^{mn} a_0^m b_0^n = r \prod_{i=1}^{n} (-1)^m b_0. \tag{31}$$

从(31)式得出,$r = a_0^m$。因此(28)式可写成

$$\mathrm{Res}_x(\widetilde{f},\widetilde{g}) = a_0^m \prod_{i=1}^{n} \widetilde{g}(y_i, z_1, \cdots, z_m). \tag{32}$$

把 $y_1,\cdots,y_n,z_1,\cdots,z_m$ 分别用 $c_1,\cdots,c_n,d_1,\cdots,d_m$ 代入,从(17)式和(13)式得

$$\begin{aligned} \widetilde{g}(c_i,d_1,\cdots,d_m,) &= b_0(c_i-d_1)(c_i-d_2)\cdots(c_i-d_m) \\ &= g(c_i). \end{aligned} \tag{33}$$

于是从(32)式得

$$\mathrm{Res}(f,g) = a_0^m \prod_{i=1}^{n} g(c_i). \tag{34}$$

由定义 1 和行列式的性质容易推出

$$\mathrm{Res}(f,g) = (-1)^{mn} \mathrm{Res}(g,f). \tag{35}$$

因此据刚才证得的(34)式以及(35)式,得

$$\mathrm{Res}(f,g) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(d_j). \tag{36}$$

这样我们证明了下述定理 2:

定理 2 设 $f(x),g(x)$如定义 1 中所设,且 $a_0 \neq 0, b_0 \neq 0$。设 $f(x)$的 n 个复根为 c_1, $c_2,\cdots,c_n$,$g(x)$的 m 个复根为 $d_1,d_2,\cdots,d_m$,则

$$\begin{aligned}\operatorname{Res}(f,g) &= a_0^m \prod_{i=1}^{n} g(c_i)\\ &= (-1)^{mn} b_0^n \prod_{j=1}^{m} f(d_j).\end{aligned}$$ ■

定理 2 给出了求 $\operatorname{Res}(f,g)$ 的另一种方法：如果 $f(x)$ 的复根容易求出，那么用公式(34)可以很容易地求出 $\operatorname{Res}(f,g)$；如果 $g(x)$ 的复根容易求出，那么可用公式(36)很快地求出 $\operatorname{Res}(f,g)$。

根据定理 2 可以利用 $f(x)$ 与 $f'(x)$ 的结式 $\operatorname{Res}(f,f')$ 来求 $f(x)$ 的判别式 $D(f)$。$f(x)$ 的首项系数为 a_0，我们规定 $f(x)$ 的判别式 $D(f)$ 为

$$\begin{aligned}D(f) &:= a_0^{2n-2} \prod_{1\leqslant j<i\leqslant n} (c_i - c_j)^2\\ &= \Big[a_0^{n-1} \prod_{1\leqslant j<i\leqslant n} (c_i - c_j)\Big]^2,\end{aligned} \tag{37}$$

其中 $c_1, c_2, \cdots, c_n$ 是 $f(x)$ 的 n 个复根。由于

$$f(x) = a_0(x-c_1)(x-c_2)\cdots(x-c_n),$$

因此
$$f'(x) = a_0 \sum_{j=1}^{n} (x-c_1)\cdots(x-c_{j-1})(x-c_{j+1})\cdots(x-c_n).$$

从而

$$\begin{aligned}f'(c_i) &= a_0(c_i-c_1)\cdots(c_i-c_{i-1})(c_i-c_{i+1})\cdots(c_i-c_n).\\ &= a_0 \prod_{j\neq i} (c_i - c_j).\end{aligned} \tag{38}$$

于是

$$\begin{aligned}\operatorname{Res}(f,f') &= a_0^{n-1} \prod_{i=1}^{n} f'(c_i)\\ &= a_0^{n-1} \prod_{i=1}^{n} \Big[a_0 \prod_{j\neq i} (c_i - c_j)\Big]\\ &= a_0^{2n-1} \prod_{i=1}^{n} \prod_{j\neq i} (c_i - c_j).\end{aligned} \tag{39}$$

由于

$$\begin{aligned}\prod_{i=1}^{n} \prod_{j\neq i} (c_i - c_j) &= (c_1-c_2)(c_1-c_3)\cdots(c_1-c_n)\\ &\quad \cdot (c_2-c_1)(c_2-c_3)\cdots(c_2-c_n)\\ &\quad \cdot (c_3-c_1)(c_3-c_2)(c_3-c_4)\cdots(c_3-c_n)\\ &\quad \cdots \quad \cdots \quad \cdots \quad \cdots\end{aligned}$$

$$\begin{aligned}&\cdot (c_n-c_1)(c_n-c_2)\cdots(c_n-c_{n-1})\\=&(-1)^{\frac{n(n-1)}{2}}(c_2-c_1)^2(c_3-c_1)^2\cdots(c_n-c_1)^2\\&\cdot (c_3-c_2)^2(c_4-c_2)^2\cdots(c_n-c_2)^2\\&\cdots\quad\cdots\quad\cdots\quad\cdot(c_n-c_{n-1})^2.\end{aligned}$$

因此

$$\begin{aligned}\mathrm{Res}(f,f')&=a_0^{2n-1}(-1)^{\frac{n(n-1)}{2}}\prod_{1\leqslant j<i\leqslant n}(c_i-c_j)^2\\&=a_0(-1)^{\frac{n(n-1)}{2}}D(f).\end{aligned}\tag{40}$$

于是我们证明了下述结论：

定理 3 设 $f(x)$是数域 K 上 n 次多项式，首项系数为 a_0，则

$$D(f)=(-1)^{\frac{n(n-1)}{2}}a_0^{-1}\mathrm{Res}(f,f').\tag{41}$$

利用定理 3，通过求 $\mathrm{Res}(f,f')$来求 $D(f)$，比 7.10 节讲的方法较简便一些。

如果 $f(x)$的首项系数为 1，那么 $D(f)$与 $\mathrm{Res}(f,f')$或者相等，或者相差一个负号(即它们互为相反数)。

定理 1 的第四个用处是化曲线的参数方程为直角坐标方程，详见本节典型例题的例 9。

7.11.2 典型例题

例 1 设 $f(x)=x^3-x+2$，$g(x)=x^4+x-1$，判断 $f(x)$与 $g(x)$有没有公共复根。

解

$$\mathrm{Res}(f,g)=\begin{vmatrix}1&0&-1&2&0&0&0\\0&1&0&-1&2&0&0\\0&0&1&0&-1&2&0\\0&0&0&1&0&-1&2\\1&0&0&1&-1&0&0\\0&1&0&0&1&-1&0\\0&0&1&0&0&1&-1\end{vmatrix}=11.$$

因此 $f(x)$与 $g(x)$没有公共复根。

例 2 解方程组

$$\begin{cases}x^2-7xy+4y^2+6y-4=0,\\x^2-14xy+9y^2-2x+14y-8=0.\end{cases}\tag{42}$$

解 把(42)式左端的两个多项式 $f(x,y)$，$g(x,y)$分别按 x 的降幂排列写出：

$$f(x,y)=x^2-7xy+(4y^2+6y-4), \tag{43}$$

$$g(x,y)=x^2-(14y+2)x+(9y^2+14y-8). \tag{44}$$

$$\begin{aligned}R_x(f,g)&=\begin{vmatrix}1 & -7y & 4y^2+6y-4 & 0\\ 0 & 1 & -7y & 4y^2+6y-4\\ 1 & -14y-2 & 9y^2+14y-8 & 0\\ 0 & 1 & -14y-2 & 9y^2+14y-8\end{vmatrix}\\ &=(5y^2+8y-4)^2-(7y+2)(7y^3+6y^2-12y+8)\\ &=-24y(y-1)(y-2)(y+2). \end{aligned}\tag{45}$$

于是 $R_x(f,g)$的 4 个根是 0,1,2,−2。对于 $y=0$,解方程组

$$\begin{cases}x^2-4=0,\\ x^2-2x-8=0,\end{cases}$$

第一个方程减去第二个方程,得

$$2x+4=0.$$

从而 $x=-2$。对于 $y=1$,解方程组

$$\begin{cases}x^2-7x+6=0,\\ x^2-16x+15=0,\end{cases}$$

得 $x=1$。对于 $y=2$,解方程组

$$\begin{cases}x^2-14x+24=0,\\ x^2-30x+56=0,\end{cases}$$

得 $x=2$。对于 $y=-2$,解方程组

$$\begin{cases}x^2+14x=0,\\ x^2+26x=0,\end{cases}$$

得 $x=0$。因此方程组(42)的全部解是:

$$\begin{cases}x=-2\\ y=0;\end{cases}\quad\begin{cases}x=1\\ y=1;\end{cases}\quad\begin{cases}x=2\\ y=2;\end{cases}\quad\begin{cases}x=0\\ y=-2.\end{cases}$$

方程组(42)的全部解也可以写成(−2,0),(1,1),(2,2),(0,−2)。

例 3　设 $f(x)=x^4+a_1x+a_0\in K[x]$,求 $f(x)$的判别式 $D(f)$。

解　$f'(x)=4x^3+a_1$

$$\mathrm{Res}(f,f')=\begin{vmatrix}1&0&0&a_1&a_0&0&0\\0&1&0&0&a_1&a_0&0\\0&0&1&0&0&a_1&a_0\\4&0&0&a_1&0&0&0\\0&4&0&0&a_1&0&0\\0&0&4&0&0&a_1&0\\0&0&0&4&0&0&a_1\end{vmatrix}=-27a_1^4+256a_0^3.$$

于是

$$D(f)=(-1)^{\frac{4(4-1)}{2}}\mathrm{Res}(f,f')=-27a_1^4+256a_0^3. \tag{46}$$

点评 7.10 节习题的第 8 题也求过 $f(x)=x^4+a_1x+a_0$ 的判别式 $D(f)$，现在例 3 用 $\mathrm{Res}(f,f')$来求 $D(f)$，比较简便一些。在 7.6 节用辗转相除法求出过 $f(x)=x^4+a_1x+a_0$ 有重根的充分必要条件，这与 $f(x)$的判别式 $D(f)$有关系。显然，现在例 3 求 $D(f)$的方法较简便一些。

例 4 求数域 K 上 n 次多项式 $f(x)=x^n+a_1x+a_0$ 的判别式。

解 $f'(x)=nx^{n-1}+a_1$

$$\mathrm{Res}(f,f')=\begin{vmatrix}1&0&0&\cdots&0&a_1&a_0&0&0&\cdots&0&0&0\\0&1&0&\cdots&0&0&a_1&a_0&0&\cdots&0&0&0\\\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots\\0&0&0&\cdots&1&0&0&0&0&\cdots&0&a_1&a_0\\n&0&0&\cdots&0&a_1&0&0&0&\cdots&0&0&0\\0&n&0&\cdots&0&0&a_1&0&0&\cdots&0&0&0\\\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots\\0&0&0&\cdots&0&n&0&0&0&\cdots&0&0&a_1\end{vmatrix}.$$

每一次都把第 1 行的$(-n)$倍加到第 n 行上，接着按第 1 列展开，这样做 $n-1$ 次，便得到下述 n 阶行列式：

$$\begin{vmatrix}(1-n)a_1&-na_0&0&0&\cdots&0&0\\0&(1-n)a_1&-na_0&0&\cdots&0&0\\0&0&(1-n)a_1&-na_0&\cdots&0&0\\\vdots&\vdots&\vdots&\vdots&&\vdots&\vdots\\0&0&0&0&\cdots&(1-n)a_1&-na_0\\n&0&0&0&\cdots&0&a_1\end{vmatrix}$$

$$=n(-1)^{n+1}(-na_0)^{n-1}+a_1(-1)^{n+n}[(1-n)a_1]^{n-1}$$
$$=n^n a_0^{n-1}+(-1)^{n-1}(n-1)^{n-1}a_1^n.$$

于是

$$D(f)=(-1)^{\frac{n(n-1)}{2}}[n^n a_0^{n-1}+(-1)^{n-1}(n-1)^{n-1}a_1^n]. \tag{47}$$

点评　例 4 通过先计算 $\mathrm{Res}(f,f')$，然后求 $D(f)$，这比起 7.10 节讲的求 $D(f)$ 的方法要简便得多。例 4 求得的 $D(f)$ 的(47)式对一切 $n\geqslant 2$ 都成立，如表 7-2 所示。

表 7-2

n	$f(x)$	$D(f)$
2	$x^2+a_1x+a_0$	$a_1^2-4a_0$
3	$x^3+a_1x+a_0$	$-4a_1^3-27a_0^2$
4	$x^4+a_1x+a_0$	$-27a_1^4+256a_0^3$
5	$x^5+a_1x+a_0$	$256a_1^5+3125a_0^4$

例 5　设 $f(x)=x^{n-1}+x^{n-2}+\cdots+x+1$，求 $D(f)$。

解　令 $g(x)=(x-1)f(x)=x^n-1$。

根据 7.10 节中典型例题的例 15 的结论，得

$$D(g)=(-1)^{\frac{n(n-1)}{2}}n^n(-1)^{n-1}=(-1)^{\frac{(n-2)(n-1)}{2}}n^n.$$

根据 7.10 节习题第 11 题的结论，得

$$D(g)=D(f)f(1)^2=n^2D(f).$$

因此

$$D(f)=(-1)^{\frac{(n-2)(n-1)}{2}}n^{n-2}. \tag{48}$$

例 6　设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$，$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m$，其中 $a_0\neq 0$，$b_0\neq 0$。设 $f(x)$ 的 n 个复根为 $c_1,c_2,\cdots,c_n$，$g(x)$ 的 m 个复根为 $d_1,d_2,\cdots,d_m$，证明：

$$\mathrm{Res}(f,g)=a_0^m b_0^n\prod_{i=1}^{n}\prod_{j=1}^{m}(c_i-d_j). \tag{49}$$

证明　由于 $g(c_i)=b_0(c_i-d_1)(c_i-d_2)\cdots(c_i-d_m)=b_0\prod_{j=1}^{m}(c_i-d_j)$，因此

$$\mathrm{Res}(f,g)=a_0^m\prod_{i=1}^{n}b_0\prod_{j=1}^{m}(c_i-d_j)$$
$$=a_0^m b_0^n\prod_{i=1}^{n}\prod_{j=1}^{m}(c_i-d_j).$$

■

例 7 设 $f(x)$和 $g(x)$分别是数域 K 上 n 次、m 次多项式，且 $n>1, m>1$。证明：

$$D(fg) = D(f)D(g)[\mathrm{Res}(f,g)]^2. \tag{50}$$

证明 设 $f(x), g(x)$的首项系数分别是 a_0, b_0，$f(x)$的 n 个复根为 $c_1, c_2, \cdots, c_n$，$g(x)$的 m 个复根为 $d_1, d_2, \cdots, d_m$。则

$$f(x) = a_0(x-c_1)(x-c_2)\cdots(x-c_n),$$
$$g(x) = b_0(x-d_1)(x-d_2)\cdots(x-d_m).$$

从而

$$f(x)g(x) = a_0b_0(x-c_1)(x-c_2)\cdots(x-c_n)(x-d_1)\cdots(x-d_m).$$

于是

$$\begin{aligned} D(fg) =& (a_0b_0)^{2(n+m)-2}\prod_{1\leqslant j<i\leqslant n}(c_i-c_j)^2 \cdot \prod_{1\leqslant k<l\leqslant m}(d_l-d_k)^2 \\ & \cdot \prod_{i=1}^{n}\prod_{j=1}^{m}(d_j-c_i)^2 \\ =& D(f)D(g)[\mathrm{Res}(f,g)]^2. \end{aligned}$$

