定义1. 设 K 是一个数域，形为

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

的一个表达式称为 K 上的一个多项式，其中$a_n, a_{n-1}, \ldots, a_1, a_0 \in K$. 当 $a_n \neq 0$ 时 n 称为这个多项式的次数。 $a_n x^n$ 称为该多项式的首项，a_n 称为首项系数。 x 称为不定元（或变量）。a_0 称为常数项。 0 是一个特殊的多项式，规定其次数等于 $-\infty$.

数域 K 上以 x 为不定元的多项式全体所构成的集合记作 $K[x]$.

多项式可以简记为 $f(x), g(x), \alpha(x)$ 等。

设 $f(x) \in K[x]$. 则 $f(x)$ 的次数记作 $\deg(f(x))$ 或 $\deg(f)$.

多项式之间可以按通常的方式定义加减法和乘法和乘方。它们满足交换律、结合律、分配律等。

设 $f(x), g(x) \in K[x]$, 则 $f(g(x))$ 也按通常的法则计算。

- $\deg(fg) = \deg(f) + \deg(g)$.
- 设 $c \in K$, $c \neq 0, f(x) \in K[x]$, 则$\deg(cf(x)) = \deg(f)$.
- $\deg(f \pm g) \leq \max(\deg(f), \deg(g))$.
- 如果 $f(x), g(x) \in K[x]$ 满足 $f(x) \neq 0, f(x)g(x) = 0$ 则 $g(x) = 0$.

证明：$\deg(f)+\deg(g) = \deg(0) = -\infty$ 得 $\deg(g) = -\infty$ $\square$

- 如果 $f(x), g(x), h(x) \in K[x]$ 满足 $f(x) \neq 0, f(x)g(x) = f(x)h(x)$, 则 $g(x) = h(x)$.

证明：$f(x)[g(x) - h(x)] = 0$. $\square$

带余除法

定理1. 设 K 是一个数域,$f(x), g(x) \in K[x]$. 如果 $g(x) \neq 0$ 则存在唯一的一对多项式 $q(x), r(x)$ 满足

1) $f(x) = g(x)q(x) + r(x)$;
2) $\deg(r) < \deg(g)$.

$q(x)$ 称为**商**, $r(x)$ 称为**余式**.

证明：存在性：对 $f(x)$ 的次数进行归纳即可。

唯一性：利用次数。

$\square$

例1. 设 $f(x) = 2x^4 - 5x + 1, g(x) = x^2 - x + 2$, 求 $g(x)$ 除 $f(x)$ 的商和余式。

求解的方法叫带余除法或长除法（long division）。

作业：

p.187: 1,2,6,7

多项式的整除性

定义2. 设 $f(x), g(x) \in K[x]$. 如果 $f(x) \neq 0$ 且存在 $h(x) \in K[x]$ 使 $g(x) = f(x)h(x)$, 则称 $f(x)$ 整除 $g(x)$ 记作 $f(x)|g(x)$ 或$f|g$.

一些基本事实:

1) 任何一个非零常数整除任何一个多项式;

2) 任何一个非零多项式整除 0;

3) 0 不能整除任何多项式;

4) 若 $g(x)|f(x), g(x)|h(x)$, 则对任何多项式 $a(x), b(x)$ 都有$g(x)|a(x)f(x) + b(x)h(x)$.

5) 若 $g(x)|f(x)$ 且 $f(x) \neq 0$, 则 $\deg(g) \leq \deg(f)$.

6) $g(x)|f(x) \Rightarrow g(h(x))|f(h(x))$.

7) 两个常用公式：二项式定理和

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}).$$

引理2. 设 $f(x), g(x) \in K[x], g(x) \neq 0$. 则 $g(x)|f(x)$ 当且仅当$f(x)$ 被 $g(x)$ 除的余式等于零.

证: $\Rightarrow$: 存在 $b(x) \in K[x]$ 使 $f(x) = g(x)b(x)$. 故$f(x) = g(x)b(x) + 0$. 由于 $\deg(0) < \deg(g)$, 所以 $f(x)$ 被 $g(x)$ 除的余式等于零.

$\Leftarrow$: 余式等于零意味着 $f(x) = g(x)q(x)$, 即 $g(x)|f(x)$. $\square$

引理3. 设 $f(x), g(x)$ 都是非零多项式.若 $f(x)|g(x)$ 且 $g(x)|f(x)$, 则$f(x) = c \cdot g(x)$, 其中 c 是一个非零常数.

证: 设 $f(x) = g(x)a(x), g(x) = f(x)b(x)$. 则 $f(x) = f(x)b(x)a(x)$, 从而$a(x)b(x) = 1$, 所以 $a(x), b(x)$ 只能是非零常数. $\square$

多项式的最大公因式

定义3. 设 $f(x), g(x), h(x) \in K[x]$. 如果 $h(x)|f(x), h(x)|g(x)$, 则 $h(x)$ 称为 $f(x)$ 和 $g(x)$ 的一个公因式. 设 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的一个公因式并且具有如下性质: 对 $f(x), g(x)$ 的任何一个公因式 $h(x)$ 都有 $h(x)|d(x)$, 则 $d(x)$ 称为 $f(x)$ 和$g(x)$ 的最大公因式, 记作 $(f(x), g(x))$ 或$\gcd(f(x), g(x))$. (greatest common divisor)

例2.) $2x-1$ 和 $x-\frac{1}{2}$ 都是 $4x^2-4x+1$ 与 $x^3-\frac{x^2}{2}$ 的最大公因式.一般把 $x-\frac{1}{2}$ 定为$\gcd(4x^2-4x+1, x^3-\frac{x^2}{2})$, 因为它的首项系数等于1. 首项系数为1的多项式叫首一多项式。

例3. $\gcd(0,0)$ 不存在.

例4. 若 $f(x)\neq 0$, 则 $\gcd(f(x),0)=f(x)$.

引理4. 设 $d_1(x), d_2(x)$ 都是 $f(x), g(x)$ 的最大公因式,则 $d_1(x) = c \cdot d_2(x)$, 其中 c 是个非零常数.

证: 由定义得 $d_1(x)|d_2(x), d_2(x)|d_1(x)$. $\square$

引理5. 设 $f(x) = g(x)q(x) + r(x)$, 其中 $g(x) \neq 0$. 如果$d(x) = \gcd(g(x), r(x))$, 则 $d(x) = \gcd(f(x), g(x))$.

证明: 显然 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的一个公因式. 设 $h(x)$ 是$f(x)$ 和 $g(x)$ 的任意一个公因式, 由于 $r(x) = f(x) - g(x)q(x)$, 故$h(x)$ 整除 $r(x)$. 由于 $d(x) = \gcd(g(x), r(x))$, 因此 $h(x)|d(x)$. $\square$

定理6. 设 $f(x), g(x)$ 不全为零,则

$$\gcd(f(x), g(x))$$

存在,并且存在 $a(x), b(x)$ 使

$$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

第一种证法: [要点] 降低次数

如果 $f(x), g(x)$ 有一个是 0, 则结果成立.以下设 $f(x), g(x)$ 都不等于零.

对 $\deg(f) + \deg(g)$ 进行归纳.

当 $\deg(f) + \deg(g) = 0$ 时,

$$\gcd(f, g) = 1.$$

结论成立.

当 $\deg(f)+\deg(g)>0$ 时,设 $deg(f) \geq deg(g)$. 根据带余除法,存在$q(x), r(x)$ 使 $f(x)=g(x)q(x)+r(x)$ 且 $\deg(r)<\deg(g)$. 由于$\deg(r)+\deg(g)<\deg(f)+\deg(g)$ 且 $g(x), r(x)$ 不全为零, 根据归纳假设 $\gcd(r(x), g(x))$ 存在,并且有 $a_1(x), b_1(x)$ 使$\gcd(r(x), g(x))=a_1(x)r(x)+b_1(x)g(x)$. 由上面引理得知$\gcd(f(x), g(x))=\gcd(r(x), g(x))=a_1(x)(f(x)-g(x)q(x))+b_1(x)g(x)=a_1(x)f(x)+(b_1(x)-a_1(x)q(x))g(x)$. 令$a(x)=a_1(x)$,$b(x)=b_1(x)-a_1(x)q(x)$ 即可. $\square$

[注] 上面的证明是构造性的,它给出了gcd 的计算方法,叫做辗转相除法(Euclidean algorithm).

第二种证法:

令 $\Gamma = \{a(x)f(x)+b(x)g(x)|a(x),b(x)\in K[x]\}$. 由于$f(x),g(x)$ 不全为零,在集合 Γ 中存在一个非零元素. 在 Γ 的非零元素中任选一个次数最低的元素 $d(x)=a_1(x)f(x)+b_1(x)g(x)$.

根据带余除法,存在 $q(x),r(x)$ 使

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

满足 $\deg(r)<\deg(d)$. 由于

$$r(x)=(1-a_1(x)q(x))f(x)-(b_1(x)q(x))g(x),$$

故 $r(x)\in\Gamma$. 假如 $r(x)\neq 0$, 则与 $\deg(d)$ 的最低性矛盾,故 $r(x)=0$. 这证明了 $d(x)|f(x)$. 同理 $d(x)|g(x)$. 所以 $d(x)$ 是 $f(x)$和 $g(x)$ 的公因式.

设 $h(x)$ 是 $f(x),g(x)$ 的任意一个公因式,则

$$h(x)|a_1(x)f(x)+b_1(x)g(x),$$

即 $h(x)|d(x)$. $\square$

[注]这种证法是非构造性的.

例5. 求证 $x+1|x^{2m}+x^{2n+1}$ 对任何非负整数 m,n 成立.

证明:

$$\begin{aligned}&(x-1)(x^{2m}+x^{2n+1})\\=&x^{2m+1}-x^{2n+1}+x^{2n+2}-x^{2m}\\=&x(x^{2m}-x^{2n})+(x^{2n+2}-x^{2m})\end{aligned}$$

被 x^2-1 整除,故存在 $h(x)$ 使

$$(x-1)(x^{2m}+x^{2n+1})=(x^2-1)h(x),$$

由此得

$$x^{2m}+x^{2n+1}=(x+1)h(x).$$

□

定义4. 设 $f_1(x),\ldots,f_n(x)\in K[x]$ 不全为零,$h(x)$ 是一个非零多项式。如果对每个 i 都有 $h(x)|f_i(x)$, 则 $h(x)$ 称为$f_1(x),\ldots,f_n(x)$ 的一个公因式. 设 $d(x)$ 是$f_1(x),\ldots,f_n(x)$ 的一个公因式并且具有如下性质: 对$f_1(x),\ldots,f_n(x)$ 的任何一个公因式 $h(x)$ 都有 $h(x)|d(x)$, 则$d(x)$ 称为 $f_1(x),\ldots,f_n(x)$ 的最大公因式, 记作 $(f_1(x),\ldots,f_n(x))$ 或 $\gcd(f_1(x),\ldots,f_n(x))$.

[注]

1) 如果 $n=1$, 则 $d(x)=f_1(x)$.

2) 如果 $n=2$, 则新的定义和以前的定义一致。

3) 如果 $f_k(x)=0$, 则

$$\gcd(f_1(x),\ldots,f_n(x))$$

$$=\gcd(f_1(x),\ldots,f_{k-1}(x),f_{k+1}(x),\ldots,f_n(x)).$$

引理7. 设 $f_1(x), \ldots, f_n(x) \in K[x]$ 全不为零。假定 $n > 2$. 设 $1 \le r < n$. 记

$$d_1(x) = \gcd(f_1(x), \ldots, f_r(x)),$$

$$d_2(x) = \gcd(f_{r+1}(x), \ldots, f_n(x)),$$

$$d(x) = \gcd(d_1(x), d_2(x)).$$

则 $d(x)$ 是 $f_1(x), \ldots, f_n(x)$ 的最大公因式。

证明：由 $d(x)|d_1(x), d(x)|d_2(x)$ 得知 $d(x)$ 整除每个 $f_i(x)$.

假定 $h(x)$ 整除每个 $f_i(x)$, 则 $h(x)$ 整除 $f_1(x), \ldots, f_r(x)$ 中任何一个，因而 $h(x)|d_1(x)$. 同理 $h(x)|d_2(x)$. 所以$h(x)|d(x)$. $\square$

练习

设 $f_1(x),\ldots,f_n(x)$ 不全为零，则它们的最大公因式存在且在相差一个非零常数的意义下唯一。

作业：

p.194: 1,2,3,

定义5. 若 $\gcd(f(x), g(x)) = 1$，则称 $f(x)$ 和 $g(x)$ 互素。

引理8. $f(x)$ 和 $g(x)$ 互素的充要条件是存在 $u(x), v(x) \in K[x]$ 使$f(x)u(x) + g(x)v(x) = 1$.

证明：$\Rightarrow$: 由定义立得。

$\Leftarrow$: 令 $\Gamma = \{a(x)f(x) + b(x)g(x) | a(x), b(x) \in K[x]\}$. 则 $1 \in \Gamma$. 而 1 在 Γ 的非零元素中次数达到最小值，所以 $\gcd(f(x), g(x)) = 1$. $\square$

[注] 对任意一组多项式 $f(x), g(x), u(x), v(x), d(x)$, 即使$f(x)u(x) + g(x)v(x) = d(x)$, 也不能说 $d(x) = \gcd(f(x), g(x))$. [见习题3,p.190]

系9. 如果 $g(x)$ 与 $f_1(x),\ldots,f_n(x)$ 中每个多项式互素，则 $g(x)$ 与$f_1(x)\cdots f_n(x)$ 互素。

证明：对每个 i 都存在 $u_i(x),v_i(x)$ 使

$$f_i(x)u_i(x)+g(x)v_i(x)=1.$$

移项得

$$f_i(x)u_i(x)=1-g(x)v_i(x).$$

全部相乘得

$$f_1(x)\cdots f_n(x)u_1(x)\cdots u_n(x)=1-g(x)b(x).$$

再次移项得

$$f_1(x)\cdots f_n(x)u_1(x)\cdots u_n(x)+g(x)b(x)=1.$$

$\square$

[注] 书上推论(5.3.5) 是本推论的特殊情形。

系10. 设 $\gcd(f_1(x), f_2(x)) = 1$ 且 $f_1(x)|g(x), f_2(x)|g(x)$, 则$f_1(x)f_2(x)|g(x)$.

证明：设 $g(x) = f_1(x)s(x) = f_2(x)t(x)$. 由于 $\gcd(f_1(x), f_2(x)) = 1$, 存在 $u(x), v(x)$ 使

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

从而

$$\begin{aligned}
g(x) &= g(x) \cdot 1 \\
&= g(x)[f_1(x)u(x) + f_2(x)v(x)] \\
&= g(x)f_1(x)u(x) + g(x)f_2(x)v(x) \\
&= f_2(x)t(x)f_1(x)u(x) + f_1(x)s(x)f_2(x)v(x) \\
&= f_1(x)f_2(x)[t(x)u(x) + s(x)v(x)].
\end{aligned}$$

□

系11. 设 $\gcd(f(x), g(x)) = 1$ 且 $f(x)|g(x)h(x)$，则 $f(x)|h(x)$.

