§5.4–§5.5 Standard Factorization and Polynomial Functions

illusion

Especially made for smy

School of Mathematical Science, XMU

Monday 3rd March, 2025

http://illusion-hope.github.io/25-Spring-SMY-Discussion-Session/

例 1

设 $f(x), g(x) \in F[x]$, $(f(x), g(x)) = d(x)$，求证：对于任意的正整数 n，

$$(f^n(x), f^{n-1}(x)g(x), \ldots, g^n(x)) = d^n(x).$$

pf: Bézout's Theorem.

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

2° ✓

Key: 1°

Goal $\begin{cases} 1^\circ\ d^n \in \langle f^n, f^{n-1}g, \cdots, g^n \rangle \checkmark \\ 2^\circ\ d^n \text{ common divisor} \checkmark \end{cases}$

$d^n(x) = (uf+vg)^n = u^n f^n + C_n^1 u^{n-1} v f^{n-1} g + \cdots + C_n^n v^n g^n$

$\in \langle f^n, f^{n-1}g, \cdots, g^n \rangle.$

例 2

设非零多项式 $f(x), g(x) \in F[x]$. 证明： $(f(x), g(x)) \neq 1$ 的充分必要条件是存在 $p(x), q(x) \in F[x]$，使得

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

其中 $0 \leq \deg p(x) < \deg g(x), 0 \leq \deg q(x) < \deg f(x)$.

⇒ $(f,g)=d \neq 1 \Rightarrow f = f_1 d$, $g = g_1 d$, $(f_1, g_1)=1$.

取 $p = g_1$, $\deg g_1 < \deg g$; $q = f_1$

$\Rightarrow pf = qg = f_1 g_1 d$ ✓. （$f \sim g$ 时取 "="）

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

$\Rightarrow g(x)=0 \Rightarrow p(x)f(x)=0$

a≠0 时 p(x)=0 与 deg g≥0, deg p≥0 矛盾!

例 3

Assume $f(x), g(x), h(x) \in F[x]$, prove that

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

(2) There exists $a(x), b(x), c(x), u(x), v(x), r(x) \in F[x]$ such that

$$(f(x), g(x), h(x)) = \det \begin{bmatrix} f(x) & g(x) & h(x) \\ a(x) & b(x) & c(x) \\ u(x) & v(x) & r(x) \end{bmatrix}.$$

(1) 令 $d_1 = (f,g,h)$, $d_2 = ((f,g),h)$

· $d_1 \mid d_2$ → To show d_2 c.d. of f,g,h.

$d_2 \mid h$ ✓ $d_2 \mid (f,g) \mid f$, $d_2 \mid (f,g) \mid g$ ✓.

· $d_2 \mid d_1$ $\begin{cases} d_1 \mid f, d_1 \mid g. & \text{且 } uf+vg=(f,g) \xrightarrow{\deg} d_1 \mid (f,g) \\ d_1 \mid h \end{cases}$ ⇒ d_1 is a c.d. of $(f,g),h$ ⇒ $d_2 \mid d_1$ ∎

$$\begin{pmatrix} f & g & h \\ a & b & c \\ u & v & r \end{pmatrix} \xrightarrow{\text{Euclidean}} \begin{pmatrix} c_1(f,g) & 0 & h \\ * & * & c \\ * & * & r \end{pmatrix} \xrightarrow{\det} \begin{pmatrix} c_2(f,g,h) & 0 & 0 \\ * & *_2 & * \\ * & * & * \end{pmatrix}$$

$= c_2$: 最后那个根据 除去末的所有 的行列式 × 主项交换次数 $(-1)^{\ldots}$

$\rightsquigarrow c_2 \neq 0$

待定 a, b, c, u, v, r.

初等变换 ⇒ det 不变 $= (f, g, h)$

$f = qg + r$

①−②·q. 逆变换

$$\begin{pmatrix} f & g \\ a & b \\ u & v \end{pmatrix} \rightarrow \begin{pmatrix} f-qg & g \\ a-qb & b \\ u-qv & v \end{pmatrix}$$

①+②·q. 逆变换

引入 Bézout's Theorem

Note: 这个证明也可以推到 [illegible] for case.

