§5.3 The Greatest Common Divisor and Chinese Remainder Theorem (CRT)

illusion

Especially made for smy

School of Mathematical Science, XMU

Friday 21$^{\text{st}}$ February, 2025

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

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 $\rightsquigarrow$ $(f(x), f'(x)) = 1$?

HW-1

(1) (USTC, 2019) 已知 $(x-1)^2(x+1) \mid (ax^4+bx^2+cx+1)$，求 a, b, c ;

(2) 求 $(x+1)(x-1)$ 除 $f(x)=x^4+x^3+x+1$ 所得的商和余式;

(2’) 求 99999999 除 100010000000010001 所得的商和余数。

Revisit Two Examples

例 1

If $m, n, p \in \mathbb{N}^*$ have the same parity, then $x^2 - x + 1 \mid x^{3n} - x^{3m+1} + x^{3p+2}$.
Check the converse of this proposition is also true.

Hint: $x^2 - x + 1 \mid x^3 + 1 \mid x^{3(2k)+l} + x^{3+l}$, $x^2 - x + 1 \mid x^3 + 1 \mid x^{3(2k-1)+l} + x^l$.

例 2

Determine all polynomials $f(x) \in F[x]$ such that $f[f(x)] = f^n(x)$, where $n \in \mathbf{N}^*$ is a given positive integer. **Note: You can only use the method of divisibility.**

Hint: $f^l(x) \mid f^n(x) = f[f(x)]$, $\forall\ 1 \le l \le n$.

Euclidean Algorithm and Bézout's Theorem

Slogan: $f(x) = q(x)g(x) + r(x) \rightsquigarrow (f(x), g(x)) = (g(x), r(x))$.

Thm 3

(Bézout's Theorem) Given two polynomials $f(x), g(x) \in F[x]$, then $(f(x), g(x))$ exists and there exist $u(x), v(x) \in F[x]$ such that

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

Notes:

- $u(x), v(x)$ **are not unique**. The non-uniqueness comes from the fact that if $u(x), v(x)$ satisfy the equation, then so do $\tilde{u}(x) = u(x) + kg(x), \tilde{v}(x) = v(x) - kf(x)$ for any constant $k \in F$, i.e.,

$$(f(x), g(x)) = [u(x) + kg(x)]f(x) + [v(x) - kf(x)]g(x).$$

Euclidean Algorithm and Bézout's Theorem

- (最大公因式，互素与数域扩大无关) Suppose K is another number field such that $F \subseteq K$, then $(f(x), g(x))$ in $K[x]$ will be **equal** to what is obtained over $F[x]$. $\rightsquigarrow$ Key: Division Theorem!
- How to determine $(f(x), g(x))$? $\rightsquigarrow$ Euclidean Algorithm.
- **Special Case**: $(f(x), g(x)) = 1 \rightsquigarrow u(x), v(x)$ are **unique** if $\deg u(x) < \deg g(x), \deg v(x) < \deg f(x)$! $\rightsquigarrow$ Try to prove it.

  $\rightsquigarrow$ This conclusion will be used in the proof of Lagrange Interpolation Formula.

Try

Suppose $f(x) = x^4 - x^3 - x^2 + 2x - 1, g(x) = x^3 - 2x + 1$. Figure out $u(x)$, $v(x), (f(x), g(x))$.

Explore Corresponding Characterizations of GCD

Def 4

We say that $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$ if $d(x)$ is a common divisor of $f(x)$ and $g(x)$ that all other common divisors divide.

Set $\Omega := \{u(x)f(x) + v(x)g(x) \mid u(x), v(x) \in F[x]\}$, then the definition is equal to:

(1) A common divisor that has the maximal degree;

$\rightsquigarrow$ GCDs have the same degree and are associate.

$\rightsquigarrow\rightsquigarrow$ The one whose leading coefficient is 1 is denoted as $(f(x), g(x))$.

(2) A **nonzero** polynomial $d(x) \in \Omega$ with minimal degree;

(3) A nonzero polynomial $d(x) \in \Omega$ divides all other elements in Ω.

(3') (3) $\Leftrightarrow d(x) \mid f(x)$, $d(x) \mid g(x)$.