证明：存在 $u(x), v(x)$ 使

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

两边同乘 $h(x)$ 得

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

$\square$

[练习] 自己独立证明书上推论(5.3.3),(5.3.4).

例6. 设 K, K' 是两个数域且满足 $K \subset K'$. 设 $f(x), g(x) \in K[x]$. 则 $f(x)$ 在 $K[x]$ 中整除 $g(x)$ 当且仅当 $f(x)$ 在$K'[x]$ 中整除 $g(x)$.

证明：$\Rightarrow$: $f(x)$ 在 $K[x]$ 中整除 $g(x)$ 意味着存在 $h(x) \in K[x]$ 使 $g(x) = f(x)h(x)$. 然而 $h(x) \in K'[x]$. 所以$f(x)$ 在 $K'[x]$ 中也整除 $g(x)$。

$\Leftarrow$: 在 $K[x]$ 中作带余除法得

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

其中 $\deg(r) < \deg(f)$. 由于 $q(x), r(x)$ 也属于 $K'[x]$, 在$K'[x]$ 中 $f(x)$ 除 $g(x)$ 的余式也是 $r(x)$. 从而 $r(x) = 0$. 所以 $f(x)$ 在 $K[x]$ 中整除 $g(x)$. $\square$

例7. 设 $f(x), g(x), h(x) \in K[x]$ 为非零多项式， $h(x)$ 被 $g(x)$ 除的余式是个非零常数 c, $f(x)$ 被 $g(x)$ 除的余式是 $r(x)$, 则$f(x)h(x)$ 被 $g(x)$ 除的余式是 $c \cdot r(x)$。

证明：由

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

和

$$h(x) = g(x)q_1(x) + c$$

得

$$f(x)h(x) = g(x)[q(x)q_1(x)g(x)+c\cdot q(x)+r(x)q_1(x)]+c\cdot r(x).$$

而 $\deg(c \cdot r(x)) = \deg(r(x)) < \deg(g(x))$, 所以 $c \cdot r(x)$ 是$f(x)h(x)$ 被 $g(x)$ 除的余式。□

定理12 (中国剩余定理)**.** 设 $g_1(x), \ldots, g_n(x)$ 是一组两两互素的非零多项式。对于任给的多项式

$$a_1(x), \ldots, a_n(x),$$

假如 $\deg(a_i(x)) < \deg(g_i(x))$ 对 $1 \leq i \leq n$ 都成立，则存在一个多项式 $f(x)$, 使得对每个 i, 多项式 $f(x)$ 被 $g_i(x)$ 除的余式恰好是 $a_i(x)$.

证明：记 $h_i(x) = g_1(x) \cdots g_{i-1}(x) g_{i+1}(x) \cdots g_n(x)$. 则 $g_i(x)$ 与 $h_i(x)$ 互素。于是存在 $u_i(x), v_i(x)$ 使

$$g_i(x)u_i(x) + h_i(x)v_i(x) = 1.$$

移项得

$$h_i(x)v_i(x) = 1 - g_i(x)u_i(x)$$

令 $f(x) = h_1(x)v_1(x)a_1(x) + \cdots + h_n(x)v_n(x)a_n(x)$. 对每个$i$, 多项式 $f(x)$ 均可写成

$$f(x) = h_i(x)v_i(x)a_i(x) + g_i(x)b(x)$$

$$= a_i(x) + g_i(x)[b(x) - u_i(x)].$$

这表明 $f(x)$ 被 $g_i(x)$ 除的余式恰好是 $a_i(x)$. □

初等数论中的平行结果

定理13 (带余除法)**.** 设 m, n 是两个整数，$m \neq 0$. 则存在唯一的一对整数 q, r 满足

1) $n = mq + r$;

2) $0 \leq r < |m|$.

这个数 r 称为 n 被 m 除的余数。

证明：令 $\Gamma = \{ma | a \in \mathbb{Z}, ma \leq n\}$. 显然 $\Gamma \neq \emptyset$. 由于整数集合 Γ 以 n 作为一个上界，故Γ 中有一个最大数，记作 mq. 令 $r = n - mq$. 则

$$n = mq + r,$$

并且

$$0 \leq r.$$

余下只要证明 $r < |m|$ 即可。假定 $r \geq |m|$. 如果 $m > 0$, 则$m(q+1) = mq + m = n - r + m \leq n$, 故 $m(q+1) \in \Gamma$, 与 mq 的选取矛盾。如果 $m < 0$, 则 $m(q-1) = mq - m = n - r - m \leq n$, 故 $m(q-1) \in \Gamma$, 同样与 mq 的选取矛盾。

唯一性的证明留作练习。 $\square$

定义6. 设 m, n 是不全为零的两个整数。若正整数 d 是 m, n 的公因子，并且m, n 的任何一个公因子都整除 d, 则称 d 为 m, n 的最大公因子，记作 $\gcd(m, n)$.

定理14. 设 m, n 是不全为零的两个整数，则它们的最大公因子存在且唯一, 并且存在整数 u, v 使

$$\gcd(m, n) = mu + nv.$$

定理15 (孙子定理)**.** 设$g_1, \ldots, g_r$ 是一组两两互素的自然数。对于任给的非负整数$a_1, \ldots, a_r$, 假如 $a_i < g_i$ 对 $1 \leq i \leq r$ 都成立，则存在一个整数 n 使得对每个 i, 整数 n 被 g_i 除的余数恰好是a_i.

〈孙子算经〉

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”

作业：

p.194:4,5,6,7

多项式的因式分解

定义7. 设 K 是一个数域，$p(x) \in K[x]$ 满足以下条件：

(1) $\deg(p) > 0$;

(2) $p(x)$ 不能分解成两个次数小于 $\deg(p)$ 的多项式的乘积。

则 $p(x)$ 称为 $K[x]$ 中的一个不可约多项式。满足条件(1)但不满足条件(2)的多项式称为可约多项式。

[注] 不可约性与数域 K 有很大关系。

例8.) x^2+1 是 $\mathbb{R}[x]$ 中的不可约多项式，但不是 $\mathbb{C}[x]$ 中的不可约多项式，因为在$\mathbb{C}[x]$ 中$x^2+1=(x-i)(x+i)$.

2) x^2-2 是 $\mathbb{Q}[x]$ 中的不可约多项式，但不是 $\mathbb{R}[x]$ 中的不可约多项式，因为在$\mathbb{R}[x]$ 中$x^2-2=(x-\sqrt{2})(x+\sqrt{2})$.

3) 任何一个一次多项式是不可约多项式。

4) 注意 $2x+4$ 是不可约多项式。

设 $f(x)$ 是一个可约多项式，则存在一个多项式 $g(x)$ 满足

1) $g(x)|f(x)$;

2) $0<\deg(g)<\deg(f)$.

这样的 $g(x)$ 叫做 $f(x)$ 的一个真因式。

引理16. 设 $f(x),g(x)\in K[x]$ 且 $f(x)$ 不可约。如果 $f(x)$ 不整除$g(x)$, 则 $\gcd(f(x),g(x))=1$.

证明：记 $d(x)=\gcd(f(x),g(x))$. 则存在 $h(x)$ 使 $f(x)=d(x)h(x)$. 由于 $f(x)$ 不可约，$\deg(d)=0$ 或 $\deg(h)=0$. 假如 $\deg(h)=0$, 则$h(x)$ 是个非零常数 c. 此时 $d(x)=f(x)/c$. 而 $d(x)|g(x)$, 故$f(x)|g(x)$, 产生矛盾。因此 $\deg(d)=0$. □

定理17. 设 $p(x)$ 是一个不可约多项式，$p(x)|f(x)g(x)$. 则 $p(x)|f(x)$ 或$p(x)|g(x)$.

证明：如果 $p(x)$ 不整除 $f(x)$, 由上面引理知 $p(x)$ 与 $f(x)$ 互素，从而 $p(x)|g(x)$. □

系18. 设 $p(x)$ 是一个不可约多项式，

$$p(x)|f_1(x)\cdots f_n(x).$$

则 $p(x)$ 整除某个 $f_i(x)$.

证明：用数学归纳法。

定理19 (因式分解基本定理)**.** 设 $f(x)$ 是数域 K 上的一个次数大于 0 的多项式。则

$$f(x) = cp_1(x)\cdots p_n(x),$$

其中 c 是一个非零常数，$p_1(x),\ldots,p_n(x)$ 是首一不可约多项式。以上等式称为 $f(x)$ 的不可约分解式。

这里的 c 和真因式列 $\{p_1(x),\ldots,p_n(x)\}$ 在相差一个次序的意义下由 $f(x)$ 唯一确定的。

证明：(1) 存在性：

对 $\deg(f)$ 进行归纳。当 $\deg(f)=1$ 时，将 $f(x)$ 写成 $cf_1(x)$, 其中 c 是 $f(x)$ 的首项系数。立见结论成立。

假定结论对 $\deg(f)<n$ 的 $f(x)$ 均成立。现来证明当 $\deg(f)=n$ 时结论也成立。

如果 $f(x)$ 已经是不可约多项式，则证毕，否则 $f(x)=f_1(x)f_2(x)$, 其中 $f_1(x), f_2)$ 都是次数小于 $\deg(f)$ 的非零多项式，由归纳假设

$$f_1(x) = cp_1(x)\cdots p_r(x). \tag{1}$$

$$f_2(x) = c'p_{r+1}(x)\cdots p_n(x), \tag{2}$$

其中 c, c' 是一个非零常数， $p_1(x),\ldots,p_n(x)$ 是首一不可约多项式。将(2) 和(1) 代入$f(x)=f_1(x)f_2(x)$ 即得所需。

唯一性：

对 $f(x)$ 的因式个数 n 进行归纳。当 $n=1$ 时结论成立。

设 $n>1$, 假如

$$f(x)=c'q_1(x)\dots q_m(x)$$

是另一个不可约分解式。

由于 $p_i(x), q_j(x)$ 都是首一多项式，c 和 c' 都等于 $f(x)$ 的首项系数，故 $c=c'$.

由于 $p_1(x)|f(x)$, 根据上面引理 $p_1(x)$ 整除某个 $q_j(x)$, 不妨设$p_1(x)|q_1(x)$. 但是 $q_1(x)$ 也是不可约的，故 $p_1(x)=q_1(x)$. 因此

$$p_2(x)\cdots p_n(x)=q_2(x)\cdots q_m(x).$$

利用归纳假设得知 $m=n$ 且序列 $\{p_2(x),\dots,p_n(x)\}$ 和 $\{q_2(x),\dots,q_m(x)\}$ 只相差一个次序。 $\square$

设

$$f(x) = cp_1(x)\cdots p_n(x)$$

是 $f(x)$ 的不可约分解式。其中的不可约因式不一定两两不同。把相同的因式乘在一起就可将上式改写为

$$f(x) = cp_1(x)^{e_1}\cdots p_r(x)^{e_r}, \tag{3}$$

其中 $p_1(x),\ldots,p_r(x)$ 是两两不同的首一不可约多项式，把这样的分解式称为 $f(x)$ 的标准不可约分解式。

指数 e_i 称为因式 $p_i(x)$ 在 $f(x)$ 中的重数。重数大于 1 的因式称为重因式。例如在$f(x) = (x-1)^2(x^2+x+1)^3$ 中 $x-1$ 是一个 2 重因式， x^2+x+1 是一个 3 重因式。

由分解式(3) 可推出下面公式

$$\deg(f) = \sum_{i=1}^{r} e_i \deg(p_i).$$

如果 A 是一个由某些首一不可约多项式

$$q_1(x), \ldots, q_N(x)$$

组成的集合，并且对每个 $1 \leq i \leq r$, 都有 $p_i(x) \in A$. 则$f(x)$ 还可写成

$$f(x) = cq_1(x)^{k_1} \ldots q_N(x)^{k_N},$$

允许某些 k_i 等于 0.

特别，对于一组多项式 $f_1(x), \ldots, f_m(x)$, 可取集合$A = \{p_1(x), \ldots, p_N(x)\}$ 为 $f_1(x), \ldots, f_m(x)$ 的所有首一不可约因式全体。这样每个 $f_i(x)$ 可唯一地表示为

$$f_i(x) = c_i p_1(x)^{e_{i1}} \cdots p_N(x)^{e_{iN}},$$

其中 e_{ij} 都是非负整数，而 c_i 是非零常数。即使$\deg(f_i) = 0$. 这种表示也是有效的，这时所有的 e_{ij} 全等于零。这样的表示方法在讨论与整除性有关的问题时是有用的。

例9. 设

$$f_1(x) = 2(x-1)^2(x^2+1)^3,$$
$$f_2(x) = -(x-1)^3(x+1)^4(x^2+1),$$
$$f_3(x) = 4(x-1)^2(x-2)^5(x^2+1)^2.$$

它们可改写为

$$f_1(x) = 2(x-1)^2(x+1)^0(x-2)^0(x^2+1)^3,$$
$$f_2(x) = -(x-1)^3(x+1)^4(x-2)^0(x^2+1),$$
$$f_3(x) = 4(x-1)^2(x+1)^0(x-2)^5(x^2+1)^2.$$

由此求得

$$\gcd(f_1, f_2, f_3) = (x-1)^2(x^2+1).$$

作业：

p.198: 1,2,3,4

下面两条命题是明显的。

命题20. 设 $p_1(x), \ldots, p_N(x)$ 是一组两两不同的首一不可约多项式，

$$f(x) = cp_1(x)^{e_1} \ldots p_N(x)^{e_N},$$

$$g(x) = c' p_1(x)^{k_1} \ldots p_N(x)^{k_N},$$

其中 c, c' 是非零常数，则 $g(x) | f(x)$ 当且仅当 $k_i \leq e_i$ 对 $i = 1, \ldots, N$ 都成立。

命题21. 设 $p_1(x), \ldots, p_N(x)$ 是一组两两不同的首一不可约多项式。非零多项式 $f_1(x), \ldots, f_m(x)$ 分解为

$$f_1(x) = c_1 p_1(x)^{e_{11}} \cdots p_N(x)^{e_{1N}},$$

$$f_2(x) = c_2 p_1(x)^{e_{21}} \cdots p_N(x)^{e_{2N}},$$

$$\cdots\cdots$$

$$f_m(x) = c_m p_1(x)^{e_{m1}} \cdots p_N(x)^{e_{mN}},$$

其中 e_{ij} 都是非负整数，c_i 是非零常数。则

$$\gcd(f_1(x), \ldots, f_m(x)) = \prod_{i=1}^{N} p_i(x)^{\min_{j=1}^{m}\{e_{ji}\}}.$$

定义8. 设 $f_1(x), \ldots, f_n(x), h(x) \in K[x]$ 是一组非零多项式。如果对每个 i 都有 $f_i(x)|h(x)$, 则 $h(x)$ 称为$f_1(x), \ldots, f_n(x)$ 的一个公倍式. 设首一多项式 $m(x)$ 是 $f_1(x), \ldots, f_n(x)$ 的一个公倍式并且具有如下性质: 对$f_1(x), \ldots, f_n(x)$ 的任何一个公倍式 $h(x)$ 都有 $m(x)|h(x)$, 则$m(x)$ 称为 $f_1(x), \ldots, f_n(x)$ 的最小公倍式, 记作 $[f_1(x), \ldots, f_n(x)]$ 或 $lcm(f_1(x), \ldots, f_n(x))$.