Examples

例 3

Assume $f(x), g(x), h(x) \in F[x]$, prove that

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

(2) There exists $a(x), b(x), c(x), u(x), v(x), r(x) \in F[x]$ such that

$$(f(x), g(x), h(x)) = \det \begin{bmatrix} f(x) & g(x) & h(x) \\ a(x) & b(x) & c(x) \\ u(x) & v(x) & r(x) \end{bmatrix}.$$

Notes:

- 一般地，(1) 可以推广为
$$((f_1(x), f_2(x), \cdots, f_{n-1}(x)), f_n(x)) = (f_1(x), f_2(x), \cdots, f_{n-1}(x), f_n(x)).$$
- 存在 $u_i(x) \in F[x]$ 使 $\sum_{i=1}^{n} u_i(x) f_i(x) = (f_1(x), \cdots, f_n(x))$.

Properties of Relatively Prime

The following statements are equivalent with $(f(x), g(x)) = 1$:

(1) $u(x)f(x) + v(x)g(x) = 1 \rightsquigarrow 1 \mid f(x), 1 \mid g(x)$ is trivial;

(2) We can conclude $f(x) \mid h(x)$ from $f(x) \mid g(x)h(x)$, for all $h(x) \in F[x]$;

(3) We can conclude $f(x)g(x) \mid h(x)$ from $f(x) \mid h(x)$, $g(x) \mid h(x)$, for all $h(x) \in F[x]$;

(4) $(f(x^n), g(x^n)) = 1$ for any given positive integer n;

(5) $(f^n(x), g^n(x)) = 1$ for any given positive integer n;

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

(7) For any $n_1, n_2 \in \mathbf{N}^*$, we hold $(f^{n_1}, g^{n_2}) = (f, g)$;

(8) f, g do not have common irreducible factors in their standard factorization;

(9) f, g do not have common roots over $\mathbf{C}$.

(2) We can conclude $f(x) \mid h(x)$ from $f(x) \mid g(x)h(x)$, for all $h(x) \in F[x]$; ✡

$(f,g)=1 \Rightarrow$ (1)

$uf+vg=1 \Rightarrow ufh+vgh=h$

$\Rightarrow f \mid h-vgh$ 又 $f \mid gh \Rightarrow f \mid h$.

$\Leftarrow$

反证: $(f,g)=d\neq 1$ 取 h 使 conclu. 不成立.

$f=f_1 d,\ g=g_1 d$ 取 $h=f_1$ $f_1 d \mid f_1 g_1 d$ ✓

check $f=f_1 d \mid f_1 \neq h$ 不成立.

$d\neq 1 \Rightarrow \deg f_1 d > \deg f_1$!

□

(3) We can conclude $f(x)g(x) \mid h(x)$ from $f(x) \mid h(x)$, $g(x) \mid h(x)$, for all $h(x) \in F[x]$;

$(f,g)=1 \Rightarrow (3)$ $\quad f \mid h = fu \quad g \mid h = fv \quad (f,g)=1$

(3) 中 $g \mid u$ 令 $u = gv \Rightarrow h = fgv \Rightarrow fg \mid h$.

$\Leftarrow$ 反证：构造 $h = f_1 g_1 d$ 使结论不成立.

$(f,g) = d \neq 1$. $\quad f = f_1 d$, $g = g_1 d$ $\quad f \mid h$, $g \mid h$ ✓

$fg = f_1 g_1 d^2 \mid f_1 g_1 d$ 矛盾!

$\Rightarrow d^2 \mid d$ 于是 $\deg d^2 > \deg d$

□□□.

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

$(f,g)=1 \Rightarrow (6)$ 令: Lemma.

$(f,g)=1 \Rightarrow (f+g, g)=(f+g, f)=1$.

$u_1(f+g)+v_1 g = u_2(f+g)+v_2 f = 1$.

$[u_1(f+g)+v_1 g][u_2(f+g)+v_2 f]$

$= u(f+g)+v_1 v_2 fg = 1$ (1)

$\Rightarrow (f+g, fg)=1$.

$\Leftarrow$ 反证, $(f,g)=d\neq 1$ $d \mid f+g$, $d \mid d^2 \mid fg$.

