§5.1—§5.2 Division Theorem and Divisibility

illusion

Especially made for smy

School of Mathematical Science

XMU

Saturday 15^{th} February, 2025

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
- $\rightsquigarrow\rightsquigarrow$ (Chapter 7) Jordan-Chevalley Decomposition
- In PID, Irreducible $\Leftrightarrow$ Prime
- (PID $\Rightarrow$ UFD) Unique Factorization
- Repeated Factor $\rightsquigarrow$ $(f(x), f'(x)) = 1$?

Outline of Chapter 5: Polynomial

Polynomial Functions:

- Remainder Theorem
- Roots

Examples:

- $\mathbf{C}[x]$: Factorization, Viéta Theorem
- $\mathbf{R}[x]$: Factorization, Complex Roots Come in Pairs
- $\mathbf{Q}[x]$: Rational Root Theorem, Eisenstein's Criterion
- $\mathbf{Z}[x]$: Gauss's Lemma, Factorization

Multivariate Polynomials $F[x_1, \cdots, x_n]$:

- Perturbation Method
- Fundamental Theorem of Symmetric Polynomials, Newton's Formulas

Try

令

$$f(x)=\left\{\sum_{k=0}^{2n}(-1)^k x^k\right\}\left\{\sum_{k=0}^{2n}x^k\right\}$$

那么其中 x^{2p} 的系数均为 1，x^{2p-1} 的系数均为 0. $(1\le p\le 2n^2,\ p\in\mathbb{N}^*)$

$F[x]$ is an integral domain:

- $f(x),g(x)\in F[x]$, if $f(x),g(x)\neq 0$，then $f(x)g(x)\neq 0$;
- $f(x),g(x),h(x)\in F[x]$, if $f(x)h(x)=g(x)h(x),\ h(x)\neq 0$, then $f(x)=g(x)$.

Examples

例 1

If $f(x), g(x), h(x) \in \mathbf{R}[x]$ and we have $xf^2(x) + xg^2(x) = h^2(x)$, then $f(x) = g(x) = h(x) = 0$.

Notes:

- 回顾 $f(x), g(x) \in \mathbf{R}[x], f^2(x) + g^2(x) = 0 \rightsquigarrow f(x) = g(x) = 0$.
- 上述两个结论在 $\mathbf{C}[x]$ 上还成立吗?

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.

Hint: $f(x) \neq 0 \rightsquigarrow \deg f[f(x)] = (\deg f(x))^2$.

Review of §5.2 Division Theorem

Thm 3

Suppose $f(x), g(x) \in F[x]$ and $g(x) \neq 0$, then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x), \tag{1}$$

where $\deg r(x) < \deg g(x)$.

Notes:

- 若 $r(x) = 0$，那么 $\deg 0 = -\infty < \deg g(x)$ 也成立；
- (带余除法与数域扩大无关) 若 $F \subseteq K$，在 $K[x]$ 中存在 $\tilde{q}(x), \tilde{r}(x) \in K[x]$ 满足

$$f(x) = \tilde{q}(x)g(x) + \tilde{r}(x) \rightsquigarrow \tilde{q}(x) = q(x),\ \tilde{r}(x) = r(x).$$

A Direct Corollary of Division Theorem

例 4

Suppose $f(x), g(x) \in F[x]$ and $g(x) \neq 0$. Let $k \in \mathbf{N}^*$ and assume $k \deg g(x) \leq \deg f(x) < (k+1) \deg g(x)$. Then, there exist unique polynomials $p_i(x) \in F[x]$ $(i = 0, 1, 2, \cdots, k)$ such that

$$f(x) = p_0(x) + p_1(x)g(x) + \cdots + p_k(x)g^k(x), \tag{2}$$

where $\deg p_i(x) < \deg g(x)$.

Hint: We can repeatedly apply the division theorem to the quotient $q(x)$.

Examples

例 5

(1) Find the quotient $q(x)$ and the reminder $r(x)$ when $f(x) = 3x^4 - 4x^3 + 5x - 1$ is divided by $g(x) = x^2 - x + 1$.

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

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

Note: (2) will be revisited after we learn CRT and Lagrange Interpolation Formula.

Thm 6

Given conditions in Division Theorem, if we have $r(x) = 0$, i.e., $f(x) = q(x)g(x)$, we say that $g(x)$ divides $f(x)$ (or $g(x)$ is a divisor of $f(x)$), and we denote this as $g(x) \mid f(x)$. Otherwise, we write $g(x) \nmid f(x)$.

Notes:

- 整除有自反性和传递性，以及相伴性(associate)：

$$f(x) \mid g(x), g(x) \mid f(x) \rightsquigarrow \exists\, c \in F, f(x) = cg(x);$$

- (整除与数域扩大无关) 若 $F \subseteq K$，在 $K[x]$ 中存在 $\tilde{q}(x) \in K[x]$ 满足

$$f(x) = \tilde{q}(x)g(x) \rightsquigarrow \tilde{q}(x) = q(x).$$

Examples

Slogan: $r(x) = 0 \Leftrightarrow g(x) \mid f(x)$.

例 7

(1) $f(x), g(x) \in F[x]$, $f(x^2) \mid g(x^2) \Rightarrow f(x) \mid g(x)$;

(2) $f(x), g(x) \in F[x]$, $f^2(x) \mid g^2(x) \Rightarrow f(x) \mid g(x)$;

(3) Given $a \neq 0, d, n \in \mathbf{N}^*$, $x^m - a^m \mid x^n - a^n \Leftrightarrow m \mid n$.

Notes:

- 修改 (1) 为 $f(x^n) \mid g(x^n)$ $(n \in \mathbf{N}^*, n \geq 3) \Rightarrow f(x) \mid g(x)$ 还成立吗?
- 修改 (2) 为 $f^n(x) \mid g^n(x)$ $(n \in \mathbf{N}^*, n \geq 3) \Rightarrow f(x) \mid g(x)$ 还成立吗?
- 回顾: $x \mid f(x) \Leftrightarrow x^2 \mid f^2(x)$;
- (HW) $x^m - 1 \mid x^n - 1 \Leftrightarrow m \mid n$.

Examples

Slogan: $g(x) \mid f_k(x) \rightsquigarrow g(x) \left| \sum_k h_k(x) f_k(x) \right.$, For all $h_k(x) \in F[x]$.

例 8

(1) $x^2 + x + 1 \mid x^{3n} + x^{3m+1} + x^{3p+2}$, For all $n, m, p \in \mathbb{N}^*$;

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

Notes:

- (§5.5 Polynomial Functions) Alternative: $x^2 + x + 1 = (x - \omega_1)(x - \omega_2) = 0$, $\omega_i^3 = 1, \omega_i \neq 1 \rightsquigarrow \omega_i^{3n} + \omega_i^{3m+1} + \omega_i^{3p+2} = 1 + \omega_i^1 + \omega_i^2 = 0$.
- When we have $x^2 + x + 1 \left| \sum_i x^{a_i} \right. \ (a_i \in \mathbb{N}^*)$?