命题22. 设 $p_1(x), \ldots, p_N(x)$ 是一组两两不同的首一不可约多项式。非零多项式 $f_1(x), \ldots, f_m(x)$ 分解为

$$f_1(x) = c_1 p_1(x)^{e_{11}} \cdots p_N(x)^{e_{1N}},$$

$$f_2(x) = c_2 p_1(x)^{e_{21}} \cdots p_N(x)^{e_{2N}},$$

$$\cdots\cdots$$

$$f_m(x) = c_m p_1(x)^{e_{m1}} \cdots p_N(x)^{e_{mN}},$$

其中 e_{ij} 都是非负整数，c_i 是非零常数。则

$$lcm(f_1(x), \ldots, f_m(x)) = \prod_{i=1}^{N} p_i(x)^{\max_{j=1}^{m}\{e_{ji}\}}.$$

命题23. 设 $f(x), g(x)$ 是数域 K 上的非零的首一多项式，则

$$\gcd(f(x), g(x)) \cdot lcm(f(x), g(x)) = f(x)g(x).$$

证明：由因式分解基本定理 $f(x), g(x)$ 可分别表示为

$$f(x) = p_1(x)^{e_1} \cdots p_N(x)^{e_N},$$
$$g(x) = p_1(x)^{k_1} \cdots, p_N(x)^{k_N}.$$

于是

$$\gcd(f(x), g(x)) \cdot lcm(f(x), g(x)) = \prod_{i=1}^{N} p_i(x)^{\min\{e_i,k_i\}+max\{e_i,k_i\}}.$$

但是$min\{a, b\} + max\{a, b\} = a + b$ 对任何整数 a, b 成立，因此

$$\gcd(f(x), g(x)) \cdot lcm(f(x), g(x)) = \prod_{i=1}^{N} p_i(x)^{e_i+k_i}.$$

□

多项式的重因式

设 $f(x)=cp_1(x)^{e_1}\cdots p_r(x)^{e_r}$ 是一个次数大于 1 的多项式 $f(x)$ 的标准不可约分解式。令 $g(x)=cp_2(x)^{e_2}\cdots p_r(x)^{e_r}$. 则 $f(x)=p_1(x)^{e_1}g(x)$ 且 $p_1(x)$ 与 $g(x)$ 互素。

根据求导法则

$$f'(x)=e_1p_1(x)^{e_1-1}p_1'(x)g(x)+p_1(x)^{e_1}g'(x).$$

$$=p_1(x)^{e_1-1}[e_1p_1'(x)g(x)+p_1(x)g'(x)].$$

由于 $0\le\deg(p_1'(x))<\deg(p_1(x))$, 不可约多项式$p_1(x)$ 不能整除 $p_1'(x)$. 因此 $p_1(x)$ 不能整除 $e_1p_1'(x)g(x)+p_1(x)g'(x)$. 这表明 $p_1(x)$ 在$f'(x)$ 中的重数是 e_1-1.

对所有 $i=1,\dots,r$ 有同样结果。这样就推出如下公式

$$\gcd(f(x),f'(x))=\prod_{i=1}^{r}p_i(x)^{e_i-1}.$$

特别，下面结论成立

命题24. 非零多项式 $f(x)$ 无重因式当且仅当 $\gcd(f(x),f'(x))=1$.

部分分式分解

What ?

我们在中学里学过分式的四则运算，例如

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

现在我们考虑它的反问题：
已知(4) 式的右边，求左边。
解决这样的问题的过程叫做部分分式分解。

Where？

什么函数的导数是

$$\frac{x}{x^2-1}?$$

一下不容易看出来。
作了部分分式分解后就得

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

我们知道

$$(ln(x-1))'=\frac{1}{x-1},(ln(x+1))'=\frac{1}{x+1}.$$

于是

$$(\frac{ln(x-1)+ln(x+1)}{2})'=\frac{1}{2(x-1)}+\frac{1}{2(x+1)}.$$

给出了问题的解答。

Why ?

上面的例子很简单，能不能推广？在回答这个问题前我们先学习部分分式分解的理论基础。

引理25. 设 $f(x), g_1(x), g_2(x)$ 都是数域 K 上的非零多项式。若 $g_1(x)$ 和$g_2(x)$ 互素，则存在多项式 $a(x), b(x)$ 使

$$\frac{f(x)}{g_1(x)g_2(x)} = \frac{a(x)}{g_1(x)} + \frac{b(x)}{g_2(x)}.$$

证明：由于 $g_1(x)$ 和 $g_2(x)$ 互素，存在 $u(x), v(x)$ 使$g_1(x)u(x) + g_2(x)v(x) = 1$. 于是

$$\frac{f(x)}{g_1(x)g_2(x)} = \frac{f(x)[g_1(x)u(x) + g_2(x)v(x)]}{g_1(x)g_2(x)}$$
$$\frac{f(x)v(x)}{g_1(x)} + \frac{f(x)u(x)}{g_2(x)}.$$

□

引理26. 设 $f(x), g(x) \in K[x]$, 其中 $\deg(g) > 0$. 设 m 是一个自然数。则存在分解式

$$\frac{f(x)}{g(x)^m} = h(x) + \frac{h_1(x)}{g(x)} + \frac{h_2(x)}{g(x)^2} + \cdots + \frac{h_m(x)}{g(x)^m},$$

其中 $h(x)$ 是多项式，而$h_1(x), \ldots, h_m(x)$ 的次数都小于 $\deg(g)$.

证明：对 $\deg(f)$ 进行归纳。

当 $\deg(f) < \deg(g)$ 时取 $h(x) = h_1(x) = \cdots = h_{m-1}(x) = 0$, $h_m(x) = f(x)$ 即可。

对任意 $f(x)$, 根据带余除法的原理，存在 $q(x), r(x)$ 使

$$f(x) = g(x)q(x) + h_m(x), \tag{5}$$

满足 $\deg(h_m) < \deg(g)$.

由 $\deg(g) > 0$ 推出 $\deg(q) < \deg(f)$. 根据归纳假设$q(x)/g(x)^{m-1}$ 可表示为

$$\frac{q(x)}{g(x)^{m-1}} = h(x) + \frac{h_1(x)}{g(x)} + \frac{h_2(x)}{g(x)^2} + \cdots + \frac{h_{m-1}(x)}{g(x)^{m-1}}, \tag{6}$$

其中 $h(x)$ 是多项式，而 $h_1(x), \ldots, h_{m-1}(x)$ 的次数都小于$\deg(g)$.

将(5) 和(6) 代入

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

即可。 $\square$

定理27（部分分式分解定理）**.** 设 $f(x), g(x)$ 是两个非零多项式，$\deg(g) > 0$. 设 $g(x)$ 的标准不可约分解式是

$$g(x) = cp_1(x)^{e_1} \cdots p_n(x)^{e_n}.$$

则

$$\frac{f(x)}{g(x)} = h(x) + \sum_{i=1}^{n} \sum_{j=1}^{e_i} \frac{h_{ij}(x)}{p_i(x)^j},$$

满足 $\deg(h_{ij}(x)) < \deg(p_i(x))$.

如果 $\deg(f) < \deg(g)$, 则 $h(x) = 0$.

证明：重复利用引理25得

$$\frac{f(x)}{g(x)} = \frac{b_1(x)}{p_1(x)^{e_1}} + \cdots + \frac{b_n(x)}{p_n(x)^{e_n}}.$$

再对右式中每一项应用引理26即可。

如果 $h(x) \neq 0$, 将分解式右边通分相加后得到的分式中分子的次数将大于等于分母的次数，这证明了最后一个论断。□

How ?

待定系数法

举例说明：求

$$\frac{x^5-x+1}{(x-1)^2(x^2+1)}$$

的部分分式分解。

首先通过带余除法得

$$\frac{x^5-x+1}{(x-1)^2(x^2+1)} = x+2+\frac{2x^3-2x^2+2x-1}{(x-1)^2(x^2+1)}.$$

根据定理，应有分解式

$$\frac{2x^3-2x^2+2x-1}{(x-1)^2(x^2+1)} = \frac{A}{x-1}+\frac{B}{(x-1)^2}+\frac{Cx+D}{x^2+1}.$$

将上式右边通分后相加后与左边比较得知常数 A, B, C, D 必须满足

$$\begin{aligned} A+C&=2,\\ B-A+D-2C&=-2,\\ C-2D+A&=2,\\ B-A+D&=-1. \end{aligned}$$

最后解这个线性方程组就行了。

作业：
p.198:5,6

多项式函数

定义9. 设 K 是一个数域，

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

$b \in K$. 则

$$f(b) = a_n b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 \in K$$

称为多项式 $f(x)$ 在 b 点的值。若 $f(b) = 0$, 则称 b 为 $f(x)$ 的一个零点。

定理28 (余式定理)**.** 设 $f(x) \in K[x], b \in K$. 则 $x - b$ 除 $f(x)$ 的余式是 $f(b)$.

证明：由带余除法，存在 $q(x), r(x)$ 使

$$f(x) = (x - b)q(x) + r(x), \qquad (7)$$

其中 $\deg(r) < \deg(x - 1) = 1$. 故 $r(x)$ 是个常数 c.
将(7)中的 x 用 b 取代，则得 $f(b) = c$. □

系29. 常数 b 是 $f(x)$ 的零点当且仅当 $(x-b)|f(x)$.

系30. 一个非零多项式的零点的总数不超过该多项式的次数。

证明：设非零多项式 $f(x)$ 的次数为 n. 假如 $f(x)$ 的零点个数超过n. 任取 $f(x)$ 的 $n+1$ 个两两不同的零点 $b_1, \ldots, b_{n+1}$. 则$(x-b_i)|f(x)$ 对 $i=1, \ldots, n+1$ 成立，故 $(x-b_1)\cdots(x-b_{n+1})|f(x)$, 这不可能，因为 $(x-b_1)\cdots(x-b_{n+1})$ 的次数大于 $f(x)$ 的次数。□

系31. 设 $f(x), g(x)$ 是数域 K 上的两个次数不超过 n 的非零多项式。如果有 $n+1$ 个互不相同的数 $b_1, \ldots, b_{n+1} \in K$ 使$f(b_i)=g(b_i)$ 对每个 i 成立，则 $f(x)=g(x)$.

证明：令 $h(x)=f(x)-g(x)$. 假如 $h(x) \neq 0$, 则 $h(x)$ 是一个具有$n+1$ 个零点 $b_1, \ldots, b_{n+1}$ 的多项式，形成矛盾。故$h(x)=0$，即 $f(x)=g(x)$. □

定义10. 设 $(x-b)^d|f(x)$ 但 $(x-b)^{d+1}$ 不整除 $f(x)$. 则称 b 为 $f(x)$ 的一个 d 重零点。

定理32. 设 $f(x)$ 是一个非零多项式，$n=\deg(f)$. 设 $b_1,\ldots,b_r$ 为$f(x)$ 的全体零点，其重数依次为 $d_1,\ldots,d_r$. 则

$$d_1+\ldots+d_r\leq n.$$

证明：由因式分解基本定理，

$$f(x)=(x-b_1)^{d_1}\cdots(x-b_r)^{d_r}g(x).$$

其中 $g(x)$ 是某个非零多项式。于是

$$d_1+\ldots+d_r\leq d_1+\ldots+d_r+\deg(g)=\deg(f)=n.$$

□

定理33 (Lagrange 插值定理). 设 $a_1, \dots, a_n$ 是数域 K 中 n 个互不相同的数，$b_1, \dots, b_n$ 是 K 中任意 n 个数，则存在唯一的一个次数不超过$n-1$的多项式 $f(x)$ 使 $f(a_i) = b_i$ 对每个 i 成立。

证明：本问题等价于求证存在一组常数

$$c_{n-1}, c_{n-2}, \dots, c_1, c_0$$

满足下面 n 个条件：

$$\begin{gathered}
c_{n-1}a_1^{n-1} + c_{n-2}a_1^{n-2} + \cdots + c_1 a_1 + c_0 = b_1, \\
c_{n-1}a_2^{n-1} + c_{n-2}a_2^{n-2} + \cdots + c_1 a_2 + c_0 = b_2, \\
\cdots\cdots \\
c_{n-1}a_n^{n-1} + c_{n-2}a_n^{n-2} + \cdots + c_1 a_n + c_0 = b_n.
\end{gathered}$$

这是关于变量 $c_{n-1}, c_{n-2}, \dots, c_1, c_0$ 的线性方程组，其系数矩阵的行列式是Vandermonde 行列式，其值不等于零（为什么？）。因此该方程组有唯一的解。□

复系数多项式

定理34 (代数基本定理)**.** 任何一个次数大于 0 的多项式在复数域里都有一个零点。

有各种证明，最简单的证明在复变函数论中给出。

系35. 设 $p(x)$ 是 $\mathbb{C}[x]$ 中的多项式，则 $p(x)$ 不可约当且仅当$\deg(p) = 1$.

证明：$\Rightarrow$: 由不可约多项式的定义，$\deg(p) \geq 1$. 假如$\deg(p) = n > 1$. 由代数基本定理，存在 $a \in \mathbb{C}$ 使 $p(a) = 0$. 即 $p(x) = (x - a)h(x)$. 而 $\deg(h) = \deg(p) - 1 < \deg(p)$ 且$\deg(x - a) = 1 < \deg(p)$. 这与 $p(x)$ 的不可约性矛盾。

$\Leftarrow$: 我们已经知道所有的一次多项式都是不可约的。$\Box$

系36. 设 $f(x) \in \mathbb{C}[x]$, $\deg(f) > 0$. 则 $f(x)$ 的标准不可约分解式是

$$f(x) = c(x - a_1)^{e_1} \cdots (x - a_r)^{e_r}.$$

等式

$$\deg(f) = e_1 + \cdots + e_r$$

成立。

零点和系数的关系：Vieta定理。

求根公式：次数大于4的多项式没有求根公式。

作业：

p.201:1,4,5

p.206:2,5

实系数多项式

设 $\alpha = a + bi \in \mathbb{C}$. 复数 $a - bi$ 称为 α 的共轭，记作 $\overline{\alpha}$.

容易验证下面诸等式

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta},$$
$$\overline{\alpha - \beta} = \overline{\alpha} - \overline{\beta},$$
$$\overline{\alpha\beta} = \overline{\alpha}\overline{\beta},$$
$$\overline{\alpha^n} = \overline{\alpha}^n.$$

$\overline{\alpha} = \alpha$ 当且仅当 $\alpha \in \mathbb{R}$.