$\Rightarrow d \mid (f+g, fg)$ 矛盾!

(7) For any $n_1, n_2 \in \mathbf{N}^*$, we hold $(f^{n_1}, g^{n_2}) = (f, g)$;

(7) $\Rightarrow$ $(f,g)=1$.

反证: $(f,g)=d\neq 1 \Rightarrow d^2 \mid (f^2, g^2) \neq (f,g)$ 矛盾! □

Properties of Relatively Prime

The following statements are equivalent with $(f(x), g(x)) = 1$:

(1) $u(x)f(x) + v(x)g(x) = 1 \rightsquigarrow 1 \mid f(x), 1 \mid g(x)$ is trivial;

(2) We can conclude $f(x) \mid h(x)$ from $f(x) \mid g(x)h(x)$, for all $h(x) \in F[x]$;

(3) We can conclude $f(x)g(x) \mid h(x)$ from $f(x) \mid h(x)$, $g(x) \mid h(x)$, for all $h(x) \in F[x]$;

(4) $(f(x^n), g(x^n)) = 1$ for any given positive integer n;

(5) $(f^n(x), g^m(x)) = 1$ for any given positive integer n, m;

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

(7) For any $n_1, n_2 \in \mathbf{N}^*$, we hold $(f^{n_1}, g^{n_2}) = (f, g)$;

(8) f, g do not have common irreducible factors in their standard factorization;

(9) f, g do not have common roots over $\mathbf{C}$.

(5) 推(7)

$(f, g) = 1 \Rightarrow$ (7).

Properties of Relatively Prime

(1) ⇒ $uf+v_1h=u_2g+v_2h=1$ $(u_1f+v_1h)(u_2g+v_2h)=u_1u_2fg+\tilde{v}h=1$.

⇐ 反证 $(f,h)=d\neq 1$ $d\mid (fg,h)\neq 1$ 矛盾同理于 g.

Try

Just check them:

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

(2) Assume $d(x)\neq 1$ is a common divisor of $f(x)$ and $g(x)$, let $f(x)=f_1(x)d(x),g(x)=g_1(x)d(x)$, prove that $(f_1,g_1)=1\Leftrightarrow(f,g)=d$. (Important!)

(2) ⇒ i° $uf_1+vg_1=1\Rightarrow udf_1+vdg_1=uf+vg=d\in\langle f,g\rangle$ ✓

ii° d is c.d. of f,g

⇐ $uf+vg=d\Rightarrow uf_1d+vg_1d=d\Rightarrow uf_1+vg_1=1\Rightarrow(f_1,g_1)=1$ □

Properties of Relatively Prime $\rightsquigarrow (f,g)=d\neq 1$ Case

Slogan: $d(x)\neq 1$ is a common divisor, $(f_1,g_1)=1 \Leftrightarrow (f,g)=d$.

例 4

(1) $(f(x),g(x))=d(x)$, then $(f(x)h(x),g(x)h(x))=d(x)h(x)$;

(2) $(f(x),g(x))=1$, then $(f(x)g(x),h(x))=(f(x),h(x))(g(x),h(x))$;

(3) Only use two conditions from $(f_i(x),g_j(x))=1\ (i,j=1,2)$ to prove that

$$(f_1(x)g_1(x),f_2(x)g_2(x))=(f_1(x),f_2(x))(g_1(x),g_2(x)).$$

例 5

Prove that $(x^n-1,x^m-1)=x^{(m,n)}-1$, where m,n are given positive integers.

Hint: For $m,n\in\mathbf{Z}$, there always exists $u,v\in\mathbf{Z}$ such that $um+vn=(m,n)$.

(2) $(f(x), g(x)) = 1$, then $(f(x)g(x), h(x)) = (f(x), h(x))(g(x), h(x))$;

Let $(f, h) = d_1$, $(g, h) = d_2$ $\quad f = f_1 d_1$, $g = g_2 d_2$

$(f_1, h_1) = (g_2, h_2) = 1$ $\quad h = h_1 d_1 = h_2 d_2$.

$(f, g) = 1 = (f_1 d_1, g_2 d_2) = 1$.

