第五章 多项式

第1章 多项式

§1 数域

例1 限定在整数Z范围内，我们可以作加法，减法，乘法. 但不可以作除法，这是因为两个整数的商不一定是整数.

例2 限定在有理数Q，实数域R或复数域C内只要除数不为零，除法总是可以做的.

对于全体有理数Q，全体实数R，全体复数C，它们显然具有一些不同的性质．但它们也有很多共同的性质，在代数学中经常将有共同性质的对象统一进行讨论.

关于数的加、减、乘、除等运算的性质通常称为**代数性质**.

代数学所研究的问题主要涉及数的代数性质，而这方面的大部分性质是有理数、实数和复数所共有的.

为了方便起见，当我们把这些数当作整体来考虑的时候，常称它围一个数的集合，简称**数集**．有些数集也具有与有理数、实数、复数的全体所共有的代数性质，为了在讨论中能够把它们统一起来，我们引入一个一般的概念.

定义1 设 P 是由一些复数组成的集合，其中包括0和1．如果P中任意两个数（这两个数可以相同）的和、差、积、商（除数不为0）仍然是P中的数，那么P就称为一个**数域**.

如果数集 P 中任意两个数做某一运算的结果都仍在P中，称数集P对这种运算是**封闭的**.

思考 定义1中的前提"包括0与1"是否需要?

只要P非空，就不需要，则任取$a \in P$,

$$a - a = 0, \frac{a}{a} = 1$$

又因为P对减法和除法封闭，所以我们自然就有

$$0, 1 \in P.$$

例1 有理数集Q，实数集R，复数集C都是数域.
整数集Z不是数域.

例2 所有就有形式

$$a+b\sqrt{2}$$

的数（其中a，b是任何有理数），构成一个数域. 通常记为

$$Q(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in Q\}.$$

显然，$Q(\sqrt{2})$非空，且它对加法，减法是封闭的.
下面证明它对乘法和除法也是封闭的.

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

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

若 $a+b\sqrt{2} \neq 0$, 则 $a-b\sqrt{2} \neq 0$, 故

$$\frac{c+d\sqrt{2}}{a+b\sqrt{2}}=\frac{(c+d\sqrt{2})(a-b\sqrt{2})}{(a+b\sqrt{2})(a-b\sqrt{2})}$$

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

$$\because a,b,c,d \in P, \therefore \frac{ac-bd}{a^2-2b^2}, \frac{ad-bc}{a^2-2b^2} \in P$$

例3 所有可以表成

$$\frac{a_0 + a_1\pi + \cdots + a_n\pi^n}{b_0 + b_1\pi + \cdots + b_m\pi^m}$$

的数组成一数域，其中n, m为任意非负整数，a_i, b_j $(i = 0, 1, \cdots, n\ ; j = 0, 1, \cdots, m)$ 是整数.

上页 下页 返回 结束

命题 所有的数域包含有理数作为它的一部分. 也就是说，有理数域是最小的数域.

证明： 设P为任一数域，故$1 \in P$, 又因为P对加法封闭，所以

$$n = \underbrace{1 + 1 + \cdots + 1}_{n\text{个}1} \in P,$$

即数域P包含所有的正整数. 又因为$0 \in P$, 所以

$$-n = 0 - n \in P.$$

即数域P包含了所有的整数.

数域P对除法封闭，故任一分数$\frac{m}{n} \in P$. 于是，$Q \subset P$.

§2 一元多项式

定义2 设n是一非负整数. 形如表达式

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

其中$a_0, a_1, \cdots, a_n$全属于数域P，称为**系数在数域*P*中的的一元多项式**，或者简称为**数域*P*上的一元多项式.**

$a_i x^i$ 称为i次项，a_i 称为i次项的系数.

今后，常用$f(x), g(x), \cdots$ 或$f, g, \cdots$ 等来代表多项式.

上页 下页 返回 结束

定义3 如果在多项式 $f(x)$ 与 $g(x)$ 中，除去系数为零的项外，同次项的系数全相等，那么 $f(x)$ 与 $g(x)$ 就称为**相等**，记为

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

系数全为零的多项式称为**零多项式**，记为0.

对于多项式

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

如果 $a_n \neq 0,$ 那么 $a_n x^n$ 就称为该多项式的**首项**，a_n 成为首项系数，n 称为多项式的**次数**. 零多项式是唯一不定义次数的多项式. 多项式的次数记为

$$\partial(f(x)).$$

即一个多项式的次数最高项的次数称为该多项式的次数.

我们可以引入两个多项式的加法，减法和乘法.

例如：

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

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

$$=2x^4-2x^3+x^2+x-1.$$

设

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

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0$$

是数域 P 上的两个多项式. 那么可以写成

$$f(x)=\sum_{i=0}^{n}a_ix^i,$$

$$g(x)=\sum_{j=0}^{m}b_jx^j.$$

在表示多项式 $f(x)$ 与 $g(x)$ 的和时，如 $n \geq m$，为了方便起见，在 $g(x)$ 中令 $b_n = b_{n-1} = \cdots = b_{m+1} = 0$. 那么 $f(x)$ 与 $g(x)$ 的和为

$$f(x) + g(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

$$= \sum_{i=0}^{n} (a_i + b_i)x^i .$$

而 $f(x)$与$g(x)$的乘积为

$$f(x)\cdot g(x)=a_nb_mx^{n+m}+(a_nb_{m-1}+a_{m-1}b_n)x^{n+m-1}$$

$$+\cdots+(a_1b_0+a_0b_1)x+a_0b_0$$

其中s 次项的系数是

$$a_sb_0+a_{s-1}b_1+\cdots+a_1b_{s-1}+a_0b_s=\sum_{i+j=s}a_ib_j.$$

故

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

显然，数域P上的两个多项式经过加、减、乘等运算后，所得结果仍然是数域P上的多项式.

关于多项式运算结果的次数

(1) $\partial(f(x) \pm g(x)) \le \max(\partial(f(x)), \partial(g(x))).$

(2) 若 $f(x) \ne 0, g(x) \ne 0$，那么 $f(x)g(x) \ne 0$，且

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

事实上，设

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

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0,$$

其中 $a_n \ne 0, b_m \ne 0$，于是 $f(x)g(x)$ 的首项是 $a_n b_m x^{n+m}$.