特别，$\alpha + \overline{\alpha}$ 和 $\alpha\overline{\alpha}$ 是实数。

引理37. 设 $f(x) \in \mathbb{R}[x]$, $\alpha \in \mathbb{C}$. 如果$f(\alpha) = 0$, 则 $f(\overline{\alpha}) = 0$,

证明：设

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

则

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

取共轭得

$$\overline{a_n\alpha^n} + \overline{a_{n-1}\alpha^{n-1}} + \cdots + \overline{a_1\alpha} + \overline{a_0} = 0.$$

$$\overline{a_n} \cdot \overline{\alpha}^n + \overline{a_{n-1}} \cdot \overline{\alpha}^{n-1} + \cdots + \overline{a_1} \cdot \overline{\alpha} + \overline{a_0} = 0.$$

$$a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \cdots + a_1\overline{\alpha} + a_0 = 0.$$

这意味着$f(\overline{\alpha}) = 0$. □

系38. 非零多项式 $f(x) \in \mathbb{R}[x]$ 在复数域中的标准不可约分解式可写成

$$f(x) = c(x-a_1)^{e_1} \dots (x-a_r)^{e_r}$$

$$(x-\alpha_1)^{k_1}(x-\overline{\alpha_1})^{k_1} \cdots (x-\alpha_s)^{k_s}(x-\overline{\alpha_s})^{k_s},$$

其中$a_1, \dots, a_r \in \mathbb{R}$, $\alpha_1, \dots, \alpha_s \notin \mathbb{R}$.

证明：用数学归纳法对 $\deg(f)$ 进行归纳。当 $\deg(f) = 1$ 时结论显然成立。

设 $n = \deg(f) > 1$ 并且结论对任何次数小于 n 的多项式成立。由代数基本定理，存在 $b \in \mathbb{C}$ 使 $f(b) = 0$.

如果 $b \in \mathbb{R}$, 则 $f(x) = (x-b)g(x)$, 其中 $g(x) \in \mathbb{R}[x]$. 由于 $\deg(g) < n$, 利用归纳假设 $g(x)$ 的标准分解式满足条件，将这个分解式代入 $f(x) = (x-b)g(x)$ 即知结论对$f(x)$ 成立。

如果 $b \notin \mathbb{R}$, 则 $f(\bar{b}) = 0$ 且 $\bar{b} \neq b$, 故 $x-b$ 和 $x-\bar{b}$ 互素，从而$(x-b)(x-\bar{b})$ 在 $\mathbb{C}[x]$ 中整除 $f(x)$. 令$d(x) = (x-b)(x-\bar{b})$. 则$d(x) = x^2-(b+\bar{b})x+b\bar{b} \in \mathbb{R}[x]$. 于是$d(x)$ 在 $\mathbb{R}[x]$ 中也整除 $f(x)$. 即 $f(x) = d(x)g(x), g(x) \in \mathbb{R}[x]$. 由于 $\deg(g) < \deg(f)$, 和上面情形一样可推得所需结论。 □

以上结果可总结成：“实系数多项式的虚根成对出现”。

系39. 是 $p(x)$ 是 $\mathbb{R}[x]$ 中的不可约多项式，则 $1 \leq \deg(p) \leq 2$.

证明：根据代数基本定理存在 $\alpha \in \mathbb{C}$ 使$p(\alpha) = 0$. 如果 $\alpha \in \mathbb{R}$, 则 $x - \alpha \in \mathbb{R}[x]$ 且 $(x-\alpha)|p(x)$. 因而$\deg(p) = \deg(x-\alpha) = 1$.

如果 $\alpha \notin \mathbb{R}$, 则 $\overline{\alpha} \neq \alpha$. 由于 $p(\overline{\alpha}) = 0$, 多项式$(x-\alpha)(x-\overline{\alpha})|p(x)$. 然而$(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha + \overline{\alpha}) + \alpha\overline{\alpha} \in \mathbb{R}[x]$. 所以$\deg(p) = \deg((x-\alpha)(x-\overline{\alpha})) = 2$. □

系40. 任何一个实系数多项式可分解成若干个次数不超过 2 的多项式的乘积。

命题41. 任何一个奇数次的实系数多项式 $f(x)$ 有实数零点。

证法一：将这个多项式看成复系数多项式作标准不可约分解，由于虚根成对出现，至少有一个 $x-a$ 因式，其中 $a \in \mathbb{R}$.

证法二：由于该多项式可分解成若干个次数不超过 2 的实系数多项式的乘积，要是所有的不可约因式全是二次的，则多项式的总次数是偶数，形成矛盾，故至少有一个一次的因式。

证法三：

由于次数是奇数，$\lim_{x\to+\infty} f(x)$ 和 $\lim_{x\to-\infty} f(x)$ 中一个等于 $+\infty$，另一个等于$-\infty$。因此存在实数 N 使 $f(N)$ 和 $f(-N)$ 中一个为正另一个为负。由于 $f(x)$ 是实数轴上的连续函数，存在实数a 使 $f(a)=0$. $\square$

有理系数多项式

定理42. 设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, 其中$a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$. 假定 $a_n \neq 0, a_0 \neq 0$. 设 p, q 是两个互素的非零整数。如果 $f(q/p) = 0$, 则$p|a_n, q|a_0$.

证明：由条件 $f(q/p) = 0$ 得

$$a_n(\frac{q}{p})^n + a_{n-1}(\frac{q}{p})^{n-1} + \cdots + a_1(\frac{q}{p}) + a_0 = 0.$$

两边同乘 p^n 得

$$a_n q^n + a_{n-1} p q^{n-1} + \cdots + a_1 p^{n-1} q + a_0 p^n = 0. \quad (8)$$

因此

$$p(a_{n-1}q^{n-1} + \cdots + a_1 p^{n-2} q + a_0 p^{n-1}) = -a_n q^n,$$

所以 $p|a_n$.

(8)还推出

$$q(a_n q^{n-1} + a_{n-1} p q^{n-2} + \cdots + a_1 p^{n-1}) = -a_0 p^n,$$

所以 $q|a_0$. □

例：找出方程

$$x^3 + \frac{5}{4}x - \frac{21}{4} = 0$$

的所有有理根。

解：原方程等价于整系数方程

$$4x^3 + 5x - 21 = 0.$$

设 q/p 是一个有理根，其中p, q互素。则 $p|4, q|21$. 于是 q/p 可能的值是：

$$\begin{aligned}
&\pm 1, \pm 3, \pm 7, \pm 21,\\
&\pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{7}{2}, \pm\frac{21}{2},\\
&\pm\frac{1}{4}, \pm\frac{3}{4}, \pm\frac{7}{4}, \pm\frac{21}{4}.
\end{aligned}$$

逐一代入得知原方程只有一个有理根 $3/2$.

定义11. 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一个非零多项式，其中 $a_n,a_{n-1},\ldots,a_1,a_0\in\mathbb{Z}$. 如果 $\gcd(a_n,a_{n-1},\ldots,a_1,a_0)=1$, 则称 $f(x)$ 为一个本原多项式(primitive polynomial).

定理43 (Gauss 引理)**.** 两个本原多项式的乘积仍然是本原多项式。

证明：设

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

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0.$$

都是本原多项式。将 $f(x)g(x)$ 展开成

$$f(x)g(x)=c_{n+m}x^{n+m}+c_{n+m-1}x^{n+m-1}+\cdots+c_1x+c_0.$$

则

$$c_k=\sum_{i+j=k}a_ib_j.$$

假如 $f(x)g(x)$ 不是本原多项式，则存在素数 p 整除每个 c_i. 设a_r 是 $f(x)$ 中从左边数起第一个不被 p 整除的系数。设 b_s 是$g(x)$ 中从左边数起第一个不被 p 整除的系数。则

$$c_{r+s}=a_rb_s+\sum_{i>0}a_{r-i}b_{s+i}+\sum_{i>0}a_{r+i}b_{s-i},$$

它不被 p 整除，矛盾。□

引理44. 设 $f(x), g(x)$ 都是本原多项式，且首项系数都是正数。假如$f(x) = cg(x)$, 其中 c 是一个有理数，则 $c = 1$.

证明：将 c 表为 $c = a/b$，其中 a, b 为互素的两个整数，$b > 0$. 由于$f(x), g(x)$ 的首项系数都是正数，a 也一定是正数。于是有等式

$$bf(x) = ag(x). \tag{9}$$

设 $f(x)$ 和 $g(x)$ 的第 i 次项系数分别为 c_i 和 d_i, 比较(9) 式两边第 i 次项的系数得

$$bc_i = ad_i.$$

假如 $b \neq 1$, 由于 b 与 a 互素，上面等式推出 b 整除 d_i, 从而 b 整除 $g(x)$ 的每个系数，这与 $g(x)$ 是本原多项式相矛盾。所以 $b = 1$. 同理可证 $a = 1$. $\square$

定理45. 若一个本原多项式在 $\mathbb{Q}[x]$ 中可约，则它可分解成两个次数较低的整系数多项式的乘积。

证明：设 $f(x)$ 是一个本原多项式，并且 $f(x)=g(x)h(x)$, 其中$g(x),h(x)\in\mathbb{Q}[x]$ 满足$\deg(g)<\deg(f),\deg(h)<\deg(f)$. 则存在有理数 r,s 使$rg(x),sh(x)$为首项系数为正的本原多项式。

不失一般性可设 $f(x)$ 的首项系数大于 0. 根据Gauss 引理，等式

$$rsf(x)=[rg(x)][sh(x)]$$

的右边是一个本原多项式，再由上面引理得知 $rs=1$. □

系46. 若一个非零的整系数多项式 $f(x)$ 在 $\mathbb{Q}[x]$ 中可约，则它可分解成两个次数较低的整系数多项式的乘积。

证明：设 d 是 $f(x)$ 的所有系数的最大公因子，则 $f(x)=dg(x)$, 多项式 $g(x)$ 是本原多项式。由于 $f(x)$ 在 $\mathbb{Q}[x]$ 中可约, $g(x)$ 在 $\mathbb{Q}[x]$ 中也可约。由上述定理得知 $g(x)$ 可分解成两个次数较低的整系数多项式的乘积,因此 $f(x)$ 也可分解成两个次数较低的整系数多项式的乘积。□

Eisenstein 判别法

设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 是一个整系数多项式，$a_n \neq 0, n \geq 1$. 设 p 是一个素数。假定$p \nmid a_n$, $p|a_i(i=0,\ldots,n-1)$, $p^2 \nmid a_0$. 则 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约。

证明：（反证法）假定 $f(x)$ 在 $\mathbb{Q}[x]$ 中可约，由上述推论

$$f(x) = (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0)(c_k x^k + c_{k-1}x^{k-1} + \cdots + c_0), \tag{10}$$

$b_i, c_j \in \mathbb{Z}, b_m \neq 0, c_k \neq 0, m > 0, k > 0.$

由于 $p \nmid a_n = b_m c_k$, 故 $p \nmid b_m, p \nmid c_k$. 由于$a_0 = b_0 c_0$, 而 $p|a_0, p^2 \nmid a_0$, 所以 p 只能整除 b_0, c_0 中的一个。不妨设 $p|b_0, p \nmid c_0$. 设 $p|b_0, \ldots, p|b_{j-1}, p \nmid b_j$. 则

$$a_j = \sum_{i+k=j} b_i c_k = b_j c_0 + \sum_{i+k=j, i<j} b_i c_k.$$

由此得 $p \nmid a_j$, 矛盾。□

例10. $x^n - 5$ 在 $\mathbb{Q}[x]$ 中不可约。

例11. 设 p 是一个素数，则

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

在 $\mathbb{Q}[x]$ 中不可约。

证明：只要证明 $f(x+1)$ 不可约即可。由于

$$f(x) = \frac{x^p - 1}{x - 1},$$

所以

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= \frac{x^p + C_p^1 x^{p-1} + \cdots + C_p^{p-1} x}{x} \\ &= x^{p-1} + C_p^1 x^{p-2} + \cdots + C_p^{p-1} \\ &= x^{p-1} + C_p^1 x^{p-2} + \cdots + p. \end{aligned}$$

而 $p | C_p^i$ 对所有 $i = 1, \ldots, p-1$ 成立。根据Eisenstein判别法 $f(x+1)$ 不可约。□

作业

p.211:

4(1)(2),5,8,9

多变量多项式

设 K 是一个数域，$x_1, x_2, \ldots, x_n$ 是一组未定元，表达式 $cx_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ 称为一个**单项式**，其中c 是 K 中一个非零元，$e_1, \ldots, e_n$ 是非负整数。

例如：$-2x_1^3x_2^4$ 是 x_1, x_2 的一个单项式。

$3x_1^2x_2^0x_3^4$ 一般记作 $3x_1^2x_3^4$.

对于固定的不定元 $x_1, x_2, \ldots, x_n$ 有限多个单项式的和及 0 称为(这组不定元的)多项式，它们全体所构成的集合记作$K[x_1, \ldots, x_n]$.

$K[x_1, \ldots, x_n]$ 中一个元素可表示成

$$f(x_1, \ldots, x_n) = \sum a_{e_1,\ldots,e_n} x_1^{e_1} \ldots x_n^{e_n},$$

其中 $a_{e_1,\ldots,e_n} \in K$, 求和号只包含有限项。

多项式的加减乘法按通常的法则进行。

单项式 $cx_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ 的次数规定为 $e_1+\cdots+e_n$. 非零多项式的次数定义为构成它的单项式的次数的最大值。多项式 0 的次数规定为 $-\infty$. 多项式 $f(x_1, \ldots, x_n)$ 的次数记作 $\deg(f)$.

等式

$$\deg(fg) = \deg(f) + \deg(g)$$

对任何 $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ 成立。

单变量多项式可写成降幂或升幂的形式，但对于多变量多项式却没有这么好的标准形式。现举例介绍三种常用的表达方式：

设有多项式

$$f(x_1,x_2,x_3)=x_2-2x_1x_2^2x_3+x_1^2x_3-x_1.$$

1) 字典式排列:

按常识

$$f(x_1,x_2,x_3)=-x_1+x_1^2x_3-2x_1x_2^2x_3+x_2.$$

但是在多项式中通常排成

$$f(x_1,x_2,x_3)=x_1^2x_3-2x_1x_2^2x_3-x_1+x_2.$$

法则如下：设 $x_1^{e_1}\cdots x_n^{e_n}$ 和 $x_1^{d_1}\ldots x_n^{d_n}$ 是两个单项式，如果 $e_1=d_1,\ldots,e_{j-1}=d_{j-1}$, 而$e_j>d_j$, 则 $x_1^{e_1}\cdots x_n^{e_n}$ 先于 $x_1^{d_1}\ldots x_n^{d_n}$。

2) 次数优先的字典式排列：

$$f(x_1,x_2,x_3)=-2x_1x_2^2x_3+x_1^2x_3-x_1+x_2.$$

3) 按某个变量降幂的形式：

$$f(x_1,x_2,x_3)=(x_1^2-2x_1x_2^2)x_3+(x_2-x_1).$$

最后一种表示方式在数学归纳法中十分有效。

命题47. 设 $f(x_1,\ldots,x_n), g(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n], f \neq 0, g \neq 0$. 则 $fg \neq 0$.

证明：对 n 进行归纳。当 $n=1$ 时是单变量多项式，结果成立。

设命题对 $n-1$ 成立。将 $f(x_1,\ldots,x_n), g(x_1,\ldots,x_n)$ 写成按变量 x_n 降幂的形式：

$$f(x_1,\ldots,x_n) = a_m(x_1,\ldots,x_{n-1})x_n^m + \cdots + a_0(x_1,\ldots,x_{n-1}),$$

$$g(x_1,\ldots,x_n) = b_k(x_1,\ldots,x_{n-1})x_n^k + \cdots + b_0(x_1,\ldots,x_{n-1}),$$

其中 $a_m(x_1,\ldots,x_{n-1}), b_k(x_1,\ldots,x_{n-1})$ 是$K[x_1,\ldots,x_{n-1}]$ 中的非零元素。由归纳法假设

$$a_m(x_1,\ldots,x_{n-1})b_k(x_1,\ldots,x_{n-1}) \neq 0.$$

因此

$$f(x_1,\ldots,x_n)g(x_1,\ldots,x_n) =$$
$$a_m(x_1,\ldots,x_{n-1})b_k(x_1,\ldots,x_{n-1})x_n^{m+k} + \cdots \neq 0.$$

□

命题48. 设 $f(x_1,\ldots,x_n)$ 是一个非零多项式，则存在 $a_1,\ldots,a_n\in K$ 使 $f(a_1,\ldots,a_n)\neq 0$.