$\Rightarrow (d_1, d_2) = 1$. 不妨假设 $d_1 \mid d_2$.

$fg = f_1 g_2 \boxed{d_1 d_2}$ $\quad d_2 \mid h_1 d_1 \Rightarrow d_2 \mid h_1 \Rightarrow h_1 = h_3 d_2$.

$\Rightarrow h = h_3 d_1 d_2 = h_2 d_2 \Rightarrow h_2 = h_3 d_1$

To show $\boxed{(f_1 g_2, h_3) = 1}$. $\quad (f_1, h_1) = (g_2, h_2) = 1$

$h_1 = h_3 d_2$ $\quad h_2 = h_3 d_1$

$\Rightarrow (f_1, h_3) = (g_2, h_3) = 1$

Try (1) $\Rightarrow (f_1 g_2, h_3) = 1$ (1) (1).

(3) Only use two conditions from $(f_i(x), g_j(x)) = 1$ $(i, j = 1, 2)$ to prove that

$$(f_1(x)g_1(x), f_2(x)g_2(x)) = (f_1(x), f_2(x))(g_1(x), g_2(x)).$$

Let $(f_1, f_2) = d_1$, $(g_1, g_2) = d_2$.

$f_1 = \tilde{f}_1 d_1$, $f_2 = \tilde{f}_2 d_1$, $(\tilde{f}_1, \tilde{f}_2) = 1$

$g_1 = \tilde{g}_1 d_2$, $g_2 = \tilde{g}_2 d_2$, $(\tilde{g}_1, \tilde{g}_2) = 1$

$f_1 g_1 = \tilde{f}_1 \tilde{g}_1 d_1 d_2$ $f_2 g_2 = \tilde{f}_2 \tilde{g}_2 d_1 d_2$ To show $(\tilde{f}_1 \tilde{g}_1, \tilde{f}_2 \tilde{g}_2) = 1$

$(\tilde{f}_1, \tilde{f}_2) = (\tilde{f}_1, \tilde{g}_2) = 1 \Rightarrow (\tilde{f}_1, \tilde{f}_2 \tilde{g}_2) = 1$

$(\tilde{g}_1, \tilde{g}_2) = (\tilde{g}_1, \tilde{f}_2) = 1 \Rightarrow (\tilde{g}_1, \tilde{f}_2 \tilde{g}_2) = 1$

III.

例 5

Prove that $(x^n-1, x^m-1) = x^{(m,n)}-1$, where m, n are given positive integers.

Hint: For $m, n \in \mathbf{Z}$, there always exists $u, v \in \mathbf{Z}$ such that $um + vn = (m, n)$.

pf: Let $(m,n)=d$, $m = m_1 d$, $n = n_1 d$, $(m_1, n_1) = 1$.

$$x^n - 1 = (x^d - 1)\left[x^{(n_1-1)d} + x^{(n_1-2)d} + \cdots + x^d + 1\right]$$

$$\left(x^d\right)^{m_1} - 1 \qquad x^m - 1 = (x^d - 1)\left[x^{(m_1-1)d} + \cdots + x^d + 1\right]$$

To show $\left(x^{(n_1-1)d} + \cdots + x^d + 1,\ x^{(m_1-1)d} + \cdots + x^d + 1\right) = 1$.

$(m_1, n_1) = 1$

$\Rightarrow um_1 + vn_1 = 1$

$m, n_1 > 0$

$\Rightarrow u > 0, v < 0$

$um_1 = 1 - vn_1$

$n_1 x$ $\quad -vn_1 x$ $\quad m_1 x$

$x^{(n_1-1)d} + \cdots + x^d + 1$ $\quad n_1$

$x^{(m_1-1)d} + \cdots + x^d + 1$ $\quad m_1$

$um_1 x$

$$-x^{d}\cdot\left(x^{(v-1)n_1d}+\cdots-x^{2n_1d}+x^{n_1d}+1\right)\left(x_0^{(n-1)d}+\cdots+x^{d}+1\right)\quad①$$

$$+\left(x^{(u-1)m_1d}+\cdots+x^{m_1d}+1\right)\left(x^{(m_1-1)d}+\cdots+x^{d}+1\right)=1.\quad②$$

② 比①多一个最高次项

□□.