显然 $a_n b_m \ne 0$，因此 $f(x)g(x) \ne 0$ 且它的次数为 $n+m$.

运算规律

1.加法交换律

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

2.加法结合律

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

3.乘法交换律

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

4.乘法结合律

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

5.乘法对加法的分配律

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

6. 乘法消去律

如果 $f(x)g(x)=f(x)h(x)$ 且 $f(x)\neq 0$，则

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

定义4 所有系数在数域P中的一元多项式的全体，称为数域P上的**一元多项式环**，记为$P[x]$，P称为$P[x]$的**系数域**.

§3 整除的概念

设

$$f(x) = 3x^2 + 4x^2 - 5x + 6,$$

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

除式　　**被除式**

$$\begin{array}{r|r|l} \boxed{x^2 - 3x + 1} & \boxed{3x^2 + 4x^2 - 5x + 6} & \boxed{3x + 13} \\ & 3x^3 - 9x^2 + 3x & \\ \cline{2-2} & 13x^2 - 8x + 6 & \\ & 13x^2 - 39x + 13 & \\ \cline{2-2} & \boxed{31x - 7} & \end{array}$$

商

余式

$$3x^3 + 4x^2 - 5x + 6 = (3x + 13)(x^2 - 3x + 1) + (31x - 7).$$

带余除法

对于$P[x]$中任意两个多项式$f(x)$与$g(x)$，其中$g(x)\neq 0$，则必存在$P[x]$中的多项式$q(x)$，$r(x)$，使得

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

成立，其中$\partial(r(x))<\partial(g(x))$或者$r(x)=0$，并且这样的$q(x)$, $r(x)$是唯一决定的.

证明： $q(x)$和$r(x)$的存在性可以由上面所说的除法直接得出. 下面将用归纳法给出证明.

如果 $f(x)=0$. 取$q(x)=r(x)=0$即可.

以下设 $f(x)\neq 0$. 令$f(x)$, $g(x)$的次数分别为n, m. 对$f(x)$的次数n作（第二）数学归纳法.

当$n<m$时，显然取$q(x)=0$, $r(x)=f(x)$, (1)式成立.

$$\boxed{f(x)=0\,g(x)+f(x)}$$

下面讨论$n\geq m$ 的情形.

假设当次数小于n时，$q(x), r(x)$的存在已证.

现来看次数为n的情形.

令ax^n, bx^m 分别是$f(x), g(x)$的首项,显然

$b^{-1}ax^{n-m}g(x)$与$f(x)$有相同的首项，因而多项式

$$f_1(x) = f(x) - b^{-1}ax^{n-m}g(x)$$

的次数$\boxed{小于n}$或为0.

对于后者，取$q(x) = b^{-1}ax^{n-m}, r(x) = 0$

对于前者，由归纳法假设，对$f_1(x), g(x)$ 有$q_1(x)$,

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

其中$\partial(r_1(x)) < \partial(g(x))$ 或者$r_1(x) = 0$.

上页 下页 返回 结束

于是

$$f(x)=(q_1(x)+b^{-1}ax^{n-m})g(x)+r_1(x),$$

也就是说，有 $q(x)=q_1(x)+b^{-1}ax^{n-m}, r(x)=r_1(x)$ 使

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

成立. 由归纳法原理，对任意的 $f(x), g(x)\neq 0, q(x),$ $r(x)$ 的存在性就证明了.

下面来证明唯一性. 设 $q'(x), r'(x)$ 使

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

其中 $\partial(r(x))<\partial(g(x))$ 或者 $r(x)=0$，于是

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

即

$$(q'(x)-q(x))g(x)=r'(x)-r(x).$$

如果 $q'(x)\neq q(x)$, 又据假设 $g(x)\neq 0$, 则

$$r'(x)-r(x)\neq 0,$$

且有

$$\partial(q'(x)-q(x))+\partial(g(x))=\partial(r'(x)-r(x)).$$

但是

$$\partial(g(x))>\partial(r'(x)-r(x)),$$

所有上式不可能成立. 这就证明了 $q'(x)=q(x)$, 同时 $r'(x)=r(x)$.

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

被除式　商　除式　余式

定义5

数域 P 上的多项式 $g(x)$ 称为**整除** $f(x)$，如果有数域 P 上的多项式 $h(x)$ 使等式

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

成立．用“$g(x)\mid f(x)$”表示 $g(x)$ 整除 $f(x)$．用“$g(x)\nmid f(x)$”表示 $g(x)$ 不能整除 $f(x)$．

定理1

对于数域P上的任意两个多项式$f(x), g(x)$，其中 $g(x)\neq 0$, $g(x)|f(x)$的充要条件为$g(x)$除$f(x)$的余式$r(x)$为零.

证明：（略）.

注

带余除法中g(x)必须不为零. 但$g(x)|f(x)$中，g(x)可以为零. 此时

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

当$g(x)|f(x)$时，如$g(x)\neq 0$，$g(x)$除$f(x)$所得的商$q(x)$有时也用

$$\frac{f(x)}{g(x)}$$

来表示.

注1 任一个多项式$f(x)$一定整除它自身. 因为

$$f(x)=1\cdot f(x).$$

注2 任一个多项式$f(x)$一定整除零多项式. 因为

$$0=0\cdot f(x).$$

注3 零次多项式，即非零常数一定能任一多项式，因为$f(x)=a(a^{-1}f(x)).$

整除性的常用性质：

(1) $f(x) \mid g(x), g(x) \mid f(x) \Rightarrow f(x) = cg(x),$

其中c 为非零常数.

证明：

$$\left.\begin{array}{l} f(x) \mid g(x) \Rightarrow g(x) = h_1(x) f(x) \\ g(x) \mid f(x) \Rightarrow f(x) = h_2(x) g(x) \end{array}\right\} \Rightarrow$$

$$f(x) = h_1(x) h_2(x) f(x) \Rightarrow h_1(x) h_2(x) = 1 \Rightarrow$$

$$\partial(h_1(x)) + \partial(h_2(x)) = 0 \Rightarrow \partial(h_1(x)) = \partial(h_2(x)) = 0 \Rightarrow$$

$h_2(x)$ 为一非零常数

（2）整除的传递性

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

证明：

$$\left.\begin{array}{l} f(x) \mid g(x) \Rightarrow g(x) = h_1(x) f(x) \\ g(x) \mid h(x) \Rightarrow h(x) = h_2(x) g(x) \end{array}\right\} \Rightarrow$$

$$h(x) = h_1(x) h_2(x) f(x)$$

(3) $f(x)\mid g_i(x), i=1,2,\cdots,r \Rightarrow$

$$f(x)\mid u_1(x)g_1(x)+u_2(x)g_2(x)+\cdots+u_r(x)g_r(x),$$

其中 $u_i(x)$ 为数域 P 上任意的多项式.