证明：对 n 归纳。当 $n=1$ 时，$f(x_1)$ 只有有限多个零点，故结论成立。

设命题对 $n-1$ 成立。将 $f(x_1,\ldots,x_n)$ 写成按变量 x_n 降幂的形式：

$$f(x_1,\ldots,x_n)=a_m(x_1,\ldots,x_{n-1})x_n^m+\cdots+a_0(x_1,\ldots,x_{n-1}),$$

其中 $a_m(x_1,\ldots,x_{n-1})$ 是$K[x_1,\ldots,x_{n-1}]$ 中的非零元素。由归纳法假设存在$b_1,\ldots,b_{n-1}\in K$ 使 $a_m(b_1,\ldots,b_{n-1})\neq 0$. 于是

$$f(b_1,\ldots,b_{n-1},x_n)$$

$$=a_m(b_1,\ldots,b_{n-1})x_n^m+\ldots,a_0(b_1,\ldots,b_{n-1})$$

是单变量 x_n 的非零多项式。因此存在 $b_n\in K$ 使$f(b_1,\ldots,b_n)\neq 0$. $\square$

命题49. 设 $f(x_1,\ldots,x_n)$ 是一个不等于常数的多项式，则存在$c_1,\ldots,c_n\in\mathbb{C}$ 使 $f(c_1,\ldots,c_n)=0$.

证明: 由于按所给条件 $f(x_1,\ldots,x_n)$ 不是常数，至少有一个变量出现，不妨设 x_n 出现。将$f(x_1,\ldots,x_n)$ 写成按变量 x_n 降幂的形式：

$$f(x_1,\ldots,x_n)=a_m(x_1,\ldots,x_{n-1})x_n^m+\cdots+a_0(x_1,\ldots,x_{n-1}),$$

其中 $a_m(x_1,\ldots,x_{n-1})$ 是$K[x_1,\ldots,x_{n-1}]$ 中的非零元素,$m>0$。

根据刚才的命题，存在 $c_1,\ldots,c_{n-1}\in K$ 使

$$a_m(c_1,\ldots,c_{n-1})\neq 0.$$

这样 $f(c_1,\ldots,c_{n-1},x_n)$ 就成为一个次数大于零的关于变量x_n 的多项式。根据代数基本定理存在复数 c_n 使$f(c_1,\ldots,c_n)=0$. □

设 $f(x_1,\ldots,x_n),g(x_1,\ldots,x_n)\in K[x_1,\ldots,x_n]$ 且$g(x_1,\ldots,x_n)\neq 0$. 若存在 $q(x_1,\ldots,x_n)\in K[x_1,\ldots,x_n]$ 使

$$f(x_1,\ldots,x_n)=g(x_1,\ldots,x_n)q(x_1,\ldots,x_n),$$

则称 g 整除 f, 记作 $g|f$. 也称 g 是 f 的一个因式。

一个次数大于 0 的多项式叫做一个不可约多项式，若它不能分解成两个次数更低的多项式的乘积。

对于 $K[x_1,\ldots,x_n]$ 也有唯一因式分解定理，将在抽象代数课程中证明。

多变量多项式一般没有带余除法，然而当对比较简单的情形还是可以作带余除法的。

命题50. 设 $f(x_1,\dots,x_n)\in K[x_1,\dots,x_n], g(x_1,\dots,x_n)=x_n-h(x_1,\dots,x_{n-1})$, 其中$h(x_1,\dots,x_{n-1})\in K[x_1,\dots,x_{n-1}]$. 则存在唯一的$q(x_1,\dots,x_n)\in K[x_1,\dots,x_n]$ 和 $r(x_1,\dots,x_{n-1})\in K[x_1,\dots,x_{n-1}]$ 使

$$f(x_1,\dots,x_n)=g(x_1,\dots,x_n)q(x_1,\dots,x_n)+r(x_1,\dots,x_{n-1}).$$

证：（存在性）如果 $f(x_1,\dots,x_n)=0$ 则取 $q=r=0$ 即可，否则将$f(x_1,\dots,x_n)$ 写成按变量 x_n 降幂的形式：

$$f(x_1,\dots,x_n)=a_m(x_1,\dots,x_{n-1})x_n^m+\cdots+a_0(x_1,\dots,x_{n-1}),$$

其中 $a_m(x_1,\dots,x_{n-1})$ 是$K[x_1,\dots,x_{n-1}]$ 中的非零元素。对 m 进行归纳。

当 $m=0$ 时取 $q(x_1,\dots,x_n)=0, r(x_1,\dots,x_{n-1})=a_0(x_1,\dots,x_{n-1})$ 即可。

设 $m>0$ 。令

$$\begin{aligned}&s(x_1,\dots,x_n)\\=&f(x_1,\dots,x_n)-a_m(x_1,\dots,x_{n-1})x_n^{m-1}(x_n-h(x_1,\dots,x_{n-1})).\end{aligned}$$

则$s(x_1,\dots,x_n)$ 关于 x_n 的次数小于 m。由归纳假设，存在$q_1(x_1,\dots,x_n)$ 和 $r_1(x_1,\dots,x_{n-1})$ 使

$$s(x_1,\dots,x_n)=g(x_1,\dots,x_n)q_1(x_1,\dots,x_n)+r_1(x_1,\dots,x_{n-1}).$$

从而

$$\begin{gathered}f(x_1,\ldots,x_n)\\ = g(x_1,\ldots,x_n)(q_1(x_1,\ldots,x_n)+a_m(x_1,\ldots,x_{n-1})x_n^{m-1}))\\ +r_1(x_1,\ldots,x_{n-1}).\end{gathered}$$

（唯一性）设

$$\begin{aligned}&g(x_1,\ldots,x_n)q(x_1,\ldots,x_n)+r(x_1,\ldots,x_{n-1})\\ =&\, g(x_1,\ldots,x_n)q_1(x_1,\ldots,x_n)+r_1(x_1,\ldots,x_{n-1}).\end{aligned}$$

则

$$g(q-q_1)=r_1-r.$$

如果 $q-q_1\neq 0$. 则 $g(q-q_1)$ 是一个含有 x_n 的非零多项式，但$r_1-r\in K[x_1,\ldots,x_{n-1}]$, 产生矛盾。所以 $q-q_1=r_1-r=0$. □

系51. 设 $f(x_1,\ldots,x_n)\in K[x_1,\ldots,x_n], h(x_1,\ldots,x_{n-1})\in K[x_1,\ldots,x_{n-1}]$. 则$f(x_1,\ldots,x_{n-1},h(x_1,\ldots,x_{n-1}))=0$ 当且仅当$x_n-h(x_1,\ldots,x_{n-1})$ 是 $f(x_1,\ldots,x_n)$ 的因式。

证明：$\Leftarrow$: 设$f(x_1,\ldots,x_n)=(x_n-h(x_1,\ldots,x_{n-1}))q(x_1,\ldots,x_n)$. 将$h(x_1,\ldots,x_{n-1})$ 替换 x_n 即得所求。

$\Rightarrow$:根据命题存在 $q(x_1,\ldots,x_n)\in K[x_1,\ldots,x_n]$ 和 $r(x_1,\ldots,x_{n-1})\in K[x_1,\ldots,x_{n-1}]$ 使

$$f(x_1,\ldots,x_n)=(x_n-h(x_1,\ldots,x_{n-1}))q(x_1,\ldots,x_n)+r(x_1,\ldots,x_{n-1}).$$

将 $h(x_1,\ldots,x_{n-1})$ 替换 x_n 即得

$$r(x_1,\ldots,x_{n-1})=0.$$

□

例12. 设 $f(x_1,\ldots,x_n)\in K[x_1,\ldots,x_n]$, 且$(x_j-x_i)|f(x_1,\ldots,x_n)$ 对任何 $1\le i<j\le n$ 成立。则

$$\prod_{1\le i<j\le n}(x_j-x_i)|f(x_1,\ldots,x_n).$$

证明：将所有形为 $x_j-x_i(1\le i<j\le n)$ 的多项式排成一排：$g_1,\ldots,g_N$. 需要证明 $g_1\cdots g_N|f$. 为此，我们证明对任意 $1\le r\le N$, 都有 $g_1\cdots g_r|f$.

对 r 进行归纳。当 $r=1$ 时已经知道结论成立。设 $1<r\le N$ 且$g_1\cdots g_{r-1}|f$. 则存在多项式 q 使

$$f=qg_1\cdots g_{r-1}. \tag{11}$$

设 $g_r=x_j-x_i$. 由于 $(x_j-x_i)|f(x_1,\ldots,x_n)$, 故$f(x_1,\ldots,x_n)$ 中 x_j 用 x_i 替代后等于零。另一方面，$g_1,\ldots,g_{r-1}$ 中 x_j 用 x_i 替代后每一个都不等于零。将(11)两边的 x_j 都替换成 x_i 后得知 $q(x_1,\ldots,x_{j-1},x_i,x_{j+1},\ldots,x_n)=0$. 这说明 $g_r|q$, 也就是说，存在多项式 q_1 使 $q=g_rq_1$. 代入(11) 即得 $f=g_1\cdots g_rq_1$. □

重温Vandermonde 行列式

把

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ & & \cdots & \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

看成多项式，记作 $f(x_1, \ldots, x_n)$. 则

$$\deg(f) = \frac{n(n-1)}{2}.$$

由于 $f(x_1, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n) = 0$ 对任何 $1 \le i < j \le n$ 成立，因此 $(x_j - x_i)|f$. 所以

$$\prod_{1 \le i < j \le n} (x_j - x_i)|f.$$

比较次数后得知存在 $c \in K$ 使

$$f = c \prod_{1 \le i < j \le n} (x_j - x_i).$$

f 中含一项 $x_2 x_3^2 \cdots x_n^{n-1}$. 而这一项在 $\prod_{1 \le i < j \le n} (x_j - x_i)$ 中的系数也是1. 所以 $c = 1$. 因此

$$f = \prod_{1 \le i < j \le n} (x_j - x_i).$$

齐次多项式

设 d 是一个非负整数。假如多项式 $f(x_1, \ldots, f_n)$ 的每项的次数都等于 d 则 $f(x_1, \ldots, x_n)$ 称作一个 d 次齐次多项式（或 d 次型）。规定 0 是任意次齐次多项式。

例13. $x_1 + 3x_4$ 是一个一次型（或线性型）。

$2x_1 + x_2 - 1$ 不是齐次多项式。

$x_1^n + x_2^n - x_3 x_4^{n-1}$ 是一个 n 次型。

基本性质：

1）两个 d 次型的和或差是 d 次型。

2）d_1 次型和 d_2 次型的乘积是 $d_1 + d_2$ 次型。

3）d 次型全体构成一个有限维向量空间，维数为 C_{n+d-1}^d.

4) 任何一个多项式 $f(x_1, \ldots, x_n)$ 可以唯一地表示成

$$f(x_1, \ldots, x_n) = \sum_{d \geq 0} f_d(x_1, \ldots, x_n)$$

其中 $f_d(x_1, \ldots, x_n)$ 是 d 次型。

5) 设 $f(x_1, \ldots, x_n)$ 是一个 d 次型，则对任何 $c \in K$ 等式$f(cx_1, \ldots, cx_n) = c^d f(x_1, \ldots, x_n)$ 成立。

特别，如果 $f(a_1, \ldots, a_n) = 0$ 则 $f(ca_1, \ldots, ca_n) = 0$ 对任何$c \in K$ 成立。

作业：

p.215: 1,2,3

对称多项式

设 $f(x_1,\ldots,x_n)\in K[x_1,\ldots,x_n]$ 满足下面（等价的）两个条件中的一个，则称 $f(x_1,\ldots,x_n)$ 为一个对称多项式：

1）$f(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n)$

$$=f(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$$

对任何 $1\le i<j\le n$ 成立；

2）$f(x_1,\ldots,x_n)=f(x_{\sigma(1)},\ldots,x_{\sigma(n)})$ 对$1,\ldots,n$ 的任何一个置换都成立。

例14. 令 $n=3$.

$$x_1^r+x_2^r+x_3^r,$$

$$x_1x_2+x_2x_3+x_1x_3-x_1x_2x_3,$$

$$(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$$

都是对称多项式。

$$x_1+x_2-x_3,$$

$$(x_1-x_2)(x_2-x_3)(x_3-x_1)$$

都不是对称多项式。

基本性质：

1）对称多项式的和、差、积仍是对称多项式；

2）设 $f_1(x_1,\ldots,x_n),\ldots,f_k(x_1,\ldots,x_n)$ 都是对称多项式， $g(y_1,\ldots,y_k)\in K[y_1,\ldots,y_k]$. 则

$$g(f_1(x_1,\ldots,x_n),\ldots,f_k(x_1,\ldots,x_n))$$

仍然是对称多项式。

例15. $(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2-(x_1+x_2+x_3)^4$ 是对称多项式。

初等对称多项式：

$$\sigma_1 = x_1 + \cdots + x_n = \sum_{i=1}^{n} x_i,$$

$$\sigma_2 = \sum_{1 \leq i \leq jn} x_i x_j,$$

$$\cdots$$

$$\sigma_n = x_1 \cdots x_n.$$

例16.

$$(x - x_1)(x - x_2) \cdots (x - x_n)$$
$$= x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \cdots + (-1)^n \sigma_n.$$

定理52. 设 $f(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$ 是一个对称多项式，则存在唯一的 $g(y_1,\ldots,y_n) \in K[y_1,\ldots,y_n]$ 使$f(x_1,\ldots,x_n) = g(\sigma_1,\ldots,\sigma_n)$.

例17. 设 $n=3$,

$$f(x_1,x_2,x_3) = x_1^2x_2+x_2^2x_3+x_3^2x_1+x_2^2x_1+x_3^2x_2+x_1^2x_3.$$

由于

$$\sigma_1\sigma_2 = (x_1+x_2+x_3)(x_1x_2+x_2x_3+x_3x_1)$$

$$= x_1^2x_2+x_2^2x_3+x_3^2x_1+x_2^2x_1+x_3^2x_2+x_1^2x_3+3x_1x_2x_3,$$

所以

$$f-\sigma_1\sigma_2 = -3x_1x_2x_3 = -3\sigma_3.$$

因此

$$f = \sigma_1\sigma_2 - 3\sigma_3.$$

也就是说 $g(y_1,y_2,y_3) = y_1y_2 - 3y_3$ 满足定理的要求。

定理的证明：

(存在性)

设 $f(x_1,\ldots,x_n)$ 按字典式排列的首项是 $ax_1^{e_1}\cdots x_n^{e_n}$. 则 $e_1\geq e_2\geq\cdots\geq e_n$.