Chinese Reminder Theorem (CRT)

Thm 6

Given polynomials $f_1(x), \cdots, f_n(x)$, any two of which are relatively prime, then for $g_1(x), \cdots, g_n(x)$ such that $\deg g_i(x) < \deg f_i(x)$, there exists a unique polynomial $g(x)$ such that

$$g(x) \equiv g_i(x) \pmod{f_i(x)},$$

where $\deg g(x) < \sum_{i=1}^{n} \deg f_i(x)$.

(1) Create one $g(x)$ satisfying all the conditions $\rightsquigarrow \sum_{i=1}^{n} \left\{ u_i(x) \prod_{j \neq i} f_j(x) \right\} \cdot g_i(x)$

(2) Unique $\rightsquigarrow$ Relatively Prime

例 7

Suppose $a_1, \cdots, a_m \in F$ are different, for $b_1, \cdots, b_m \in F$, there exists a unique polynomial $L(x)$ such that $L(a_i) = b_i$ $(i = 1, 2, \cdots, m)$:

$$L(x) = \sum_{j=1}^{m} b_j \prod_{i \neq j} \frac{x - a_i}{a_j - a_i},$$

where $\deg L(x) < m$.

Hint: $L(a_i) = b_i \Leftrightarrow L(x) \equiv b_i \pmod{x - a_i}$.

$x-a_i \mid L(x)-b_i$

① $\sum_{j=1}^{n} b_j \prod_{i \neq j} \frac{1}{a_j - a_i} \prod_{i \neq j} (x-a_i)$

u_j

$= \sum_{j=1}^{n} b_j \prod_{i \neq j} \frac{x-a_i}{a_j-a_i}$ ☆

② $\left(\prod_{i \neq j} (x-a_i),\ x-a_j \right) = 1$ $(\forall j)$

$u(x) \prod_{i \neq j} (x-a_i) + v(x)(x-a_j) = 1$ $\exists\, x = a_j$

u 0 or 2. $\deg u < \deg (x-a_j) = 1$ ☆

$u = \frac{1}{\prod_{i \neq j} (a_j - a_i)}$

Irreducible $\Leftrightarrow$ Prime

Def 8

In $F[x]$, a polynomial $f(x)$ is called prime if for all $g(x), h(x) \in F[x]$, we can conclude $f(x) \mid g(x)$ or $f(x) \mid h(x)$ from $f(x) \mid g(x)h(x)$.

Def 9

In $F[x]$, a polynomial $f(x)$ is called irreducible if

(1) $f(x)$ is not a unit, i.e., $\deg f(x) > 0$;

(2) If we hold $f(x) = g(x)h(x)$ in $F[x]$, then $g(x)$ or $h(x)$ must be a unit.

Notes:

- (Irreducible $\Rightarrow$ Prime) If $f \mid gh$ and $f \nmid g$, we set $(f, g) = d$. Then, d is a divisor of $f \rightsquigarrow d = 1$ or $d = cf$. But we have $f \nmid g$, which implies $(f, g) = 1$ $\rightsquigarrow uf + vg = 1 \rightsquigarrow f \mid ufh = h - vgh \rightsquigarrow f \mid h$. (c is the reciprocal of the leading coefficient of $f(x)$.)

Irreducible $\Leftrightarrow$ Prime

- (Prime $\Rightarrow$ Irreducible) If $f = gh \mid gh$. We have $f \mid g$ or $f \mid h$. WLOG, $f \mid g$. But we also hold $g \mid f \rightsquigarrow g, f$ are associate. Then, h can only be a unit.
- (Cor.1) Assume $p(x)$ is irreducible, then for all $f(x) \in F[x]$, we hold either $p(x) \mid f(x)$ or $(p(x), f(x)) = 1$.
- (Cor.2) Assume $p(x)$ is irreducible, and we have $p(x) \mid f_1(x)f_2(x)\cdots f_n(x)$. Then, there must exists i such that $p(x) \mid f_i(x)$.