证明:

$$f(x)\mid g_i(x) \Rightarrow g_i(x)=h_i(x)f(x) \Rightarrow$$

$$u_1(x)g_1(x)+u_2(x)g_2(x)+\cdots+u_r(x)g_r(x)$$

$$=u_1(x)h_1(x)f(x)+\cdots+u_r(x)h_r(x)f(x)$$

$$=[u_1(x)h_1(x)+\cdots+u_r(x)h_r(x)]f(x)$$

$$\Rightarrow\ f(x)\mid u_1(x)g_1(x)+u_2(x)g_2(x)+\cdots+u_r(x)g_r(x),$$

注1 $f(x)$与$cf(x)$（c为非零常数）有着相同的因式，也有相同的倍式.

注2 两个多项式之间的整除关系不因为系数域的扩大而改变．也就是说：

设$f(x), g(x)$为$P[x]$中两个多项式，$\bar{P}$ 为包含P的一个较大的数域，则$f(x), g(x)$在$\bar{P}[x]$ 中与在$P[x]$中有着相同的整除关系.

注3 $u_1(x)g_1(x)+u_2(x)g_2(x)+\cdots+u_r(x)g_r(x)$称为 $g_1(x), g_2(x), \cdots, g_r(x)$ 的一个**组合**.

§4 最大公因式

定义6

设 $f(x), g(x)$是$P[x]$中两个多项式，$P[x]$中多项式 $d(x)$称为$f(x), g(x)$的一个**最大公因式**，如果它满足下面两个条件：

（1）$d(x)|f(x), d(x)|g(x)$；

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

类似地，可以定义两个多项式 $f(x)$ 与 $g(x)$ 的**最小公倍式** $m(x)$:

（1）$f(x) \mid m(x), f(x) \mid m(x)$;

（2）若 $f(x) \mid h(x), g(x) \mid h(x)$，则 $m(x) \mid h(x)$.

记 $f(x)$ 与 $g(x)$ 的首项系数为1的最小公倍式为

$$[f(x), g(x)].$$

例1 若 $f(x) \mid g(x)$，则 $(f(x), g(x)) = f(x)$.

引理　如果有等式

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

成立，那么$f(x)$, $g(x)$和$g(x)$, $r(x)$有相同的公因式.

证明:

$$\left.\begin{array}{l}\varphi(x)\mid g(x),\varphi(x)\mid r(x)\\ f(x)=q(x)g(x)+r(x)\end{array}\right\}\Rightarrow \varphi(x)\mid f(x)$$

即$g(x)$, $r(x)$的公因式是$f(x)$, $g(x)$的公因式.

$$\left.\begin{array}{l}\varphi(x)\mid f(x),\varphi(x)\mid g(x)\\ r(x)=f(x)-q(x)g(x)\end{array}\right\}\Rightarrow \varphi(x)\mid r(x)$$

即$f(x)$, $g(x)$的公因式是$g(x)$, $r(x)$的公因式.

定理2

对于$P[x]$中任意两个多项式$f(x), g(x)$，在$P[x]$中存在一个最大公因式$d(x)$，且$d(x)$可以表成$f(x), g(x)$的一个组合，即有$P[x]$中多项式$u(x), v(x)$使

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

证明：

如果$f(x), g(x)$有一个为零，不妨设$g(x)=0$，则$f(x)$本身就是最大公因式，且

$$f(x) = 1 \cdot f(x) + 1 \cdot 0.$$

下面来看一般的情形．不妨设 $g(x)\neq 0$.

按带余除法，用 $g(x)$ 除 $f(x)$，得到商 $q_1(x)$，余式 $r_1(x)$

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

如果 $r_1(x)\neq 0$，就再用 $r_1(x)$ 除 $g(x)$，得到商 $q_2(x)$，余式 $r_2(x)$

$$g(x)=q_2(x)r_1(x)+r_2(x),$$

如果 $r_2(x)\neq 0$，就再用 $r_2(x)$ 除 $r_1(x)$，得到商 $q_3(x)$，余式 $r_3(x)$

$$r_1(x)=q_3(x)r_2(x)+r_3(x),$$

如此辗转相除下去，显然，所得余式的次数不断降低，即

$$\partial(g(x)) > \partial(r_1(x)) > \partial(r_2(x)) > \cdots$$

因此在有限次之后，必然有余式为零．于是我们有一串等式：

$$f(x) = q_1(x)g(x) + r_1(x),$$
$$g(x) = q_2(x)r_1(x) + r_2(x),$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$r_{i-2}(x) = q_i(x)r_{i-1}(x) + r_i(x),$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$r_{s-3}(x) = q_{s-1}(x)r_{s-2}(x) + r_{s-1}(x),$$
$$r_{s-2}(x) = q_s(x)r_{s-1}(x) + r_s(x),$$
$$r_{s-1}(x) = q_{s+1}(x)r_s(x) + 0,$$

上页 下页 返回 结束

$r_s(x)$ 与0的最大公因式是 $r_s(x)$
$r_{s-1}(x) = q_{s+1}(x) r_s(x) + 0$ $\Bigg\} \Longrightarrow$

$r_s(x)$ 与 $r_{s-1}(x)$ 的最大公因式是 $r_s(x)$
$r_{s-2}(x) = q_s(x) r_{s-1}(x) + r_s(x)$ $\Bigg\} \Longrightarrow$

$r_{s-1}(x)$ 与 $r_{s-2}(x)$ 的最大公因式是 $r_s(x)$
$r_{s-3}(x) = q_{s-1}(x) r_{s-2}(x) + r_{s-1}(x)$ $\Bigg\} \Longrightarrow$