■

例 8 设 $f(x), g_1(x), g_2(x)\in K[x]$，证明：

$$\mathrm{Res}(f,g_1g_2) = \mathrm{Res}(f,g_1)\mathrm{Res}(f,g_2).$$

证明 设 $f(x)$的次数为 n，首项系数为 a_0，n 个复根为 $c_1, c_2, \cdots, c_n$，$g_1(x), g_2(x)$的次数分别为 m_1, m_2。则

$$\begin{aligned} \mathrm{Res}(f,g_1g_2) &= a_0^{m_1+m_2}\prod_{i=1}^{n}g_1g_2(c_i) \\ &= a_0^{m_1}a_0^{m_2}\prod_{i=1}^{n}g_1(c_i)g_2(c_i) \\ &= \Big[a_0^{m_1}\prod_{i=1}^{m}g_1(c_i)\Big]\Big[a_0^{m_2}\prod_{i=1}^{n}g_2(c_i)\Big] \\ &= \mathrm{Res}(f,g_1)\mathrm{Res}(f,g_2). \end{aligned}$$

■

例 9 求下述曲线的直角坐标方程：

$$x = \frac{-t^2+2t}{t^2+1}, y = \frac{2t^2+2t}{t^2+1}.$$

解 在所给曲线 S 上任取一点 $P(x,y)$，则存在 $t_0\in\mathbf{R}$，使得

$$x = \frac{-t_0^2+2t_0}{t_0^2+1}, y = \frac{2t_0^2+2t_0}{t_0^2+1}.$$

即

$$(t_0^2+1)x + t_0^2 - 2t_0 = 0,$$

$$(t_0^2+1)y-2t_0^2-2t_0=0.$$

令　　$f(t)=(t^2+1)x+t^2-2t, g(t)=(t^2+1)y-2t^2-2t.$

则 $f(t)$与 $g(t)$有公共根 t_0，从而 $\mathrm{Res}(f,g)=0$。

反之，考虑坐标适合方程 $\mathrm{Res}(f,g)=0$ 的点 $Q(x,y)$，因为 $\mathrm{Res}(f,g)=0$，所以 $x+1=0=y-2$，或者 $f(t)$与 $g(t)$不互素。在前一情形，直接验证可知点 $M(-1,2)$不是曲线 S 上的点；在后一情形，由于 $f(t)$与 $g(t)$的次数至多为 2，且它们不相伴，因此 $f(t)$与 $g(t)$有公共的一次因式，从而 $f(t)$与 $g(t)$有公共的实根 t_1。于是点 $Q(x,y)$在曲线 S 上。

综上所述，$\mathrm{Res}(f,g)=0$（排除点 $M(-1,2)$）就是所求的直角坐标方程。计算 $\mathrm{Res}(f,g)$。由于

$$f(t)=(x+1)t^2-2t+x, g(t)=(y-2)t^2-2t+y.$$

因此

$$\mathrm{Res}(f,g)=\begin{vmatrix} x+1 & -2 & x & 0 \\ 0 & x+1 & -2 & x \\ y-2 & -2 & y & 0 \\ 0 & y-2 & -2 & y \end{vmatrix}$$

$$=8x^2-4xy+5y^2+12x-12y.$$

于是所给曲线 S 的直角坐标方程为

$$8x^2-4xy+5y^2+12x-12y=0,$$

并且$(x,y)\neq(-1,2)$。

点评　例 9 表明结式可以用于在解析几何中化平面曲线的参数方程为直角坐标方程，这是本节定理 1 的第四个用处。

习题 7.11

1. 判断 $f(x)=2x^3+3x^2-8x+3$ 与 $g(x)=4x^2+7x-15$ 有无公共复根。

2. 解下列方程组：

(1) $\begin{cases} 2x^2-xy+y^2-2x+y-4=0, \\ 5x^2-6xy+5y^2-6x+10y-11=0; \end{cases}$

(2) $\begin{cases} x^2+y^2+4x+2=0, \\ x^2+4xy-y^2+4x+8y=0. \end{cases}$

3. 求多项式 $f(x)$与 $g(x)$的结式：

(1) $f(x)=x^4+x^3+x^2+1, g(x)=x^6+x^5+x^4+x^3+x^2+x+1$；

(2) $f(x)=x^n+2x+1, g(x)=x^2-x-6$;

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

(4) $f(x)=x^4+x^3+x^2+x+1, g(x)=x^6+x^5+x^4+x^3+x^2+x+1$.

4. 设 $f(x), x-a\in K[x]$,且 $\deg f(x)=n$,求 $\mathrm{Res}(f, x-a)$。

5. 设数域 K 上三次多项式 $f(x)=a_0x^3+a_1x^2+a_2x+a_3$,求 $D(f)$。

6. 讨论数域 K 上的多项式 $f(x)=x^2+1$ 与 $g(x)=x^{2m}+1$ 是否互素。

7. 求下列曲线的直角坐标方程:

(1) $x=t^2-t, y=2t^2+t-2$;

(2) $x=\dfrac{2t+1}{t^2+1}, y=\dfrac{t^2+2t-1}{t^2+1}$.

8. 在实数域中解方程组:

$$\begin{cases} y^2+z^2+2yz-x-y+z+3=0, \\ x^2+z^2+xz+x-y+z+1=0, \\ x^2-y^2+xy-x+y-z-1=0. \end{cases}$$

7.12 域与域上的一元多项式环

7.12.1 内容精华

一、分式域

数域 K 上的一元多项式环 $K[x]$中有加法和乘法运算,进而有减法运算:$f(x)-g(x):=f(x)+(-g(x))$,但是没有除法运算。设 $g(x)\neq 0$,当 $g(x)$不能整除 $f(x)$时,$f(x)$除以 $g(x)$不是多项式,此时可以引进分式的概念,把 $f(x)$除以 $g(x)$记作$\dfrac{f(x)}{g(x)}$,称它为分式。规定分式的基本性质:分子与分母乘以同一个非零多项式,所得分式与原分式相等。为了说明分式的基本性质是怎么来的,我们用现代数学的观点来阐述分式的概念。从分式$\dfrac{f(x)}{g(x)}$联想到有序多项式对$(f(x), g(x))$,其中 $g(x)\neq 0$,它是$K[x]\times K[x]^*$ 中的元素,这里用 $K[x]^*$ 表示 $K[x]$中所有非零多项式组成的集合,令 $T=K[x]\times K[x]^*$。在 T 中规定一个二元关系$\sim$,如下:

$$(f_1, g_1)\sim(f_2, g_2) \quad\Leftrightarrow\quad f_1g_2=g_1f_2. \tag{1}$$

显然，$(f,g)\sim(f,g)$，$\forall(f,g)\in T$，即$\sim$具有反身性。

若$(f_1,g_1)\sim(f_2,g_2)$，则 $f_1g_2=g_1f_2$。由此推出，$(f_2,g_2)\sim(f_1,g_1)$，即$\sim$具有对称性。

若$(f_1,g_1)\sim(f_2,g_2)$且$(f_2,g_2)\sim(f_3,g_3)$，则

$$f_1g_2=g_1f_2,f_2g_3=g_2f_3$$

从而

$$f_1g_2g_3=g_1f_2g_3=g_1g_2f_3.$$

由于 $g_2\neq0$，因此 $f_1g_3=g_1f_3$，于是$(f_1,g_1)\sim(f_3,g_3)$。这表明$\sim$具有传递性。

上述证明了$\sim$是 T 中的一个等价关系，我们把(f,g)确定的等价类记作$\frac{f}{g}$。于是

$$\frac{f_1}{g_1}=\frac{f_2}{g_2}\quad\Leftrightarrow\quad(f_1,g_1)\sim(f_2,g_2)\quad\Leftrightarrow\quad f_1g_2=g_1f_2. \tag{2}$$

把所有等价类组成的集合记作 $K(x)$(注意这里是圆括号)，$K(x)$称为 T 对于等价关系$\sim$的商集(参看丘维声. 高等代数(上册). 第 3 版. 北京：高等教育出版社，2015 年，第161 页)。

在 $K(x)$中，规定加法和乘法运算如下：

$$\frac{f_1}{g_1}+\frac{f_2}{g_2}:=\frac{f_1g_2+g_1f_2}{g_1g_2}, \tag{3}$$

$$\frac{f_1}{g_1}\cdot\frac{f_2}{g_2}:=\frac{f_1f_2}{g_1g_2}. \tag{4}$$

不难验证，(3)式和(4)式不依赖于等价类中代表的选择。

容易验证，上述定义的加法和乘法都满足交换律、结合律和分配律。$\frac{0}{1}$是 $K(x)$中的零元，把$\frac{0}{1}$记作 0。$\frac{f}{g}$的负元是$\frac{-f}{g}$，记作$-\frac{f}{g}$。$\frac{1}{1}$是 $K(x)$的单位元，记作 1。因此$K(x)$成为一个有单位元的交换环。

对于 $K(x)$中每一个非零元$\frac{f}{g}$，都存在$\frac{g}{f}\in K(x)$，使得

$$\frac{f}{g}\cdot\frac{g}{f}=\frac{fg}{gf}=\frac{1}{1}=1,\frac{g}{f}\cdot\frac{f}{g}=\frac{gf}{fg}=\frac{1}{1}=1.$$

这表明$\frac{f}{g}$是可逆的，$\frac{g}{f}$是$\frac{f}{g}$的逆元，记作$\left(\frac{f}{g}\right)^{-1}$。即

$$\left(\frac{f}{g}\right)^{-1}=\frac{g}{f}. \tag{5}$$

由于 $K(x)$的每个非零元都可逆，因此可以在 $K(x)$中定义除法如下：

设$\frac{f_2}{g_2}\neq0$，对于任意$\frac{f_1}{g_1}\in K(x)$，规定

$$\frac{f_1}{g_1}\div\frac{f_2}{g_2}\overset{\text{def}}{=\!=}\frac{f_1}{g_1}\cdot\left(\frac{f_2}{g_2}\right)^{-1}. \tag{6}$$

$K(x)$中的减法运算的定义跟环中的减法定义一样。

综上所述，$K(x)$中有加、减、乘、除四种运算(除式不为 0)，并且满足与实数域一样的运算规律。由此受到启发，引进下述重要概念：

定义 1 一个有单位元 $1(\neq 0)$的交换环 F，如果它的每个非零元都可逆，那么称 F 是一个**域**。

例如，$K(x)$是一个域，称它为数域 K 上的**一元分式域**。把 $K(x)$中的元素$\frac{f}{g}$称为 K 上的**一元分式**(或者**分式**)，其中 f 称为**分子**，g 称为**分母**。

分式的基本性质现在可以证明如下：

设$\frac{f}{g}\in K(x)$。任取 $h(x)\in K[x]^*$，由于 $fgh=gfh$，因此

$$\frac{f}{g}=\frac{fh}{gh}. \tag{7}$$

将(7)式从右到左看：分子与分母可以消去同一个非零公因式。

对于一个非零的一元分式$\frac{f}{g}$，分子的次数减去分母的次数所得的差 $\deg f-\deg g$ 不依赖于等价类的代表的选取。证明如下：设$\frac{f}{g}=\frac{f_1}{g_1}$，则 $fg_1=gf_1$，从而 $\deg f+\deg g_1=\deg g+\deg f_1$。因此

$$\deg f-\deg g=\deg f_1-\deg g_1. \tag{8}$$

把 $\deg f-\deg g$ 称为一元分式$\frac{f}{g}$的**次数**。一元分式 0 是$\frac{0}{1}$，它的次数为$-\infty$。

一个一元分式，如果它的分子与分母是互素的，那么称它为**既约分式**。

由于$(0,1)=1$，因此$\frac{0}{1}$是既约分式，即一元分式 0 是既约分式。

类似于一元分式域的构造方法，我们还可以构造出数域 K 上的 n 元分式域，记作$K(x_1,x_2,\cdots,x_n)$。

一元分式域与 n 元分式域都是域，任一数域也是域。注意：数域的元素是数；而一元或 n 元分式域的元素不是数，是分式。

命题 1 域 F 中没有非平凡的零因子，从而域一定是整环。

二、模 p(p 是素数)剩余类域与模 m 剩余类环

读者都非常熟悉“星期几”这个词。在时间的长河中,我们可以把每一天对应于一个整数,于是时间的长河可以用整数集 $\mathbf{Z}$ 来刻画,星期日可以看成是被 7 除后余数为 0 的所有整数组成的子集,星期一可以看成是被 7 除后余数为 1 的所有整数组成的子集,…,星期六可以看成是被 7 除后余数为 6 的所有整数组成的子集。由此受到启发,在整数集 $\mathbf{Z}$ 中规定一个二元关系$\sim$,如下:

$$a \sim b \quad \Leftrightarrow \quad a \text{ 与 } b \text{ 被 7 除所得余数相同}$$

也就是

$$a \sim b \quad \Leftrightarrow \quad 7 \mid a-b. \tag{9}$$

容易看出,$\sim$具有反身性、对称性和传递性。因此$\sim$是 $\mathbf{Z}$ 上的一个等价关系,把它称为**模 7 同余关系**,把 $a \sim b$ 记作

$$a \equiv b \pmod 7,$$

读作“a 模 7 同余 b”。于是

$$a \equiv b \pmod 7 \quad \Leftrightarrow \quad 7 \mid a-b. \tag{10}$$

模 7 同余关系有下述性质:

命题 2 若 $a \equiv b \pmod 7$,$c \equiv d \pmod 7$,则

$$a+c \equiv b+d \pmod 7,\ ac \equiv bd \pmod 7. \tag{11}$$

在模 7 同余关系下的等价类称为**模 7 剩余类**。

$$\bar{i} = \{a \in \mathbf{Z} \mid a \equiv i \pmod 7\} = \{7k+i \mid k \in \mathbf{Z}\}. \tag{12}$$

其中 $i=0,1,2,3,4,5,6$。$\bar{i}$ 里的任一元素都可以作为代表,例如 $8,-6$ 都可以作为 $\bar{1}$ 的代表(注意 $-6=(-1)\times 7+1$),因此 $\bar{8}=\bar{1}$,$\overline{-6}=\bar{1}$。类似地,$\bar{9}=\bar{2}$,$\overline{-5}=\bar{2}$,…;$\overline{10}=\bar{3}$,$\overline{-4}=\bar{3}$,…;$\overline{11}=\bar{4}$,$\overline{-3}=\bar{4}$,…;$\overline{12}=\bar{5}$,$\overline{-2}=\bar{5}$,…;$\overline{13}=\bar{6}$,$\overline{-1}=\bar{6}$,…。

由模 7 剩余类组成的集合称为 $\mathbf{Z}$ 对于模 7 同余关系的商集,记作 $\mathbf{Z}_7$ 或 $\mathbf{Z}/(7)$,即

$$\mathbf{Z}_7 = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}. \tag{13}$$

在 $\mathbf{Z}_7$ 中可以规定加法和乘法运算:

$$\bar{i}+\bar{j} \overset{\text{def}}{=\!=} \overline{i+j},\ \bar{i}\cdot\bar{j} \overset{\text{def}}{=\!=} \overline{ij}. \tag{14}$$

(14)式定义的加法和乘法运算是合理的,即与剩余类的代表的选取无关。

容易看出,$\bar{0}$ 是 $\mathbf{Z}_7$ 的零元,$\bar{i}$ 有负元$\overline{-i}$。$\bar{1}$ 是 $\mathbf{Z}_7$ 的单位元,容易验证 $\mathbf{Z}_7$ 是一个有单位元的交换环。由于

$$\bar{1}\cdot\bar{1}=\bar{1},\ \bar{2}\cdot\bar{4}=\bar{1},\ \bar{3}\cdot\bar{5}=\bar{1},\ \bar{6}\cdot\bar{6}=\bar{1},$$

