第十一章　一元多项式的因式分解

§1　一元多项式

1. 计算 $(x^2+ax-b)(x^2-1)+(x^2-ax+b)(x^2+1)$.

解: $2x^4-2ax+2b$.

2. 计算多项式 x^3+2x^2+3x-1 与 $3x^2+2x+4$ 的乘积.

解: $3x^5+8x^4+17x^3+11x^2+10x-4$.

3. 设

$$\begin{aligned} f(x) &= 3x^2-5x+3, \\ g(x) &= ax(x-1)+b(x+2)(x-1)+cx(x+2), \end{aligned}$$

试确定 a,b,c, 使 $f(x)=g(x)$.

解: 取 $x=-2$, 得 $a=\dfrac{25}{6}$; 取 $x=0$, 得 $b=-\dfrac{3}{2}$, 取 $x=1$, 得 $c=\dfrac{1}{3}$.

4. 设 $f(x)$, $g(x)$ 和 $h(x)$ 都是实系数多项式, 证明: 如果

$$f^2(x)=xg^2(x)+xh^2(x),$$

那么

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

证明: 如 $f(x)\neq 0$, 则左式的次数为偶数, 而右式的次数为奇数, 矛盾, 故 $f(x)=0$. 从而

$$g^2(x)+h^2(x)=0.$$

又, $g(x),h(x)$ 皆为实系数多项式, 从而 $g^2(x),h^2(x)$ 的首项系数都是非负数, 而这两个数之和为零, 故 $g(x),h(x)$ 的首项系数都是零, 从而 $g(x)=h(x)=0$.

§ 2　整除的概念

1. 用 $g(x)$ 除 $f(x)$, 求商 $q(x)$ 与余式 $r(x)$:

(1) $f(x)=x^4+4x^2-x+6$, $g(x)=x^2+x+1$;

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

解: (1) $q(x)=x^2-x+4$, $r(x)=-4x+2$.

(2) $q(x)=\dfrac{1}{9}(3x+11)$, $r(x)=\dfrac{10}{9}(x-2)$.

2. m, p, q 适合什么条件时, 有

(1) $x^2+mx+1 \mid x^3+px+q$;

(2) $x^2+mx+1 \mid x^4+px^2+q$.

解: (1) $p=1-m^2$, $q=-m$.

(2) $\begin{cases} m=0 \\ p=1+q \end{cases}$ 或 $\begin{cases} p=-m^2+2 \\ q=1 \end{cases}$

3. 用综合除法求商 $q(x)$ 及余式 $r(x)$:

(1) $f(x)=x^4-2x^3+4x^2-6x+8$, $g(x)=x-2$;

(2) $f(x)=2x^5-5x^3-8x$, $g(x)=x+2$.

解: (1) $q(x)=x^3+4x+2$, $r(x)=12$.

(2) $q(x)=2x^4-4x^3+3x^2-6x+4$, $r(x)=-8$.

4. 用综合除法表 $f(x)$ 为 $x-x_0$ 的方幂:

(1) $f(x)=x^4-2x^3+3x^2-2x+1$, $x_0=2$;

(2) $f(x)=x^4-2x^2+3$, $x_0=-2$;

(3) $f(x)=x^4+2\mathrm{i}x^3-(1+\mathrm{i})x^2-3x+1-2\mathrm{i}$, $x_0=-\mathrm{i}$.

解: (1) $f(x)=(x-2)^4+6(x-2)^3+15(x-2)^2+18(x-2)+9$.

(2) $f(x)=(x+2)^4-8(x+2)^3+22(x+2)^2-24(x+2)+11$.

(3) $f(x)=(x+\mathrm{i})^4-2\mathrm{i}(x+\mathrm{i})^3-(1+\mathrm{i})(x+\mathrm{i})^2-5(x+\mathrm{i})+(1+2\mathrm{i})$.

5. 记 $\langle x\rangle^0=1$, $\langle x\rangle^k=x(x-1)(x-2)\cdots(x-k+1)$, $(k>1)$. 试将 $f(x)$ 表为

$$c_0+c_1\langle x\rangle+c_2\langle x\rangle^2+\cdots$$

的形式:

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

(2) $f(x)=x^5$.

解: (1)
$$\begin{array}{r|rrrrr}
1 & 1 & -2 & 1 & 0 & \underline{-1} \\
 & & 1 & -1 & 0 & \\
\hline
2 & 1 & -1 & 0 & \underline{0} & \\
 & & 2 & 2 & & \\
\hline
3 & 1 & 1 & \underline{2} & & \\
 & & 3 & & & \\
\hline
 & \underline{1} & \underline{4} & & &
\end{array}$$

因此$f(x) = -1 + 2\langle x\rangle^2 + 4\langle x\rangle^3 + \langle x\rangle^4$.

(2) $f(x) = \langle x\rangle + 15\langle x\rangle^2 + 25\langle x\rangle^3 + 10\langle x\rangle^4 + \langle x\rangle^5$.

6. k 是正整数, 证明: $x \mid f^k(x)$ 当且仅当 $x \mid f(x)$;

证明: 设 $f(x)$ 的常数项为 a, 则 $f^k(x)$ 的常数项为 a^k. 因此 $x \mid f^k(x) \iff a^k = 0 \iff a = 0 \iff x \mid f(x)$.

7. 设a, b 为两个不相等的常数, 证明: 多项式 $f(x)$ 被 $(x-a)(x-b)$ 除所得余式为

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

证明: 设 $f(x) = (x-a)(x-b)q(x) + Ax + B$, 则

$$f(a) = aA + B, \qquad f(b) = bA + B,$$

由此得

$$A = \frac{f(a)-f(b)}{a-b}, \qquad B = \frac{af(b)-bf(a)}{a-b}.$$

因此结论成立.

8. 设 $f_1(x)$, $f_2(x)$, $g_1(x)$, $g_2(x)$ 都是数域 K 上的多项式, 其中 $f_1(x) \neq 0$.

证明: 如果 $g_1(x)g_2(x) \mid f_1(x)f_2(x)$, $f_1(x) \mid g_1(x)$, 则 $g_2(x) \mid f_2(x)$.

证明: 设 $f_1(x)f_2(x) = g_1(x)g_2(x)q_1(x)$, $g_1(x)=f_1(x)q_2(x)$. 则$f_1(x)f_2(x) = f_1(x)q_2(x)g_2(x)q_1(x)$, 由于 $f_1(x) \neq 0$, 可得 $f_2(x) = g_2(x)q_2(x)q_1(x)$, 即 $g_2(x) \mid f_2(x)$.

***9.** 证明: $x^d - 1 \mid x^n - 1$ 当且仅当 $d \mid n$.

证明: $(\Rightarrow)$ 若 $n = dq$, 则

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

因此 $x^d - 1 \mid x^n - 1$.

$(\Leftarrow)$ 设 $n = dq + r$, $0 \leq r < d$. 由上证, $x^{dq} - 1 \equiv 0 \pmod{x^d - 1}$. 即

$$x^{dq} \equiv 1 \pmod{x^d - 1},$$

$$x^n \equiv x^{dq+r} \equiv x^{dq} \cdot x^r \equiv x^r \pmod{x^d - 1},$$

$$x^n - 1 \equiv x^r - 1 \pmod{x^d - 1}.$$

而 $x^d - 1 \mid x^r - 1 \Leftrightarrow r = 0$, 因此 $x^d - 1 \mid x^n - 1 \Leftrightarrow r = 0 \Leftrightarrow d \mid n$.

§ 3　最大公因式

1. 求最大公因式 $(f(x), g(x))$:

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

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

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

解: (1) $x + 1$.

(2) 1.

(3) 1.

2. 求 $u(x)$, $v(x)$, 使 $u(x)f(x) + v(x)g(x) = (f(x), g(x))$:

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

(2) $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$, $g(x) = 2x^3 - x^2 - 5x + 4$;

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

解: (1) $u(x) = -x - 1$, $v(x) = x + 2$, $d(x) = x^2 - 2$.

(2) $u(x) = -\dfrac{1}{3}(x - 1)$, $v(x) = \dfrac{1}{3}(2x^2 - 2x - 3)$, $d(x) = x - 1$.

(3) $u(x) = -\dfrac{1}{6}(2x^2 + 3x)$, $v(x) = \dfrac{1}{6}(2x^3 + 5x^2 - 6)$, $d(x) = 1$.

3. 证明: 如果 $d(x) \mid f(x)$, $d(x) \mid g(x)$, 且 $d(x)$ 为 $f(x)$ 与 $g(x)$ 的一个组合, 那么 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式.

证明: 设 $d(x) = u(x)f(x) + v(x)g(x)$, 则对任意的 $h(x) \in K[x]$, 如 $h(x) \mid f(x)$, $h(x) \mid g(x)$, 则 $h(x) \mid d(x)$.