$r_{s-2}(x)$ 与 $r_{s-3}(x)$ 的最大公因式是 $r_s(x) \Longrightarrow \cdots$

$\Longrightarrow$ $f(x)$与$g(x)$的最大公因式是 $r_s(x)$

$$r_{s-2}(x) = q_s(x) r_{s-1}(x) + r_s(x) \Rightarrow$$

$$\left.\begin{aligned} r_s(x) &= r_{s-2}(x) - q_s(x) r_{s-1}(x) \\ r_{s-3}(x) = q_{s-1}(x) r_{s-2}(x) + r_{s-1}(x) \Rightarrow \quad & \\ r_{s-1}(x) &= r_{s-3}(x) - q_{s-1}(x) r_{s-2}(x) \end{aligned}\right\} \Rightarrow$$

$$r_s(x) = (1 + q_s(x) q_{s-1}(x)) r_{s-2}(x) - q_s(x) r_{s-3}(x)$$

然后根据同样的方法用它上面的等式逐个地消去

$r_{s-2}(x), \cdots, r_1(x),$ 再并项就得到

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

若 $d_1(x), d_2(x)$ 都是 $f(x), g(x)$ 的两个最大公因式，则

$$\left.\begin{array}{l} d_1(x) \mid d_2(x) \\ d_2(x) \mid d_1(x) \end{array}\right\} \Rightarrow d_1(x) = c d_2(x), c \neq 0.$$

这就是说，两个多项式的最大公因式在相差一个非零常数倍的意义下是唯一确定的.

记 $f(x)$ 与 $g(x)$ 的首项系数为1的最大公因式为

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

辗转相除法

例 设

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

$$g(x)=3x^3+10x^2+2x-3,$$

求$(f(x),g(x))$，并求$u(x),v(x)$使

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

上页 下页 返回 结束

$q_2(x)=$	$g(x)$	$f(x)$	
$-\frac{27}{5}x+9$	$3x^3+10x^2+2x-3$ $3x^3+15x^2+18x$	$x^4+3x^3-x^2-4x-3$ $x^4+\frac{10}{3}x^3+\frac{2}{3}x^2-x$	$\frac{1}{3}x-\frac{1}{9}$ $=q_1(x)$
	$-5x^2-16x-3$ $-5x^2-25x-30$	$-\frac{1}{3}x^3-\frac{5}{3}x^2-3x-3$ $-\frac{1}{3}x^3-\frac{10}{9}x^2-\frac{2}{9}x+\frac{1}{3}$	
	$r_2(x)=9x+27$	$r_1(x)=-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}$ $-\frac{5}{9}x^2-\frac{5}{3}x$	$-\frac{5}{81}x-\frac{10}{81}$ $=q_3(x)$
		$-\frac{10}{9}x-\frac{10}{3}$ $-\frac{10}{9}x-\frac{10}{3}$	
		0	

上页 下页 返回 结束

用等式写出来，就是

$$f(x)=(\frac{1}{3}x-\frac{1}{9})g(x)+(-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}),$$

$$g(x)=(-\frac{27}{5}x+9)(-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3})+(9x+27),$$

$$-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3}=(-\frac{5}{81}x-\frac{10}{81})(9x+27)$$

因此

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

上页 下页 返回 结束

而

$$9x+27=g(x)-(-\frac{27}{5}x+9)(-\frac{5}{9}x^2-\frac{25}{9}x-\frac{10}{3})$$

$$=g(x)-(-\frac{27}{5}x+9)[f(x)-(\frac{1}{3}x-\frac{1}{9})g(x)]$$

$$=(\frac{27}{5}x-9)f(x)+[1-(\frac{27}{5}x-9)(\frac{1}{3}x-\frac{1}{9})]g(x)$$

$$=(\frac{27}{5}x-9)f(x)+(-\frac{9}{5}x^2+\frac{18}{5}x)g(x)$$

于是，令 $u(x)=\frac{3}{5}x-1, v(x)=-\frac{1}{5}x^2+\frac{2}{5}x,$ 就有

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

定义7

$P[x]$中两个多项式$f(x), g(x)$称为**互素**（也称为**互质**）的，如果$(f(x), g(x))=1$.

定理3

$P[x]$中两个多项式$f(x), g(x)$互素的充要条件是有$P[x]$中的多项式$u(x), v(x)$使

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

定理4

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

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

证明:

由$(f(x),g(x))=1$可知，有 $u(x), v(x)$使

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

等式两边乘上 $h(x)$，得

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

因为 $f(x)\mid g(x)h(x)$，所以$f(x)$整除等式左端，从而

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

推论

如果 $f_1(x) \mid g(x), f_2(x) \mid g(x)$, 且 $(f_1(x), f_2(x)) = 1$,

那么 $f_1(x)f_2(x) \mid g(x)$.

证明： 由 $f_1(x) \mid g(x)$ 有

$$g(x) = f_1(x)h_1(x),$$

因为 $f_2(x) \mid g(x) = f_1(x)h_1(x)$, 且 $(f_1(x), f_2(x)) = 1$, 故

$f_2(x) \mid h_1(x)$, 即 $h_1(x) = f_2(x)h_2(x)$.

代入上式即得 $g(x) = f_1(x)f_2(x)h_2(x)$.

故

$$f_1(x)f_2(x) \mid g(x).$$

最大公因式与互素的概念都可以推广到两个以上的多项式.

(1) 任意多个多项式 $f_1(x), f_2(x), \cdots, f_s(x)(s \geq 2)$ 的最大公因式 $d(x)$:

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

② 如果 $\varphi(x) \mid f_i(x), i = 1, 2, \cdots, s$, 那么 $\varphi(x) \mid d(x)$.

仍用符号 $(f_1(x), f_2(x), \cdots, f_s(x))$ 表示首项系数为1的最大公因式.

注1

$$\big((f_1(x),f_2(x),\cdots,f_{s-1}(x)),f_s(x)\big)$$

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

注2 存在 $u_i(x),i=1,2,\cdots,s$ 使得

$$u_1(x)f_1(x)+u_2(x)f_2(x)+\cdots+u_s(x)f_s(x)$$

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

类似地，可以定义任意多个多项式互素：

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

§5 因式分解定理

在不同数域内，形式上相同的因式的分解不同.