因此 $\mathbf{Z}_7$ 的每个非零元都可逆,从而 $\mathbf{Z}_7$ 是一个域,称它为**模 7 剩余类域**,它只含有 7 个元素。

只含有限多个元素的域称为**有限域**，否则称为**无限域**。

数域 K，K 上的一元分式域，n 元分式域都是无限域；$\mathbf{Z}_7$ 是一个有限域。

一般地，设 m 是大于 1 的正整数。在 $\mathbf{Z}$ 中规定

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid a-b. \tag{15}$$

这给出了 $\mathbf{Z}$ 上的一个二元关系，它是一个等价关系，称它为模 m 同余关系，模 m 同余关系具有类似于命题 2 的性质：

若 $a \equiv b \pmod{m}$，$c \equiv d \pmod{m}$，则

$$a+c \equiv b+d \pmod{m}, ac \equiv bd \pmod{m}. \tag{16}$$

模 m 同余关系下的等价类称为**模 m 剩余类**。

$$\bar{i} = \{a \in \mathbf{Z} \mid a \equiv i \pmod{m}\} = \{km+i \mid k \in \mathbf{Z}\}, \tag{17}$$

其中 $i=0,1,2,\cdots,m-1$。

由模 m 剩余类组成的集合称为 $\mathbf{Z}$ 对于模 m 同余关系的商集，记作 $\mathbf{Z}_m$ 或 $\mathbf{Z}/(m)$，即

$$\mathbf{Z}_m = \{\bar{0},\bar{1},\bar{2},\cdots,\overline{m-1}\}. \tag{18}$$

在 $\mathbf{Z}_m$ 中可以规定加法和乘法运算：

$$\bar{i}+\bar{j} \xlongequal{\text{def}} \overline{i+j}, \bar{i}\,\bar{j} \xlongequal{\text{def}} \overline{ij}. \tag{19}$$

利用(16)式容易证明(19)式规定的加法和乘法运算是合理的，在 $\mathbf{Z}_m$ 中规定减法运算为

$$\bar{i}-\bar{j} \xlongequal{\text{def}} \bar{i}+(-\bar{j}). \tag{20}$$

容易验证，$\mathbf{Z}_m$ 对于加法和乘法运算成为一个有单位元 $\bar{1}(\neq\bar{0})$ 的交换环，称它为**模 m 剩余类环**。

$\mathbf{Z}_m$ 是不是域？例如，$\mathbf{Z}_4$，由于 $\bar{2}\cdot\bar{2}=\bar{0}$，因此 $\mathbf{Z}_4$ 有非平凡的零因子，从而 $\mathbf{Z}_4$ 不是域(根据命题 1)。由于 $\bar{1}\cdot\bar{1}=\bar{1}$，因此 $\mathbf{Z}_2=\{\bar{0},\bar{1}\}$ 是域。由于在 $\mathbf{Z}_3$ 中，

$$\bar{1}\cdot\bar{1}=\bar{1}, \quad \bar{2}\cdot\bar{2}=\bar{1},$$

因此 $\mathbf{Z}_3$ 的每个非零元都可逆，从而 $\mathbf{Z}_3$ 是一个域，猜想并且可以证明有下述结论：

定理 1 若 p 是素数，则 $\mathbf{Z}_p$ 是一个域。

当 p 是素数时，$\mathbf{Z}_p$ 称为**模 p 剩余类域**。$\mathbf{Z}_p$ 含有 p 个元素，因此 $\mathbf{Z}_p$ 是一个有限域。

若 m 是合数，则 $\mathbf{Z}_m$ 不是一个域，理由如下：若 m 是合数，则 $m=m_1m_2$，其中 $0<m_i<m$，$i=1,2$。于是有 $\overline{m_1m_2}=\overline{m_1}\,\overline{m_2}=\bar{m}=\bar{0}$，从而 $\mathbf{Z}_m$ 有非平凡的零因子 $\bar{m}_1$。因此 $\mathbf{Z}_m$ 不是域。

三、域的特征

设 p 是素数，在模 p 剩余类域 $\mathbf{Z}_p$ 中，有

$$p\,\bar{1} = \underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{p\text{个}} = \bar{p} = \bar{0}. \tag{21}$$

当 $0<l<p$ 时，

$$l\bar{1}=\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{l个}=\bar{l}\neq\bar{0}. \tag{22}$$

在数域 K 中，对于任意正整数 n，都有

$$n1=\underbrace{1+1+\cdots+1}_{n个}=n\neq 0.$$

在任一域 F 中，它的单位元 e 的正整数倍是否等于零元有什么规律？

情形 1　对任意正整数 n 都有 $ne\neq 0$。

情形 2　不是情形 1，则存在正整数 n 使得 $ne=0$。设 n 是使 $ne=0$ 成立的最小正整数。假如 n 是合数，则

$$n=n_1n_2,\quad 0<n_i<n,\quad i=1,2.$$

于是

$$\begin{aligned}(n_1e)(n_2e)&=n_1[e(n_2e)]=n_1[n_2(ee)]=n_1(n_2e)\\&=(n_1n_2)e=ne=0.\end{aligned}$$

由于 $n_i<n$，因此根据 n 的选择得，$n_1e\neq 0$ 且 $n_2e\neq 0$。于是 n_1e 是零因子。从而 n_1e 不是可逆元，又 $n_1e\neq 0$，这与域 F 中非零元都可逆矛盾。所以 n 是素数。这样我们证明了下述定理：

定理 2　设 F 是一个域，它的单位元为 e，则或者对任意正整数 n 都有 $ne\neq 0$，或者存在一个素数 p，使得 $pe=0$，而对于 $0<l<p$ 有 $le\neq 0$。 ■

从定理 2 受到启发，引出下述概念：

定义 2　设 F 是一个域，它的单位元为 e，如果对任意正整数 n 都有 $ne\neq 0$，那么称域 F 的**特征**为 0；如果存在一个素数 p，使得 $pe=0$，而对于 $0<l<p$ 有 $le\neq 0$，那么称域 F 的**特征**为 p。把域 F 的特征记作 $\mathrm{char}\,F$。

根据定理 2 得，域 F 的特征或者为 0，或者为一个素数。

从上面所说的事实知道，模 p 剩余类域的特征为 p。任一数域的特征为 0。数域 K 上的一元分式域和 n 元分式域的特征都为 0。

有限域的特征一定是一个素数，理由如下：设域 F 是一个有限域。假如 F 的特征为 0，则对一切正整数 n 都有 $ne\neq 0$，其中 e 是域 F 的单位元。于是 $e,2e,3e,\cdots,ne,\cdots$ 中任两个元素都不相等，从而域 F 会有无穷多个元素，这与 F 是有限域矛盾，因此有限域 F 的特征一定是一个素数。

无限域有没有特征为素数的呢？考虑模 p 剩余类域 $\mathbf{Z}_p$ 上的一元分式域 $\mathbf{Z}_p(x)$，它的一个子集是 $\mathbf{Z}_p[x]$。由于 $\mathbf{Z}_p[x]$ 中非零多项式的次数 n 可以是任意非负整数，因此 $\mathbf{Z}_p[x]$

含有无穷多个元素。从而 $\mathbf{Z}_p(x)$ 含有无穷多个元素。由于 $p\bar{1}=\bar{p}=\bar{0}$，而当 $0<l<p$ 时，$l\bar{1}=\bar{l}\neq\bar{0}$。因此域 $\mathbf{Z}_p(x)$ 的特征为素数 p。从而 $\mathbf{Z}_p(x)$ 是特征为素数 p 的无限域。

命题 3 设域 F 的特征为素数 p，则

$$ne=0 \quad \Leftrightarrow \quad p \mid n.$$

命题 4 设域 F 的特征为素数 p，任取 $a\in F^*$（我们用 F^* 表示 F 中所有非零元组成的集合），则

$$na=0 \quad \Leftrightarrow \quad p \mid n.$$

命题 4 告诉我们，在特征为素数 p 的域 F 中，要注意识别零元素：若 $p|n$，则对于任一元素 a 有 $na=0$。

四、域 F 上的一元多项式环

类似于数域 K 上的一元多项式，我们可以定义任一域 F 上的一元多项式，并且得出域 F 上的一元多项式环 $F[x]$。不难看出，有关数域 K 上的一元多项式环 $K[x]$ 的结论，只要在它的证明中没有用到这个域含有无穷多个元素，并且还要注意识别零元素，那么这些结论在任一域 F 上的一元多项式环 $F[x]$ 仍然成立。

例如，在数域 K 上的一元多项式环 $K[x]$ 中，两个多项式如果不相等，那么它们诱导的多项式函数也不相等。这个结论的证明需要用到数域 K 含有无穷多个元素，因此这个结论对于有限域上的一元多项式环就不成立。譬如，在 $\mathbf{Z}_3[x]$ 中，设

$$f(x)=x^3+\bar{2}x^2+\bar{2}, g(x)=\bar{2}x^2+x+\bar{2}.$$

显然，$f(x)\neq g(x)$。由于

$$f(\bar{0})=\bar{2}, f(\bar{1})=\bar{2}, f(\bar{2})=\bar{0},$$
$$g(\bar{0})=\bar{2}, g(\bar{1})=\bar{2}, g(\bar{2})=\bar{0},$$

因此 $f=g$，即多项式函数 f 与 g 相等。

在特征为素数 p 的域中，若 $p|n$，则任一元素的 n 倍为零元，例如，在 $\mathbf{Z}_p[x]$ 中，设 $f(x)=x^p+\bar{1}$，则 $f'(x)=px^{p-1}=p(\bar{1}x^{p-1})=(p\bar{1})x^{p-1}=\bar{0}x^{p-1}=0$。

在数域 K 上的一元多项式环 $K[x]$ 中，如果不可约多项式 $p(x)$ 是 $f(x)$ 的一个 $k(k\geqslant 1)$ 重因式，那么 $p(x)$ 是 $f'(x)$ 的 $k-1$ 重因式。此结论的证明中关键一步是 $p(x)\nmid kp'(x)$。现在设 F 是特征为素数 p 的域。在 $F[x]$ 中，若 $p|k$ 或 $p'(x)=0$，则 $p(x)|kp'(x)$。从而 $p(x)$ 是 $f'(x)$ 的至少 k 重因式。若 $p\nmid k$ 且 $p'(x)\neq 0$，则 $p(x)\nmid kp'(x)$，从而 $p(x)$ 是 $f'(x)$ 的 $k-1$ 重因式。于是若 $f(x)$ 有重因式，则 $f(x)$ 与 $f'(x)$ 有次数大于 0 的公因式，从而 $(f(x),f'(x))\neq 1$。也就是说，若 $(f(x),f'(x))=1$，则 $f(x)$ 没有重因式；反之不成立。可以证明：若 $f(x)$ 没有重因式，则 $(f(x),f'(x))=1$ 或者 $f(x)$ 有一个单因式 $p(x)$，使得

$p'(x)=0$(详见本章补充题七的第 17 题)。

下面我们给出判断整系数多项式在有理数域 $\mathbf{Q}$ 上不可约的另一种方法。

命题 5 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个整系数多项式,p 是一个素数,$p\nmid a_n$。把 $f(x)$的各项系数模 p 变成 $\mathbf{Z}_p$ 的元素,得到 $\mathbf{Z}_p$ 上的一个多项式,记作$\widetilde{f}(x)$,即

$$\widetilde{f}(x)=\overline{a_n}x^n+\overline{a_{n-1}}x^{n-1}+\cdots+\overline{a_1}x+\overline{a_0}. \tag{23}$$

如果 $\widetilde{f}(x)$在 $\mathbf{Z}_p$ 上不可约,那么 $f(x)$在 $\mathbf{Q}$ 上不可约。

注意:如果 $\widetilde{f}(x)$在 $\mathbf{Z}_p$ 上可约,那么 $f(x)$在 $\mathbf{Q}$ 上可能不可约,也可能可约,需要具体问题具体分析。

为简便起见,对于首项系数为奇数的整系数多项式 $f(x)$,把它的各项系数模 2 得到 $\mathbf{Z}_2$ 上的多项式 $\widetilde{f}(x)$。若 $\widetilde{f}(x)$在 $\mathbf{Z}_2$ 上不可约,则 $f(x)$在 $\mathbf{Q}$ 上不可约。

若整系数多项式 $f(x)$的首项系数为偶数,但不是 3 的倍数,则把 $f(x)$的各项系数模 3 得到 $\mathbf{Z}_3$ 上的多项式。若 $\widetilde{f}(x)$在 $\mathbf{Z}_3$ 上不可约,则 $f(x)$在 $\mathbf{Q}$ 上不可约。

若整系数多项式 $f(x)$的首项系数是偶数,且是 3 的倍数,则把 $f(x)$的系数模 5 得到 $\mathbf{Z}_5$ 上的多项式。依此类推,选择素数 p。

命题 5 给出了判断整系数多项式在 $\mathbf{Q}$ 上是否不可约的一个新的方法。

类似于数域上的 n 元多项式,可以定义任一域 F 上的 n 元多项式,并且得出域 F 上的 n 元多项式环 $F[x_1,\cdots,x_n]$。$K[x_1,\cdots,x_n]$中的结论,只要在它的证明中没有用到数域 K 含有无穷多个元素,那么它在 $F[x_1,\cdots,x_n]$中仍成立,还需注意识别 F 中的零元。

五、中国剩余定理

整数环 $\mathbf{Z}$ 与数域 K 上一元多项式环 $K[x]$的结构很相似。现在我们利用整数环的结构来证明著名的中国剩余定理(或孙子定理)。

定理 3(中国剩余定理) 设 $m_1,m_2,\cdots,m_s$ 是两两互素的正整数,$b_1,b_2,\cdots,b_s$ 是任意给定的 s 个整数。则同余方程组

$$\begin{cases} x\equiv b_1 \pmod{m_1} \\ x\equiv b_2 \pmod{m_2} \\ \cdots \quad\quad \cdots \\ x\equiv b_s \pmod{m_s} \end{cases} \tag{24}$$

在 $\mathbf{Z}$ 中必有解,并且如果 c 和 d 是两个解,那么

$$c\equiv d \pmod{m_1m_2\cdots m_s}. \tag{25}$$

它的一个解是

$$c=\sum_{i=1}^{s}b_i\Big(v_i\prod_{j\neq i}m_i\Big) \tag{26}$$

其中 v_i 满足

$$u_i m_i + v_i \prod_{j \neq i} m_j = 1. \tag{27}$$

从(27)式知道，v_i 可以对 m_i 和 $\prod_{j \neq i} m_j$ 作辗转相除法求出。

六、默比乌斯(Möbius)函数

Möbius 函数是定义在正整数集合上的函数 $\mu(n)$，它满足：

(i) $\mu(1)=1$；

(ii) $\mu(n)=0$，当 n 能被一个素数的平方整除；

(iii) $\mu(n)=(-1)^k$，当 n 是 k 个不同的素数的乘积。

定理 4 q 元有限域 F 上的 n 次首一不可约多项式的个数为

$$N_q(n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d,$$

其中 $\sum_{d|n}$ 表示对 n 的所有正因数求和.