又, $d(x)$ 为 $f(x)$ 与 $g(x)$ 的一个公因式, 故 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个最大公因式.

4. 证明: 如果 $h(x)$ 为首一多项式, 则

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

证明: 设 $d(x) = (f(x), g(x)) \neq 0$, 则存在 $u(x), v(x)$ 使

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

所以

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

又因 $d(x)h(x) \mid f(x)h(x)$, $d(x)h(x) \mid g(x)h(x)$, 所以 $d(x)h(x)$ 是 $f(x)h(x)$ 与 $g(x)h(x)$ 的一个最大公因式. 又因 $d(x), h(x)$ 都是首一多项式, 故 $d(x)h(x)$ 也是首一多项式, 从而

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

又如 $d(x) = 0$, 则 $f(x) = g(x) = 0$, 原等式仍然成立.

5. 证明: 如果 $f(x)$, $g(x)$ 不全为零, 则

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

证明: 因 $f(x)$, $g(x)$ 不全为零, 故 $(f(x), g(x)) \neq 0$. 所以

$$\begin{aligned}(f(x), g(x)) &= \left(\frac{f(x)}{(f(x), g(x))}(f(x), g(x)), \frac{g(x)}{(f(x), g(x))}(f(x), g(x))\right) \\ &= \left(\frac{f(x)}{(f(x), g(x))}, \frac{g(x)}{(f(x), g(x))}\right)(f(x), g(x))\end{aligned}$$

(由习题 4) 两边消去 $(f(x), g(x))$, 得

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

6. 证明: 如果 $f(x)$, $g(x)$ 不全为零, 且

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

则 $(u(x), v(x)) = 1$.

证明: 因 $f(x)$, $g(x)$ 不全为零, 故 $(f(x), g(x)) \neq 0$, 因此

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

$$(u(x), v(x)) = 1.$$

7. 证明: 如果 $(f(x), g(x)) = 1$, $(f(x), h(x)) = 1$, 那么

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

证明: 存在 $u(x), v(x), s(x), t(x)$, 使

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

$$s(x)f(x)+t(x)h(x)=1,$$

所以

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

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

8. 设 $f_1(x),\cdots,f_m(x)$, $g_1(x),\cdots,g_n(x)$ 都是多项式, 且 $(f_i(x),g_j(x))=1$ $(i=1,\cdots,m;j=1,\cdots,n)$, 证明:

$$(f_1(x)f_2(x)\cdots f_m(x),g_1(x)g_2(x)\cdots g_n(x))=1.$$

证明: 由 $(f_i(x),g_j(x))=1$, 可得 $(f_i(x),g_1(x)g_2(x))=1$, …, $(f_i(x),g_1(x)g_2(x)\cdots g_n(x))=1$. 从而 $(f_1(x)f_2(x),g_1(x)\cdots g_n(x))=1$, $(f_1(x)f_2(x)f_3(x),g_1(x)\cdots g_n(x))=1$, …, $(f_1(x)f_2(x)\cdots f_m(x),g_1(x)\cdots g_n(x))=1$.

9. 证明: 如果 $(f(x),g(x))=1$, 那么 $(f(x)+g(x),f(x)g(x))=1$.

证明: 由于 $(f(x),g(x))=1$, 所以

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

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

因此

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

10. 设 $f_1(x)=af(x)+bg(x)$, $g_1(x)=cf(x)+dg(x)$, 且 $ad-bc\neq 0$, 证明:

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

证明: 由题设可得 $(f(x),g(x))\mid(f_1(x),g_1(x))$. 又

$$f(x)=\frac{d}{ad-bc}f_1(x)-\frac{b}{ad-bc}g_1(x),$$

$$g(x)=\frac{-c}{ad-bc}f_1(x)+\frac{a}{ad-bc}g_1(x),$$

所以

$$(f_1(x),g_1(x))\mid(f(x),g(x)).$$

又因 $(f_1(x),g_1(x))$ 与 $(f(x),g(x))$ 的首项系数相同, 故

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

11. 证明: 如果 $f(x)$ 与 $g(x)$ 互素, 那么 $f(x^m)$ 与 $g(x^m)$ 也互素.

证明: 由题设, 存在多项式 $u(x), v(x)$ 使

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

所以

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

故 $(f(x^m), g(x^m))=1$.

12. 证明: 对任意的正整数 n, 都有

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

证明: 设 $(f(x), g(x))=d(x)$, $f(x)=d(x)f_1(x)$, $g(x)=d(x)g_1(x)$, 则 $(f_1(x), g_1(x))=1$.

由习题 8 可得

$$(f_1^n(x), g_1^n(x))=1.$$

于是

$$\begin{aligned}(f^n(x), g^n(x))&=(d^n(x)f_1^n(x), d^n(x)g_1^n(x))\\&=d^n(x)(f_1^n(x), g_1^n(x))=d^n(x)\\&=(f(x), g(x))^n.\end{aligned}$$

***13.** 试求 x^m-1 与 x^n-1 的最大公因式.

解: 令 $d=(m,n)$, 则根据习题 10–2.9, $x^d-1\mid x^m-1$, $x^d-1\mid x^n-1$.

设 $h(x)$ 是 x^m-1 与 x^n-1 的公因式, 则有

$$x^m-1\equiv 0 \pmod{h(x)}, x^n-1\equiv 0 \pmod{h(x)}$$

$$\Longrightarrow\ x^m\equiv 1 \pmod{h(x)}, x^n\equiv 1 \pmod{h(x)}.$$

由于 $d=(m,n)$, 因此存在 $u,v\in\mathbb{Z}$ 使得 $d=um+vn$.

$$x^d=x^{um+vn}\equiv 1 \pmod{h(x)} \implies x^d-1\equiv 0 \pmod{h(x)}.$$

又设 $d=ms-nt$, $s,t\geq 0$, 则 $d+nt=ms$. 于是

$$x^{ms}-1=x^{d+nr}-1=(x^d-1)x^{nr}+x^{nr}-1.$$

若 $f(x)\in K[x]$ 满足 $f(x)\mid x^m-1$, $f(x)\mid x^n-1$, 则 $(f(x), x)=1$, 且 $f(x)\mid x^{ms}-1$, $f(x)\mid x^{nt}-1$, 于是 $f(x)\mid (x^d-1)x^{nr}$. 由 $f(x)$ 与 x 互素可得 $f(x)\mid x^d-1$. 因此 $(x^m-1, x^n-1)=x^d-1$, 其中 $d=(m,n)$.

*14. 证明: 只要 $\dfrac{f(x)}{(f(x),g(x))}$, $\dfrac{g(x)}{(f(x),g(x))}$ 的次数都大于零, 就可以适当选择适合等式

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

的 $u(x)$ 与 $v(x)$, 使

$$\deg u(x)<\deg\left(\frac{g(x)}{(f(x),g(x))}\right),\ \deg v(x)<\deg\left(\frac{f(x)}{(f(x),g(x))}\right).$$

证明: 存在多项式 $s(x),t(x)\in K[x]$ 使

$$s(x)f(x)+t(x)g(x)=(f(x),g(x)).$$

则

$$s(x)\frac{f(x)}{(f(x),g(x))}+t(x)\frac{g(x)}{(f(x),g(x))}=1. \tag{$*$}$$

令

$$s(x)=\frac{g(x)}{(f(x),g(x))}q(x)+u(x),$$

其中 $u(x)=0$ 或 $\deg u(x)<\deg\dfrac{g(x)}{(f(x),g(x))}$. 记 $v(x)=\dfrac{f(x)}{(f(x),g(x))}q(x)+t(x)$, 则由 (*) 知,

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

由假设, $\dfrac{f(x)}{(f(x),g(x))}$ 与 $\dfrac{g(x)}{(f(x),g(x))}$ 的次数都大于零, 所以 $u(x),v(x)$ 都不是零多项式. 于是

$$\deg u(x)<\deg\frac{g(x)}{(f(x),g(x))}.$$

由 (**) 知

$$\deg\left(u(x)\frac{f(x)}{(f(x),g(x))}\right)=\deg\left(v(x)\frac{g(x)}{(f(x),g(x))}\right),$$