例如：在有理数域Q内，

$$x^4-4=(x^2-2)(x^2+2).$$

在数域$Q(\sqrt{2})$或实数域R内，

$$x^4-4=(x+\sqrt{2})(x-\sqrt{2})(x^2+2).$$

在复数域C内，

$$x^4-4=(x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{2}i)(x-\sqrt{2}i).$$

定义8

数域P上次数≥1的多项式$p(x)$称为域P上的**不可约多项式**，如果它不能表成数域P上的两个次数比$p(x)$的次数低的多项式的乘积.

注1 显然，一次多项式都是不可约多项式.

注2 x^2+2 是实数域上的不可约多项式，但在复数域C上，

$$x^2+2=(x+\sqrt{2}i)(x-\sqrt{2}i),$$

因而不是不可约的 .

一个多项式是否不可约是依赖于系数域的.

注3

$p(x)$为不可约多项式

$\Longleftrightarrow$ $p(x)$只有非零常数与它自身的非零常数倍$cp(x)$这两种．$(\,c \neq 0\,)$

注4 不可约多项式 $p(x)$与任一多项式 $f(x)$之间只可能有两种关系：

（1）$p(x) \mid f(x)$；

（2）$(\,p(x),\ f(x)) = 1.$

事实上，设$(\,p(x),\ f(x)) = d(x)$，则$d(x)=1$或$d(x)=cp(x)$ $(c \neq 0)$．当$d(x) = cp(x)$时，就有 $p(x) \mid f(x)$．

不可约多项式的重要性质

定理5

如果$p(x)$是不可约多项式，则对于任意的两个多项式 $f(x)$, $g(x)$，由 $p(x)|f(x)g(x)$一定推出 $p(x)|f(x)$或者 $p(x)|g(x)$.

证明： 如果 $p(x)|f(x)$，那么结论已经成立 .

如果$p(x) \nmid f(x)$, 又因为$p(x)$是不可约多项式，则

$$(p(x), f(x)) = 1.$$

于是由定理4即得 $p(x) | f(x)$.

上页 下页 返回 结束

注 利用数学归纳法，上述定理可以推广为：

若不可约多项式 $p(x)$ 整除一些多项式 $f_1(x), f_2(x), \cdots, f_s(x)$ 的乘积

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

则存在 $f_i(x)$，使得 $p(x) \mid f_i(x)$.

因式分解唯一性定理

数域P上每一个次数≥1的多项式$f(x)$都可以唯一地分解成数域P上一些不可约多项式的乘积.

注 所谓唯一性是说，如果有两个分解式

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

则$s=t$，且适当排列因式的次序后有

$$p_i(x)=c_iq_i(x), i=1,2,\cdots,s,$$

其中$c_i(i=1,2,\cdots,s)$是一些非零常数.

证明： 先证分解式的存在性．

对 $f(x)$ 的次数作（第二）数学归纳法．

因为一次多项式都是不可约的，所以 $n=1$ 时结论成立．

设 $\partial(f(x))=n$，并设结论对于次数低于 n 的多项式已经成立．如果 $f(x)$ 是不可约多项式，结论是显然的，不妨设 $f(x)$ 不是不可约的，即有

$$f(x)=f_1(x)f_2(x),$$

其中 $f_1(x),f_2(x)$ 的次数都低于 n．由归纳法 $f_1(x),f_2(x)$ 都可以分解成数域P上一些不可约多项式的乘积．把 $f_1(x),f_2(x)$ 的分解式合起来就得到 $f(x)$ 的一个分解式.

再证分解式的唯一性.

设 $f(x)$ 可以分解成不可约多项式的乘积

$$f(x)=p_1(x)p_2(x)\cdots p_s(x).$$

如果 $f(x)$ 还有另一个分解式

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

其中 $q_i(x)(i=1,2,\cdots,t)$ 都是不可约多项式，于是

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

对 s 作归纳法. 当 $s=1$，$f(x)$ 是不可约多项式，由定义必有 $s=t=1$，且

$$f(x)=p_1(x)=q_1(x).$$

上页 下页 返回 结束

现设不可约因式的个数为$s-1$时唯一性已证.

由（1），$p_1(x) \mid q_1(x)q_2(x)\cdots q_t(x)$，因此，$p_1(x)$必能除尽其中的一个，不妨设$p_1(x) \mid q_1(x)$.

因为$q_1(x)$也是不可约多项式，所以有

$$p_1(x) = c_1 q_1(x), \qquad (2)$$

在(1)式两边消去$q_1(x)$，就有

$$p_2(x)\cdots p_s(x) = c_1^{-1} q_2(x)\cdots q_t(x). \qquad (3)$$

由归纳法假设，有$s-1=t-1$，即$s=t$，并且适当排列次序之后有$p_2(x) = c_2' c_1^{-1} q_2(x)$，即$p_2(x) = c_2 q_2(x)$，

$$p_i(x) = c_i q_i(x) \ (i = 3, \cdots, s). \qquad (4)$$

(2), (3), (4)合起来即为所要证的．唯一性得证.

标准分解式

在多项式 $f(x)$ 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 的的不可约因式合并．于是 $f(x)$ 的分解式成为

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

其中 c 是 $f(x)$ 的首项系数，$p_1(x), p_2(x), \cdots, p_s(x)$ 是不同的首项系数为 1 的不可约多项式，而 $r_1, r_2, \cdots, r_s$ 是正整数．这种分解称为**标准分解式**．

§5 因式分解定理

在不同数域内，形式上相同的因式的分解不同.

例如：在有理数域Q内，

$$x^4-4=(x^2-2)(x^2+2).$$

在数域$Q(\sqrt{2})$或实数域R内，

$$x^4-4=(x+\sqrt{2})(x-\sqrt{2})(x^2+2).$$

在复数域C内，

$$x^4-4=(x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{2}i)(x-\sqrt{2}i).$$

定义8

数域P上次数≥ 1的多项式$p(x)$称为域P上的**不可约多项式**，如果它不能表成数域P上的两个次数比$p(x)$的次数低的多项式的乘积.

注1 显然，一次多项式都是不可约多项式.

注2 x^2+2 是实数域上的不可约多项式，但在复数域C上，

$$x^2+2=(x+\sqrt{2}i)(x-\sqrt{2}i),$$

因而不是不可约的.

一个多项式是否不可约是依赖于系数域的.

