§5.4—§5.5 Standard Factorization and Polynomial Functions

illusion

Especially made for smy

School of Mathematical Science, XMU

Monday 24th February, 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 $\deg g(x) < \sum_{i=1}^{n} \deg f_i(x)$.

(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

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

Examples

例 8

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 $x \mid f(x) \Leftrightarrow x^2 \mid f^2(x)$.