Examples

例 5

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

(1) $(f(x), g(x)) = d(x) \Leftrightarrow (f(x^n), g(x^n)) = d(x^n)$;

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

Notes:

- (§5.4) Actually, $(f(x), g(x)) = d(x) \Leftrightarrow (f^n(x), g^n(x)) = d^n(x)$;
- Specially, $(f(x), g(x)) = 1 \Leftrightarrow (f(x^n), g(x^n)) = 1$.

Examples

例 6

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 $\sum_{i=1}^{n} u_i(x) f_i(x) = (f_1(x), \cdots, f_n(x))$.

Examples

例 7

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

例 8

Given two polynomials in $\mathbf{C}[x]$: $f(x) = a_0 + a_1 x + a_2 x^2 + a_{10} x^{10} + \cdots + a_{13} x^{13}$ $(a_{13} \neq 0)$ and $g(x) = b_0 + \cdots + b_3 x^3 + b_{11} x^{11} + \cdots + b_{13} x^{13}$ $(b_3 \neq 0)$, try to prove that $\deg(f(x), g(x)) \leq 6$.

Hint: Recall that $\deg(f, g) = \arg\min_{u,v} \{\deg(uf + vg) \mid u, v \in F[x]\}$.

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 9

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

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

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

Examples

例 10

Suppose $f(x), g(x), h(x) \in F[x]$, $\boldsymbol{A} \in M_n(F)$ and $f(\boldsymbol{A}) = \boldsymbol{O}$.

(1) If $(f(x), g(x)) = d(x)$, then $r[g(\boldsymbol{A})] = r[d(\boldsymbol{A})]$;

(2) If $(f(x), g(x)) = 1$, then $g(\boldsymbol{A})$ is invertible;

(3) If $f(x) = g(x)h(x)$, then $g(\boldsymbol{A}), h(\boldsymbol{A})$ will not be invertible at the same time.

Notes:

- (Chapter 1) $\boldsymbol{A}^2 - \boldsymbol{A} + 2\boldsymbol{E} = \boldsymbol{O} \rightsquigarrow \boldsymbol{A} - 3\boldsymbol{E}$ 必定可逆；
- (Chapter 1) $\boldsymbol{A}^2 = \boldsymbol{E}, \boldsymbol{A} - \boldsymbol{E} \neq \boldsymbol{O} \rightsquigarrow \boldsymbol{A} + \boldsymbol{E}$ 必不可逆；
- (Chapter 4) $\varphi \in \mathcal{L}(V), \varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_1\varphi + a_0 = \mathscr{O}\ (a_0 \neq 0) \rightsquigarrow \varphi$ 必定可逆(为同构映射)。

Revisit An Example in Lecture 1

例 11

Prove that when $f(x) \in F[x]$ is divided by $(x-a)(x-b)$ $(a \neq b)$, the reminder $r(x)$ is

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

We only need to find $g(x)$ such that $f(x) \equiv g(x) \pmod{(x-a)(x-b)}$ with its degree lower than 2.

$\rightsquigarrow$ Notice that $f(a)=f(a) \Leftrightarrow x-a \mid f(x)-f(a) \Leftrightarrow f(x) \equiv f(a) \pmod{x-a}$.

$$\rightsquigarrow \begin{cases} f(x) \equiv f(a) \pmod{x-a} \\ f(x) \equiv f(b) \pmod{x-b} \end{cases} \rightsquigarrow \text{CRT}$$

Chinese Reminder Theorem (CRT)

Thm 12

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 13

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

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

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

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

Examples

例 14

求一个次数最低的 $f(x) \in F[x]$ 满足 $(x-3)^2$ 除 $f(x)$ 余 $3x-7$, x^2 除 $f(x)$ 余 x^2+2x+3.

例 15

已知 $r_1(x) = x^2+2x+3, r_2(x) = 3x-7, A = \mathrm{diag}\{A_1, A_2\}, B = \mathrm{diag}\{B_1, B_2\}$,

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, A_2 = \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix}, B_1 = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 3 & 2 \\ 0 & 0 & 3 \end{bmatrix}, B_2 = \begin{bmatrix} 2 & 3 \\ 0 & 2 \end{bmatrix}.$$

先验证 $r_i(A_i) = B_i$，再求一个次数最低的多项式 $f(x)$ 满足 $f(A) = B$.