注3

$p(x)$为不可约多项式

$\Longleftrightarrow$ $p(x)$只有非零常数与它自身的非零常数倍$cp(x)$这两种．$(\, c \neq 0 \,)$

注4 不可约多项式 $p(x)$与任一多项式 $f(x)$之间只可能有两种关系：

（1）$p(x) \mid f(x)$;

（2）$(\, p(x),\ f(x)) = 1.$

事实上，设$(\, p(x),\ f(x)) = d(x)$，则$d(x)$=1或$d(x)$= $cp(x)$ $(c \neq 0)$．当$d(x) = cp(x)$时，就有 $p(x) \mid f(x)$．

不可约多项式的重要性质

定理5

如果$p(x)$是不可约多项式，则对于任意的两个多项式 $f(x)$, $g(x)$，由 $p(x)\mid f(x)g(x)$一定推出 $p(x)\mid f(x)$或者 $p(x)\mid g(x)$.

证明： 如果 $p(x)\mid f(x)$，那么结论已经成立 .

如果$p(x)\nmid f(x)$, 又因为$p(x)$是不可约多项式，则

$$(p(x), f(x)) = 1.$$

于是由定理4即得 $p(x)\mid f(x)$.

上页 下页 返回 结束

注 利用数学归纳法，上述定理可以推广为：

若不可约多项式 $p(x)$ 整除一些多项式 $f_1(x), f_2(x),$ $\cdots, f_s(x)$ 的乘积

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

则存在 $f_i(x)$，使得 $p(x) \mid f_i(x)$.

因式分解唯一性定理

数域P上每一个次数≥1的多项式$f(x)$都可以唯一地分解成数域P上一些不可约多项式的乘积.

注 所谓唯一性是说，如果有两个分解式

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

则$s=t$，且适当排列因式的次序后有

$$p_i(x)=c_iq_i(x), i=1,2,\cdots,s,$$

其中$c_i(i=1,2,\cdots,s)$是一些非零常数.

证明： 先证分解式的存在性．

对 $f(x)$ 的次数作（第二）数学归纳法．

因为一次多项式都是不可约的，所以 $n=1$ 时结论成立．

设 $\partial(f(x))=n$，并设结论对于次数低于 n 的多项式已经成立．如果 $f(x)$ 是不可约多项式，结论是显然的，不妨设 $f(x)$ 不是不可约的，即有

$$f(x)=f_1(x)f_2(x),$$

其中 $f_1(x),f_2(x)$ 的次数都低于 n．由归纳法 $f_1(x),f_2(x)$ 都可以分解成数域P上一些不可约多项式的乘积．把 $f_1(x),f_2(x)$ 的分解式合起来就得到 $f(x)$ 的一个分解式．

再证分解式的唯一性.

设 $f(x)$ 可以分解成不可约多项式的乘积

$$f(x)=p_1(x)p_2(x)\cdots p_s(x).$$

如果 $f(x)$ 还有另一个分解式

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

其中 $q_i(x)(i=1,2,\cdots,t)$ 都是不可约多项式，于是

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

对 s 作归纳法. 当 $s=1$，$f(x)$ 是不可约多项式，由定义必有 $s=t=1$，且

$$f(x)=p_1(x)=q_1(x).$$

现设不可约因式的个数为$s-1$时唯一性已证.

由（1），$p_1(x) \mid q_1(x)q_2(x)\cdots q_t(x)$，因此，$p_1(x)$必能除尽其中的一个，不妨设$p_1(x) \mid q_1(x)$.

因为$q_1(x)$也是不可约多项式，所以有

$$p_1(x) = c_1 q_1(x), \qquad (2)$$

在(1)式两边消去$q_1(x)$，就有

$$p_2(x)\cdots p_s(x) = c_1^{-1} q_2(x)\cdots q_t(x). \qquad (3)$$

由归纳法假设，有$s-1=t-1$，即$s=t$，并且适当排列次序之后有$p_2(x)=c_2'c_1^{-1}q_2(x)$，即$p_2(x)=c_2q_2(x)$,

$$p_i(x) = c_i q_i(x) \quad (i=3,\cdots,s). \qquad (4)$$

(2), (3), (4)合起来即为所要证的．唯一性得证.

标准分解式

在多项式 $f(x)$ 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 的不可约因式合并．于是 $f(x)$ 的分解式成为

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

其中 c 是 $f(x)$ 的首项系数，$p_1(x),p_2(x),\cdots,p_s(x)$ 是不同的首项系数为 1 的不可约多项式，而 $r_1,r_2,\cdots,r_s$ 是正整数．这种分解称为**标准分解式**．

§7 多项式函数

直到现在为止，始终是纯形式地讨论多项式，也就是把多项式看作的表达式．在这一节，我们将从另一个观点，即函数的观点来考察多项式．

设

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

是$P[x]$中的多项式，α 是P中的数，在(1)中用α 代x所得的数

$$a_n\alpha^n+a_{n-1}\alpha^{n-1}+a_1\alpha+a_0$$

称为$f(x)$当 $x=\alpha$ 时的值，记为$f(\alpha)$. 这样一来，多项式$f(x)$就定义了一个数域P上的函数．可以由一个多项式来定义的函数称为数域P上的多项式函数．

当P是实数域R时，这就是数学分析中所讨论的多项式函数.

显然，若

$$h_1(x) = f(x) + g(x),$$

$$h_2(x) = f(x)g(x),$$

则

$$h_1(\alpha) = f(\alpha) + g(\alpha),$$

$$h_2(\alpha) = f(\alpha)g(\alpha),$$

定理7（余数定理）

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

证明： 用 $x-\alpha$ 去除 $f(x)$，设商为 $q(x)$，余式为一常数 c，于是

$$f(x)=(x-\alpha)q(x)+c.$$

以 α 代 x，得

$$f(\alpha)=c.$$

如果$f(x)$在$x=\alpha$时函数值$f(\alpha)=0$，则称α为$f(x)$的一个**根**或**零点**.

推论

α是$f(x)$的根的充要条件是$(x-\alpha)\mid f(x)$.

α是$f(x)$的k**重根**，如果$(x-\alpha)$是$f(x)$的k重因式.当$k=1$时，α称为**单根**；当$k>1$时，α称为**重根**.