证明可看 Rudolf Lidl, Harald Niederreiter, *Introduction to finite fields and their applications*, Revised edition, Cambridge University Press, 1994, 第 86 页的 *Theorem* 3.25。

7.12.2 典型例题

例 1 证明：在 $K(x)$ 中，如果一个分式有两个既约分式：$\frac{f_1}{g_1}$ 与 $\frac{f_2}{g_2}$，那么 f_1 与 f_2 相伴，且 g_1 与 g_2 相伴。

证明 由已知条件得，$\frac{f_1}{g_1}=\frac{f_2}{g_2}$。于是 $f_1g_2=g_1f_2$。由于 $\frac{f_1}{g_1}$ 是既约分式，因此 $(f_1,g_1)=1$，于是从 $f_1 \mid g_1f_2$ 可以推出 $f_1 \mid f_2$。同理，由于 $(f_2,g_2)=1$，因此从 $f_2 \mid f_1g_2$ 可以推出 $f_2 \mid f_1$，从而 f_1 与 f_2 相伴。类似可证 $g_1 \sim g_2$。 ■

例 2 如果一元分式 $\frac{f}{g}$ 的次数小于 0，并且它是既约分式，那么称它为**真分式**。证明：$K(x)$ 中每一个分式都可以唯一地表示成一个多项式与一个真分式的和。

证明 设 $\frac{f}{g}$ 是一个既约分式，对 f 与 g 作带余除法得

$$f = gh + r, \deg r < \deg g. \tag{28}$$

于是

$$\frac{f}{g}=\frac{gh+r}{g}=\frac{gh}{g}+\frac{r}{g}=\frac{h}{1}+\frac{r}{g}=h+\frac{r}{g}. \tag{29}$$

由于$(f,g)=1$,因此从(28)式得,$(g,r)=(f,g)=1$。于是$\frac{r}{g}$是一个既约分式,又由于$\deg\frac{r}{g}=\deg r-\deg g<0$,因此$\frac{r}{g}$是一个真分式。可表性证毕。

唯一性。假设还有$\frac{f}{g}=h_1+\frac{r_1}{g_1}$,其中$h_1,r_1,g_1\in K[x]$,$\deg r_1<\deg g_1$,且$(r_1,g_1)=1$,则

$$h-h_1=\frac{r_1}{g_1}-\frac{r}{g}=\frac{r_1g-rg_1}{g_1g}.$$

假如$h\neq h_1$,则$\deg(h-h_1)\geqslant 0$。然而

$$\deg\frac{r_1g-rg_1}{g_1g}=\deg(r_1g-rg_1)-\deg(g_1g)<0,$$

矛盾。因此$h=h_1$,从而$r_1g-rg_1=0$。由此得出,$\frac{r}{g}=\frac{r_1}{g_1}$。唯一性证毕。 ■

例 3　设$K(x)$中的非零既约分式$\frac{f}{g}$满足方程

$$a_0(x)y^n+a_1(x)y^{n-1}+\cdots+a_{n-1}(x)y+a_n(x)=0. \tag{30}$$

其中$a_i(x)\in K[x]$,$i=0,1,\cdots,n$,且$a_0(x)\neq 0$。证明:

$$f(x)\mid a_n(x),\ g(x)\mid a_0(x).$$

证明　由已知条件得

$$a_0(x)\frac{f^n}{g^n}+a_1(x)\frac{f^{n-1}}{g^{n-1}}+\cdots+a_{n-1}(x)\frac{f}{g}+a_n(x)=0.$$

于是

$$a_0(x)f^n+a_1(x)f^{n-1}g+\cdots+a_{n-1}(x)fg^{n-1}+a_n(x)g^n=0. \tag{31}$$

由此得出

$$a_0(x)f^n=-[a_1(x)f^{n-1}+\cdots+a_{n-1}(x)fg^{n-2}+a_n(x)g^{n-1}]g. \tag{32}$$

于是$g\mid a_0(x)f^n$。由于$(f,g)=1$,因此$(f^n,g)=1$,从而$g\mid a_0(x)$。

从(31)式又可得出

$$f[a_0(x)f^{n-1}+a_1(x)f^{n-2}g+\cdots+a_{n-1}(x)g^{n-1}]=-a_n(x)g^n. \tag{33}$$

于是$f\mid a_n(x)g^n$。由于$(f,g)=1$,因此$(f,g^n)=1$,从而$f\mid a_n(x)$。 ■

点评　例 3 的结论类似于“如果一个既约分数$\frac{q}{p}$是整系数多项式的根,那么分子q整除常数项,分母p整除首项系数。”

例 4 设 $K(x)$中的非零既约分式$\frac{f}{g}$满足方程

$$y^n + a_1(x)y^{n-1} + \cdots + a_{n-1}(x)y + a_n(x) = 0, \tag{34}$$

其中 $a_i(x)\in K[x]$,$i=1,2,\cdots,n$;$n\geqslant 1$。证明:$\frac{f}{g}\in K[x]$。

证明 据例 3 的结论得,$g\mid 1$,又 $1\mid g$,因此 $g\sim 1$。从而 $g=c$ 对某个 $c\in K^*$。于是 $\frac{f}{g}=c^{-1}f\in K[x]$。 ■

* **例 5** 设 $f(x),p(x)\in K[x]$,且 $p(x)$不可约。证明:如果 $\deg f(x)<\deg p^l(x)$。那么存在 $r_i(x)\in K[x]$,且 $\deg r_i(x)<\deg p(x)$,$i=1,2,\cdots,l$,使得

$$\frac{f(x)}{p^l(x)} = \frac{r_l(x)}{p(x)} + \frac{r_{l-1}(x)}{p^2(x)} + \cdots + \frac{r_2(x)}{p^{l-1}(x)} + \frac{r_1(x)}{p^l(x)}. \tag{35}$$

证明 若 $\deg f(x)<\deg p(x)$,则取 $r_1(x)=f(x)$,$r_2(x)=\cdots=r_l(x)=0$,有

$$\frac{f(x)}{p^l(x)} = \frac{0}{p(x)} + \cdots + \frac{0}{p^{l-1}(x)} + \frac{f(x)}{p^l(x)}.$$

下面设 $\deg f(x)\geqslant\deg p(x)$,对于 $f(x)$与 $p(x)$作带余除法得

$$f(x) = h_1(x)p(x) + r_1(x),\ \deg r_1(x) < \deg p(x).$$

于是 $\deg f(x)=\deg h_1(x)p(x)=\deg h_1(x)+\deg p(x)$。从而

$$\deg h_1(x) < \deg f(x).$$

若 $\deg h_1(x)\geqslant\deg p(x)$,对于 $h_1(x)$与 $p(x)$作带余除法得

$$h_1(x) = h_2(x)p(x) + r_2(x),\ \deg r_2(x) < \deg p(x).$$

同理可得,$\deg h_2(x)<\deg h_1(x)$。

依此类推,$h_i(x)$的次数不断降低,从而经有限步后,此过程必终止。设到第 s 步时终止,即

$$h_{s-1}(x) = h_s(x)p(x) + r_s(x),\ \deg r_s(x) < \deg p(x).$$

且 $0\leqslant\deg h_s(x)<\deg p(x)$。于是

$$\begin{aligned} f(x) &= [h_2(x)p(x) + r_2(x)]p(x) + r_1(x) \\ &= h_2(x)p^2(x) + r_2(x)p(x) + r_1(x) \\ &= \cdots = [h_s(x)p(x) + r_s(x)]p^{s-1}(x) + r_{s-1}(x)p^{s-2}(x) + \cdots + r_2(x)p(x) + r_1(x) \\ &= h_s(x)p^s(x) + r_s(x)p^{s-1}(x) + r_{s-1}(x)p^{s-2}(x) + \cdots + r_2(x)p(x) + r_1(x). \end{aligned}$$

把 $h_s(x)$记成 $r_{s+1}(x)$,则

$$\frac{f(x)}{p^s(x)} = r_{s+1}(x) + \frac{r_s(x)}{p(x)} + \frac{r_{s-1}(x)}{p^2(x)} + \cdots + \frac{r_2(x)}{p^{s-1}(x)} + \frac{r_1(x)}{p^s(x)}. \tag{36}$$

已知 $\deg f(x)<\deg p^l(x)$，于是 $\deg \frac{f(x)}{p^l(x)}<0$。不妨设 $p(x)$ 与 $f(x)$ 互素（否则 $p(x)\mid f(x)$，设 $p^t(x)\mid f(x)$，但是 $p^{t+1}(x)\nmid f(x)$，则 $f(x)=f_1(x)p^t(x)$，$p(x)\nmid f_1(x)$。于是 $\frac{f(x)}{p^l(x)}=\frac{f_1(x)}{p^{l-t}(x)}$。我们可以一开始就考虑 $\frac{f_1(x)}{p^{l-t}(x)}$），从而 $\frac{f(x)}{p^l(x)}$ 是真分式。据本节例 2 的唯一性，从(36)式可以推导出 $l>s$，于是在(36)式两边乘以 $\frac{1}{p^{l-s}(x)}$，得

$$\frac{f(x)}{p^l(x)}=\frac{r_{s+1}(x)}{p^{l-s}(x)}+\frac{r_s(x)}{p^{l-s+1}(x)}+\cdots+\frac{r_2(x)}{p^{l-1}(x)}+\frac{r_1(x)}{p^l(x)}. \tag{37}$$

令 $r_{s+2}(x)=\cdots=r_l(x)=0$，得

$$\frac{f(x)}{p^l(x)}=\frac{r_l(x)}{p(x)}+\cdots+\frac{r_{s+2}(x)}{p^{l-s-1}(x)}+\frac{r_{s+1}(x)}{p^{l-s}(x)}+\cdots+\frac{r_2(x)}{p^{l-1}(x)}+\frac{r_1(x)}{p^l(x)}. \tag{38}$$

■

* **例 6** 设 $f(x),g(x)\in K[x]$，且 $\deg g(x)>0$，设

$$g(x)=p_1^{l_1}(x)p_2^{l_2}(x)\cdots p_m^{l_m}(x), \tag{39}$$

其中 $p_1(x),p_2(x),\cdots,p_m(x)$ 是两两不等的不可约多项式，$l_i\in\mathbf{Z}^+$，$i=1,2,\cdots,m$。证明：如果 $\deg f(x)<\deg g(x)$，那么存在 $A_{ij_i}(x)\in K[x]$，且 $\deg A_{ij_i}(x)<\deg p_i(x)$，$i=1,2,\cdots,m$；$j_i=1,2,\cdots,l_i$，使得

$$\frac{f(x)}{g(x)}=\sum_{i=1}^{m}\sum_{j_i=1}^{l_i}\frac{A_{ij_i}(x)}{p_i^{j_i}(x)}. \tag{40}$$

证明 令

$$B_i(x)=p_1^{l_1}(x)\cdots p_{i-1}^{l_{i-1}}(x)p_{i+1}^{l_{i+1}}(x)\cdots p_m^{l_m}(x), \tag{41}$$

其中 $i=1,2,\cdots,m$。则 $(B_1(x),B_2(x),\cdots,B_m(x))=1$。从而存在 $u_i(x)\in K[x]$，$i=1,2,\cdots,m$，使得

$$u_1(x)B_1(x)+\cdots+u_m(x)B_m(x)=1. \tag{42}$$

在(42)式两边乘 $f(x)$，得

$$f(x)u_1(x)B_1(x)+\cdots+f(x)u_m(x)B_m(x)=f(x). \tag{43}$$

令 $\tilde{u}_i(x)=f(x)u_i(x)$，$i=1,2,\cdots,m$。则

$$\tilde{u}_1(x)B_1(x)+\cdots+\tilde{u}_m(x)B_m(x)=f(x). \tag{44}$$

对 $\tilde{u}_i(x)$ 和 $p_i^{l_i}(x)$ 作带余除法，得

$$\tilde{u}_i(x)=h_i(x)p_i^{l_i}(x)+r_i(x),\deg r_i(x)<\deg p_i^{l_i}(x).$$

其中 $i=1,2,\cdots,m$。代入(44)式，得

$$\sum_{i=1}^{m}[h_i(x)p_i^{l_i}(x)B_i(x)+r_i(x)B_i(x)]=f(x). \tag{45}$$

即

$$\Big[\sum_{i=1}^{m}h_i(x)\Big]g(x)+\sum_{i=1}^{m}r_i(x)B_i(x)=f(x). \tag{46}$$

(46)式两边同除以 $g(x)$,得

$$\frac{f(x)}{g(x)}=\sum_{i=1}^{m}h_i(x)+\sum_{i=1}^{m}\frac{r_i(x)}{p_i^{l_i}(x)}. \tag{47}$$

由于 $\deg f(x)<\deg g(x)$,且不妨设 $f(x)$与 $g(x)$互素,因此$\dfrac{f(x)}{g(x)}$是真分式,据本节例 2 的唯一性,从(47)式得

$$\sum_{i=1}^{m}h_i(x)=0.$$

从而

$$\frac{f(x)}{g(x)}=\sum_{i=1}^{m}\frac{r_i(x)}{p_i^{l_i}(x)}. \tag{48}$$

由于 $\deg r_i(x)<\deg\ p_i^{l_i}(x)$,因此据本节例 5 的结论得,存在 $A_{ij_i}(x)\in K[x]$,且 $\deg A_{ij_i}(x)<\deg\ p_i(x)$,$j_i=1,2,\cdots,l_i$,使得

$$\frac{r_i(x)}{p_i^{l_i}(x)}=\sum_{j_i=1}^{l_i}\frac{A_{ij_i}(x)}{p_i^{j_i}(x)},i=1,2,\cdots,m. \tag{49}$$

因此

$$\frac{f(x)}{g(x)}=\sum_{i=1}^{m}\sum_{j_i=1}^{l_i}\frac{A_{ij_i}(x)}{p_i^{j_i}(x)}. \tag{50}$$

■

点评 例 6 的本质是给出了真分式可以表示成若干个形如$\dfrac{A_{ij_i}(x)}{p_i^{j_i}(x)}$的真分式的和,其中分子的次数小于分母中不可约多项式 $p_i(x)$的次数。这通常称为把一个真分式表示成部分分式的和。当 K 是实数域 $\mathbf{R}$ 时,就得到下述例 7。

* **例 7** 设 $f(x),g(x)\in\mathbf{R}[x]$,$g(x)$的首次系数为 1,且 $\deg g(x)>0$。设

$$g(x)=\prod_{i=1}^{m}(x-a_i)^{l_i}\prod_{j=1}^{s}(x^2+p_jx+q_j)^{t_j}, \tag{51}$$

其中 $a_1,a_2,\cdots,a_m$ 是两两不等的实数,$p_j^2-4q_j<0$,$j=1,\cdots,s$;$(p_1,q_1),\cdots,(p_s,q_s)$是两两不等的实数对,$l_i,t_j\in\mathbf{N}$,$i=1,2,\cdots,m$;$j=1,2,\cdots,s$。证明:如果 $\deg f(x)<\deg g(x)$,那么存在 $A_{ik_i},B_{jv_j},C_{jv_j}\in\mathbf{R}$,$i=1,2,\cdots,m$;$k_i=1,\cdots,l_i$;$j=1,\cdots,s$;$v_j=1,\cdots,t_j$,使得

$$\frac{f(x)}{g(x)}=\sum_{i=1}^{m}\sum_{k_i=1}^{l_i}\frac{A_{ik_i}}{(x-a_i)^{k_i}}+\sum_{j=1}^{s}\sum_{v_j=1}^{t_j}\frac{B_{jv_j}x+C_{jv_j}}{(x^2+p_jx+q_j)^{v_j}}. \tag{52}$$

证明 由于实数域上的不可约多项式只有一次多项式和判别式小于 0 的二次多项式，因此从例 6 立即得到例 7。 ■

点评 例 7 的结论在数学分析课程中求有理函数的不定积分时有重要应用。例 7 告诉我们，一个真分式可以表示成(52)式右端所示的若干个真分式的和，它们的分子是常数，而分母是一次多项式的方幂，或者分子是一次多项式，而分母是二次不可约多项式的方幂。有了这个结论，在具体求各个真分式的分子时可以用待定系数法。在数学中往往是这样：有了明确的方向后，具体计算就不难了，明确方向是关键。

例 8 下列模 m 剩余类环中，哪些是域？哪些不是域？写出其中的可逆元，并且求出每个可逆元的逆元。

$$\mathbf{Z}_4,\mathbf{Z}_6,\mathbf{Z}_8,\mathbf{Z}_9,\mathbf{Z}_{11},\mathbf{Z}_{13}.$$

解 由于 11 和 13 是素数，因此 $\mathbf{Z}_{11},\mathbf{Z}_{13}$ 是域；由于 4,6,8,9 是合数，因此 $\mathbf{Z}_4,\mathbf{Z}_6,\mathbf{Z}_8,\mathbf{Z}_9$ 不是域。

$\mathbf{Z}_4$ 中，$\overline{1}\cdot\overline{1}=\overline{1},\overline{2}\cdot\overline{2}=\overline{0},\overline{3}\cdot\overline{3}=\overline{1}$，因此 $\overline{1},\overline{3}$ 是可逆元，$\overline{1}^{-1}=\overline{1},\overline{3}^{-1}=\overline{3},\overline{2}$ 不是可逆元。