从而

$$\deg v(x)<\deg\frac{f(x)}{(f(x),g(x))}.$$

§4 不定方程与同余式

1. 设 $(f(x), m(x)) = 1$, 证明: 对任何的多项式 $g(x)$, 都存在多项式 $h(x)$, 使

$$h(x)f(x) \equiv g(x) \pmod{m(x)}.$$

证明: 由假设, 存在 $u(x), v(x) \in K[x]$, 使

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

所以

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

于是

$$g(x)u(x)f(x) \equiv g(x) \pmod{m(x)}.$$

令 $h(x) = g(x)u(x)$, 则

$$h(x)f(x) \equiv g(x) \pmod{m(x)}.$$

***2.** 设 $m_1(x), \cdots, m_s(x)$ 为一组两两互素的多项式, 证明: 对任何的多项式 $f_1(x), \cdots, f_s(x)$, 都存在多项式 $F(x)$, 使

$$F(x) \equiv f_i(x) \pmod{m_i(x)}, \quad i = 1, \cdots, s.$$

证明: 令 $M(x) = m_1(x)m_2(x)\cdots m_s(x)$, $R_i(x) = \dfrac{M(x)}{m_i(x)}$.
则 $(R_i(x), m_i(x)) = 1$, $m_j(x) \mid R_i(x)$, $i \neq j$. 存在 $h_i(x)$ 使 (习题 1)

$$h_i(x)R_i(x) \equiv f_i(x) \pmod{m_i(x)}$$

令

$$F(x) = \sum_{i=1}^{s} h_i(x)R_i(x),$$

则

$$\begin{aligned} F(x) &\equiv \sum_{i=1}^{s} h_i(x)R_i(x) \pmod{m_k(x)} \\ &\equiv h_k(x)R_k(x) \pmod{m_k(x)} \\ &\equiv f_k(x) \pmod{m_k(x)}. \end{aligned}$$

***3.** 设 $m(x)$ 为复系数多项式, 且 $m(0) \neq 0$. 证明: 存在复系数多项式 $f(x)$, 使

$$f^2(x) \equiv x \pmod{m(x)}.$$

证明: (a) 首先证明对任意的 $a \neq 0$, 同余式

$$f^2(x) \equiv x \pmod{(x-a)^m}$$

有解. 设 $\sqrt{a}$ 是 a 的任意一个平方根, 则

$$\begin{aligned}(x-a)^m &= ((\sqrt{x}-\sqrt{a})(\sqrt{x}+\sqrt{a}))^m = (\sqrt{x}-\sqrt{a})^m(\sqrt{x}+\sqrt{a})^m \\ &= (h(x)\sqrt{x}-g(x))(h(x)\sqrt{x}+g(x)) = h^2(x)x - g^2(x).\end{aligned}$$

于是

$$g^2(x) \equiv h^2(x)x \pmod{(x-a)^m}$$

而 $h(a)\sqrt{a}+g(a) = (\sqrt{a}+\sqrt{a})^m \neq 0$, 而 $h(a)\sqrt{a}-g(a) = (\sqrt{a}-\sqrt{a})^m = 0$, 因此 $g(a)h(a) \neq 0$, 从而 $(h(x),(x-a)^m) = 1$, 存在 $h_1(x) \in K[x]$ 使 $h_1(x)h(x) \equiv 1 \pmod{(x-a)^m}$. 于是

$$(h_1(x)g(x))^2 \equiv x \pmod{(x-a)^m}$$

取 $f(x) = h_1(x)g(x)$, 则有

$$f^2(x) \equiv x \pmod{(x-a)^m}.$$

(b) 设 $m(x) = (x-a_1)^{m_1}(x-a_2)^{m_2}\cdots(x-a_s)^{m_s}$, $a_i \neq a_j$ 对 $i \neq j$. 则 $(x-a_1)^{m_1},\cdots,(x-a_s)^{m_s}$ 两两互素. 由 (a), 存在 $f_i(x) \in K[x]$, 使

$$f_i^2(x) \equiv x \pmod{(x-a_i)^{m_i}}.$$

由习题 2, 存在 $f(x)$ 使

$$f(x) \equiv f_i(x) \pmod{(x-a_i)^{m_i}}$$

于是

$$f^2(x) \equiv x \pmod{(x-a_i)^{m_i}}$$

由 $(x-a_1)^{m_1},\cdots,(x-a_s)^{m_s}$ 两两互素可得

$$f^2(x) \equiv x \pmod{m(x)}.$$

§5 因式分解定理

1. 证明: $g^m(x) \mid f^m(x) \iff g(x) \mid f(x)$.

证明: 设

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

$$g(x) = bp_1^{k_1}(x)p_2^{k_2}(x)\cdots p_s^{k_s}(x),$$

其中 $a, b \in K$, $p_1(x), \cdots, p_s(x)$ 是两两互素的不可约多项式, 且 $l_i, k_i \geq 0$, $i = 1, \cdots, s$. 则

$$\begin{aligned} g(x) \mid f(x) &\iff k_i \leq l_i, \qquad i = 1, \cdots, s \\ &\iff mk_i \leq ml_i, \qquad i = 1, \cdots, s \\ &\iff g^m(x) \mid f^m(x). \end{aligned}$$

2. 设 $f(x), g(x) \in K[x]$, 且有分解式

$$\begin{aligned} f(x) &= ap_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x), \quad r_i \geqslant 0,\ i = 1, \cdots, s; \\ g(x) &= bp_1^{t_1}(x)p_2^{t_2}(x)\cdots p_s^{t_s}(x), \quad t_i \geqslant 0,\ i = 1, \cdots, s, \end{aligned}$$

其中 $p_1(x), \cdots, p_s(x)$ 是不同的首一不可约多项式. 证明:

$$[f(x), g(x)] = p_1^{\max(r_1,t_1)}(x)p_2^{\max(r_2,t_2)}(x)\cdots p_s^{\max(r_s,t_s)}(x).$$

证明: 令 $m_i = \max(r_i, t_i)$, $i = 1, \cdots, s$.

$$m(x) = p_1^{m_1}(x)p_2^{m_2}(x)\cdots p_s^{m_s}(x),$$

则因 $r_i \leq m_i$, $t_i \leq m_i$, 因此

$$f(x) \mid m(x), \quad g(x) \mid m(x) \implies [f(x), g(x)] \mid m(x).$$

设 $s(x) \in K[x]$ 是 $f(x), g(x)$ 的公倍式, 则有

$$s(x) = p_1^{l_1}(x)p_2^{l_2}(x)\cdots p_s^{l_s}(x)h(x),$$

$$l_i \leq r_i,\ l_i \leq t_i,\ (h(x), p_i(x)) = 1,\ i = 1, \cdots, s.$$

于是

$$l_i \geq \max(r_i, t_i), \quad i = 1, \cdots, s, \implies m(x) \mid s(x).$$

因此

$$[f(x),g(x)]=p_1^{m_1}(x)p_2^{m_2}(x)\cdots p_s^{m_s}(x).$$

3. 设 $f(x),g(x)\in K[x]$ 都是首一多项式, 证明:

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

证明: 设

$$f(x)=p_1^{r_1}(x)p_2^{r_2}(x)\cdots p_s^{r_s}(x),\quad r_i\geqslant 0,\ i=1,\cdots,s;$$
$$g(x)=p_1^{t_1}(x)p_2^{t_2}(x)\cdots p_s^{t_s}(x),\quad t_i\geqslant 0,\ i=1,\cdots,s,$$

其中 $p_1(x),\cdots,p_s(x)$ 是不同的首一不可约多项式. 令

$$m_i=\max(r_i,t_i),\qquad l_i=\min(r_i,t_i),\qquad i=1,\cdots,s.$$

则

$$f(x)g(x)=p_1^{r_1+t_1}(x)p_2^{r_2+t_2}(x)\cdots p_s^{r_s+t_s}(x),$$
$$(f(x),g(x))=p_1^{l_1}(x)p_2^{l_2}(x)\cdots p_s^{l_s}(x),$$

由于 $r_i+t_i-l_i=m_i$, $i=1,\cdots,s$. 因此

$$\frac{f(x)g(x)}{(f(x),g(x))}=p_1^{m_1}(x)p_2^{m_2}(x)\cdots p_s^{m_s}(x)=[f(x),g(x)].$$

4. 求下列多项式的最小公倍式:

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

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

解: (1) 由于 $(f(x),g(x))=1$, $[f(x),g(x)]=f(x)g(x)=x^7-7x^6+12x^5+x^4-3x^3-3x^2+1$.

(2) 由于 $(f(x),g(x))=x-\mathrm{i}$, $[f(x),g(x)]=f(x)(x+\mathrm{i})=x^5+\mathrm{i}x^4-x^2-x-(1+\mathrm{i})$.

5. 设 $p(x)$ 是次数大于零的多项式. 证明: 如果对于任何多项式 $f(x),g(x)$, 由 $p(x)\mid f(x)g(x)$ 可以推出 $p(x)\mid f(x)$ 或者 $p(x)\mid g(x)$, 则 $p(x)$ 是不可约多项式.

证明: 若 $p(x)$ 可约, 则存在次数小于 $p(x)$ 的非常数多项式 $f(x),g(x)$ 使 $p(x)=f(x)g(x)$. 从而 $p(x)\mid f(x)g(x)$. 但因

$$\deg f(x)<\deg p(x),\qquad \deg g(x)<\deg p(x),$$

$p(x) \nmid f(x)$, $p(x) \nmid g(x)$, 与假设矛盾, 因此 $p(x)$ 不可约.