定理8

$P[x]$中n次多项式$(n\geq 0)$在数域P中的根不可能多于n个，重根按重数计算．

证明： 对零次多项式定理显然成立．

设$f(x)$是一个次数>0的多项式．把$f(x)$分解成不可约多项式的乘积．由上面的推论与根的重数的定义，显然$f(x)$在数域P中根的个数等于分解式中一次因式的个数，这个数目当然不超过n．

定理9

如果多项式 $f(x), g(x)$ 的次数都不超过 n，而它们对 $n+1$ 个不同的数 $a_1, a_2, \cdots, a_{n+1}$ 有相同的值，即

$$f(a_i) = g(a_i), i = 1, 2, \cdots, n+1,$$

则 $f(x) = g(x)$.

证明： 由定理的条件，有

$$f(a_i) - g(a_i) = 0, i = 1, 2, \cdots, n+1,$$

这就是说，多项式 $f(x) - g(x)$ 有 $n+1$ 个不同的根 . 如果 $f(x) - g(x) \neq 0$，则它就是一个次数不超过 n 的多项式，由定理8，它不可能有 $n+1$ 个根 . 因此，$f(x) = g(x)$.

§8 复系数与实系数多项式的因式分解

对与复数域，有下面重要的定理：

代数基本定理

每个次数 ≥ 1的复系数多项式在复数域中有一个根．

注1 代数基本定理的内容十分明了，但它的证明需要用到进一步的知识，例如复变函数论，或微分拓扑学．

注2 代数基本定理显然可以等价叙述为：

每个次数 ≥ 1 的复系数多项式，在复数域上一定有一个一次因式．

由此可知，在复数域上所有次数大于 1 的多项式全是可约的．换句话说，不可约多项式只有一次多项式．于是我们有

复系数多项式因式分解定理

每个次数 ≥ 1 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，复系数多项式具有标准分解式

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

其中 $\alpha_1,\alpha_2,\cdots,\alpha_s$ 是不同的复数，$l_1,l_2,\cdots,l_s$ 是正整数．标准分解式说明了每个n个复系数多项式恰有n个复根（重根按重数计算）．即

$$l_1+l_2+\cdots+l_s=n.$$

实系数多项式的分解

如果 α 是实系数多项式 $f(x)$ 的复根，则 α 的共轭复数 $\bar{\alpha}$ 也是 $f(x)$ 的根 .

因为设

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

其中 $a_0,a_1,\cdots,a_n$ 是实数 . 由假设

$$f(\alpha)=a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_0=0.$$

两边取共轭数，有

$$f(\bar{\alpha})=a_n\bar{\alpha}^n+a_{n-1}\bar{\alpha}^{n-1}+\cdots+a_0=0,$$

即 $f(\bar{\alpha})=0$, $\bar{\alpha}$ 也是 $f(x)$ 的根 .

实系数多项式因式分解定理

每个次数 ≥ 1的实系数多项式在复数域上都可以唯一地分解成一次因式与二次不可约因式的乘积．

证明： 定理对一次多项式显然成立．

假设定理对次数$< n$的多项式已经证明．

设 $f(x)$是n次实系数多项式．由代数基本定理，$f(x)$有一复根 α 是实数，则

$$f(x) = (x - \alpha) f_1(x),$$

其中$f_1(x)$是$n-1$次实系数多项式．如果α 不是实数，则 $\bar{\alpha}$ 也是$f(x)$的根且$\bar{\alpha} \neq \alpha.$

上页 下页 返回 结束

于是

$$f(x)=(x-\alpha)(x-\bar{\alpha})f_2(x).$$

显然 $(x-\alpha)(x-\bar{\alpha})=x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$ 是一实系数二次不可约多项式．从而 $f_2(x)$ 是 $n-2$ 次实系数多项式．由归纳法假设，$f_1(x)$ 与 $f_2(x)$ 可以分解成一次与二次不约多项式的乘积，因此 $f(x)$ 也可以如此分解．

注 实系数多项式具有标准分解式

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

其中 $c_1,\cdots,c_s,p_1,\cdots,p_r,q_1,\cdots,q_r$ 全是实数，$l_1,l_2,\cdots,l_s,k_1,\cdots,k_r$ 是正整数．且

$$x^2 + p_i x + q_i (i = 1, 2, \cdots, r)$$

是不可约的，也就是满足

$$p_i^2 - 4q_i < 0, i = 1, 2, \cdots, r.$$

§9 有理系数多项式

有理系数多项式的分解远比复系数多项式和实系数多项式的分解要复杂的多，这是因为判别哪些有理系数多项式是不可约的是非常困难的．

但有以下基本事实：

每个次数 ≥ 1的有理系数多项式都能唯一地分解成不可约的有理系数多项式的乘积．

设

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

是一有理系数多项式．选取适当的整数c乘$f(x)$，总可以使$cf(x)$是一个整系数多项式．如果$cf(x)$的各项系数有公因子，就可以提出来，得到

$$cf(x)=dg(x),$$

也就是

$$f(x)=\frac{d}{c}g(x),$$

其中$g(x)$是整系数多项式，且各项系数没有异于±1的的公因子．

定义（本原多项式）

如果一个非零的整系数多项式

$$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_0$$

的系数 $b_n,b_{n-1},\cdots,b_0$ 没有异于±1的公因子，也就是说，它们是互素的，则称$g(x)$为**本原多项式**.

注 显然，任一个非零的有理系数多项式 $f(x)$都可以表示为一个有理数 r 与一个本原多项式 $g(x)$的乘积，即

$$f(x)=rg(x).$$

容易证明，这种表示法除了差一个正负号是唯一的.

亦即，如果

$$f(x)=rg(x)=r_1g_1(x),$$

其中$g(x)$, $g_1(x)$都是本原多项式，则必有

$$r=\pm r_1, g(x)=\pm g_1(x).$$

因为$f(x)$与$g(x)$只差一个常数倍，所以$f(x)$的因式分解问题，可以归结为本原多项式$g(x)$的分解问题.

下面进一步指出：

一个本原多项式能否分解成两个次数较低的有理系数多项式的乘积与它能否分解成两个次数较低的整系数多项式的乘积的问题是一致的.

定理10　(Gauss引理)

两个本原多项式的乘积还是本原多项式.