$\mathbf{Z}_6$ 中，$\overline{1}\cdot\overline{1}=\overline{1},\overline{2}\cdot\overline{3}=\overline{0},\overline{4}\cdot\overline{3}=\overline{0},\overline{5}\cdot\overline{5}=\overline{1},\overline{6}\cdot\overline{2}=\overline{0}$，因此 $\overline{1},\overline{5}$ 是可逆元，$\overline{1}^{-1}=\overline{1},\overline{5}^{-1}=\overline{5}$，其余元素不是可逆元。

$\mathbf{Z}_8$ 中，$\overline{1}\cdot\overline{1}=\overline{1},\overline{2}\cdot\overline{4}=\overline{0},\overline{3}\cdot\overline{3}=\overline{1},\overline{5}\cdot\overline{5}=\overline{1},\overline{6}\cdot\overline{4}=\overline{0},\overline{7}\cdot\overline{7}=\overline{1}$，因此 $\overline{1},\overline{3},\overline{5},\overline{7}$ 是可逆元，$\overline{1}^{-1}=\overline{1},\overline{3}^{-1}=\overline{3},\overline{5}^{-1}=\overline{5},\overline{7}^{-1}=\overline{7}$，其余元素不是可逆元。

$\mathbf{Z}_9$ 中，$\overline{1}\cdot\overline{1}=\overline{1},\overline{2}\cdot\overline{5}=\overline{1},\overline{3}\cdot\overline{3}=\overline{0},\overline{4}\cdot\overline{7}=\overline{1},\overline{6}\cdot\overline{3}=\overline{0},\overline{8}\cdot\overline{8}=\overline{1}$，因此 $\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8}$ 是可逆元，$\overline{1}^{-1}=\overline{1},\overline{2}^{-1}=\overline{5},\overline{5}^{-1}=\overline{2},\overline{4}^{-1}=\overline{7},\overline{7}^{-1}=\overline{4},\overline{8}^{-1}=\overline{8}$，其余元素不是可逆元。

$\mathbf{Z}_{11}$ 中每个非零元都可逆，由于 $\overline{1}\cdot\overline{1}=\overline{1},\overline{2}\cdot\overline{6}=\overline{1},\overline{3}\cdot\overline{4}=\overline{1},\overline{5}\cdot\overline{9}=\overline{1},\overline{7}\cdot\overline{8}=\overline{1},\overline{10}\cdot\overline{10}=\overline{1}$，因此 $\overline{1}^{-1}=\overline{1},\overline{2}^{-1}=\overline{6},\overline{6}^{-1}=\overline{2},\overline{3}^{-1}=\overline{4},\overline{4}^{-1}=\overline{3},\overline{5}^{-1}=\overline{9},\overline{9}^{-1}=\overline{5},\overline{7}^{-1}=\overline{8},\overline{8}^{-1}=\overline{7},\overline{10}^{-1}=\overline{10}$。

$\mathbf{Z}_{13}$ 中每个非零元都可逆，由于 $\overline{1}\cdot\overline{1}=\overline{1},\overline{2}\cdot\overline{7}=\overline{1},\overline{3}\cdot\overline{9}=\overline{1},\overline{4}\cdot\overline{10}=\overline{1},\overline{5}\cdot\overline{8}=\overline{1},\overline{6}\cdot\overline{11}=\overline{1},\overline{12}\cdot\overline{12}=\overline{1}$，因此 $\overline{1}^{-1}=\overline{1},\overline{2}^{-1}=\overline{7},\overline{7}^{-1}=\overline{2},\overline{3}^{-1}=\overline{9},\overline{9}^{-1}=\overline{3},\overline{4}^{-1}=\overline{10},\overline{10}^{-1}=\overline{4},\overline{5}^{-1}=\overline{8},\overline{8}^{-1}=\overline{5},\overline{6}^{-1}=\overline{11},\overline{11}^{-1}=\overline{6},\overline{12}^{-1}=\overline{12}$。

例 9 从例 8 等例子，你能猜测 $\mathbf{Z}_m$ 中，$\overline{a}$ 是可逆元的充分必要条件是什么吗？你能给予证明吗？

解 猜测 $\mathbf{Z}_m$ 中 $\overline{a}$ 是可逆元当且仅当 a 与 m 互素。

证明：充分性。设 a 与 m 互素，则存在 $u,v\in\mathbf{Z}$，使得

$$ua+vm=1.$$

从而 $\overline{1}=\overline{ua+vm}=\overline{u}\,\overline{a}+\overline{v}\,\overline{m}=\overline{u}\,\overline{a}$。因此 $\overline{a}$ 可逆。

必要性。设 a 与 m 不互素，且 $0<a<m$，则 $(a,m)=d$，其中 $d>1$。于是 $a=db,m=dl$，其中 $b,l\in\mathbf{Z}^+$。由于 $d>1$，因此 $l<m$。由于 $la=ldb=mb$，因此

$$\bar{l}\,\bar{a}=\bar{m}\,\bar{b}=\bar{0}.$$

假如 $\bar{a}$ 可逆，则在上式两边乘 $\bar{a}^{-1}$ 得，$\bar{l}=\bar{0}$。矛盾。因此 $\bar{a}$ 不可逆。 ■

点评 从例 9 的必要性的证明还看出：当 a 与 m 不互素时（其中 $0<a<m$），$\bar{a}$ 是 $\mathbf{Z}_m$ 中的零因子。由此可见：$\mathbf{Z}_m$ 中的元素或者是可逆元，或者是零因子，二者必居其一且只居其一。

例 10 令

$$F=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\middle| a,b\in \mathbf{Z}_3\right\}, \tag{53}$$

证明：F 是一个有 9 个元素的域，并且 $\operatorname{char} F=3$。

证明 由于

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}+\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}=\begin{pmatrix} a_1+a_2 & b_1+b_2 \\ -(b_1+b_2) & a_1+a_2 \end{pmatrix}, \tag{54}$$

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}=\begin{pmatrix} a_1a_2-b_1b_2 & a_1b_2+b_1a_2 \\ -(a_1b_2+b_1a_2) & a_1a_2-b_1b_2 \end{pmatrix}, \tag{55}$$

因此 F 有加法和乘法运算，显然，加法满足交换律，结合律，有零元 $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$，每个元素有负元；乘法满足结合律，以及乘法对于加法的分配律。因此 F 是一个环，又 $\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$ 是 F 的单位元。由于

$$\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}=\begin{pmatrix} a_2a_1-b_2b_1 & a_2b_1+b_2a_1 \\ -(a_2b_1+b_2a_1) & a_2a_1-b_2b_1 \end{pmatrix}, \tag{56}$$

由(55)、(56)式得出，F 的乘法满足交换律，因此 F 是一个有单位元的交换环。

$$\begin{vmatrix} a & b \\ -b & a \end{vmatrix}=a^2+b^2, \tag{57}$$

$$a^2+b^2=0 \quad\Leftrightarrow\quad a^2=-b^2.$$

当 $b=\bar{0}$ 时，$a=\bar{0}$。当 $b=\bar{1}$ 时，$a^2=-\bar{1}=\bar{2}$。由于 $\bar{1}^2=\bar{1}$，$\bar{2}^2=\bar{1}$，因此在 $\mathbf{Z}_3$ 中 $a^2=\bar{2}$ 无解。当 $b=\bar{2}$ 时，$a^2=-\bar{1}=\bar{2}$，无解。这证明了 $a^2+b^2=0 \quad\Leftrightarrow\quad a=b=0$。因此 F 中每个非零矩阵都可逆。从而 F 是一个域。

由于 a 可取 $\bar{0},\bar{1},\bar{2}$；b 也可取 $\bar{0},\bar{1},\bar{2}$，因此 F 有 9 个元素。由于

$$3\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}=\begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix},$$

$$2\begin{pmatrix}\overline{1} & \overline{0}\\ \overline{0} & \overline{1}\end{pmatrix}=\begin{pmatrix}\overline{2} & \overline{0}\\ \overline{0} & \overline{2}\end{pmatrix},$$

因此域 F 的特征为 3。 ■

例 11 证明:在特征为 p 的域 F 中,下式成立:

$$(a+b)^p=a^p+b^p. \tag{58}$$

证明 $(a+b)^p=a^p+pa^{p-1}b+C_p^2a^{p-2}b^2+\cdots+C_p^ka^{p-k}b^k+\cdots+b^p$。我们已经证明 $p\mid C_p^k$,$1\leqslant k<p$。因此 $C_p^ka^{p-k}b^k=0$,$1\leqslant k<p$。从而 $(a+b)^p=a^p+b^p$。 ■

例 12 证明**费马小定理**:设 p 是素数,则对任意整数 a 都有

$$a^p\equiv a \pmod p. \tag{59}$$

证明 设 $a=hp+r$,$0<r<p$,则 $\overline{a}=\overline{r}$。于是

$$\overline{a^p}=\overline{a}^p=\overline{r}^p=(\underbrace{\overline{1}+\cdots+\overline{1}}_{r\text{个}})^p=\underbrace{\overline{1}^p+\cdots+\overline{1}^p}_{r\text{个}}=\overline{r}=\overline{a}.$$

因此 $a^p\equiv a \pmod p$。若 $p\mid a$,则(59)式显然成立。 ■

例 13 写出 $\mathbf{Z}_2[x]$ 中所有一次多项式和二次不可约多项式。

解 一次多项式有 x,$x+\overline{1}$。

二次多项式有 x^2,x^2+x,$x^2+\overline{1}$,$x^2+x+\overline{1}$。由于 $x^2+x=x(x+1)$,$x^2+\overline{1}=(x+\overline{1})^2$,因此 x^2,x^2+x,$x^2+\overline{1}$ 都可约。由于 $\overline{0}$ 和 $\overline{1}$ 都不是 $x^2+x+\overline{1}$ 的根,因此 $x^2+x+\overline{1}$ 没有一次因式,从而它不可约。

例 14 设 $f(x)=3x^5+11x^2+7\in\mathbf{Z}[x]$,判断 $f(x)$ 在 $\mathbf{Q}$ 上是否不可约。

解 把 $f(x)$ 的各项系数模 2 以后得到 $\mathbf{Z}_2$ 上的多项式:

$$\begin{aligned}\widetilde{f}(x)&=x^5+x^2+\overline{1}\\&=x^2(x^3+\overline{1})+\overline{1}\\&=x^2(x+\overline{1})(x^2-x\cdot\overline{1}+\overline{1}^2)+\overline{1}\\&=x^2(x+\overline{1})(x^2+x+\overline{1})+\overline{1}.\end{aligned} \tag{60}$$

$\widetilde{f}(x)$ 是 $\mathbf{Z}_2$ 上的五次多项式,如果它在 $\mathbf{Z}_2$ 上可约,那么它必有一次因式或二次不可约因式。但是 $\mathbf{Z}_2$ 上的一次多项式只有 x,$x+\overline{1}$;二次不可约多项式只有 $x^2+x+\overline{1}$。从(60)式看出,它们都不是 $\widetilde{f}(x)$ 的因式。因此 $\widetilde{f}(x)$ 在 $\mathbf{Z}_2$ 上不可约。据本节命题 5 得,$f(x)$ 在 $\mathbf{Q}$ 上不可约。

例 15 设 $f(x)=8x^3-5x^2+22x+28\in\mathbf{Z}[x]$,判断 $f(x)$ 在 $\mathbf{Q}$ 上是否不可约。

解 $f(x)$ 的首项系数 8 是偶数,但不能被 3 整除,因此把 $f(x)$ 的各项系数模 3 得到 $\mathbf{Z}_3$ 上的多项式:

$$\tilde{f}(x) = \bar{2}x^3 + x^2 + x + \bar{1}.$$

由于 $\tilde{f}(\bar{0}) = \bar{1} \neq \bar{0}$，$\tilde{f}(\bar{1}) = \bar{2} \neq \bar{0}$，$\tilde{f}(\bar{2}) = \bar{2} \neq \bar{0}$，因此 $\bar{0}$，$\bar{1}$，$\bar{2}$ 都不是 $\tilde{f}(x)$ 的根，从而 $\tilde{f}(x)$ 在 $\mathbf{Z}_3[x]$ 中没有一次因式。由于 $\tilde{f}(x)$ 是三次多项式，因此 $\tilde{f}(x)$ 在 $\mathbf{Z}_3$ 上不可约，据本节命题 5 得，$f(x)$ 在 $\mathbf{Q}$ 上不可约。

点评 $f(x)$ 是三次整系数多项式，也可以判断 $f(x)$ 没有有理根，从而证明 $f(x)$ 在 $\mathbf{Q}$ 上不可约。但是由于 $f(x)$ 的首项系数为 8，常数项为 28，因此 $f(x)$ 可能的有理根较多，一个一个地筛选，计算量较大。把 $f(x)$ 的各项系数模 3 得到 $\mathbf{Z}_3$ 上的多项式 $\tilde{f}(x)$，只需计算 $\tilde{f}(\bar{0})$，$\tilde{f}(\bar{1})$，$\tilde{f}(\bar{2})$ 就可判断 $\tilde{f}(x)$ 在 $\mathbf{Z}_3$ 中没有根，从而 $\tilde{f}(x)$ 在 $\mathbf{Z}_3$ 上不可约。计算量减少了许多。从例 14 和例 15 都看出，把一个整系数多项式的各项系数模 2（或模 3，…）得到 $\mathbf{Z}_2$（或 $\mathbf{Z}_3$，…）上的多项式，起着简化问题的作用。

例 16 设 $f(x) = 5x^4 + 17x^3 - 9x^2 + 3 \in \mathbf{Z}[x]$，判断 $f(x)$ 在 $\mathbf{Q}$ 上是否不可约。

解 把 $f(x)$ 的各项系数模 2 得到 $\mathbf{Z}_2$ 上的多项式：

$$\begin{aligned}\tilde{f}(x) &= x^4 + x^3 + x^2 + \bar{1} \\ &= x^3(x + \bar{1}) + (x + \bar{1})^2 \\ &= (x + \bar{1})(x^3 + x + \bar{1}).\end{aligned} \tag{61}$$

由于 $\bar{0}$ 和 $\bar{1}$ 都不是 $x^3 + x + \bar{1}$ 的根，因此三次多项式 $x^3 + x + \bar{1}$ 在 $\mathbf{Z}_2$ 上不可约。从而(61)式是 $\tilde{f}(x)$ 在 $\mathbf{Z}_2[x]$ 中的唯一因式分解式。

假如 $f(x)$ 在 $\mathbf{Q}$ 上可约，则

$$f(x) = f_1(x)f_2(x),\ \deg f_i(x) < \deg f(x), i = 1,2.$$

把上式的每一个多项式的各项系数模 2 得到

$$\tilde{f}(x) = \tilde{f}_1(x)\tilde{f}_2(x).$$

由于 $f(x)$ 的首项系数 5 是奇数，因此 $f_i(x)$ 的首项系数必为奇数，$i=1,2$。从而 $\deg \tilde{f}_i(x) = \deg f_i(x) < \deg f(x) = \deg \tilde{f}(x)$，$i=1,2$。从(61)式看出，$\tilde{f}_1(x)$ 与 $\tilde{f}_2(x)$ 中必有一个是一次因式。从而 $f_1(x)$ 与 $f_2(x)$ 中必有一个是一次因式。由此推出 $f(x)$ 有有理根。$f(x)$ 的有理根只可能是 $\pm 1, \pm 3, \pm\frac{1}{5}, \pm\frac{3}{5}$。由于

$$f(1) = 16, f(-1) = -18,$$

$$\frac{f(-1)}{1+3} = \frac{-18}{4} \notin \mathbf{Z},$$

因此 1，−1，3 都不是 $f(x)$ 的根。由于

5	17	−9	0	3	−3
	−15	−6	45	−135	
5	2	−15	45	−132	

因此−3 不是 $f(x)$的根,由于

$$\frac{f(1)}{5-(-1)}=\frac{16}{6}\notin \mathbf{Z},\frac{f(-1)}{5+3}=\frac{18}{8}\notin \mathbf{Z},$$

因此$-\frac{1}{5},\frac{3}{5}$都不是 $f(x)$的根。

用综合除法可以知道$\frac{1}{5},-\frac{3}{5}$不是 $f(x)$的根。

综上所述,$f(x)$没有有理根,矛盾。因此 $f(x)$在 $\mathbf{Q}$ 上不可约。

点评 例 16 中,$f(x)$的系数模 2 得到的多项式 $\tilde{f}(x)$在 $\mathbf{Z}_2$ 上可约。运用 $\mathbf{Z}_2[x]$中唯一因式分解定理,用反证法证明了 $f(x)$在 $\mathbf{Q}$ 上不可约。这表明当 $\tilde{f}(x)$在 $\mathbf{Z}_2$ 上可约时,$f(x)$是否在 $\mathbf{Q}$ 上可约必须具体问题具体分析。

例 17 设 p 是素数。

(1) $\mathbf{Z}_p$ 上的一元函数(即 $\mathbf{Z}_p$ 到 $\mathbf{Z}_p$ 的映射)有多少个?