令 $g_1(y_1,\ldots,y_n)=ay_1^{e_1-e_2}\cdots y_{n-1}^{e_{n-1}-e_n}y_n^{e_n}$. 则 $g_1(\sigma_1,\ldots,\sigma_n)$ 的首项是

$$ax_1^{e_1-e_2}(x_1x_2)^{e_2-e_3}\cdots(x_1\ldots x_{n-1})^{e_{n-1}-e_n}(x_1\cdots x_n)^{e_n}$$

$$=ax_1^{e_1}\cdots x_n^{e_n}.$$

令$f_1(x_1,\ldots,x_n)=f(x_1,\ldots,x_n)-g_1(\sigma_1,\ldots,\sigma_n)$. 则 $f(x_1,\ldots,x_n)$ 的首项先于 $f_1(x_1,\ldots,x_n)$ 的首项，并且$\deg(f)\geq\deg(f_1)$.

重复以上过程，得序列

$$f_1=f-g_1(\sigma_1,\ldots,\sigma_n),$$

$$f_2=f_1-g_2(\sigma_1,\ldots,\sigma_n),$$

$$\cdots$$

满足条件：

1) f_i 的首项先于 f_{i+1} 的首项；

2) $\deg(f_i)\geq\deg(f_{i+1})$.

这样的序列不能是无限的。因此存在 r, 使$f_r=f_{r-1}-g_r(\sigma_1,\ldots,\sigma_n)=0$. 所以

$$f=g_1(\sigma_1,\ldots,\sigma_n)+\cdots+g_r(\sigma_1,\ldots,\sigma_n).$$

(唯一性)

假定 $g(y_1,\ldots,y_n),h(y_1,\ldots,y_n)\in K[y_1,\ldots,y_n]$ 是两个不同的多项式满足

$$g(\sigma_1,\ldots,\sigma_n)=h(\sigma_1,\ldots,\sigma_n). \tag{12}$$

令 $u(y_1,\ldots,y_n) = g(y_1,\ldots,y_n)-h(y_1,\ldots,y_n)$. 则$u(y_1,\ldots,y_n)\neq 0$.

设 $ay_1^{e_1}\cdots y_n^{e_n}$ 是 $u(y_1,\ldots,y_n)$ 的任意一个非零项。则 $a\sigma_1^{e_1}\cdots\sigma_n^{e_n}$ 展开以后按字典式排列的首项是

$$ax_1^{e_1+\cdots+e_n}x_2^{e_2+\cdots+e_n}\cdots x_n^{e_n}.$$

所有这些首项是互不相同的，所以 $u(\sigma_1,\ldots,\sigma_n)\neq 0$, 与条件(12) 矛盾。 □

齐次对称多项式的简便算法

设 $cx_1^{e_1}\cdots x_n^{e_n}$ 是一个单项式，正数列$(e_1,\ldots,e_n)$叫做该单项式的指数组。$e_1+\cdots+e_n$ 叫做该指数组的次数。在 $e_1,\ldots,e_n$ 的一切排列中一定有一组是递降的。所以一个对称多项式 f 的首项的指数组满足条件

$$e_1\geq e_2\geq\cdots\geq e_n.$$

找 $\sigma_1^{d_1}\ldots,\sigma_n^{d_n}$ 使其展开式的首项指数组是$(e_1,\ldots,e_n)$. 则有某个常数 c 使 $f_1=f-c\sigma_1^{d_1}\ldots,\sigma_n^{d_n}$ 的首项后于 f 的首项，如果 f 是齐次多项式，则 f_1 也是齐次多项式。按照标准算法，需要找到 f_1 的首项，... 这会牵涉到比较麻烦的计算。可以通过待定系数法来避免之。

例18.

$f(x_1,x_2,x_3)=x_1^2x_2+x_2^2x_3+x_3^2x_1+x_2^2x_1+x_3^2x_2+x_1^2x_3.$

首项指数组是 $(2,1,0)$. 后于它的 3 次递减指数组只有 $(1,1,1)$. 因此

$$f=a\sigma_1\sigma_2+b\sigma_3, \tag{13}$$

其中 a,b 是待定系数。

分别用 $x_1=1,x_2=1,x_3=0$ 和 $x_1=1,x_2=1,x_3=1$ 代入(13)两边得

$$2=2a,$$

$$6=9a+b.$$

解得 $a=1,b=-3$.

例19. 设 $f(x_1,x_2,x_3)=(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$.

它的首项是 $x_1^4x_2^2$, 其指数组是 $(4,2,0)$. 后于它的 6 次递减指数组全体为

$$(4,1,1),(3,3,0),(3,2,1),(2,2,2).$$

于是

$$f(x_1,x_2,x_3)=\sigma_1^2\sigma_2^2+a\sigma_1^3\sigma_3+b\sigma_2^3+c\sigma_1\sigma_2\sigma_3+d\sigma_3^2.$$

$$\begin{gathered}0=f(1,1,0)=4+b,\\ 0=f(1,1,1)=81+27b+27b+9c+d,\\ 0=f(2,-1,-1)=-27b+4d,\\ 0=f(2,2,-1)=-108a+16d.\end{gathered}$$

解得 $a=-4,b=-4,c=18,d=-27$.

记 $s_k = x_1^k + \cdots + x_n^k$. 这是对称多项式。

$$s_{k-1}\sigma_1 = (x_1^{k-1} + \cdots + x_n^{k-1})(x_1 + \cdots + x_n)$$
$$= x_1^k + \cdots + x_n^k + \sum_{i \neq j} x_i^{k-1} x_j.$$

$$s_{k-2}\sigma_2 = (x_1^{k-2} + \cdots + x_n^{k-2})(x_1 x_2 + \cdots + x_{n-1} x_n)$$
$$= \sum_{i \neq j} x_i^{k-1} x_j + \sum x_i^{k-2} x_j x_l.$$

上式的第二个和式中 i, j, l 跑遍所有满足 $j < l, i \neq j, i \neq l$ 的指标。如果 $k > 3$ 则这个表达式实际上是包含单项式 $x_1^{k-2} x_2 x_3$ 的最小的对称多项式。

对任何 $r > 1, t > 1$,用记号 $S(x_1^r x_2 \ldots x_t)$ 来表示包含 $x_1^r x_2 \ldots x_t$ 的最小的对称多项式。

在这个记号下上面两个等式可写成

$$s_{k-1}\sigma_1 = s_k + S(x_1^{k-1} x_2),$$
$$s_{k-2}\sigma_2 = S(x_1^{k-1} x_2) + S(x_1^{k-2} x_2 x_3).$$

例20 (Newton 公式)**.** 若 $k \leq n$, 则

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 + \cdots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^k k\sigma_k = 0;$$

若 $k > n$, 则

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 + \cdots + (-1)^n s_{k-n}\sigma_n = 0.$$

证明：先设 $k \leq n$. 根据

$$\begin{gathered}
s_{k-1}\sigma_1 = s_k + S(x_1^{k-1}x_2),\\
s_{k-2}\sigma_2 = S(x_1^{k-1}x_2) + S(x_1^{k-2}x_2x_3),\\
\cdots\\
s_2\sigma_{k-2} = S(x_1^3x_2\cdots x_{k-2}) + S(x_1^2x_2\cdots x_{k-1}),\\
s_1\sigma_{k-1} = S(x_1^2x_2\cdots x_{k-1}) + k\sigma_k.
\end{gathered}$$

把以上等式交错相加即得第一个等式。

再设 $k > n$. 将

$$\begin{gathered}
s_{k-1}\sigma_1 = s_k + S(x_1^{k-1}x_2),\\
s_{k-2}\sigma_2 = S(x_1^{k-1}x_2) + S(x_1^{k-2}x_2x_3),\\
\cdots\\
s_{k-n+1}\sigma_{n-1} = S(x_1^{k-n+2}x_2\cdots x_{n-1}) + S(x_1^{k-n+1}x_2\cdots x_n),\\
s_{k-n}\sigma_n = S(x_1^{k-n+1}x_2\cdots x_n)
\end{gathered}$$

交错相加即得第二个等式。 □

例21 (p.224.2)**.** 设 $f(x)=x^3+px^2+qx+r$. 求出方程 $f(x)=0$ 的某个根的平方等于另外两个根的乘积的充要条件。

解：设 x_1,x_2,x_3 是 $f(x)=0$ 三个根，则某个根的平方等于另外两个根的乘积的充要条件是

$$(x_1^2-x_2x_3)(x_2^2-x_1x_3)(x_3^2-x_1x_2)=0.$$

将 $g(x_1,x_2,x_3)=(x_1^2-x_2x_3)(x_2^2-x_1x_3)(x_3^2-x_1x_2)$ 通过初等对称多项式表出：

$g(x_1,x_2,x_3)$ 的首项指数组是 $(4,1,1)$. 排在它后面的指数组有：$(3,3,0),(3,2,1),(2,2,2)$. 所以

$$g(x_1,x_2,x_3)=\sigma_1^3\sigma_3+a\sigma_2^3+b\sigma_1\sigma_2\sigma_3+c\sigma_3^2,$$

其中 a,b,c 是待定系数。

$$-1=g(1,1,0)=a,$$
$$27=g(1,1,-2)=-27a-8c,$$
$$0=g(1,1,1)=27+27a+9b+c.$$

解得 $a=-1,b=0,c=0$. 也就是说$(x_1^2-x_2x_3)(x_2^2-x_1x_3)(x_3^2-x_1x_2)=\sigma_1^3\sigma_3-\sigma_2^3=p^3r-q^3$.

答：所求充要条件是 $p^3r-q^3=0$. □

作业：p.220
1(1),2,3,4,6

结式与判别式

设

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n,$$

$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$$

是两个正次数的单变量多项式，其中 $a_0 \neq 0, b_0 \neq 0$.

考虑 $m+n$ 阶矩阵

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_n & & & \\ & a_0 & a_1 & \cdots & a_n & & \\ & & \ddots & & \ddots & & \\ & & & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & & & \\ & b_0 & b_1 & \cdots & b_m & & \\ & & \ddots & & \ddots & & \\ & & & b_0 & b_1 & \cdots & b_m \end{pmatrix}.$$

例如当 $n=2, m=3$ 时

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & & \\ & a_0 & a_1 & a_2 & \\ & & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & \\ & b_0 & b_1 & b_2 & b_3 \end{pmatrix}.$$

引理53. 设 $f(x), g(x)$ 是两个非零多项式，则 $\gcd(f,g)$ 的次数大于零当且仅当存在 $u(x), v(x)$ 满足

1）$f(x)u(x) = g(x)v(x)$;

2) $0 \leq \deg(u) < \deg(g)$, $0 \leq \deg(v) < \deg(f)$.

证明：$\Rightarrow$: 设 $d(x) = \gcd(f,g)$. 取$u(x) = g(x)/d(x), v(x) = f(x)/d(x)$ 即可。

$\Leftarrow$: 如果 $\gcd(f,g)$ 的次数等于零，则 f, g 互素，于是由条件1）知 $f(x)|v(x)$. 因此 $\deg(f) \leq \deg(v)$, 与条件2）矛盾。□

回到开始的问题。假定 f,g 不互素，则存在非零的

$$u(x)=c_0x^{m-1}+c_1x^{m-2}+\cdots+c_{m-1},$$

$$v(x)=d_0x^{n-1}+d_1x^{n-2}+\cdots+d_{n-1}$$

使 $f(x)u(x)-g(x)v(x)=0$.

于是

$$(c_0,\ldots,c_{m-1},-d_0,\ldots,-d_{n-1})A\begin{pmatrix}x^{m+n-1}\\ \vdots\\ x\\ 1\end{pmatrix}$$

$$=(c_0,\ldots,c_{m-1},-d_0,\ldots,-d_{n-1})\begin{pmatrix}x^{m-1}f(x)\\ x^{m-2}f(x)\\ \vdots\\ f(x)\\ x^{n-1}g(x)\\ x^{n-2}g(x)\\ \vdots\\ g(x)\end{pmatrix}$$

$$=f(x)u(x)-g(x)v(x)=0.$$

这表明

$$(c_0,\ldots,c_{m-1},d_0,\ldots,d_{n-1})A=(0,\ldots,0).$$

因此 $|A|=0$.

反过来，设 $|A|=0$. 则存在非零行向量

$$(c_0,\ldots,c_{m-1},-d_0,\ldots,-d_{n-1})$$

满足

$$(c_0,\ldots,c_{m-1},-d_0,\ldots,-d_{n-1})A=(0,\ldots,0).$$

由于矩阵 A 的前 m 行线性无关，后 n 行也线性无关，所以$c_0,\ldots,c_{m-1}$ 不全为零，$d_0,\ldots,d_{n-1}$ 也不全为零。

令

$$u(x)=c_0x^{m-1}+c_1x^{m-2}+\cdots+c_{m-1},$$

$$v(x)=d_0x^{n-1}+d_1x^{n-2}+\cdots+d_{n-1}.$$

则

$$f(x)u(x)-g(x)v(x)$$

$$=(c_0,\ldots,c_{m-1},-d_0,\ldots,-d_{n-1})\begin{pmatrix} x^{m-1}f(x)\\ x^{m-2}f(x)\\ \vdots\\ f(x)\\ x^{n-1}g(x)\\ x^{n-2}g(x)\\ \vdots\\ g(x)\end{pmatrix}$$

$$= (c_0, \ldots, c_{m-1}, -d_0, \ldots, -d_{n-1}) A \begin{pmatrix} x^{m+n-1} \\ \vdots \\ x \\ 1 \end{pmatrix} = 0.$$

由引理得知 $f(x), g(x)$ 不互素。

定义12. 行列式 $|A|$ 称为多项式 $f(x)$ 和 $g(x)$ 的**结式**(resultant), 记作 $R(f,g)$.

归纳一下，我们证明了

定理54. 多项式 $f(x)$ 和 $g(x)$ 互素当且仅当 $R(f,g) \neq 0$.

定理55. 多项式 $f(x)$ 和 $g(x)$ 有公共复根当且仅当 $R(f,g) = 0$.

定理56. 设 $x_1,\dots,x_n,y_1,\dots,y_m\in K$, a,b 是 K 中非零数，

$$f(x)=a(x-x_1)\cdots(x-x_n),$$

$$g(x)=b(x-y_1)\cdots(x-y_m).$$

则

$$\begin{aligned}R(f,g)&=a^mb^n\prod_{1\le i\le n,1\le j\le m}(x_i-y_j)\\&=a^m\prod_{1\le i\le n}g(x_i)\\&=(-1)^{mn}b^n\prod_{1\le j\le m}f(y_j).\end{aligned}$$

证明：不妨设 $a=b=1$. 则

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

$$g(x)=x^m+b_1x^{m-1}+\cdots+b_m,$$

其中

$$a_1=-(x_1+\cdots+x_n),$$

$$\cdots$$

$$a_n=(-1)^nx_1\cdots x_n,$$

$$b_1=-(y_1+\cdots+y_m),$$

$$\cdots$$

$$b_m = (-1)^m y_1 \cdots y_m.$$

所以若把 $x_1, \ldots, x_n, y_1, \ldots, y_m$ 看成变量，则 $R(f,g) \in K[x_1, \ldots, x_n, y_1, \ldots, y_m]$.