*__6.__ 证明: 次数大于 0 的首一多项式 $f(x)$ 是某一不可约多项式的方幂的充分必要条件是, 对任意的多项式 $g(x)$ 或者有 $(f(x), g(x)) = 1$, 或者对某一正整数 m, $f(x) \mid g^m(x)$.

证明: $(\Rightarrow)$ 设 $f(x) = p^m(x)$, 其中 $p(x)$ 不可约, 则若 $g(x) \in K[x]$ 满足 $p(x) \mid g(x)$, 有

$$f(x) = p^m(x) \mid g^m(x).$$

如 $p(x) \nmid g(x)$, 则 $(p(x), g(x)) = 1$, 从而 $(p^m(x), g(x)) = 1$, 即 $(f(x), g(x)) = 1$.

$(\Leftarrow)$ 设 $p(x)$ 是 $f(x)$ 的一个首一不可约因子, 则 $(p(x), f(x)) = p(x)$, 从而存在某个正整数 m, 使 $f(x) \mid p^m(x)$, 这说明 $p(x)$ 是 $f(x)$ 的唯一不可约因子. 所以 $f(x) = cp^r(x)$. 又因 $f(x), p(x)$ 的首项系数都是 1, 故 $c = 1$. 从而 $f(x) = p^r(x)$.

*__7.__ 证明: 次数大于 0 的首一多项式 $f(x)$ 是某一不可约多项式的方幂的充分必要条件是, 对任意的多项式 $g(x), h(x)$, 由 $f(x) \mid g(x)h(x)$ 可以推出 $f(x) \mid g(x)$, 或者对某一正整数 m, $f(x) \mid h^m(x)$.

证明: $(\Rightarrow)$ 设 $f(x) = p^m(x)$, 其中 $p(x)$ 是首一不可约多项式, 则由 $f(x) \mid g(x)h(x)$, 可得 $p(x) \mid g(x)h(x)$, 从而 $p(x) \mid g(x)$ 或 $p(x) \mid h(x)$. 于是 $f(x) = p^m(x) \mid g^m(x)$ 或 $f(x) = p^m(x) \mid h^m(x)$.

$(\Leftarrow)$ 设 $p(x)$ 是 $f(x)$ 的一个首一不可约因子, 则 $f(x) = p(x)f_1(x)$. 从而 $f(x) \mid p(x)f_1(x)$. 而 $f(x) \nmid f_1(x)$, 从而存在某个正整数 m, 使 $f(x) \mid p^m(x)$, 这说明 $p(x)$ 是 $f(x)$ 的唯一不可约因子. 所以 $f(x) = cp^r(x)$. 又因 $f(x), p(x)$ 的首项系数都是 1, 故 $c = 1$. 从而 $f(x) = p^r(x)$.

§6 重因式

1. 判别下列有理系数多项式有无重因式, 若有, 则求出重因式:

(1) $f(x) = x^5 - 10x^3 - 20x^2 - 15x - 4$;

(2) $f(x) = x^4 - 4x^3 + 16x - 16$;

(3) $f(x) = x^5 - 6x^4 + 16x^3 - 24x^2 + 20x - 8$;

(4) $f(x) = x^6 - 15x^4 + 8x^3 + 51x^2 - 72x + 27$.

解: (1) $x + 1$, 4 重.

(2) $x - 2$, 3 重.

(3) $x^2 - 2x + 2$, 2 重.

(4) $x+3$, 2 重, $x-1$, 3 重.

2. a,b 应满足什么条件, 下列多项式有重因式?

(1) $f(x)=x^3+3ax+b$; (2) $f(x)=x^4+4ax+b$.

解: (1) 当 $a=b=0$ 有 3 重因式 x, 当 $4a^3=-b^2$ 且 $a\neq 0$, 有 2 重因式 $2ax+b$.

(2) 当 $a=b=0$ 有 4 重因式 x, 当 $27a^4=b^3$ 且 $a\neq 0$, 有 2 重因式 $3ax+b$.

3. 设 $p(x)$ 是 $f'(x)$ 的 k 重因式, 能否说 $p(x)$ 是 $f(x)$ 的 $k+1$ 重因式, 为什么?

解: 不能. 因为又可能 $f'(x)$ 任一重因式都不是 $f(x)$ 的因式. 例如 $f(x)=x^4-1$, $f'(x)=4x^3$.

4. 证明: 如果 $(f'(x),f''(x))=1$, 那么, $f(x)$ 的重因式都是 $f(x)$ 的二重因式.

证明: 由于 $(f'(x),f''(x))=1$, $f'(x)$ 的任一因式都不是 $f''(x)$ 的因式. 设 $p(x)$ 是 $f(x)$ 的重因式, 则 $p(x)\mid f'(x)$, 于是 $p(x)\nmid f''(x)$, 说明 $p(x)$ 是 $f'(x)$ 的单因式, 故 $p(x)$ 是 $f(x)$ 的二重因式.

5. 证明: $K[x]$ 中不可约多项式 $p(x)$ 是 $f(x)\in K[x]$ 的 k $(k\geqslant 1)$ 重因式的充分必要条件是 $p(x)$ 是 $f(x),f'(x),\cdots,f^{(k-1)}(x)$ 的因式, 但不是 $f^{(k)}(x)$ 的因式.

证明: $(\Rightarrow)$ 对 k 用归纳法. 当 $k=1$ 时结论显然成立. 现设结论对 $k-1$ 成立. 设 $p(x)$ 是 $f(x)$ 的 k 重因式, 则 $f(x)=p^k(x)g(x)$, 其中 $(p(x),g(x))=1$. 则

$$f'(x)=kp^{k-1}(x)g(x)+p^k(x)g'(x)=p^{k-1}(x)(kg(x)+p(x)g'(x)).$$

由 $(p(x),g(x))=1$ 可得 $(p(x),kg(x)+p(x)g'(x))=1$, 因此 $p(x)$ 是 $f'(x)$ 的 $k-1$ 重因式. 根据归纳假设, $p(x)$ 是 $f'(x),\cdots,f^{(k-1)}(x)$ 的因式, 但不是 $f^{(k)}(x)$ 的因式. 而 $p(x)$ 是 $f(x)$ 的因式是已知的.

$(\Leftarrow)$ 如 $p(x)$ 是 $f(x),f'(x),\cdots,f^{(k-1)}(x)$ 的因式, 但不是 $f^{(k)}(x)$ 的因式, 则 $p(x)$ 是 $f^{(k-1)}(x)$ 的一重因式, 进而, $p(x)$ 是 $f^{(k-2)}(x)$ 的二重因式, 依次类推, 可知 $p(x)$ 是 $f(x)$ 的 k 重因式.

6. 试求多项式 $x^{1999}+1$ 除以 $(x-1)^2$ 所得余式.

解: 设 $x^{1999}+1=(x-1)^2q(x)+ax+b$, 则两边求导后得

$$1999x^{1998}=2(x-1)q(x)+(x-1)^2q(x)+a.$$

以 $x=1$ 代入上两式, 得

$$a=1999, \qquad b=-1997.$$

故所求余式为 $1999x-1997$.

§7 多项式的根

1. 求下列多项式的公共根:

(1) $f(x)=x^4+2x^2+9$, $g(x)=x^4-4x^3+4x^2-9$;

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

解: (1) $1+\sqrt{2}\mathrm{i}$, $1-\sqrt{2}\mathrm{i}$.

(2) $\dfrac{-1+\sqrt{3}\mathrm{i}}{2}$, $\dfrac{-1-\sqrt{3}\mathrm{i}}{2}$.

2. 如果 $(x-1)^2 \mid Ax^4+Bx^2+1$, 求 A, B.

解: $A=1$, $B=-2$.

3. 已知 $x^4-3x^3+6x^2+ax+b$ 能被 x^2-1 整除, 求 a, b.

解: $a=3$, $b=-7$.

4. 证明: 如果 $f(x) \mid f(x^n)$, 那么 $f(x)$ 的根只能是零或单位根.

证明: 设 a 是 $f(x)$ 的一个根, 则 $f(a)=0$, 于是 $f(a^n)=0$, 又可得到 $f((a^n)^n)=f(a^{n^2})=0, \ldots, f(a^{n^n})=0$. 因而 $a, a^n, a^{n^2}, \cdots, a^{n^n}$ 都是 $f(x)$ 的根. 但 $f(x)$ 的不同根仅有有限多个, 故必有 $k<l$ 使 $a^{n^k}=a^{n^l}$, 即

$$a^{n^k}(a^{n^l-n^k}-1)=0.$$

于是 $a=0$ 或 $a^{n^l-n^k}=1$, 故 a 为 0 或单位根.

5. 证明: $\sin x$ 不是多项式.