(2) 证明 $\mathbf{Z}_p$ 上的一元函数都是 $\mathbf{Z}_p$ 上的一元多项式函数,并且 $\mathbf{Z}_p$ 上的每一个一元函数都可以唯一地表示成 $\mathbf{Z}_p$ 上的次数小于 p 的一元多项式函数。

(1)**解** 任取 $\mathbf{Z}_p$ 上的一个一元函数 f,f 完全被 p 元有序组$(f(\bar{0}),f(\bar{1}),f(\bar{2}),\cdots,f(\overline{p-1}))$决定。即存在由 $\mathbf{Z}_p$ 上的一元函数组成的集合 S 到 $\mathbf{Z}_p$ 上的 p 元有序组形成的集合$\mathbf{Z}_p^p$的一个映射$\sigma:f\longmapsto(f(\bar{0}),f(\bar{1}),\cdots,f(\overline{p-1}))$,显然 σ 是单射。易知 σ 是满射,从而 σ 是双射。由于$\mathbf{Z}_p^p$共有$\underbrace{p\,p\cdots p}_{p\text{个}}=p^p$ 个元素,因此 S 有 p^p 个元素。即 $\mathbf{Z}_p$ 上的一元函数共有 p^p 个。

(2) **证明** $\mathbf{Z}_p$ 上的一元多项式函数是由 $\mathbf{Z}_p$ 上的一元多项式诱导的函数,考虑 $\mathbf{Z}_p$ 上次数小于 p 的一元多项式组成的集合。

$$W=\{a_0+a_1x+\cdots+a_{p-1}x^{p-1}\mid a_i\in\mathbf{Z}_p,i=0,1,2,\cdots,p-1\}.$$

由于 $a_0,a_1,\cdots,a_{p-1}$各有 p 种取法,因此$|W|=p^p$。设

$$f(x)=a_0+a_1x+\cdots+a_{p-1}x^{p-1},g(x)=b_0+b_1x+\cdots+b_{p-1}x^{p-1}.$$

假如 $f(x)$诱导的一元多项式函数 f 与 $g(x)$诱导的一元多项式函数 g 相等,则 $f(\bar{i})=g(\bar{i}),i=0,1,2,\cdots,p-1$。令 $h(x)=f(x)-g(x)$,则 $\deg h(x)\leqslant p-1$。如果 $h(x)\neq 0$,那

么 $h(x)$ 在 $\mathbf{Z}_p$ 中的根至多有 $p-1$ 个。现在 $h(\bar{i})=f(\bar{i})-g(\bar{i})=\bar{0}, i=0,1,\cdots,p-1$，这表明 $h(x)$ 在 $\mathbf{Z}_p$ 中的根有 p 个。因此 $h(x)=0$。从而 $f(x)=g(x)$。这证明了 W 中不相等的多项式诱导的多项式函数也不相等。因此 $\mathbf{Z}_p$ 上次数小于 p 的一元多项式函数组成的集合 S_1 的元素个数等于 $|W|=p^p$。由于 S_1 是 S 的子集，且 $|S_1|=p^p=|S|$，因此 $S_1=S$。这证明了 $\mathbf{Z}_p$ 上的一元函数可以唯一地表示成 $\mathbf{Z}_p$ 上的一元多项式函数，从而 $\mathbf{Z}_p$ 上的一元函数都是 $\mathbf{Z}_p$ 上的一元多项式函数。 ■

点评 例 17 表明 $\mathbf{Z}_p$ 上的一元函数只有多项式函数，而实数域上的一元函数有多项式函数、指数函数、正弦函数、余弦函数等。这开拓了读者的视野。同时 $\mathbf{Z}_p$ 上的一元函数都是多项式函数这个结论在信息时代有重要应用。例 17 第(2)小题的证明体现了数学思维方式的严谨性：证明了 $\mathbf{Z}_p$ 上次数小于 p 的两个多项式 $f(x)$ 与 $g(x)$ 如果不相等，那么它们诱导的一元多项式函数 f 与 g 也不相等。从而 $\mathbf{Z}_p$ 上次数小于 p 的一元多项式组成的集合 W 与它们诱导的一元多项式函数组成的集合 S_1 的元素个数相等。于是 $|S_1|=|W|=p^p$。

例 18 令 $F=K(x)$，其中 K 是数域，$F[y]$ 中的非零多项式

$$g_x(y)=b_n(x)y^n+\cdots+b_1(x)y+b_0(x), \tag{62}$$

其中 $b_i(x)\in K[x], i=0,1,\cdots,n$。如果 $(b_n(x),\cdots,b_1(x),b_0(x))=1$，那么称 $g_x(y)$ 是 F 上的一个**本原多项式**。证明：F 上的任意一个非零多项式 $f_x(y)$ 都与 F 上的一个本原多项式相伴。

证明 设

$$f_x(y)=\frac{q_n(x)}{p_n(x)}y^n+\cdots+\frac{q_1(x)}{p_1(x)}y+\frac{q_0(x)}{p_0(x)},$$

其中 $\frac{q_n(x)}{p_n(x)},\cdots,\frac{q_0(x)}{p_0(x)}$ 不全为 0，令

$$m(x)=[p_n(x),\cdots,p_1(x),p_0(x)],$$

则

$$m(x)=h_i(x)p_i(x), h_i(x)\in K[x], i=0,1,\cdots,n.$$

于是

$$f_x(y)=\frac{1}{m(x)}[q_n(x)h_n(x)y^n+\cdots+q_1(x)h_1(x)y+q_0(x)h_0(x)].$$

令

$$d(x)=(q_n(x)h_n(x),\cdots,q_1(x)h_1(x),q_0(x)h_0(x)).$$

则

$$q_i(x)h_i(x)=b_i(x)d(x), i=0,1,\cdots,n.$$

于是

$$f_x(y)=\frac{d(x)}{m(x)}[b_n(x)y^n+\cdots+b_1(x)y+b_0(x)].$$

记 $g_x(y)=b_n(x)y^n+\cdots+b_1(x)y+b_0(x)$，则 $g_x(y)$ 是 F 上的一个本原多项式，且 $f_x(y)\sim g_x(y)$。 ■

例 19 令 $F=K(x)$，其中 K 是数域，证明：F 上的两个本原多项式 $g_x(y)$ 与 $h_x(y)$ 在 $F[y]$ 中相伴当且仅当 $g_x(y)=c\,h_x(y)$，其中 $c\in K^*$。

证明 设 $g_x(y)$ 与 $h_x(y)$ 是 F 上的两个本原多项式。

必要性。设 $g_x(y)$ 与 $h_x(y)$ 在 $F[y]$ 中相伴，则存在 F 中的非零元 $\frac{q(x)}{p(x)}$，使得 $g_x(y)=\frac{q(x)}{p(x)}h_x(y)$，其中 $q(x)$ 与 $p(x)$ 互素。假如 $\frac{q(x)}{p(x)}$ 不是 K 中的非零数，则 $q(x)$ 与 $p(x)$ 中至少有一个不是 K 中的非零数。不妨设 $p(x)$ 不是 K 中的非零数，则 $p(x)$ 的次数大于 0。设 $g_x(y)=\sum_{i=0}^{n}b_i(x)y^i$，$h_x(y)=\sum_{i=0}^{n}c_i(x)y^i$，其中 $b_i(x),c_i(x)\in K[x]$，$i=0,1,\cdots,n$。由于 $p(x)g_x(y)=q(x)h_x(y)$，因此通过比较 y^i 的系数得

$$p(x)b_i(x)=q(x)c_i(x). \tag{63}$$

于是 $p(x)\mid q(x)c_i(x)$。由于 $(p(x),q(x))=1$，因此

$$p(x)\mid c_i(x),i=0,1,\cdots,n. \tag{64}$$

于是 $(c_0(x),c_1(x),\cdots,c_n(x))\neq 1$，这与 $h_x(y)$ 是 F 上的本原多项式矛盾。因此 $\frac{q(x)}{p(x)}=c$，其中 $c\in K^*$，从而 $g_x(y)=c\,h_x(y)$。

充分性是显然的。 ■

例 20 设 $F=K(x)$，其中 K 是数域。证明：F 上两个本原多项式的乘积还是本原多项式。

证明 设

$$f_x(y)=a_n(x)y^n+\cdots+a_1(x)y+a_0(x), \tag{65}$$

$$g_x(y)=b_m(x)y^m+\cdots+b_1(x)y+b_0(x) \tag{66}$$

是 F 上的两个本原多项式，令

$$h_x(y)=f_x(y)g_x(y)=c_{n+m}(x)y^{n+m}+\cdots+c_1(x)y+c_0(x). \tag{67}$$

其中 $$c_s(x)=\sum_{i+j=s}a_i(x)b_j(x),s=0,1,\cdots,n+m.$$

假如 $h_x(y)$ 不是 F 上的本原多项式，则存在 $K[x]$ 中的一个不可约多项式 $p(x)$，使得 $p(x)\mid c_s(x)$，$s=0,1,\cdots,n+m$。因为 $f_x(y)$ 是 F 上本原的，所以 $p(x)$ 不能同时整除 $f_x(y)$ 的每一项系数。于是存在 $k(0\leqslant k\leqslant n)$ 满足

$$p(x)\mid a_0(x),\cdots,p(x)\mid a_{k-1}(x),p(x)\nmid a_k(x). \tag{68}$$

同理，存在 $l(0\leqslant l\leqslant m)$ 满足

$$p(x)\mid b_0(x),\cdots,p(x)\mid b_{l-1}(x),p(x)\nmid b_l(x). \tag{69}$$

考虑 $h_x(y)$的 $k+l$ 次项的系数：

$$\begin{aligned}c_{k+l}(x)=&a_{k+l}(x)b_0(x)+a_{k+l-1}(x)b_1(x)+\cdots+a_{k+1}(x)b_{l-1}(x)\\&+a_k(x)b_l(x)+a_{k-1}(x)b_{l+1}(x)+\cdots+a_0(x)b_{k+l}(x).\end{aligned} \tag{70}$$

由(68)、(69)、(70)式得 $p(x)\nmid c_{k+l}(x)$，矛盾。因此 $h_x(y)$是 F 上的本原多项式。 ■

例 21 设 $F=K(x)$，其中 K 是数域，证明：F 上的一个次数大于 0 的本原多项式 $g_x(y)$在 F 上可约当且仅当 $g_x(y)$可以分解成两个次数较低的 F 上的本原多项式的乘积。

证明 充分性是显然的，下面证必要性。

设 F 上的本原多项式 $g_x(y)$在 F 上可约，则存在 $p_x(y),q_x(y)\in F[y]$，使得

$$g_x(y)=p_x(y)q_x(y),\deg p_x(y)<\deg g_x(y),\deg q_x(y)<\deg g_x(y).$$

设 $p_x(y)=\dfrac{u_1(x)}{u_2(x)}\tilde{p}_x(y)$，$q_x(y)=\dfrac{v_1(x)}{v_2(x)}\tilde{q}_x(y)$，其中 $\tilde{p}_x(y),\tilde{q}_x(y)$是 F 上的本原多项式，$\dfrac{u_1(x)}{u_2(x)},\dfrac{v_1(x)}{v_2(x)}$是 F 中的非零元，则

$$g_x(y)=\frac{u_1(x)}{u_2(x)}\frac{v_1(x)}{v_2(x)}\tilde{p}_x(y)\tilde{q}_x(y). \tag{71}$$

(71)式表明 $g_x(y)$与 $\tilde{p}_x(y)\tilde{q}_x(y)$在 $F[y]$中相伴，根据例 20 得，$\tilde{p}_x(y)\tilde{q}_x(y)$仍是 F 上的本原多项式；根据例 19 得，存在 $c\in K^*$ 使得 $g_x(y)=c\,\tilde{p}_x(y)\tilde{q}_x(y)$。由于

$$\deg\tilde{p}_x(y)=\deg p_x(y)<\deg g_x(y),\deg\tilde{q}_x(y)=\deg q_x(y)<\deg g_x(y),$$

因此 $g_x(y)$分解成了两个次数较低的 F 上的本原多项式 $c\,\tilde{p}_x(y)$与 $\tilde{q}_x(y)$的乘积。 ■

例 22 设 $F=K(x)$，其中 K 是数域。证明：$F[y]$中的次数大于 0 且系数属于 $K[x]$的多项式 $f_x(y)$在 F 上可约当且仅当 $f_x(y)$可以分解成两个次数较低的系数属于 $K[x]$的多项式的乘积。

证明 必要性。设 $f_x(y)=c(x)g_x(y)$，其中 $g_x(y)$是 F 上的本原多项式，$c(x)\in K[x]$，且 $c(x)\neq0$。由于 $f_x(y)$在 F 上可约，因此 $g_x(y)$也在 F 上可约，根据例 21 得，

$$g_x(y)=p_x(y)q_x(y),\deg p_x(y)<\deg g_x(y),\deg q_x(y)<\deg g_x(y),$$

其中 $p_x(y),q_x(y)$是 F 上的两个本原多项式。从而

$$f_x(y)=[c(x)p_x(y)]q_x(y).$$

这表明 $f_x(y)$分解成了两个次数较低的系数属于 $K[x]$的多项式 $c(x)p_x(y)$与 $q_x(y)$的乘积。

充分性是显然的。 ■

例 23 设 $F=K(x)$,其中 K 是数域,设

$$f_x(y)=a_n(x)y^n+\cdots+a_1(x)y+a_0(x)$$

是 $F[y]$中一个次数 n 大于 0 的系数属于 $K[x]$的多项式。证明:如果存在 K 上一个不可约多项式 $p(x)$,使得

$$p(x)\nmid a_n(x),p(x)\mid a_i(x),i=0,1,\cdots,n-1;p^2(x)\nmid a_0(x),$$

那么 $f_x(y)$在 $F[y]$中是不可约的。

证明 假如 $f_x(y)$在 F 上可约,则根据例 22 得

$$f_x(y)=[b_m(x)y^m+\cdots+b_1(x)y+b_0(x)][c_l(x)y^l+\cdots+c_1(x)y+c_0(x)],\tag{72}$$

其中 $b_i(x),c_j(x)\in K[x],i=0,1,\cdots,m;j=0,1,\cdots,l,b_m(x)\neq 0,c_l(x)\neq 0$。$m<n,l<n$,且 $m+l=n$。分别比较(72)式两边 y 的多项式的首项系数和常数项得

$$a_n(x)=b_m(x)c_l(x),a_0(x)=b_0(x)c_0(x).\tag{73}$$

已知不可约多项式 $p(x)\mid a_0(x)$,因此 $p(x)\mid b_0(x)$或 $p(x)\mid c_0(x)$。又因为 $p^2(x)\nmid a_0(x)$,所以 $p(x)$不能同时整除 $b_0(x)$和 $c_0(x)$。不妨设 $p(x)\mid b_0(x)$,但是 $p(x)\nmid c_0(x)$。由于 $p(x)\nmid a_n(x)$,因此 $p(x)\nmid b_m(x)$。假设 $b_0(x),b_1(x),\cdots,b_m(x)$中第一个不能被 $p(x)$整除的是 $b_k(x)$,即

$$p(x)\mid b_0(x),\cdots,p(x)\mid b_{k-1}(x),p(x)\nmid b_k(x),0<k\leqslant m.\tag{74}$$