将 $f(x)$ 中的 x_i 用 y_j 替换后 $f(x)$ 和 $g(x)$ 不互素，由上面的定理知道此时 $R(f,g) = 0$. 所以 $(x_i - y_j)|R(f,g)$ 对任何 $1 \leq i \leq n, 1 \leq j \leq m$ 成立。因此

$$\prod_{1\leq i\leq n, 1\leq j\leq m} (x_i - y_j)|R(f,g).$$

比较次数得

$$R(f,g) = c \prod_{1\leq i\leq n, 1\leq j\leq m} (x_i - y_j), \qquad (14)$$

其中 c 是一个非零常数。

将 $x_1 = \cdots = x_n = 0$ 代入(14) 式得

$$b_m^n = \begin{vmatrix} 1 &&&&&&& \\ & 1 &&&&&& \\ && \ddots &&&&& \\ &&& 1 &&&& \\ 1 & b_1 & \cdots && b_m &&& \\ & 1 & b_1 & \cdots && b_m && \\ &&&&&\ddots&& \\ &&& 1 & b_1 & \cdots && b_m \end{vmatrix}$$

$$= c \prod_{1 \leq j \leq m} (-y_j)^n = c[(-1)^m y_1 \cdots y_m]^n = c b_m^n.$$

因此 $c = 1$.

其它两个等式的证明比较明显。□

定义13. 设 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, 其中 $n > 1, a_0 \neq 0$. 则

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{-1} R(f, f')$$

称为 f 的**判别式**(discriminant).

定理57. 设 $f(x) = a_0(x - x_1) \cdots (x - x_n)$. 则

$$\begin{aligned}\Delta(f) &= a_0^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} a_0^{2n-2} \prod_{i \neq j} (x_i - x_j)\end{aligned}$$

证明：由上面定理知

$$R(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(x_i).$$

而 $f'(x) = a_0 \sum_{i=1}^{n} (x - x_1) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_n)$. 因此

$$f'(x_i) = a_0(x_i - x_1) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_n),$$

由此得到

$$\prod_{i=1}^{n} f'(x_i) = a_0^n \prod_{i \neq j} (x_i - x_j),$$

即
$$R(f,f') = a_0^{2n-1}\prod_{i\neq j}(x_i - x_j).$$
代入 $\Delta(f)$ 的定义式即得所需。 □

例22. $n = 2$.

$$\prod_{1\leq i<j\leq 2}(x_i - x_j)^2 = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2$$
$$= (\frac{a_1}{a_0})^2 - \frac{4a_2}{a_0}.$$
所以
$$\Delta(f) = a_1^2 - 4a_0a_2. \tag{15}$$

也可直接计算

$$R(f,f') = \begin{vmatrix} a_0 & a_1 & a_2 \\ 2a_0 & a_1 & 0 \\ 0 & 2a_0 & a_1 \end{vmatrix}$$
$$= -a_0a_1^2 + 4a_0^2a_2.$$
代入定义式得(15) 式。

例23 (p.233-20)**.** 求参数曲线

$$x=\frac{2(t+1)}{t^2+1}, y=\frac{t^2}{2t-1}$$

的直角坐标方程。

解：映射

$$f:\mathbb{R}\backslash\{\frac{1}{2}\}\to\mathbb{R}^2$$

$$t\mapsto(\frac{2(t+1)}{t^2+1},\frac{t^2}{2t-1})$$

的象 C 就是所涉及的曲线。

先证明：平面上的点 (x,y) 在曲线 C 上当且仅当存在某个实数 t 使

$$2(t+1)-(t^2+1)x=0, t^2-(2t-1)y=0 \quad (16)$$

同时成立。

$\Leftarrow$: 从(16)中第二个方程知道 $t\neq 1/2$. 于是

$$x=\frac{2(t+1)}{t^2+1}, y=\frac{t^2}{2t-1}.$$

这表明 $(x,y)\in C$.

$\Rightarrow$: 设 $(x,y)\in C$. 则存在 $t\in\mathbb{R}\backslash\{1/2\}$ 使

$$x=\frac{2(t+1)}{t^2+1}, y=\frac{t^2}{2t-1}.$$

因此(16) 成立。

将(16) 中两个方程的左边看成关于变量 t 的多项式$f(t), g(t)$，则刚才所证的结果表示 $(x, y) \in C$ 当且仅当 $f(t)$ 和$g(t)$ 有公共零点。也就是说 $(x, y) \in C$ 当且仅当

$$R(f, g) = 0.$$

上式正是所求的方程。

答：所求方程是

$$5x^2y^2 - 2x^2y + 4 - 4x + x^2 - 12xy^2 + 12y.$$

例24. 设 C 是空间中两个曲面

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

和

$$xyz - x^2 + y^3 - z^2 + 3 = 0$$

的交。求 C 在 x, y 平面的投影的方程。

解：x, y 平面上的点 (x, y) 在 C 的投影上当且仅当存在 z 使两个方程同时成立。把这两个方程的左边看作变量 z 的多项式$f(z), g(z)$。则 (x, y) 在 C 的投影上当且仅当

$$R(f, g) = 0.$$

上式就是所求方程。

作业：

p.226:

1(1),2,3,5,6,7

多项式习题选

例25 (p.188,6)**.** 设 $g(x) = ax^2 + bx + c$, 且 $abc \neq 0$, $f(x) = x^3 + px^2 + qx + r$. 若$g(x)|f(x)$, 则

$$\frac{ap-b}{a} = \frac{aq-c}{b} = \frac{ar}{c}.$$

证明：由于 $g(x)|f(x)$, 存在 $d \in K$ 使

$$f(x) = (\frac{x}{a} + \frac{d}{a})g(x).$$

将上式两边同乘 a 后展开得

$$ax^3+apx^2+aqx+ar = ax^3+(b+ad)x^2+(c+bd)x+cd.$$

比较两边系数得

$$d = \frac{ap-b}{a} = \frac{aq-c}{b} = \frac{ar}{c}.$$

□

例26. 设 $f(x)$ 是数域 K 上的 n 次多项式，$n \geq 1, a \in K$. 求证

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

证明：将 $f(y+a)$ 展开成一个关于变量 y 的多项式

$$f(y+a) = b_0 + b_1 y + b_2 y^2 + \cdots + b_n y^n. \qquad (17)$$

再将 $y = x - a$ 代入上式即得

$$f(x) = b_0 + b_1(x-a) + b_2(x-a)^2 + \cdots + b_n(x-a)^n. \qquad (18)$$

我们来决定系数 $b_0, b_1, \ldots, b_n$.

对任意 $0 \leq j \leq n$, 对(18)两边求 j 阶导数得

$$f^{(j)}(x) = (j!)b_j + (x-a)h(x).$$

将 $x = a$ 代入上式即得

$$b_j = \frac{f^{(j)}(a)}{j!}.$$

□

例27 (p.201,2)**.** 求证 a 是非零多项式 $f(x)$ 的 k 重零点的充要条件是$f(a)=f'(a)=\cdots=f^{(k-1)}(a)=0$, $f^{(k)}(a)\neq 0$.

证明：由上题知

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

由于 $f(x)\neq 0$, 数$f(a),f'(a),\ldots,f^{(n)}(a)$ 不全为零。设$f(a)=f'(a)=\cdots=f^{(r-1)}(a)=0, f^{(r)}(a)\neq 0$. 则

$$f(x)=(x-a)^r[\frac{f^{(r)}(a)}{r!}+(x-a)h(x)].$$

由于 a 不是 $\frac{f^{(n)}(a)}{r!}+(x-a)h(x)$ 的零点，$(x-a)^{r+1}\not|f(x)$. 因此 a 是 $f(x)$ 的 r 重零点。 □

例28 (p.206,1). 设方程 $x^3+px^2+qx+r=0$ 的三个根成等差数列，求证

$$2p^3-9pq+27r=0.$$

证明：设三个根为 $a-d,a,a+d$. 则有

$$3a=-p,3a^2-d^2=q,a(a^2-d^2)=-r.$$

代入 $2p^3-9pq+27r$ 计算即可。□

例29 (p.207,3)**.** 设多项式 x^3+3x^2+mx+n 的三个根成等差数列，而多项式$x^3-(m-2)x^2+(n-3)x+8$ 的三个根成等比数列，求 m 和 n.

证明：设 x^3+3x^2+mx+n 的三个根为 $a-d, a, a+d$. 则

$$3a=-3, 3a^2-d^2=m, a(a^2-d^2)=-n.$$

得

$$m=3-d^2, n=1-d^2.$$

从而

$$m=n+2 \tag{19}$$

设 $x^3-(m-2)x^2+(n-3)x+8$ 的三个根为 $b/q, b, bq$. 则

$$b^3=-8.$$

故 $b=-2$. 现在 $x^3-(m-2)x^2+(n-3)x+8$ 的三个根为 $-2/q, -2, -2q$. 进一步有等式

$$m-2=-2(\frac{1}{q}+1+q).$$

$$n-3=4(\frac{1}{q}+1+q).$$

得

$$n-3=-2(m-2) \tag{20}$$

解(19)和(20)组成的方程组得

$$m = 3, n = 1.$$

□

例30 (p.207,4)**.** 证明方程 $x^3+px+q=0$ 有重根的充分必要条件是

$$4p^3+27q^2=0.$$

证明：记 $f(x)=x^3+px+q$. 则$x^3+px+q=0$ 有重根的充分必要条件是$\gcd(f(x),f'(x))\neq 1$.

$f'(x)=3x^2+p$. 故

$$f(x)=\frac{1}{3}xf'(x)+(\frac{2}{3}px+q).$$

于是

$$\gcd(f(x),f'(x))=\gcd(3x^2+p,\frac{2}{3}px+q).$$

如果 $p=0$, 则

$$\gcd(3x^2+p,\frac{2}{3}px+q)\neq 1$$

当且仅当 $q=0$.

以下设 $p\neq 0$. 则

$$\gcd(3x^2+p,\frac{2}{3}px+q)\neq 1$$

当且仅当 $\frac{2}{3}px+q$ 的零点也是 $3x^2+p$ 的零点。而$\frac{2}{3}px+q$ 的零点是 $-\frac{3q}{2p}$, 代入方程

$$3x^2 + p = 0$$

得

$$\frac{27q^2}{4p^2} + p = 0,$$

等价于条件

$$4p^3 + 27q^2 = 0.$$

□

例31 (p.207,6). 设 $f(x) \in \mathbb{C}[x]$, 若对所有 $c \in \mathbb{R}$ 都有$f(c) \in \mathbb{R}$, 则 $f(x) \in \mathbb{R}[x]$.

证明：

证法1）

求证的命题等价于下列命题：

设 $f(x) \in \mathbb{C}[x]$ 且 $f(x) \notin \mathbb{R}[x]$. 则存在$\alpha \in \mathbb{R}$ 使 $f(\alpha) \notin \mathbb{R}$.

我们来证明后一命题。

设

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

设 $a_j = b_j + ic_j, (j = 0, \ldots, n)$, 其中 $b_j, c_j \in \mathbb{R}$. 记

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0.$$

$$h(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0.$$

则 $g(x), h(x) \in \mathbb{R}[x], f(x) = g(x)+ih(x)$ 且 $h(x) \neq 0$.

由于 $h(x)$ 在 $\mathbb{R}$ 中至多只有有限多个零点，存在 $\alpha \in \mathbb{R}$ 使 $h(\alpha) \neq 0$. 于是 $f(\alpha) = g(\alpha)+ih(\alpha) \notin \mathbb{R}$. □

证法2）
设

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

任取 $n+1$ 个两两不同的实数 $b_0, b_1, \ldots, b_n$. 设

$$c_0 = f(b_0), c_1 = f(b_1), \ldots, c_n = f(b_n).$$

根据给定条件 $c_0, c_1, \ldots, c_n \in \mathbb{R}$.
以 $y_n, y_{n-1}, \ldots, y_1, y_0$ 为变量，线性方程组

$$b_0^n y_n + b_0^{n-1} y_{n-1} + \cdots + b_0 y_1 + y_0 = c_0,$$

$$b_1^n y_n + b_1^{n-1} y_{n-1} + \cdots + b_1 y_1 + y_0 = c_1,$$

$$\cdots$$

$$b_n^n y_n + b_n^{n-1} y_{n-1} + \cdots + b_n y_1 + y_0 = c_n$$

有唯一解（为什么？），并且由Cramer 法则这个解是实数解。然而，$a_n, a_{n-1}, \ldots, a_0$ 是这个方程组的解。所以$a_n, a_{n-1}, \ldots, a_0 \in \mathbb{R}$. □

例32 (p.227-9, 1984 年上海市数学竞赛试题). 设

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_n)-1,$$

其中 $a_1, a_2, \ldots, a_n$ 是两两互不相同的整数，求证 $f(x)$ 在有理数内不可约。

证明：（反证法）假定 $f(x)$ 在有理数内可约,则存在次数小于 $\deg(f)$ 的两个整系数多项式 $g(x), h(x)$ 使

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

因 $f(x)$ 是首一多项式，可设 $g(x)$ 和 $h(x)$ 也是首一多项式。记$r = \deg(g), s = \deg(h)$. 则

$$r + s = n.$$

对每个 a_i 都有 $f(a_i) = -1$. 因此

$$g(a_i)h(a_i) = -1$$

对 $i = 1, \ldots, n$ 成立。然而 $g(a_i)$ 和 $h(a_i)$ 都是整数，因此$g(a_i), h(a_i)$ 中一个等于1，另一个等于-1。不妨设

$$g(a_1) = \cdots = g(a_k) = 1,$$

$$g(a_{k+1}) = \cdots = g(a_n) = -1.$$

则 $k \le r, n-k \le r$. 故 $n \le 2r$. 同理 $n \le 2s$. 所以$n = 2r = 2s$, 否则会有 $2n < 2(r+s) = 2n$. 同理推得 $k = r$.

由于 $a_1, \ldots, a_r$ 是 r 次首一多项式 $g(x)-1$ 的 r 个两两不同的零点，故有

$$g(x)-1=(x-a_1)\cdots(x-a_r).$$

而 $a_1, \ldots, a_r$ 也是 r 次首一多项式 $h(x)+1$ 的 r 个两两不同的零点, 因此

$$h(x)+1=(x-a_1)\cdots(x-a_r).$$

所以

$$g(x)h(x)+1=(x-a_1)^2\cdots(x-a_r)^2.$$

由此推出

$$(x-a_1)\cdots(x-a_n)=(x-a_1)^2\cdots(x-a_r)^2.$$

这不可能。 □

复习

方程 $x^n - 1 = 0$ 有 n 个复根

$$cos(\frac{2k\pi}{n}) + isin(\frac{2k\pi}{n}),$$

$k = 0, 1, \ldots, n-1.$

记 $\omega = cos(\frac{2\pi}{n}) + isin(\frac{2\pi}{n})$, 那么这 n 个根可以写成 $1, \omega, \omega^2, \ldots, \omega^{n-1}$.