证明: $\sin x$ 有无限多个不同的根 $k\pi$, $k\in\mathbb{Z}$, 而多项式只有有限多个根. 因此 $\sin x$ 不是多项式.

6. 已知多项式 $f(x)=x^5-10x^2+15x-6$ 有重根, 试求它的所有根并确定根的重数.

解: $\dfrac{-3+\sqrt{15}\mathrm{i}}{2}$, $\dfrac{-3-\sqrt{15}\mathrm{i}}{2}$, 1,1,1.

7. 求 t 的值, 使 $f(x)=x^3-3x^2+tx-1$ 有重根.

解: $t=3$ 时, 1 为 3 重根; $t=-\dfrac{15}{4}$ 时, $-\dfrac{1}{2}$ 为 2 重根.

8. 求多项式 $f(x)=x^3+px+q$ 有重根的条件.

解: $4p^3+27q^2=0$.

9. 证明: 下列多项式没有重根:

(1) $f(x)=1+x+\dfrac{x^2}{2!}+\cdots+\dfrac{x^n}{n!}$;

*(2) $f(x)=1+2x+3x^2+\cdots+(n+1)x^n$.

证明: (1)

$$\begin{aligned}(f(x),f'(x))&=\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!},1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n-1}}{(n-1)!}\right)\\&=\left(\frac{x^n}{n!},1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n-1}}{(n-1)!}\right)=1.\end{aligned}$$

所以 $f(x)$ 无重根.

(2) 设

$$g(x)=(1-x)^2(1+2x+3x^2+\cdots+(n+1)x^n)=1-(n+2)x^{n+1}+(n+1)x^{n+2},$$

$$g'(x)=(n+2)(n+1)x^{n+1}-(n+2)(n+1)x^n,$$

$$(g(x),g'(x))=x-1.$$

所以 $g(x)$ 仅有的重根是 $x=1$. 又 $f(x)$ 的重根显然都是 $g(x)$ 的重根, 而 $x=1$ 不是 $f(x)$ 的根, 故 $f(x)$ 无重根.

10. 证明: $f(x)=x^n+ax^{n-m}+b$ $(n>2,n>m>0)$ 不能有非零的重数大于 2 的根.

证明: $f'(x)=x^{n-m-1}[nx^m+(n-m)a]$.

(a) 当 $a\neq 0$ 时, $nx^m+(n-m)a$ 的根都是单根, 所以 $f(x)$ 的重数大于 2 的根只可能是 $x=0$.

(b) 当 $a=0$ 时, $f'(x)$ 的仅有的重根为 $x=0$, 故 $f(x)$ 的重数大于 2 的根只可能是 $x=0$.

11. 如果 a 是 $f'''(x)$ 的一个 k 重根, 证明: a 是

$$g(x)=\frac{x-a}{2}[f'(x)+f'(a)]-f(x)+f(a)$$

的一个 $k+3$ 重根.

证明:

$$\begin{aligned}g(x)&=\frac{x-a}{2}[f'(x)+f'(a)]-f(x)+f(a),\\g'(x)&=\frac{1}{2}[f'(a)-f'(x)]+\frac{x-a}{2}f''(x),\\g''(x)&=\frac{x-a}{2}f'''(x),\end{aligned}$$

显然 a 是 $g(x), g'(x), g''(x)$ 的根, 又 a 是 $f'''(x)$ 的 k 重根, 因此 a 是 $g''(x)$ 的 $k+1$ 重根, 是 $g(x)$ 的 $k+3$ 重根.

12. 证明: x_0 是 $f(x)$ 的 k 重根的充分必要条件是$f(x_0) = f'(x_0) = \cdots = f^{(k-1)}(x_0) = 0$ 而 $f^{(k)}(x_0) \neq 0$.

证明: x_0 是 $f(x)$ 的 k 重根 $\iff$ $x - x_0$ 是 $f(x)$ 的 k 重因式

$\iff$ $x - x_0$ 是 $f(x), f'(x), \cdots, f^{(k-1)}(x)$ 的因式, 但不是 $f^{(k)}(x)$ 的因式

$\iff$ $f(x_0) = f'(x_0) = \cdots = f^{(k-1)}(x) = 0, f^{(k)}(x_0) \neq 0$.

13. 证明: 如果 $f'(x) \mid f(x)$, 则 $f(x)$ 有 n 重根, 其中 $n = \deg f(x)$.

证明: 由假设, $\dfrac{f(x)}{(f(x), f'(x))} = c(x-a)$. 从而 $x - a$ 为 $f(x)$ 仅有的不可约因式 (推论 6.4), 所以 $f(x) = c(x-a)^n$, $f(x)$ 有 n 重根.

14. 试按下表所给的数值, 求次数最低的多项式:

x	1	2	3	4
y	2	1	4	3

解: $f(x) = -\dfrac{4}{3}x^3 + 10x^2 - \dfrac{65}{3}x + 15$.

15. 若 n 次多项式 $f(x)$ 的根为 $x_1, x_2, \cdots, x_n$, 而数 c 不是 $f(x)$ 的根, 证明:

$$\sum_{i=1}^{n} \frac{1}{x_i - c} = -\frac{f'(c)}{f(c)}.$$

证明: 考察多项式 $f(x) = (x-x_1)(x-x_2)\cdots(x-x_n)$, 则

$$f'(x) = \sum_{i=1}^{n} \frac{f(x)}{x - x_i}, \qquad \frac{f'(x)}{f(x)} = \sum_{i=1}^{n} \frac{1}{x - x_i},$$

从而

$$\sum_{i=1}^{n} \frac{1}{x_i - c} = -\frac{f'(c)}{f(c)}.$$

***16.** 应用克拉默法则导出拉格朗日插值公式.

证明: 设所求多项式为

$$f(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1},$$

其中 c_i 待定. 将 a_i, b_i 代入上式两边, 得 $c_0, c_1, \cdots, c_{n-1}$ 的线性方程组:

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

此线性方程组的系数矩阵 A 是范德蒙德矩阵:

$$A = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix},$$

$$|A| = \prod_{1 \le i < j \le n} (a_j - a_i).$$

由于 a_i 互不相同, 故 $|A| \ne 0$, 所以线性方程组有唯一解.

$$\begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = A^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

故所求的唯一次数不超过 $n-1$ 的多项式

$$\begin{aligned} f(x) &= (1\ x\ \cdots\ x^{n-1}) \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \\ &= (1\ x\ \cdots\ x^{n-1}) A^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ &= \frac{1}{|A|} (1\ x\ \cdots\ x^{n-1}) A^* \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{|A|}\sum_{k=1}^{n}(-1)^{n+k}b_k \begin{vmatrix} 1 & \cdots & 1 & 1 & \cdots & 1 & 1 \\ a_1 & \cdots & a_{k-1} & a_{k+1} & \cdots & a_n & x \\ a_1^2 & \cdots & a_{k-1}^2 & a_{k+1}^2 & \cdots & a_n^2 & x^2 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1^{n-1} & \cdots & a_{k-1}^{n-1} & a_{k+1}^{n-1} & \cdots & a_n^{n-1} & x^{n-1} \end{vmatrix} \\
&= \frac{1}{|A|}\sum_{k=1}^{n}(-1)^{n+k}b_k \prod_{\substack{i=1\\ i\neq k}}^{n}(x-a_i)\prod_{\substack{1\leq i<j\leq n\\ i,j\neq k}}(a_j-a_i) \\
&= \sum_{k=1}^{n}(-1)^{n+k}\frac{b_kF(x)}{(x-a_k)(a_n-a_k)\cdots(a_{k+1}-a_k)(a_k-a_{k-1})\cdots(a_k-a_1)} \\
&= \sum_{k=1}^{n}\frac{b_kF(x)}{(x-a_k)F'(a_k)}.
\end{aligned}
$$

这里 $F(x)=(x-a_1)(x-a_2)\cdots(x-a_n)$.