比较(72)式两边 y^k 的系数,得

$$a_k(x)=b_k(x)c_0(x)+b_{k-1}(x)c_1(x)+\cdots+b_0(x)c_k(x).\tag{75}$$

因为 $k\leqslant m<n$,所以 $p(x)\mid a_k(x)$。于是从(74)、(75)式得

$$p(x)\mid b_k(x)c_0(x).\tag{76}$$

由此推出 $p(x)\mid b_k(x)$或 $p(x)\mid c_0(x)$,矛盾。因此 $f_x(y)$在 F 上不可约。 ■

例 24 设 $F=K(x)$,其中 K 是数域,证明:在 $F[y]$中存在任意次数的不可约多项式。

证明 对任意的正整数 n,设

$$f_x(y)=y^n+x.\tag{77}$$

x 是 K 上的不可约多项式,x 符合例 23 的 3 个条件,因此 y^n+x 在 F 上不可约。 ■

例 25 设 $F=K(x)$,其中 K 是数域,设 $f_x(y)$是 $F[y]$中次数 n 大于 0 的本原多项式。证明:$f_x(y)$在 $F[y]$中不可约当且仅当把 $f_x(y)$看成 K 上二元多项式时在 $K[x,y]$中不可约。

证明 必要性。设 $f_x(y)$在 $F[y]$中不可约。假如把 $f_x(y)$看成 K 上二元多项式时在 $K[x,y]$中可约,那么在 $K[x,y]$中 $f_x(y)$可以分解成

$$f_x(y)=g(x,y)h(x,y),\deg g(x,y)<\deg f_x(y),\deg h(x,y)<\deg f_x(y).\tag{78}$$

于是 $g(x,y)$和 $h(x,y)$都不是 K 中的非零数。把它们按照 y 的降幂排列写出,设 $g(x,y)$

中 y 的最高次幂为 m，$h(x,y)$ 中 y 的最高次幂为 l，则 $m+l=n$。假如 m 或 l 中有一个为 0，譬如 $m=0$，则 $g(x,y)=b_0(x)$。于是

$$f_x(y) = b_0(x)h(x,y).$$

由于 $b_0(x)$ 不是 K 中的非零数，因此 $b_0(x)$ 的次数大于 0。于是 $f_x(y)$ 的各项系数的首一最大公因式不等于 1，这与 $f_x(y)$ 是 $F[y]$ 中的本原多项式矛盾。所以 $m\neq 0$。同理，$l\neq 0$，于是 $m<n$ 且 $l<n$。这表明在 $F[y]$ 中 $f_x(y)$ 能分解成两个次数较低的多项式 $g(x,y)$ 与 $h(x,y)$ 的乘积。这与 $f_x(y)$ 在 $F[y]$ 中不可约矛盾。因此，把 $f_x(y)$ 看成 K 上的二元多项式时在 $K[x,y]$ 中不可约。

充分性。设把 $f_x(y)$ 看成 K 上二元多项式时在 $K[x,y]$ 中不可约。假如 $f_x(y)$ 在 $F[y]$ 中可约，则在 $F[y]$ 中 $f_x(y)$ 可分解成

$$f_x(y) = g_x(y)h_x(y),\deg g_x(y) < \deg f_x(y),\deg h_x(y) < \deg f_x(y), \tag{79}$$

其中 $g_x(y)$，$h_x(y)$ 都是系数属于 $K[x]$ 的多项式。记 $\deg g_x(y)=m$，$\deg h_x(y)=l$，由(79)式得，$n=m+l$。由于 $m<n$，且 $l<n$，因此 $m>0$ 且 $l>0$。把 $f_x(y)$，$g_x(y)$，$h_x(y)$ 看成 $K[x,y]$ 中的多项式，则由(79)式得，

$$\deg f_x(y) = \deg g_x(y) + \deg h_x(y). \tag{80}$$

由于在 $K[x,y]$ 中，$\deg g_x(y)\geqslant m>0$，$\deg h_x(y)\geqslant l>0$，因此在 $K[x,y]$ 中，$\deg g_x(y)<\deg f_x(y)$，$\deg h_x(y)<\deg f_x(y)$。这表明在 $K[x,y]$ 中，$f_x(y)$ 分解成了两个次数较低的多项式的乘积，于是 $f_x(y)$ 在 $K[x,y]$ 中可约，矛盾。因此 $f_x(y)$ 在 $F[y]$ 中不可约。 ■

例 26 设 K 是任一数域。证明：在 $K[x,y]$ 中存在任意次数的不可约多项式。

证明 对于任一正整数 n，设 $f(x,y)=y^n+x$。令 $F=K(x)$。在例 24 中已证 y^n+x 在 $F[y]$ 中不可约。显然 y^n+x 是 $F[y]$ 中的本原多项式。于是据例 25 的必要性得，y^n+x 在 $K[x,y]$ 中不可约。 ■

点评 例 26 的结论表明，在数域 K 上的二元多项式环 $K[x,y]$ 中存在任意次数的不可约多项式，即使 K 取复数域时也是这样。而复数域上的一元多项式环 $K[x]$ 中，不可约多项式全都是一次多项式。这显示了二元多项式环与一元多项式环有明显的不同。证明任一数域 K 上的二元多项式环 $K[x,y]$ 中有任意次数的不可约多项式，即使猜测到了对任意正整数 n 有 y^n+x 在 $K[x,y]$ 中不可约，如果想直接证明它是相当麻烦的。我们另辟蹊径：首先把 $f(x,y)$ 按 y 的降幂排列写出，把 $f(x,y)$ 看成系数属于 $K[x]$ 的 y 的多项式，这一步是容易想到的。其次我们把系数所取的范围从 $K[x]$ 扩大到一元有理函数域 $K(x)$，把 $K(x)$ 记作 F；考虑域 F 上的一元多项式环 $F[y]$，然后类比有理数域上的一元多项式环 $\mathbf{Q}[x]$，在 $F[y]$ 中引进本原多项式的概念，证明了类似于 Eisenstein 判别法的结果(即例

23),从而很容易地证明了 y^n+x 在 $F[y]$ 中不可约。最后我们证明对于 $F[y]$ 中的次数大于 0 的本原多项式 $f_x(y)$ 而言,$f_x(y)$ 在 $F[y]$ 中不可约与把 $f_x(y)$ 看成 K 上的二元多项式在 $K[x,y]$ 中不可约是等价的,从而本原多项式 y^n+x 在 $K[x,y]$ 中不可约。

从例 18～例 26,我们看到了有趣的类比关系:

(1)数域 K 上的一元多项式环 $K[x]$ 类比于整数环 $\mathbf{Z}$;

(2)$K[x]$ 中的不可约多项式类比于 $\mathbf{Z}$ 中的素数;

(3)系数属于 $K[x]$ 的 y 的多项式环类比于 $\mathbf{Z}[x]$;

(4)一元分式域 $F=K(x)$ 上的一元多项式环 $F[y]$ 类比于 $\mathbf{Q}[x]$;

(5)$F[y]$ 中的不可约多项式类比于 $\mathbf{Q}[x]$ 中的不可约多项式;

(6)$K[x,y]$ 中的不可约多项式类比于 $\mathbf{Z}[x]$ 中的不可约多项式。

例 27 给出 7.9 节典型例题中例 6 的另一种证法。即证明复数域上的二元二次多项式 $f(x,y)=x^2-2xy+y^2+y$ 是不可约的。

证明 令 $F=\mathbf{C}(y)$,把 $f(x,y)$ 按照 x 的降幂排列写出:$f(x,y)=x^2-2yx+(y^2+y)$,取 y,显然 y 是 $\mathbf{C}[y]$ 中的不可约多项式,且

$$y \mid (y^2+y),\ y \mid (-2y),\ y \nmid 1,\ y^2 \nmid (y^2+y).$$

于是根据例 23 得,$f(x,y)$ 在 $F[x]$ 中不可约。由于 $f(x,y)$ 是 $F[x]$ 中的本原多项式,因此 $f(x,y)$ 在 $\mathbf{C}[x,y]$ 中不可约。 ■

例 28 设 $F=K(x)$,其中 K 是数域。设

$$f_x(y)=a_n(x)y^n+\cdots+a_1(x)y+a_0(x),$$

其中 $a_i(x)\in K[x]$,$i=0,1,\cdots,n$,且 $a_n(x)\neq 0$,$n>0$。令

$$\tilde{f}_x(y)=f_x(y+b(x)),$$

其中 $b(x)\in K[x]$。证明:如果 $\tilde{f}_x(y)$ 在 $F[y]$ 中不可约,那么 $f_x(y)$ 也在 $F[y]$ 中不可约。

证明 假如 $f_x(y)$ 在 $F[y]$ 中可约,则

$$f_x(y)=g_x(y)h_x(y),\deg g_x(y)<\deg f_x(y),\deg h_x(y)<\deg f_x(y), \tag{81}$$

其中 $g_x(y)$,$h_x(y)$ 的系数都属于 $K[x]$,y 用 $y+b(x)$ 代入,由(81)式得

$$f_x(y+b(x))=g_x(y+b(x))h_x(y+b(x)). \tag{82}$$

显然 $\deg f_x(y+b(x))=\deg f_x(y)$,$\deg g_x(y+b(x))=\deg g_x(y)$,$\deg h_x(y+b(x))=\deg h_x(y)$,因此(82)式表明 $\tilde{f}_x(y)$ 在 $F[y]$ 中可约,矛盾。所以 $f_x(y)$ 在 $F[y]$ 中不可约。 ■

点评 例 28 的结论使得有些 $f_x(y)$ 虽然不能直接用例 23 的结论判定它是否不可约,但可以通过把 y 用 $y+b(x)$(适当选取 $b(x)\in K[x]$)代入,再用例 23 的结论证明 $f_x(y+b(x))$ 在 $F[y]$ 中不可约,从而 $f_x(y)$ 在 $F[y]$ 中不可约。

例 29 判断 $\mathbf{R}[x,y]$中的多项式 $f(x,y)=x^2-2xy+y^2-2x-4y+3$ 是否不可约。

解 令 $F=\mathbf{R}(x)$。把 $f(x,y)$按照 y 的降幂排列写出：

$$f(x,y)=y^2-2(x+2)y+(x^2-2x+3)$$

y 用 $y+x+2$ 代入，得

$$\begin{aligned}f(x,y+x+2)&=(y+x+2)^2-2(x+2)(y+x+2)+(x^2-2x+3)\\&=y^2+2(x+2)y+(x+2)^2-2(x+2)y-2(x+2)^2+x^2-2x+3\\&=y^2-(6x+1).\end{aligned}$$

取 $6x+1$，它是 $\mathbf{R}[x]$中的不可约多项式，且满足例 23 的条件，因此 $f(x,y+x+2)$在 $F[y]$中不可约，从而 $f(x,y)$在 $F[y]$中不可约。显然 $f(x,y)$是 $F[y]$中的本原多项式，因此 $f(x,y)$在 $\mathbf{R}[x,y]$中不可约。

点评 例 29 中 y 用 $y+x+2$ 代入，怎么想到取 $b(x)=x+2$ 呢？先把 y 用 $y+b(x)$代入，计算$f(x,y+b(x))$；然后为了容易满足例 23 的条件，让 y 的系数为 0，从而知道应当取 $b(x)=x+2$。

例 30 有一个连的士兵，三三数余 2，五五数余 1，七七数余 4。问：这个连的士兵有多少人？

解 设这个连的士兵有 x 人，则由已知条件得

$$\begin{cases}x\equiv 2 \pmod 3,\\ x\equiv 1 \pmod 5,\\ x\equiv 4 \pmod 7.\end{cases}\tag{83}$$

对于 3 和 $5\times 7=35$ 作辗转相除法：

$$35=11\times 3+2,\qquad 3=1\times 2+1.$$

于是 $$1=3-1\times 2=3-1\times(35-11\times 3)=(-1)\times 35+12\times 3.$$

对于 5 和 $3\times 7=21$ 作辗转相除法：

$$21=4\times 5+1.$$

于是 $$1=21-4\times 5=1\times 21+(-4)\times 5.$$

对于 7 和 $3\times 5=15$ 作辗转相除法：

$$15=2\times 7+1.$$

于是 $$1=15-2\times 7=1\times 15+(-2)\times 7.$$

令

$$c=2\times(-1)\times 35+1\times 1\times 21+4\times 1\times 15=11.$$

因此同余方程组(83)的全部解是

$$11+(3\times5\times7)k,k\in\mathbf{Z}.$$

一个连的士兵大约是一百多人,因此取 $k=1$,得 116。即这个连的士兵有 116 人。

例 31 设 m_1、m_2 是互素的正整数,b 是任一整数。证明:

$$\begin{cases}a\equiv b & (\mathrm{mod}\ m_1)\\ a\equiv b & (\mathrm{mod}\ m_2)\end{cases}$$

当且仅当

$$a\equiv b \quad (\mathrm{mod}\ m_1m_2).$$

证明 必要性。由已知条件得,a 是同余方程组

$$\begin{cases}x\equiv b & (\mathrm{mod}\ m_1)\\ x\equiv b & (\mathrm{mod}\ m_2)\end{cases} \tag{84}$$

的一个解,显然 b 也是同余方程组(84)的一个解,因此根据中国剩余定理得,$a\equiv b\ (\mathrm{mod}\ m_1m_2)$。

充分性是显然的。 ■

例 32 在 $\mathbf{Z}_{91}$ 中,求 $\overline{1}$ 的平方根。

解 $91=7\times13$。由于 7 和 13 是素数,因此 $\mathbf{Z}_7$,$\mathbf{Z}_{13}$ 都是域。从而在 $\mathbf{Z}_7$(或 $\mathbf{Z}_{13}$)中,$\overline{1}$ 的平方根有且只有两个:$\overline{1}$,$-\overline{1}$。在 $\mathbf{Z}_{91}$ 中,设 $\overline{a}$ 是 $\overline{1}$ 的平方根,则

$$\begin{aligned}
\overline{a}^2=\overline{1} &\Leftrightarrow \overline{a^2}=\overline{1}\\
&\Leftrightarrow a^2\equiv1 \quad (\mathrm{mod}\ 91)\\
&\Leftrightarrow \begin{cases}a^2\equiv1 & (\mathrm{mod}\ 7)\\ a^2\equiv1 & (\mathrm{mod}\ 13)\end{cases}\\
&\Leftrightarrow \begin{cases}a\equiv\pm1 & (\mathrm{mod}\ 7)\\ a\equiv\pm1 & (\mathrm{mod}\ 13)\end{cases}\\
&\Leftrightarrow \begin{cases}a\equiv1 & (\mathrm{mod}\ 7)\\ a\equiv1 & (\mathrm{mod}\ 13)\end{cases} \text{ 或 } \begin{cases}a\equiv1 & (\mathrm{mod}\ 7)\\ a\equiv-1 & (\mathrm{mod}\ 13)\end{cases}\\
&\Leftrightarrow \begin{cases}a\equiv-1 & (\mathrm{mod}\ 7)\\ a\equiv1 & (\mathrm{mod}\ 13)\end{cases} \text{ 或 } \begin{cases}a\equiv-1 & (\mathrm{mod}\ 7)\\ a\equiv-1 & (\mathrm{mod}\ 13).\end{cases}
\end{aligned}$$