在 $\mathbb{C}[x]$ 中有分解式

$$x^n - 1 = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1})$$

和

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

方程 $x^n + 1 = 0$ 有 n 个复根

$$cos(\frac{(2k+1)\pi}{n}) + isin(\frac{(2k+1)\pi}{n}),$$

$k = 0, 1, \ldots, n-1.$

当 $n = 2m$ 是偶数时这 n 个根也可写成

$$cos(\pm\frac{(2k+1)\pi}{n}) + isin(\pm\frac{(2k+1)\pi}{n}),$$

$k = 0, 1, \ldots, (m-1).$

而

$$cos(\frac{(2k+1)\pi}{n}) + isin(\frac{(2k+1)\pi}{n})$$

和

$$cos(-\frac{(2k+1)\pi}{n})+isin(-\frac{(2k+1)\pi}{n})$$

是互相共轭的。

例33 (p.201,1(2)). 求证

$$x^4+x^3+x^2+x+1|x^5+x^{11}+x^{17}+x^{23}+x^{29}.$$

证法1）
带余除法。
证法2）

$$\begin{aligned}
&(x-1)(x^5+x^{11}+x^{17}+x^{23}+x^{29})\\
=&\,x^6+x^{12}+x^{18}+x^{24}+x^{30}-x^5-x^{11}-x^{17}-x^{23}-x^{29}\\
=&\,(x^{30}-x^5)+(x^6-x^{11})+(x^{12}-x^{17})+(x^{18}-x^{23})+(x^{24}-x^{29})\\
=&\,x^5(x^{25}-1)-x^6(x^5-1)-x^{12}(x^5-1)-x^{18}(x^5-1)-x^{24}(x^5-1).
\end{aligned}$$

因此

$$(x-1)(x^5+x^{11}+x^{17}+x^{23}+x^{29})=(x^5-1)h(x).$$

从而得

$$x^5+x^{11}+x^{17}+x^{23}+x^{29}=(x^4+x^3+x^2+x+1)h(x).$$

证法3）

记

$$\omega = cos(\frac{2\pi}{5}) + isin(\frac{2\pi}{5}),$$

则

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

记 $f(x) = x^5 + x^{11} + x^{17} + x^{23} + x^{29}$. 则

$$f(\omega) = \omega^5 + \omega^{11} + \omega^{17} + \omega^{23} + \omega^{29}$$
$$= 1 + \omega + \omega^2 + \omega^3 + \omega^4$$
$$= 0.$$

同理可验证 $f(\omega^2) = f(\omega^3) = f(\omega^4) = 0$. 因此

$$(x - \omega^i)|f(x)$$

对 $i = 1, 2, 3, 4$ 都成立，故有

$$(x - \omega)(x - \omega^2)(x - \omega^3)(x - \omega^4)|f(x).$$

□

例34（第五届美国数学奥林匹克试题）**.** 设

$$P(x), Q(x), R(s), S(x)$$

是多项式，满足

$$P(x^5)+xQ(x^5)+x^2R(x^5) = (x^4+x^3+x^2+x+1)S(x). \tag{21}$$

求证 $x-1$ 是 $P(x)$ 的一个因式。

证明：记

$$\omega_1 = cos(\frac{2\pi}{5}) + isin(\frac{2\pi}{5}),$$

$$\omega_2 = cos(\frac{4\pi}{5}) + isin(\frac{4\pi}{5}),$$

$$\omega_3 = cos(\frac{6\pi}{5}) + isin(\frac{6\pi}{5}),$$

则 $\omega_i^5 = 1$ 及 $\omega_i^4+\omega_i^3+\omega_i^2+\omega_i+1 = 0$ 对 $i = 1, 2, 3$ 成立。将 $\omega, \omega^2, \omega^3$ 分别代入(21)式两边得

$$P(1) + \omega_1 Q(1) + \omega_1^2 R(1) = 0,$$

$$P(1) + \omega_2 Q(1) + \omega_2^2 R(1) = 0,$$

$$P(1) + \omega_3 Q(1) + \omega_3^2 R(1) = 0.$$

这表示 $(P(1), Q(1), R(1))$ 是齐次线性方程组

$$x+\omega_1 y+\omega_1^2 z=0,$$

$$x+\omega_2 y+\omega_2^2 z=0,$$

$$x+\omega_3 y+\omega_3^2 z=0$$

的一组解。但这个方程组的解只能是 $(0,0,0)$, 所以 $P(1)=0$, 也就是说$(x-1)|P(x)$. $\square$

例35 (1981 年奥地利数学竞赛试题). 问自然数 n 为何值时

$$(x^2+x+1)|[x^{2n}+1+(x+1)^{2n}].$$

证明：记

$$\omega=cos(\frac{2\pi}{3})+isin(\frac{2\pi}{3}),$$

则

$$x^2+x+1=(x-\omega)(x-\omega^2),$$

$$\omega+1=-\omega^2,$$

$$\omega^2+1=-\omega.$$

记 $f(x)=x^{2n}+1+(x+1)^{2n}$, 则

$$(x^2+x+1)|[x^{2n}+1+(x+1)^{2n}]$$

当且仅当 $f(\omega)=f(\omega^2)=0$.

分三种情形讨论：

1）$n=3m$:

这时 $f(\omega)=3\neq 0$. 不满足条件。

2）$n=3m+1$:

这时

$$f(\omega)=\omega^2+1+\omega=0,$$

$$f(\omega^2)=\omega+1+\omega^2=0.$$

满足条件。

3）$n = 3m + 2$:

这时

$$f(\omega) = \omega + 1 + \omega^2 = 0,$$
$$f(\omega^2) = \omega^2 + 1 + \omega = 0.$$

满足条件。

结论是

$$(x^2 + x + 1) | [x^{2n} + 1 + (x+1)^{2n}]$$

当且仅当 $3 \nmid n$. □

例36 (p.211-7)**.** 证明 x^8+1 在有理数域上不可约。

证明：令 $x=y+1$, 则原多项式成为

$$y^8+8y^7+28y^6+56y^5+70y^4+56y^3+28y^2+8y+2,$$

根据Eisenstein 判别法这是有理数域上的不可约多项式。 □

例37（第29届Putnam数学竞赛试题）**.** 试确定所有形如 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ 的多项式($n > 0$)，其中 $a_0, a_1, \ldots, a_n$ 只能是 1 或 -1, 并且该多项式的全部零点都是实数。

解：如果有一个满足条件并且次数n大于2的多项式$f(x)$，不妨设$a_0 = 1$. 则

$$f(x) = (x - c_1) \cdots (x - c_n),$$

其中 $c_1, \ldots, c_n$ 全是实数。根据Vieta 定理有

$$c_1 + \cdots + c_n = -a_1,$$

$$\prod_{1 \le i < j \le n} c_i c_j = a_2,$$

$$(c_1 \cdots c_n)^2 = a_n^2 = 1.$$

推得

$$c_1^2 + \cdots + c_n^2 = (c_1 + \cdots + c_n)^2 - 2 \prod_{1 \le i < j \le n} c_i c_j = a_1^2 - 2a_2 = 1 - 2a_2.$$

根据不等式

$$\frac{c_1^2 + \cdots + c_n^2}{n} \ge (c_1^2 \cdots c_n^2)^{\frac{1}{n}}$$

有

$$\frac{1 - 2a_2}{n} \ge 1.$$

因此 $n \le 3$.

对 $1 \le n \le 3$ 的系数为 ± 1 的多项式逐一验证，得知符合题意的多项式为

$$\pm(x-1), \pm(x+1),$$

$$\pm(x^2+x-1), \pm(x^2-x-1),$$

$$\pm(x^3+x^2-x-1), \pm(x^3-x^2-x+1).$$

$\square$

作业

p.227

1) 提示：

如果

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

则

$$f(x)[u(x) - g(x)a(x)] + g(x)[v(x) + f(x)a(x)] = 1.$$

2) 3) 提示：用唯一因式分解定理。

6) 提示：考虑序列 $a, a^m, a^{m^2}, a^{m^3}, \ldots.$

7) 提示：零点个数。

多元多项式例题选

例38 (p.227,6)**.** 设 $f(x)$ 是一个首一多项式，已知 $\Delta(f(x))$, 求$\Delta(f(x^2))$.

解：设 $f(x)=(x-b_1)\cdots(x-b_n)$. 则

$$f(x^2)=(x^2-b_1)\cdots(x^2-b_n).$$

对 $1\le i\le n$ 设 c_i 是方程 $x^2-b_i=0$ 的一个根，则$x^2-b_i=(x-c_i)(x+c_i)$. 于是

$$\Delta(f(x^2))$$

$$=\prod_{i=1}^{n}(c_i-(-c_i))^2\cdot\prod_{i<j}(c_i-c_j)^2(c_i+c_j)^2\cdot\prod_{i<j}(-c_i-c_j)^2(-c_i+c_j)^2$$

$$=4^n\prod_{i=1}^{n}b_i\cdot\prod_{i<j}(c_i^2-b_j)^2\cdot\prod_{i<j}(c_i^2-b_j)^2$$

$$=(-4)^nf(0)\prod_{i<j}(b_i-b_j)^2\cdot\prod_{i<j}(b_i-b_j)^2$$

$$=(-4)^nf(0)\Delta(f(x))^2.\square$$

例39. 设 Δ 是实系数三次方程 $x^3+px+q=0$ 的判别式，求证

1）若 $\Delta<0$ 则方程有一个实根和两个共轭虚根；

2）若 $\Delta=0$ 则方程有三个实根且至少有两个根相同；

3）若 $\Delta>0$ 则方程有三个互不相同的实根。

证明：设 $x^3+px+q=(x-x_1)(x-x_2)(x-x_3)$. 则

$$\Delta=(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2.$$

我们知道 x_1,x_2,x_3 中至少有一个是实数，不妨设为 x_1.

1）设 $\Delta<0$.

假如 x_2,x_3 不是一对共轭的虚数，则它们全是实数，从而 $\Delta\geq 0$, 与给定条件矛盾。

2）设 $\Delta=0$.

假如 x_2,x_3 是一对共轭的虚数，则 x_1,x_2,x_3 两两不同，与$\Delta=0$ 矛盾。因此则方程有三个实根且至少有两个根相同。

3）设 $\Delta>0$.

假如 x_2,x_3 是一对共轭的虚数，则 x_2-x_3 是一个纯虚数，故$(x_2-x_3)^2<0$. 又因 x_1-x_2 和 x_1-x_3 共轭，故$(x_1-x_2)(x_1-x_3)$ 是实数，从而 $(x_1-x_2)^2(x_1-x_3)^2\geq 0$. 这样就得 $\Delta\leq 0$, 形成矛盾。所以方程有三个互不相同的实根。

例40 (p.228-16)**.** 求 $f(x) = x^n + px + q (n > 1)$ 的判别式。

解：

$$f'(x) = nx^{n-1} + p.$$

记 $b_1, \ldots, b_{n-1}$ 为方程 $nx^{n-1} + p = 0$ 的全部根。则

$$f'(x) = n(x - b_1) \cdots (x - b_{n-1}).$$

于是

$$R(f, f') = (-1)^{n(n-1)} n^n \prod_{1 \le j \le n-1} f(b_j)$$

$$= n^n \prod_{1 \le j \le n-1} f(b_j).$$

而

$$f(b_j) = b_j^n + pb_j + q = -\frac{pb_j}{n} + pb_j + q = q + \frac{p(n-1)}{n} b_j$$

$$= -\frac{(n-1)p}{n}[-\frac{nq}{(n-1)p} - b_j].$$

$$\prod_{1 \le j \le n-1} f(b_j) = (-\frac{(n-1)p}{n})^{n-1} \frac{f'(-\frac{nq}{(n-1)p})}{n}$$

$$= \frac{(-1)^{n-1}[(-1)^{n-1} n^n q^{n-1} + (n-1)^{n-1} p^n]}{n^n}.$$

从而

$$R(f, f') = (-1)^{n-1}[(-1)^{n-1} n^n q^{n-1} + (n-1)^{n-1} p^n].$$

代入公式

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{-1} R(f, f')$$

得

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} n^n q^{n-1} + (-1)^{\frac{(n-1)(n-2)}{2}} (n-1)^{n-1} p^n.$$

□

例41 (p.228-18)**.** 求证 $\Delta((x-a)g(x)) = g(a)^2\Delta(g(x))$.

证明：设 $g(x)=b_0(x-x_1)\cdots(x-x_n)$. 则

$$(x-a)g(x)=b_0(x-a)(x-x_1)\cdots(x-x_n).$$

注意 $(x-a)g(x)$ 是一个 $n+1$ 次多项式。于是

$$\Delta((x-a)g(x))=b_0^{2n}\prod_{i=1}^{n}(a-x_i)^2\cdot\prod_{i<j}(x_i-x_j)^2$$

$$=[b_0(a-x_1)\cdots(a-x_n)]^2\cdot b_0^{2n-2}\prod_{i<j}(x_i-x_j)^2$$

$$=g(a)^2\Delta(g(x)).\square$$

例42 (p.228-19)**.** 设 $f(x) = g(h(x))$, $g(x)$ 是次数等于 $n > 1$ 的多项式，其根是$x_1, \ldots, x_n$. $h(x)$ 是 $m > 1$ 次多项式。又 $g(x), h(x)$ 均为首一多项式，求证

$$\Delta(f(x)) = [\Delta(g(x))]^m (\Delta(h(x) - x_1)) \cdots (\Delta(h(x) - x_n)).$$

证明：由 $g(x)=(x-x_1)\cdots(x-x_n)$ 得

$f(x)=g(h(x))=(h(x)-x_1)\cdots(h(x)-x_n)$.

对每个 $1\leq i\leq n$, $h(x)-x_i$ 是 x 的一个首一多项式。设

$$h(x)-x_i=(x-t_{i1})\cdots(x-t_{im}).$$

记 $(i,j)<(i',j')$ 若 $i<i'$ 或 $i=i'$ 且$j<j'$. 由判别式的定义

$$\Delta(f(x))=\prod_{(i,j)<(i',j')}(t_{ij}-t_{i'j'})^2$$

$$=(\prod_{1\leq i\leq n}\prod_{1\leq j<j'\leq m}(t_{ij}-t_{ij'})^2)(\prod_{1\leq i<i'\leq n}\prod_{1\leq j,j'\leq m}(t_{ij}-t_{i'j'})^2). \tag{22}$$

再由判别式的定义得

$$\prod_{1\leq j<j'\leq m}(t_{ij}-t_{ij'})^2=\Delta(h(x)-x_i) \tag{23}$$

对于固定的 $i<i'$, 有

$$\prod_{1\leq j,j'\leq m}(t_{ij}-t_{i'j'})^2=\prod_{1\leq j\leq m}(\prod_{1\leq j'\leq m}(t_{ij}-t_{i'j'})^2)$$

$$=\prod_{1\leq j\leq m}(h(t_{ij})-x_{i'})^2=\prod_{1\leq j\leq m}(x_i-x_{i'})^2$$

$$= (x_i - x_{i'})^{2m}.$$

于是

$$\prod_{1\le i<i'\le n} \prod_{1\le j,j'\le m} (t_{ij} - t_{i'j'})^2 = \prod_{1\le i<i'\le n} (x_i - x_{i'})^{2m}$$

$$= [\Delta(g(x))]^m. \tag{24}$$

将(23) 和(24) 代入(22) 即得所需。□