*__17.__ 设 $a_1,a_2,\cdots,a_n$ 为互不相同的数, $F(x)=(x-a_1)(x-a_2)\cdots(x-a_n)$. 证明: 任何多项式 $f(x)$ 用 $F(x)$ 除所得的余式为

$$\sum_{i=1}^{n}\frac{f(a_i)F(x)}{(x-a_i)F'(a_i)}.$$

证明: 考察

$$\frac{1}{F(x)}=\frac{A_1}{x-a_1}+\frac{A_2}{x-a_2}+\cdots+\frac{A_n}{x-a_n}.$$

两边同乘以 $x-a_i$, 再令 $x=a_i$, 可得

$$A_i=\frac{1}{F'(a_i)}.$$

因此可得恒等式

$$\frac{1}{F(x)}=\frac{1}{(x-a_1)F'(a_1)}+\frac{1}{(x-a_2)F'(a_2)}+\cdots+\frac{1}{(x-a_n)F'(a_n)}.$$

从而

$$1=\sum_{i=1}^{n}\frac{F(x)}{(x-a_i)F'(a_i)}.$$

令

$$f(x)=(x-a_i)f_i(x)+f(a_i),$$

则

$$\begin{aligned}f(x)&=\sum_{i=1}^{n}[(x-a_i)f_i(x)+f(a_i)]\frac{F(x)}{(x-a_i)F'(a_i)}\\&=\sum_{i=1}^{n}\frac{f_i(x)F(x)}{F'(a_i)}+\sum_{i=1}^{n}\frac{f(a_i)F(x)}{(x-a_i)F'(a_i)}\\&=F(x)\left(\sum_{i=1}^{n}\frac{f_i(x)}{F'(a_i)}\right)+\sum_{i=1}^{n}\frac{f(a_i)F(x)}{(x-a_i)F'(a_i)}.\end{aligned}$$

由于 $\sum\limits_{i=1}^{n}\dfrac{f(a_i)F(x)}{(x-a_i)F'(a_i)}\in K[x]$, 且 $\deg\sum\limits_{i=1}^{n}\dfrac{f(a_i)F(x)}{(x-a_i)F'(a_i)}\leq n-1$, 所以用 $F(x)$ 除 $f(x)$ 所得的余式为 $\sum\limits_{i=1}^{n}\dfrac{f(a_i)F(x)}{(x-a_i)F'(a_i)}$.

*__18.__ 已知 $a_1,\cdots,a_n;\ b_1,\cdots,b_n$ 为互不相同的数, 求解下列方程组:

$$\begin{cases}\dfrac{1}{b_1-a_1}x_1+\dfrac{1}{b_1-a_2}x_2+\cdots+\dfrac{1}{b_1-a_n}x_n=-1,\\\dfrac{1}{b_2-a_1}x_1+\dfrac{1}{b_2-a_2}x_2+\cdots+\dfrac{1}{b_2-a_n}x_n=-1,\\\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\\dfrac{1}{b_n-a_1}x_1+\dfrac{1}{b_n-a_2}x_2+\cdots+\dfrac{1}{b_n-a_n}x_n=-1.\end{cases}$$

解: 设 $x_1,\cdots,x_n$ 是此方程组的任一解, 考察有理分式

$$F(x)=1+\frac{x_1}{x-a_1}+\frac{x_2}{x-a_2}+\cdots+\frac{x_n}{x-a_n},\qquad(*)$$

则 $F(b_i)=0,\ i=1,\cdots,n$.

令 $F(x)=\dfrac{g(x)}{(x-a_1)(x-a_2)\cdots(x-a_n)}$, 则 $\deg g(x)=n$, 且 $g(x)$ 的首项为 x^n. 由于 $F(b_i)=0$, 故 $g(b_i)=0,\ i=1,\cdots,n$, 所以

$$g(x)=(x-b_1)(x-b_2)\cdots(x-b_n).$$

$$F(x)=\frac{(x-b_1)(x-b_2)\cdots(x-b_n)}{(x-a_1)(x-a_2)\cdots(x-a_n)}.$$

令

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

考察 $h(x)=g(x)-f(x)$, 则 $\deg h(x)\leq n-1$.

由于 $h(a_i)=g(a_i)$, 由拉格朗日公式,

$$h(x)=\sum_{i=1}^{n}\frac{g(a_i)f(x)}{(x-a_i)f'(a_i)},$$

$$g(x)=f(x)+\sum_{i=1}^{n}\frac{g(a_i)f(x)}{(x-a_i)f'(a_i)},$$

$$F(x)=\frac{g(x)}{f(x)}=1+\sum_{i=1}^{n}\frac{1}{(x-a_i)}\cdot\frac{g(a_i)}{f'(a_i)},$$

与 (*) 比较, 即得

$$x_1=\frac{g(a_1)}{f'(a_1)},x_2=\frac{g(a_2)}{f'(a_2)},\cdots,x_n=\frac{g(a_n)}{f'(a_n)}.$$

§8 复系数与实系数多项式

1. 分别求多项式 $f(x)=x^5-3x^4+4x^3-4x^2+3x-1$ 在复数域和实数域上的标准分解式.

解: $f(x)=(x^2+1)(x-1)^3=(x+\mathrm{i})(x-\mathrm{i})(x-1)^3$.

2. 分别求多项式 $f(x)=x^n-1$ 在复数域和实数域上的标准分解式.

解: 在复数域上的分解式:

$$f(x)=\prod_{k=0}^{n-1}\left(x-\cos\frac{2k\pi}{n}-\mathrm{i}\sin\frac{2k\pi}{n}\right);$$

在实数域上的分解式:

$$f(x)=\begin{cases}(x-1)\prod\limits_{k=1}^{\frac{n-1}{2}}\left(x^2-2\cos\dfrac{2k\pi}{n}x+1\right), & n\text{ 为奇数};\\ (x-1)(x+1)\prod\limits_{k=1}^{\frac{n-2}{2}}\left(x^2-2\cos\dfrac{2k\pi}{n}x+1\right), & n\text{ 为偶数}.\end{cases}$$

3. 已知 m,n,p 为非负整数, 证明: $x^{3m}+x^{3n+1}+x^{3p+2}$ 能被 x^2+x+1 整除.

证明: 因为

$$\begin{aligned}x^{3m}+x^{3n+1}+x^{3p+2}&=x^{3m}-1+x^{3n+1}-x+x^{3p+2}-x^2+x^2+x+1\\&=(x^{3m}-1)+x(x^{3n}-1)+x^2(x^{3p}-1)+x^2+x+1.\end{aligned}$$

由于 $x^3-1 \mid x^{3m}-1$, $x^3-1 \mid x^{3n}-1$, $x^3-1 \mid x^{3p}-1$, 所以 $x^2+x+1 \mid x^{3m}-1+x(x^{3n}-1)+x^2(x^{3p}-1)+(x^2+x+1)$.

另证: 设 $\varepsilon_1,\varepsilon_2$ 为 x^2+x+1 的根, 则 $\varepsilon_1^3=\varepsilon_2^3=1$. 所以 $f(\varepsilon_1)=\varepsilon_1^{3m}+\varepsilon_1^{3n+1}+\varepsilon_1^{3p+2}=1+\varepsilon_1+\varepsilon_1^2=0$. 同理 $f(\varepsilon_2)=0$. 所以 $x^2+x+1 \mid (x)$.

4. 证明: 如果 $x^2+x+1 \mid f_1(x^3)+xf_2(x^3)$, 那么 $f_1(1)=f_2(1)=0$.

证明: 设 $\varepsilon=\dfrac{-1+\sqrt{3}\mathrm{i}}{2}$, 则 $\varepsilon,\overline{\varepsilon}$ 都是 x^2+x+1 的根. 由于 $x^2+x+1 \mid f_1(x^3)+xf_2(x^3)$, 所以

$$f_1(1)+\varepsilon f_2(1)=0, \qquad f_1(1)+\overline{\varepsilon} f_2(1)=0.$$

由此得 $f_1(1)=f_2(1)=0$.

5. 证明: 如果 $x-1 \mid f(x^n)$, 那么 $x^n-1 \mid f(x^n)$.

证明: 由于 $x-1 \mid f(x^n)$, 所以 $f(1)=0$. 从而对任意的 n 次单位根 ε,

$$f(\varepsilon^n)=f(1)=0,$$

所以 $x^n-1 \mid f(x^n)$.

6. 已知多项式 $f(x)=x^3+\mathrm{i}x^2+(1-\mathrm{i})x-10-2\mathrm{i}$ 有实根, 试求 $f(x)$ 的全部根.

解: 2, $-1+\dfrac{-1+\sqrt{17}}{2}\mathrm{i}$, $-1+\dfrac{-1-\sqrt{17}}{2}\mathrm{i}$.

***7.** 证明: 实系数多项式 $f(x)$ 可表为两个实系数多项式的平方和的充分必要条件是对任何的实数 a, 都有 $f(a)\geqslant 0$.

证明: 必要性显然. 下证充分性.