例 10

Prove that $f(x), g(x) \in F[x]$ are irreducible at the same time:

(1) $g(x) = f(ax + b),\ a, c \in F, a \neq 0.$

(2) $f(x) = \sum_{k=0}^{n} a_k x^k, g(x) = \sum_{k=0}^{n} a_{n-k} x^k,\ a_i \in F,\ a_0 a_n \neq 0.$

例 10

Prove that $f(x), g(x) \in F[x]$ are irreducible at the same time:

(1) $g(x) = f(ax+b),\ a, c \in F, a \neq 0.$

(2) $f(x) = \sum_{k=0}^{n} a_k x^k, g(x) = \sum_{k=0}^{n} a_{n-k} x^k,\ a_i \in F,\ a_0 a_n \neq 0.$

$g(x)$ 可约. $g(x) = g_1(x) g_2(x) \Rightarrow f(ax+b) = g_1(x) g_2(x)$

$0 < \deg g_{1,2} < \deg g \quad ax+b = t \Rightarrow x = \frac{t-b}{a}$

$= \deg f \quad f(t) = g_1\left(\frac{t-b}{a}\right) g_2\left(\frac{t-b}{a}\right)$

$\Rightarrow f$ 可约.

反之 f 可约 $\Rightarrow g$ 可约 $\quad f$ 可约 $\Leftrightarrow g$ 可约.

$\Rightarrow f$ 不可约 $\Leftrightarrow g$ 不可约.

(2) $f(x)=a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_n a_0 \neq 0$

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

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

$$\Rightarrow g(x)=\boxed{x^n f\left(\frac{1}{x}\right)} \quad \star$$

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

$g(x)$ 可约. $g(x)=g_1(x)g_2(x)=x^n f\left(\frac{1}{x}\right)$ 设 $\deg g_1=n_1$, $\deg g_2=n_2$

$n_1+n_2=n$, $n_1, n_2 \in (0,n)$

$$\Rightarrow g_1\left(\frac{1}{x}\right)g_2\left(\frac{1}{x}\right)x^n=f(x)$$

$$\deg\left(x^{n_1}g_1\left(\frac{1}{x}\right)\right)\left(x^{n_2}g_2\left(\frac{1}{x}\right)\right)=f(x)$$

(n_1, n_2) 与 $f(x)$ 可约矛盾!

Unique Factorization

Thm 11

Assume $f(x) \in F[x]$ is nonzero and not a unit.

(1) $f(x)$ can be expressed as a product of irreducible polynomials, i.e.,

$$f(x) = p_1(x) \cdots p_n(x),$$

where $p_i(x)$ are irreducible polynomials.

(2) In any two such factorizations

$$f(x) = p_1(x) \cdots p_n(x) = q_1(x) \cdots q_m(x).$$

We have $n = m$ and it is possible to rearrange the factors so that $p_i(x)$ and $q_i(x)$ are associate.

Note: $F[x]$ satisfies ACC (Ascending Chain Condition) on ideals.

$f(x)$ { irreducible √.

$f_1(x)\,\widetilde{f_1}(x)$ { 对 irre √.

继续下去 ⇝ 无限进行?

$f_1 \to f_2 \to f_3 \to \cdots \to f_n \to \cdots$

$(f_{i+1} \mid f_i)$.

$\langle f_1\rangle \subseteq \langle f_2\rangle \subseteq \langle f_3\rangle \subseteq \cdots \subseteq \langle f_n\rangle \subseteq \cdots \langle f_m\rangle = \langle f_{m+p}\rangle$

Claim: PID中没有无限严格增的 ideal chain. $= \cdots = \langle f_{m+p}\rangle$

$$\bigcup_{i=1}^{n} \langle f_i \rangle = I = \langle f_m \rangle$$ PID

① 整环、加法

② $\forall u(x) \in F[x]$. $f(x) \in I$, $u(x) f(x) \in I$.

① $\forall g_1, g_2 \in I$, $g_1 \in \langle f_i \rangle$, $g_2 \in \langle f_j \rangle$ $(i > j)$ $g_1 \pm g_2 \in \langle f_i \rangle \subseteq I$.

② $\forall g_1 \in I$, $g_1 \in \langle f_i \rangle$, $\forall u(x) \in F[x]$, $u g_1 \in \langle f_i \rangle \subseteq I$.

