§5.4—§5.5 Standard Factorization and Polynomial Functions

illusion

Especially made for smy

School of Mathematical Science, XMU

Sunday 2nd March, 2025

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

HW-2

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，

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

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

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

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

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

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

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!)

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 $um + vn = (m, n)$.

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

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

(2) Unique $\rightsquigarrow$ Relatively Prime

Lagrange Interpolation Formula

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 $L(a_i) = b_i$ $(i = 1, 2, \cdots, m)$:

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

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

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

Outline of Chapter 5: Polynomial

Polynomial Algebra $\rightsquigarrow$ $F[x]$ is a PID (Principal Ideal Domain)

- Division Theorem, Divisibility
- The (Not A!) Greatest Common Divisor (GCD) and Relatively Prime
- $\rightsquigarrow$ Chinese Reminder Theorem (CRT) $\rightsquigarrow$ Lagrange Interpolation Formula
- In PID, Irreducible $\Leftrightarrow$ Prime
- (PID $\Rightarrow$ UFD) Unique Factorization
- Repeated Factor $\rightsquigarrow$ $(f(x), f'(x)) = 1$?

Polynomial Functions:

- Remainder Theorem
- Roots

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

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.

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 $f(x) \mid g(x)$? $\checkmark$

(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 $m_s \geq 2$?

Examples

例 12

Assume $f(x), g(x) \in F[x]$ and n is a given positive integer,

(1) $f(x) \mid g(x) \Leftrightarrow f^n(x) \mid g^n(x)$;

(2) $(f(x), g(x)) = d(x) \Leftrightarrow (f^n(x), g^n(x)) = d^n(x)$.

Note: (§5.2) Recall that $x \mid f(x) \Leftrightarrow x^2 \mid f^2(x)$.

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;

(3) 若 $p(x)$ 为 $f'(x)$ 的 $k-1$ 重因式，则其未必为 $f(x)$ 的 k 重因式。条件改为 (f, f') 的 $k-1$ 重因式时结论成立。

Multiple Roots

- If $f(x)$ has a multiple root a over F, then it must have repeated factors. But the converse is wrong.
- If a is a $k-$multiple root of $f(x)$, then it's a $(k-1)-$multiple root of $f'(x)$. But the converse is wrong.
- If a is a $(k-1)-$multiple root of (f', f), then it's a $k-$multiple root of $f(x)$.

例 13

(1) $p(x)$ is irreducible over $F \Rightarrow p(x)$ has no multiple roots over $\mathbf{C}$;

(2) $p(x)$ is irreducible over F and has common roots with $f(x)$ over $\mathbf{C} \Rightarrow p \mid f$.

Examples

Slogan: $p(x)$ 在 F 上不可约且在 $\mathbf{C}$ 上与 $f(x)$ 有公共根 $\Rightarrow p \mid f$.

例 14

(1) $f(x) \in \mathbf{R}[x],\ f(a+b\mathrm{i}) = 0\ (a, b \in \mathbf{R}) \rightsquigarrow f(a-b\mathrm{i}) = 0$;

(2) $f(x) \in \mathbf{Q}[x],\ f(\sqrt{2}+\sqrt{3}) = 0 \rightsquigarrow f(\sqrt{2}-\sqrt{3}) = f(-\sqrt{2}+\sqrt{3}) = f(-\sqrt{2} - \sqrt{3}) = 0$.

Hint: What is the standard factorization of $x^4 - 10x + 1$ in $\mathbf{R}[x]$?

例 15

$f(x) \in F[x]$ 在 F 上不可约，若非零常数 a, a^{-1}, b 为 $f(x)$ 在 $\mathbf{C}$ 上的根，证明：$f(b^{-1}) = 0$.

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

Examples

Slogan: $p(x)$ 在 F 上不可约且在 $\mathbf{C}$ 上与 $f(x)$ 有公共根 $\Rightarrow p \mid f$.

例 16

$f(x) \in F[x]$ 在 F 上不可约，对 $g(x) \in F[x]$，有 $\alpha \in \mathbf{C}$ 满足 $f(c) = 0, g(c) \neq 0$.

(1) 存在 $h(x) \in F[x]$ 满足 $h(c)g(c) = 1$;

(2) 求一个多项式 $h(x) \in \mathbf{Q}[x]$ 满足

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

Hint: $p \mid f \Rightarrow$ All the roots of $p(x)$ are roots of $f(x)$.