设

$$f(x)=c(x-a_1)^{l_1}(x-a_2)^{l_2}\cdots(x-a_t)^{l_t}(x^2+p_1x+q_1)^{k_1}\cdots(x^2+p_sx+q_s)^{k_s},$$

这里 $a_1<a_2<\cdots<a_t$, $p_i^2-4q_i<0$, $l_i>0$, $k_i>0$. 由条件知, $c>0$. 任取 b,c 使 $a_{r-1}<b<a_r$, $a_r<c<a_{r+1}$, 则 $f(b)$ 的符号为 $(-1)^{l_r+\cdots+l_t}$, $f(c)$ 的符号为 $(-1)^{l_{r+1}+\cdots+l_t}$. 又因 $f(b)>0$, $f(c)>0$, 故 $(-1)^{l_r}>0$, l_r 是偶数, $r=1,\cdots,t$. 从而

$$f(x)=g^2(x)(x^2+p_1x+q_1)^{k_1}\cdots(x^2+p_sx+q_s)^{k_s}.$$

设

$$x^2+p_ix+q_i=(x-\alpha_i)(x-\overline{\alpha_i}), \qquad \alpha_i\in\mathbb{C},$$

则

$$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)=u(x)+\mathrm{i}v(x), \qquad u(x),v(x)\in\mathbb{R}[x],$$

$$(x-\overline{\alpha_1})(x-\overline{\alpha_2})\cdots(x-\overline{\alpha_s})=u(x)-\mathrm{i}v(x).$$

从而

$$(x^2+p_1x+q_1)^{k_1}\cdots(x^2+p_sx+q_s)^{k_s}=u^2(x)+v^2(x).$$

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

*__8.__ 试用施图姆定理隔离下列多项式的实根:

(1) x^3-3x-1; (2) x^3+x^2-2x-1;

(3) x^4+x-1; (4) $x^4+4x^3-12x+9$.

解: (1) 施图姆列为: x^3-3x-1, $^2-1$, $2+1$, 1. 变号数如下表:

	$-\infty$	-2	-1	0	1	2	$+\infty$
$f_0(x)$	$-$	$-$	$+$	$-$	$-$	$+$	$+$
$f_1(x)$	$+$	$+$	0	$-$	0	$+$	$+$
$f_2(x)$	$-$	$-$	$-$	$+$	$+$	$+$	$+$
$f_3(x)$	$+$	$+$	$+$	$+$	$+$	$+$	$+$
$V(x)$	3	3	2	1	1	0	0

由此知, $f(x)$ 有 3 个实根, 实根范围是 $(-2,-1)$, $(-1,0)$, $(1,2)$.

(2) 施图姆列为: x^3+x^2-2x-1, $3x^2+2x-2$, $2x+1$, 1.

实根数为 3, 实根范围是 $(-2,-1)$, $(-1,0)$, $(1,2)$.

(3) 施图姆列为: x^4+x-1, $4x^3+1$, $-3x-4$, -1.

实根数为 2, 实根范围是 $(-2,-1)$, $(0,1)$.

(4) 施图姆列为: $x^4+4x^3-12x+9$, x^3+3x^2-3, x^2+3x-4, $-4x-3$, 1. 无实根.

§9 有理系数多项式

1. 试求下列多项式的有理根:

(1) $x^5-7x^3-12x^2+6x+36$; (2) $6x^4+19x^3-7x^2-26x+12$;

(3) $10x^4-13x^3+15x^2-18x-15$;

(4) $x^6-6x^5+11x^4-x^3-18x^2+20x-8$.

解: (1) 3, -2.

(2) -3, $\frac{1}{2}$.

(3) $-\frac{1}{2}$.

(4) 2, 2, 2.

2. 证明下列多项式在有理数域上不可约:

(1) $x^4-8x^3+12x^2-6x+2$;　　(2) $x^5-12x^3+36x-12$;

(3) x^4-x^3+2x+1;　　(4) $x^4+4kx+1$, k 为整数

(5) x^p+px+1, p 为奇素数;　　(6) $x^4+5x^3-3x^2-5x+1$.

证明: (1) 取 $p=2$, 由艾森斯坦因判别法知, $f(x)$ 不可约.

(2) 取 $p=3$, 由艾森斯坦因判别法知, $f(x)$ 不可约.

(3) $f(y+1)=y^4+3y^3+3y^2+3y+3$, 取 $p=3$, 由艾森斯坦因判别法知, $f(y+1)$ 不可约, 故 $f(x)$ 不可约.

(4) $f(y+1)=y^4+4y^3+6y^2+4(k+1)y+2(2k+1)$, 取 $p=2$, 由艾森斯坦因判别法知, $f(y+1)$ 不可约, 故 $f(x)$ 不可约.

(5)

$$\begin{aligned}f(y-1)=(y-1)^p+p(y-1)+1&=\sum_{k=0}^{p}C_p^k(-1)^ky^{p-k}+p(y-1)+1\\&=\sum_{k=0}^{p-1}C_p^k(-1)^ky^{p-k}+py-p\\&=y^p-py^{p-1}+\frac{p(p-1)}{2}y^{p-2}+\cdots+\frac{p(p-1)}{2}y^2+2py-p.\end{aligned}$$

由艾森斯坦因判别法知, $f(y-1)$ 不可约, 故 $f(x)$ 不可约.

(6) 因为 $f(x)$ 无有理根, 故若 $f(x)$ 可约, 则必有

$$f(x)=(x^2+ax+1)(x^2+bx+1)\quad 或\quad f(x)=(x^2+ax-1)(x^2+bx-1).$$

对于左式, 计算其 3 次项及 1 次项系数, 得 $a+b=5$, $a+b=-5$, 不可能.

对右式, 令 $x=1$, 得 $ab=-1$, 又 $a+b=5$, 也不可能.

故 $f(x)$ 不可约.

3. 试将下列分式的分母有理化:

(1) $\dfrac{1}{1+\sqrt[3]{2}+2\sqrt[3]{4}}$;　　(2) $\dfrac{1}{1-\sqrt[4]{2}+\sqrt{2}}$;

(3) $\dfrac{1}{1+\sqrt{2}-\sqrt{3}}$;

(4) $\dfrac{a^2-3a-1}{a^2+2a+1}$, 其中, a 为方程 $x^3+x^2+3x+4=0$ 的根.

解: (1) 考察 $f(x)=2x^2+x+1$ 及 $g(x)=x^3-2$. 易知 $(f(x),g(x))=1$. 经计算知

$$(2x^2+x+1)\frac{x^2+7x-3}{23}-(x^3-2)\frac{-2x+13}{23}=1.$$

所以

$$\frac{1}{1+\sqrt[3]{2}+2\sqrt[3]{4}}=\frac{1}{23}(-3+7\sqrt[3]{2}-\sqrt[3]{4}).$$

(2) $\dfrac{1}{1-\sqrt[4]{2}+\sqrt{2}}=\dfrac{1}{7}(1+3\sqrt[4]{2}+2\sqrt{2}-\sqrt[4]{8}).$

(3) $\dfrac{1}{1+\sqrt{2}-\sqrt{3}}=\dfrac{1}{4}(2+\sqrt{2}+\sqrt{6}).$

(4) $\dfrac{a^2-3a-1}{a^2+2a+1}=17a^2-3a+55.$

4. 设 $f(x)$ 是一个整系数多项式. 证明: 如果 $f(0)$ 和 $f(1)$ 都是奇数, 则 $f(x)$ 无整数根.

证明: 反证. 如 $f(x)$ 有整数根 a, 则 $f(x)=(x-a)g(x)$, 其中 $g(x)$ 为整系数多项式. 则 $0-a$ 与 $1-a$ 中至少有一个是偶数, 从而 $f(0),f(1)$ 中至少有一个为偶数, 矛盾.

5. 设 $f(x)=x^3+bx^2+cx+d$ 是一个整系数多项式. 证明: 如果 $bd+cd$ 为奇数, 则 $f(x)$ 在有理数域上不可约.

证明: 由题设, d 与 $b+c$ 都是奇数, 从而 $f(0)=d$ 以及 $f(1)=1+b+c+d$ 均为奇数, 故 $f(x)$ 无整数根. 又因 $f(x)$ 的首项系数为 1, 且 $\deg f(x)=3$, 所以 $f(x)$ 不可约.

6. 已知整系数多项式 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 无有理根. 证明: 如果有素数 p, 使

(1) $p\nmid a_0$;

(2) $p\mid a_i, i=2,3,\cdots,n$;

(3) $p^2\nmid a_n$

则 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

证明: 如 $p\mid a_1$, 则由艾森斯坦因判别法知 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

以下设 $p\nmid a_1$. 设 $f(x)=g(x)h(x)$, $g(x),h(x)\in\mathbb{Z}[x]$. 由于 $f(x)$ 无有理根, 因此 $2\le\deg g(x)\le n-2$, $2\le\deg h(x)\le n-2$. 设

$$g(x)=b_0x^k+b_1x^{k-1}+\cdots+b_k,\qquad k\ge 2, m\ge 2,$$

$$h(x)=c_0x^m+c_1x^{m-1}+\cdots+c_m,\qquad k+m=n.$$

由于 $b_kc_m=a_n$, $p\mid a_n$, $p^2\nmid a_n$, 可设 $p\mid b_k$, $p\nmid c_m$. 又因 $p\nmid b_0$, 设 b_l 是从末尾起最先一个不能被 p 整除的系数, 则

$$p\nmid a_{m+l}=c_mb_l+c_{m-1}b_{l+1}+\cdots$$

但因 $m+l\ge 2$, $p\mid a_{m+l}$, 矛盾. 因此 $f(x)$ 在 $\mathbb{Q}$ 上不可约.