由于 $13=1\times7+6$,$7=1\times6+1$,因此

$$1=7-1\times6=7-1\times(13-1\times7)=(-1)\times13+2\times7.$$

于是

$$\begin{aligned}
a&=\pm1\times(-1)\times13\pm1\times2\times7+91k\\
&=\mp13\pm14+91k
\end{aligned}$$

从而 $\bar{a}=\bar{1}$ 或 $\overline{-27}$ 或 $\overline{27}$ 或 $\overline{-1}$，即在 $\mathbf{Z}_{91}$ 中，$\bar{1}$ 的平方根有且只有下列 4 个：

$$\bar{1},\quad \overline{64},\quad \overline{27},\quad \overline{90}.$$

也就是 $\pm\bar{1},\pm\overline{27}$。

点评 在公开密钥密码学中，选取两个大的素数 p 和 q，它们不相等，令 $n=pq$，需要在 $\mathbf{Z}_n$ 中考虑一个元素 $\bar{a}$ 有没有平方根，如果有，要把它的全部平方根求出来。运用例 31 的结论，类似于例 32 的方法可以做这件事情。

习题 7.12

1. 验证 $K(x)$ 中加法、乘法分别满足交换律和结合律，还满足乘法对于加法的分配律。

2. 在 $\mathbf{R}(x)$ 中把下述真分式表示成部分分式的和：

$$\frac{x^3+x-1}{x^4-3x^3+4x^2-3x+1}.$$

3. 下列模 m 剩余类环中，哪些是域？哪些不是域？写出其中的可逆元，并且求出每个可逆元的逆元：

$$\mathbf{Z}_5,\mathbf{Z}_{10},\mathbf{Z}_{12},\mathbf{Z}_{17}.$$

4. 令

$$F=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\middle| a,b\in\mathbf{R}\right\}.$$

证明：F 对于矩阵的加法与乘法成为一个域，并且域 F 与复数域同构。

5. 求小于 7 的自然数 x，使得 $x\equiv 2007^7 \pmod 7$。

6. 设 $f(x)=x^5-x^2+1\in\mathbf{Z}[x]$，判断 $f(x)$ 在 $\mathbf{Q}$ 上是否不可约。

7. 设 $f(x)=x^4-5x+1\in\mathbf{Z}[x]$，判断 $f(x)$ 在 $\mathbf{Q}$ 上是否不可约。

8. 设 $f(x)=11x^3+4x^2+10x+34\in\mathbf{Z}[x]$，判断 $f(x)$ 在 $\mathbf{Q}$ 上是否不可约。

9. 设 $f(x)=x^4+3x^3+3x^2-5\in\mathbf{Z}[x]$，判断 $f(x)$ 在 $\mathbf{Q}$ 上是否不可约。

10. $\mathbf{Z}_3[x]$ 中，$f(x)=\bar{2}x^5-x^4+\bar{2}x^2+x-\bar{2}$，求一个次数小于 3 的多项式 $g(x)$，使得 $f=g$。

11. 设 $F=K(x)$，其中 K 是数域，设 $f_x(y)$ 是 $F[y]$ 中次数 n 大于 0 且系数属于 $K[x]$ 的多项式。证明：如果把 $f_x(y)$ 看成 K 上二元多项式时在 $K[x,y]$ 中不可约，那么 $f_x(y)$ 在 $F[y]$ 中不可约。

12. 第 11 题的逆命题成立吗？即如果 $f_x(y)$ 在 $F[y]$ 中不可约，那么把 $f_x(y)$ 看成 K

上二元多项式时在 $K[x,y]$ 中一定不可约吗?

13. 设 K 是数域,判断 $f(x,y)=x^2+xy+y^3-y$ 在 $K[x,y]$ 中是否不可约。

14. 判断 $f(x,y)=y^2-x^3+x-1$ 在 $\mathbf{R}[x,y]$ 中是否不可约。

15. 判断 $f(x,y)=x^2-4xy+2y^2-6x+8y-5$ 在 $\mathbf{R}[x,y]$ 中是否不可约。

16. 有一个连的士兵,三三数余 1,五五数余 2,七七数余 1。问:这个连的士兵有多少人?

17. 在 $\mathbf{Z}_{143}$ 中,分别求 $\overline{1}$ 的平方根和 $\overline{3}$ 的平方根。

18. 在 $\mathbf{Z}_{143}$ 中,$\overline{2}$ 的平方根存在吗?

19. 设 $f(x)=x^5+20x+16\in\mathbf{Z}[x]$,判断 $f(x)$ 在 $\mathbf{Q}$ 上是否不可约。

20. 证明对于 Möbius 函数 $\mu(n)$ 有

$$\sum_{d|n}\mu(d)=\begin{cases}1,\text{当 } n=1;\\0,\text{当 } n>1.\end{cases}$$

21. 证明 Möbius 反演定理:设 $f(n)$ 和 $g(n)$ 是 $\mathbf{N}^*$ 到 $\mathbf{Z}$ 的两个函数,则

$$g(n)=\sum_{d|n}f(d)\Leftrightarrow f(n)=\sum_{d|n}\mu(d)g\left(\frac{n}{d}\right).$$

22. 分别求 q 元有限域 F 上的二次和三次首一不可约多项式的个数。

23. 分别求 $\mathbf{Z}_2$ 和 $\mathbf{Z}_3$ 上的二次和三次首一不可约多项式的个数。

补 充 题 七

1. 设 F 是一个域,证明:在域 F 上的一元多项式环 $F[x]$ 中,有带余除法。

2. 设 F 是一个域,证明:在 $F[x]$ 中整除关系具有反身性和传递性。

3. 设 F 是一个域,证明:在 $F[x]$ 中如果 $g(x)\mid f_i(x)$,$i=1,2,\cdots,s$,那么对于任意 $u_i(x)\in F[x]$,$i=1,2,\cdots,s$,都有

$$g(x)\mid u_1(x)f_1(x)+u_2(x)f_2(x)+\cdots+u_s(x)f_s(x).$$

4. 设 F 是一个域,证明:在 $F[x]$ 中,$f(x)$ 与 $g(x)$ 相伴的充分必要条件是存在 F 中的非零元 c 使得 $f(x)=c\,g(x)$。

5. 设 F 是一个域,证明:在 $F[x]$ 中,对于任意两个多项式 $f(x)$ 与 $g(x)$,存在它们的一个最大公因式 $d(x)$,并且 $d(x)$ 可以表示成 $f(x)$ 与 $g(x)$ 的倍式和,即 $F[x]$ 中有多项式 $u(x)$,$v(x)$,使得

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

6. 设 F 是一个域,证明:在 $F[x]$ 中,两个多项式 $f(x)$ 与 $g(x)$ 互素的充分必要条件是

在 $F[x]$中存在多项式 $u(x),v(x)$,使得

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

7. 设 F 是一个域,证明:在 $F[x]$中如果 $f(x)\mid g(x)h(x)$,且$(f(x),g(x))=1$,那么 $f(x)\mid h(x)$。

8. 设 F 是一个域,证明:在 $F[x]$中,如果

$$f(x)\mid h(x),g(x)\mid h(x),(f(x),g(x))=1,$$

那么 $f(x)g(x)\mid h(x)$。

9. 设 F 是一个域,证明:在 $F[x]$中,如果

$$(f(x),h(x))=1,(g(x),h(x))=1,$$

那么$(f(x)g(x),h(x))=1$。

10. 设 F 是一个域,$F[x]$中一个次数大于 0 的多项式 $p(x)$如果在 $F[x]$中的因式只有零次多项式和 $p(x)$的相伴元,那么称 $p(x)$在 F 上是**不可约**的;否则称它为**可约**的。证明下列命题等价:

(1) $p(x)$在 F 上是不可约的;

(2) $p(x)$与 $F[x]$中任一多项式 $f(x)$的关系只有两种可能:$p(x)\mid f(x)$,或$(p(x),f(x))=1$;

(3) 在 $F[x]$中如果 $p(x)\mid f(x)g(x)$,那么 $p(x)\mid f(x)$或者 $p(x)\mid g(x)$;

(4) $p(x)$在 $F[x]$中不能分解成两个次数较 $p(x)$的次数低的多项式的乘积。

11. 设 F 是一个域,证明:在 $F[x]$中有唯一因式分解定理。

12. 设 F 是一个域,L 也是一个域,且 $L\supseteq F$。证明:对于 $F[x]$中两个多项式 $f(x)$与$g(x)$,有

(1) 在 $F[x]$中 $g(x)\mid f(x)$当且仅当在 $L[x]$中 $g(x)\mid f(x)$;

(2) $f(x)$和 $g(x)$在 $F[x]$中的首项系数为 1 的最大公因式与它们在 $L[x]$中的首项系数为 1 的最大公因式相等;

(3) $f(x)$与 $g(x)$在 $F[x]$中互素当且仅当 $f(x)$与 $g(x)$在 $L[x]$中互素。

即整除性,首一最大公因式和互素性不随域的扩大而改变。

13. 设 F 是一个域,$f(x)$是 $F[x]$中的 n 次多项式:

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0.$$

证明:(1) 如果 char $F\nmid n$,那么 $f'(x)$是 $n-1$ 次多项式;

(2) 如果 char $F\mid n$,那么 $f'(x)$的次数小于 $n-1$。

14. 设 F 是一个域,不可约多项式 $p(x)$是 $f(x)$的一个 k 重因式($k\geqslant 1$)。证明:

(1) 如果 char $F=0$,那么 $p(x)$是 $f'(x)$的 $k-1$ 重因式,特别地,$f(x)$的单因式不是

$f'(x)$的因式；

(2) 如果 char $F\neq 0$，那么 $p(x)$是 $f'(x)$的至少 $k-1$ 重因式。其中当 char $F\nmid k$ 且$p'(x)\neq 0$时，$p(x)$是 $f'(x)$的 $k-1$ 重因式；当 char $F\mid k$ 或 $p'(x)=0$ 时，$p(x)$是 $f'(x)$的至少 k 重因式。

15. 设 F 是一个域，证明：在 $F[x]$中，一个次数大于 0 的多项式 $f(x)$如果满足

$$(f(x),f'(x))=1,$$

那么 $f(x)$没有重因式。

16. 设 F 是特征为 0 的域，证明：在 $F[x]$中一个次数大于 0 的多项式 $f(x)$如果没有重因式，那么

$$(f(x),f'(x))=1.$$

17. 设 F 是特征不等于 0 的域，证明：在 $F[x]$中一个次数大于 0 的多项式 $f(x)$如果没有重因式，那么$(f(x),f'(x))=1$ 或者 $f(x)$有一个单因式 $p(x)$使得 $p'(x)=0$。

18. 设域 F 的特征为素数 p，举一个例子说明：在 $F[x]$中次数大于 0 的多项式 $f(x)$没有重因式，但是 $f(x)$与 $f'(x)$不互素。

19. 设 F 是一个域，证明：在 $F[x]$中，用一次多项式 $x-a$ 去除 $f(x)$，所得的余式是 F 中一个元素 $f(a)$。

20. 设 F 是一个域，$f(x)\in F[x]$。证明：在 $F[x]$中 $x-a$ 整除 $f(x)$当且仅当 a 是 $f(x)$在 F 中的根。

21. 设 F 是一个域，证明：$F[x]$中的 $n(n\geqslant 0)$次多项式 $f(x)$在 F 中至多有 n 个根(重根按重数计算)。

22. 设 L 是一个域，证明：在 7.12 节的典型例题中把数域 K 换成域 L 后，例 18～例 26 的结论仍然成立。

23. 设 F 是一个域，证明：F 上的 n 元多项式环 $F[x_1,x_2,\cdots,x_n]$是无零因子环，从而消去律成立。

24. 设 F 是一个域，证明：在 $F[x_1,x_2,\cdots,x_n]$中，有

$$\deg fg=\deg f+\deg g.$$

25. 设 F 是一个域，证明：$F[x_1,x_2,\cdots,x_n]$也有通用性质，即设 R 是一个有单位元的交换环，且 R 可以看成 F 的一个扩环(即 F 与 R 的一个子环 R_1 同构，且 R 的单位元是 R_1 的单位元)，则不定元 $x_1,x_2,\cdots,x_n$ 可以用 R 中的任意 n 个元素 $t_1,t_2,\cdots,t_n$ 代入，并且这种代入保持加法运算和乘法运算。

26. 设 F 是一个域，$F[x_1,x_2,\cdots,x_n]$中每一个 n 元多项式 $f(x_1,x_2,\cdots,x_n)$诱导了 F^n 到 F 的一个映射 f：

$$f: F^n \longrightarrow F$$
$$(c_1, c_2, \cdots, c_n) \longmapsto f(c_1, c_2, \cdots, c_n).$$

称 f 是域 F 上的 n 元多项式函数。举例说明，$\mathbf{Z}_p$ 上的两个 n 元多项式不相等，但是它们诱导的 n 元多项式函数相等。

27. 设 p 是素数，在 $\mathbf{Z}_p[x_1, x_2, \cdots, x_n]$ 中，用 S 表示由每个单项式中每个不定元的次数小于 p 的多项式组成的集合。证明：如果 $h(x_1, x_2, \cdots, x_n)$ 是 S 中的非零多项式，那么它诱导的 n 元多项式函数 h 不是零函数。

28. 证明：$\mathbf{Z}_2$ 上的每一个 n 元函数（即 $\mathbf{Z}_2^n$ 到 $\mathbf{Z}_2$ 的一个映射）都是 $\mathbf{Z}_2$ 上的 n 元多项式函数，且 $\mathbf{Z}_2$ 上的每一个 n 元函数都可以唯一地表示成 $\mathbf{Z}_2$ 上每个变量的次数都小于 2 的 n 元多项式函数。

29. 设 F 是一个域，在 $F[x_1, x_2, \cdots, x_n]$ 中与数域 K 上的 n 元多项式环 $K[x_1, x_2, \cdots, x_n]$ 一样，有整除的概念，因式和倍式的概念，相伴的概念，最大公因式的概念，不可约多项式的概念。证明：在 $F[x_1, x_2, \cdots, x_n]$ 中，一个次数大于 0 的多项式 $p(x_1, x_2, \cdots, x_n)$ 不可约当且仅当它不能分解成两个次数较低的多项式的乘积。

30. 设 F 是一个域，证明：在 $F[x_1, x_2, \cdots, x_n]$ 中有唯一因式分解定理。

31. 设 F 是一个域，仿照 7.12 节数域 K 上一元分式域的构造方法，可以构造出域 F 上的一元分式域，记作 $F(x)$，它的元素记作 $\dfrac{f(x)}{g(x)}$，其中 $f(x), g(x) \in F[x]$，且 $g(x) \neq 0$。证明：如果 $\operatorname{char} F = p$（$p$ 是素数），那么 $F(x)$ 是一个特征为 p 的无限域。

32. 设 F 是一个域，类似于 F 上一元分式域的构造方法可构造出域 F 上的 n 元分式域，记作 $F(x_1, x_2, \cdots, x_n)$，它的元素记作 $\dfrac{f(x_1, x_2, \cdots, x_n)}{g(x_1, x_2, \cdots, x_n)}$，其中 $f(x_1, x_2, \cdots, x_n)$，$g(x_1, x_2, \cdots, x_n) \in F[x_1, x_2, \cdots, x_n]$，且 $g(x_1, x_2, \cdots, x_n) \neq 0$。证明：如果 $\operatorname{char} F = p$（$p$ 是素数），那么 $F(x_1, x_2, \cdots, x_n)$ 是一个特征为 p 的无限域。

33. 设 K 是一个数域，$L = K(x_1, \cdots, x_{n-2})$，$F = L(x_{n-1})$，设 $f(x_1, \cdots, x_{n-1}, y) = y^m + x_1 x_2 \cdots x_{n-1}$，其中 m 是任一正整数，证明：$f(x_1, \cdots, x_{n-1}, y)$ 在 $F[y]$ 中不可约。

34. 设 K 是一个数域，证明：在 $K[x_1, x_2, \cdots, x_{n-1}, x_n]$ 中存在任意次数的不可约多项式。