Unique Factorization

We write the common standard factorization of $f(x)$ and $g(x) \in F[x]$:

$$f(x) = c_1 p_1^{e_1}(x) \cdots p_n^{e_n}(x),\ g(x) = c_2 p_1^{t_1}(x) \cdots p_n^{t_n}(x),$$

where

- $p_i(x)$ are irreducible polynomials that are pairwise relatively prime and have leading coefficients of 1;
- The constant $c_1, c_2 \in F$ represent the leading coefficients $f(x)$ and $g(x)$;
- $e_i, t_j \in \mathbf{Z}$ satisfy $e_i, t_j \geq 0$, $e_i + t_j > 0$.

(1) $(f(x), g(x)), [f(x), g(x)]$, when $f(x) \mid g(x)$? ✓

(2) $F \subseteq K \rightsquigarrow p_1(x) = q_1^{m_1}(x) \cdots q_k^{m_k}(x)$ is the standard factorization of $p_1(x)$ in $K[x]$. $\rightsquigarrow$ Does there exist $m_s \geq 2$? ✗ impossible!

例 13

Given $f(x), h(x) \in F[x]$ such that $f^{27} \mid h^{29}$, if $\deg h(x) \le 13$, then $f(x) \mid h(x)$.

For cases that we hold $\deg h(x) \ge 14$, check that the conclusion may be wrong.

整除不随数域扩大而改变. $\mathbb{C}$ 上.

$(x-a_i)^{e_i} \to f \qquad (x-a_i)^{h_i} \to h$

$27 e_i \le 29 h_i$

$e_i \le h_i$?

$\deg h \ge 14$ 矛盾

若 $e_i \ge h_i + 1$ 则 $27h_i + 27 \le 27 e_i \le 29 h_i$

$\Rightarrow h_i \ge \frac{27}{2} = 13.5$

$h = (x-1)^{14} \qquad f = (x-1)^{15}$

$15 \times 27 < 29 \times 14$ ✓.

$f \nmid h$. ▯

Repeated Factors

$$f = c_1 p_1^{e_1}(x) \cdots p_n^{e_n}(x) \rightsquigarrow f' = c_1 p_1^{e_1-1}(x) \cdots p_n^{e_n-1}(x) \sum_{i=1}^{n} \left\{ e_i p_i'(x) \prod_{j \neq i} p_j(x) \right\}.$$

Slogan: $(f, f') = p_1^{e_1-1}(x) \cdots p_n^{e_n-1}(x)$, $\dfrac{f}{(f, f')} = p_1(x) \cdots p_n(x)$.

Notes:

(1) $e_i \equiv 1 \Leftrightarrow (f(x), f'(x)) = 1$; $\rightsquigarrow$不随数域扩大而改变!

(2) $\dfrac{f}{(f, f')}$ 与 $f(x)$ 有完全相同的不可约因式且无重因式;

(2') $g(x) = \dfrac{f}{(f, f')} \rightsquigarrow (g, g') = 1.$

例 14

Assume that an irreducible polynomial $p(x)$ is a $(k-1)$-multiple factor of $f'(x)$, then the following statements are equivalent:

(1) $p(x)$ is a $(k-1)$-multiple factor of (f, f');

(2) $p(x) \mid f(x)$;

(3) $p(x)$ is a k-multiple factor of $f(x)$.

(3') $f(x) = p^k(x)h(x),\ (p(x), f(x)) = 1.$

Note: When we talk about repeated factors, $p(x)$ should firstly be irreducible.

(1) ⇒ (2) √

(2) ⇒ (3) 设 $f(x) = p^t(x)h(x),\ (p,h)=1.$

$f'(x) = t p'(x) p^{t-1}(x) h(x) + p^t(x) h'(x)$

$= p^{t-1}(x)\left[t p'(x) h(x) + p(x) h'(x) \right]$

$p(x)$ 为 $f'(x)$ 的 $t-1$ 重 ($k-t$)

$k-1 = t-1 \Rightarrow k = t$

$\Rightarrow p(x) \mid p'(x)h(x)$ $(p,h)=1 \Rightarrow p \mid p'$ 矛

(3) ⇒ (1)