*$\mathbf{7.}$ 试确定所有的整数 m, 使 x^5+mx-1 在有理数域上可约.

证明: (a) 如 $m=0$, 则 x^5-1 显然可约.

(b) 如 $f(x)$ 有一次因式, 则 $1+m-1=0$ 或 $-1-m-1=0$, 从而 $m=0$ 或 -2.

(c) 若 $f(x)$ 不含一次因式, 但可约, 则可设

$$x^5+mx-1=(x^2+ax\pm 1)(x^3+bx^2+cx\mp 1).$$

比较两边系数, 得

$$a+b=0,\quad ab+c\pm 1=0,\quad ac\pm b\mp 1=0,\quad \mp(a-c)=m.$$

故 $b=-a$,

$$\begin{cases} -a^2+c=\mp 1 \\ ac\mp a=\pm 1 \\ m=\mp(a-c) \end{cases}$$

在第一种情形下, $c=0$, $a=-1$, $m=1$; 在第二种情形下, $c=2$, $a(c+2)=-1$, 不可能. 所以 m 的可能取值为 0, 1, -2. 在此 3 种情况下 x^5+mx-1 都可约.

*$\mathbf{8.}$ 设 $a_1,a_2,\cdots,a_n$ 为互不相同的整数, 证明: 多项式

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

在 $\mathbb{Q}$ 上不可约.

证明: 设

$$f(x)=g(x)h(x),\quad g(x),h(x)\in\mathbb{Z}[x],\quad \deg g(x),\deg h(x)<\deg f(x).$$

则 $f(a_i)=g(a_i)h(a_i)=-1$, 故 $g(a_i)=-h(a_i)=\pm 1$. 从而 $g(a_i)+h(a_i)=0$. 于是多项式

$$F(x)=g(x)+h(x)$$

有 n 个不同的根, 但 $\deg F(x)<n$, 只能 $F(x)=0$, $g(x)=-h(x)$, $f(x)=-g^2(x)$. 而当 x 充分大时, 有 $f(x)>0$, $-g^2(x)\le 0$, 矛盾. 因此

*$\mathbf{9.}$ 设 $a_1,a_2,\cdots,a_n$ 为互不相同的整数, 证明: 多项式

$$f(x)=(x-a_1)^2(x-a_2)^2\cdots(x-a_n)^2+1$$

在 $\mathbb{Q}$ 上不可约.

证明: 设 $f(x)=g(x)h(x)$, $g(x),h(x)\in\mathbb{Z}[x]$, 且

$$0<\deg g(x)<2n,\qquad 0<\deg h(x)<2n.$$

又因 $\deg g(x)+\deg h(x)=2n$, 故 $g(x),h(x)$ 中至少有一个的次数 $\le n$, 不妨设 $\deg h(x)\le n$. 又设 $g(x),h(x)$ 均为首一多项式.

由于 $f(x)$ 在实数上始终取正值, 因此 $f(x)$ 无实根, $g(x),h(x)$ 亦无实根. 于是 $g(x),h(x)$ 在实数上始终取正值. 又因 $f(a_i)=1$, 故 $h(a_i)=g(a_i)=1$. $h(x)-1$ 有 n 个不同的根 $a_1,\cdots,a_n$, 所以

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

从而 $\deg g(x)=n$, 进而

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

于是

$$\begin{aligned}g(x)h(x)&=[(x-a_1)\cdots(x-a_n)+1]^2\\&=(x-a_1)^2\cdots(x-a_n)^2+2(x-a_1)\cdots(x-a_n)+1\neq f(x),\end{aligned}$$

矛盾. 因此 $f(x)$ 不可约.

*10. 设本原多项式 $f(x)$ 在有理数域上不可约. 证明: $f(x^2)$ 在有理数域上可约的充分必要条件是存在整数 $c\neq 0$ 及整系数多项式 $g(x),h(x)$, 使

$$cf(x)=g^2(x)-xh^2(x).$$

证明: 充分性显然, 以下证必要性.

设 $g(x)$ 为 $f(x^2)$ 的任一不可约因式, 则由 $g(x)\mid f(x^2)$ 可得 $g(-x)\mid f(x^2)$, 显然 $g(-x)$ 也不可约.

$g(x)$ 与 $g(-x)$ 的关系仅有以下 3 种可能:

(a) $g(x)=g(-x)$; (b) $g(x)=-g(-x)$; (3) $(g(x),g(-x))=1$.

(a) 如 $g(x)=g(-x)$, 则 $g(x)=h(x^2)$, 由 $h(x^2)\mid f(x^2)$ 得 $h(x)\mid f(x)$, 而 $f(x)$ 不可约, 所以 $h(x)=cf(x)$, $g(x)=cf(x^2)$, 与 $f(x^2)$ 可约矛盾. 因此 $g(x)\neq g(-x)$.

(b) 如 $g(x)=-g(-x)$, 则 $g(x)=-xh(x^2)$, $xh(x^2)\mid f(x^2)$, 故 $x\mid f(x)$, 于是 $\pm f(x)=-x=0^2-x\cdot 1^2$, 结论成立.

(c) 如 $(g(x),g(-x))=1$, 则 $g(x)g(-x)\mid f(x^2)$. 设 $g(x)=u(x^2)+xv(x^2)$, 则

$$g(x)g(-x)=u^2(x^2)-x^2v^2(x^2).$$

而 $u^2(x^2)-x^2v^2(x^2)\mid f(x^2)$, 因此

$$u^2(x)-xv^2(x)\mid f(x).$$

故存在 $c\neq 0$ 使 $cf(x)=u^2(x)-xv^2(x)$, 证毕.

*$\mathbf{11.}$ 证明: 对所有的正整数 n, $f(x)=x^{2^n}-x^{2^{n-1}}+1$ 在有理数域上不可约. (提示: 对 n 用归纳法并应用习题 10)

证明: 首先要把习题 10 的结论加强为: 当 $f(x)$ 是本原多项式时, 可取 $c=1$. 为证这一结论, 考察

$$f(x^2)=c^{-1}(g^2(x^2)-x^2h^2(x^2))=c^{-1}(g(x^2)+xh(x^2))(g(x^2)-xh(x^2)),$$

注意到若 $g(x^2)+xh(x^2)=r(g_1(x^2)+xh_1(x^2))$, 其中 $g_1(x^2)+xh_1(x^2)$ 是本原多项式, 则 $g_1(x^2)-xh_1(x^2)$ 也是本原多项式, 于是

$$f(x^2)=c^{-1}r^2(g_1(x^2)+xh_1(x^2))(g_1(x^2)-xh_1(x^2))=c^{-1}r^2(g_1^2(x^2)-x^2h_1^2(x^2)),$$

根据高斯引理, $c^{-1}r^2=1$, 于是 $f(x)=g_1^2(x)-xh_1^2(x)$.

对 n 用归纳法, 并应用加强了的习题 10.

当 $n=1$ 时, 易知 x^2-x+1 在有理数域上不可约.

现设 $x^{2^n}-x^{2^{n-1}}+1$ 在有理数域上不可约, 而 $x^{2^{n+1}}-x^{2^n}+1$ 在有理数域上可约, 则根据加强的习题 10, 存在 $g(x),h(x)\in\mathbb{Z}[x]$, 使

$$x^{2^n}-x^{2^{n-1}}+1=g^2(x)-xh^2(x),$$

两边求导得

$$2^nx^{2^n-1}-2^{n-1}x^{2^{n-1}-1}=2g(x)g'(x)-h^2(x)-2xh(x)h'(x).$$

则 $2\mid h^2(x)$, $2\mid h(x)$, 所以

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

令

$$g(x)=x^{2^{n-1}}-x^{2^{n-2}}+1+k(x)+2l(x),$$

其中 $k(x)$ 的各项系数都是 0 或 1. 则

$$x^{2^n}-x^{2^{n-1}}+1=x^{2^n}-x^{2^{n-1}}+1+4x^{2^{n-1}}-2x^{2^{n-2}}-2x^{3\cdot 2^{n-2}}+k^2(x)+4p_2(x).$$

因此 $2\mid k(x)$, $4\mid k^2(x)$, 进而

$$x^{2^n}-x^{2^{n-1}}+1=x^{2^n}-x^{2^{n-1}}+1-2x^{2^{n-2}}-2x^{3\cdot 2^{n-2}}+4p_3(x),$$

$$4p_3(x)=2(x^{2^{n-2}}+x^{3\cdot 2^{n-2}},$$

这不可能, 从而知 $x^{2^{n+1}}-x^{2^n}+1$ 在有理数域上不可约.