证明： 设

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

$$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_0$$

为两个本原多项式，而

$$h(x)=f(x)g(x)=d_{n+m}x^{n+m}+d_{n+m-1}x^{n+m-1}+\cdots+d_0$$

是它们的乘积 .

(反证法)

如果$h(x)$不是本原的，也就是说，$h(x)$的的系数 $d_{n+m}, d_{n+m-1}, \cdots, d_0$ 有一异于±1的公因子，则就有一个素数 p能整除 $d_{n+m}, d_{n+m-1}, \cdots, d_0$。

因为 $f(x)$是本原的，所以p不能同时整除$f(x)$的每一个系数．令a_i是第一个不能被p整除的系数，即

$$p \mid a_0, \cdots, p \mid a_{i-1}, p \nmid a_i.$$

同样的，$g(x)$也是本原的，令b_j是第一个不能被p整除的系数，即

$$p \mid b_0, \cdots, p \mid b_{j-1}, p \nmid b_j.$$

我们来看$h(x)$的系数d_{i+j}，由乘积定义

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

$$+ a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \cdots.$$

由上面的假设，p整除等式左端的d_{i+j}，p整除右端$a_i b_j$以外的每一项，但是p不能整数$a_i b_j$。这是不可能的．

这就证明了，$h(x)$一定也是本原多项式．

定理11

如果一非零的整系数多项式能够分解成两个次数较低的有理系数多项式的乘积，则它一定能分解成两个次数较低的整系数多项式的乘积．

证明： 设整系数多项式 $f(x)$ 有分解式

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

其中 $g(x)$, $h(x)$ 是有理系数多项式，且

$$\partial(g(x))<\partial(f(x)),\partial(h(x))<\partial(f(x)).$$

令

$$f(x)=af_1(x),$$

$$g(x)=rg_1(x),h(x)=sh_1(x),$$

这里 $f_1(x),g_1(x),h_1(x)$ 都是本原多项式，a 是整数，r,s 是有理数．

于是

$$af_1(x)=rsg_1(x)h_1(x).$$

由定理10，$g_1(x)h_1(x)$ 是本原多项式，从而

$$rs=\pm a,$$

这就是说，rs是一整数．因此，我们有

$$f(x)=(rsg_1(x))h_1(x).$$

这里 $rsg_1(x)$ 与 $h_1(x)$ 都是整系数多项式，且次数都低于 $f(x)$的次数．

推论

设 $f(x), g(x)$ 是整系数多项式，且 $g(x)$ 是本原的．如果 $f(x)=g(x)h(x)$，其中 $h(x)$ 是有理系数多项式，则 $h(x)$ 一定是整系数的．

定理12

设

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

是一个整系数多项式，而 $\frac{r}{s}$ 是它的一个有理数，其中 r, s互素，则必有 $s\mid a_n, r\mid a_0$.

特别地，如果 $f(x)$的首项系数 $a_n=1$, 则 $f(x)$的有理根都是整根，而且是 a_0 的因子 .

证明: 因为$\frac{r}{s}$ 是$f(x)$的一个有理根．因此在有理数域上

$$(x-\frac{r}{s})\mid f(x),$$

从而

$$(sx-r)\mid f(x).$$

因为r, s 互素，所以$sx-r$是一个本原多项式．根据上数推论，

$$f(x)=(sx-r)(b_{n-1}x^{n-1}+\cdots+b_0),$$

式中$b_{n-1},\cdots,b_0$ 都是整数．比较两边系数，即得

$$a_n=sb_{n-1}, a_0=-rb_0.$$

因此 $s\mid a_n, r\mid a_0.$

例1 求方程

$$2x^4 - x^3 + 2x - 3 = 0$$

的有理根.

解： 设 $\frac{r}{s}$ 是 $2x^4 - x^3 + 2x - 3 = 0$ 的一个根，其中 r, s 互素，则必有 $s \mid 2, r \mid 3$. 由此可知，

$s=1$或2，$r=1$或3 .

故这个方程的有理根只可能是 $\pm 1, \pm 3, \pm \frac{1}{2}, \pm \frac{1}{3}$.

容易证明除去 1 以外全不是它的根，因之这个方程的有理根只有 $x=1$.

例2 证明

$$f(x)=x^3-5x+1$$

在有理数域上不可约.

证明：（反证法）

假设 $f(x)$ 可约，则它至少有一个一次因子，也就是有一个有理根. 由定理12知，$f(x)$ 的有理根只可能是 ±1. 直接验算可知是 ±1 全不是根，矛盾.

因而 $f(x)$ 在有理数域上不可约.

定理13 (艾森斯坦（Eisenstein)判别法)

设

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

是一个整系数多项式．如果有一个素数 p，使得

(1) $p\nmid a_n$

(2) $p\mid a_{n-1},a_{n-2},\cdots,a_0$

(3) $p^2\nmid a_0$.

则 $f(x)$在有理数域上是不可约的．

证明： 如果 $f(x)$在有理数域上可约，则由定理11，$f(x)$可以分解成两个次数较低的整系数多项式的乘积：

$$f(x)=(b_lx^l+b_{l-1}x^{l-1}+\cdots+b_0)(cx^m+c_{m-1}x^{m-1}+\cdots+c_0)$$
$$(l,m<n,l+m=n).$$

因此 $a_n=b_lc_m, a_0=b_0c_0.$

因为 $p\mid a_0,$ 所以p能整除 b_0 或 $c_0.$ 但是 $p^2\nmid a_0,$ 所以p不能同时整除b_0及c_0．因此不妨设 $p\mid b_0$，但 $p\nmid c_0.$

另一方面，因为 $p\nmid a_n,$ 所以 $p\nmid b_l,$ 假设 $b_0,b_1,\cdots,$ b_l 中第一个不能被p整除的是b_k．比较$f(x)$中x^k的系数，得等式

$$a_k=b_kc_0+b_{k-1}c_1+\cdots+b_0c_k.$$

$$a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k.$$

式中$a_k, b_{k-1}, \cdots, b_0$ 都能被p整除，所以$b_k c_0$ 也必须能被p整除．这与$p \nmid b_k, p \nmid c_0$ 矛盾．

例3 证明 x^n+2 在有理数域上不可约.

证明： 取 $p=2$，由Eisenstein判别法可知，x^n+2 在有理数域上不可约.