Notes of "Polynomials"

Jinxin Wang

1 一元多项式

Definition 1 (数域 P 上的一元多项式).

Definition 2 (一元多项式相等及零多项式).

Definition 3 (数域 P 上的一元多项式环).

2 整除的概念

Proposition 1 (带余除法的成立).

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

$q(x)$ and $r(x)$ are uniquely determined. $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

Remark 1 (综合除法). 对于除式是次数为 *1* 的多项式的情况，我们有一个快速进行带余除法的技巧，叫做综合除法。它基于以下观察

$$f(x) = \Sigma_{i=0}^{n} a_i x^i, g(x) = x - c, q(x) = \Sigma_{i=0}^{n-1} b_i x^i, r(x) = r$$

$$\begin{aligned} q(x)g(x) + r(x) &= b_{n-1}x^n + (b_{n-2} - cb_{n-1})x^{n-1} + (b_{n-3} - cb_{n-2})x^{n-2} + \cdots + (b_0 - cb_1)x + r - cb_0 \\ &= \Sigma_{i=0}^{n} a_i x^i \\ &= f(x) \end{aligned}$$

则系数间有如下关系:

$$\begin{cases} b_{n-1} = a_n \\ b_{n-2} = a_{n-1} + cb_{n-1} \\ b_{n-3} = a_{n-2} + cb_{n-2} \\ \cdots \\ b_1 = a_2 + cb_2 \\ b_0 = a_1 + cb_1 \\ r = a_0 + cb_0 \end{cases}$$

根据上述关系，我们可以快速得到带余除法的结果。

注意上述关系只在除式 $g(x) = x - c$ 即一次项系数为 1 才成立，对于一次项系数不是 1 的除式，则有 $g(x) = c_1 x + c_0 = c_1(x + \frac{c_0}{c_1}) = c_1 g'(x)$.

Definition 4 (整除)**.**

Properties of Divisors:

- 对偶等价于相差常数倍
- 传递性
- 整除组合

3 最大公因式

Definition 5 (Common Divisor and Greatest Common Divisor)**.** *If $\phi(x)$ is a divisor of both $f(x)$ and $g(x)$, we say it is a common divisor of $f(x)$ and $g(x)$.*

Suppose $f(x) \in P[x]$ and $g(x) \in P[x]$. A polynomial $d(x) \in P[x]$ is the greatest common divisor of $f(x)$ and $g(x)$ if the following conditions are true:

- *$d(x)$ is a common divisor of $f(x)$ and $g(x)$.*
- *Every common divisor of $f(x)$ and $g(x)$ is a divisor of $d(x)$.*

Remark 2. *Since any polynomial $f(x) \in P[x]$ is a divisor of the zero polynomial, in other words $0 = 0 \cdot f(x)$, the greatest common divisor of $f(x)$ and 0 is $f(x)$. Especially, the greatest common divisor of 0 and 0 is 0, which is in accordance with the definition of GCD.*

Lemma 1 (Common Divisors in Euclidean Division)**.** *If it holds that $f(x) = q(x)g(x) + r(x)$ for $f(x) \in P[x]$ and $g(x) \in P[x]$, then the two pairs of polynomials $(f(x), g(x))$ and $(g(x), r(x))$ have the same common divisors.*

证明. □

Remark 3. *The pair of polynomials $(f(x), g(x))$ has the same common divisors as the pair of polynomials $(f(x) - q(x)g(x), g(x)), \forall q(x) \in P[x]$. Hence, the two pairs has the same property decided by common divisors, such as GCD and coprime.*

Application:

- *Euclid's Algorithm*
- *If $(f(x), g(x)) = 1$, then $(f(x), f(x) + g(x)) = (g(x), f(x) + g(x)) = 1$.*

Theorem 1 (Theorem of Polynomial Greatest Common Divisor)**.** *$\forall f(x) \in P[x]$ and $\forall g(x) \in P[x]$, there exists $d(x) \in P[x]$ that is the greatest common divisor of $f(x)$ and $g(x)$, and $d(x)$ can be expressed as a combination of $f(x)$ and $g(x)$, which is $\exists u(x) \in P[x], v(x) \in P[x]$ such that*

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

证明. (TODO) □

Remark 4 (The uniqueness of the expression of GCD as a combination of $f(x)$ and $g(x)$)**.** *The combination of $f(x)$ and $g(x)$ to express their greatest common divisor $d(x)$ is not unique.*

Remark 5 (Euclid's algorithm)**.**

Proposition 2. *If $d(x)$ is a common divisor of $f(x)$ and $g(x)$, then*

$$((f(x),g(x))=d(x)) \Leftrightarrow (\exists u(x),v(x)\in P[x](d(x)=u(x)f(x)+v(x)g(x)))$$

Definition 6 (Coprime)**.** $(f(x),g(x))=1$

Theorem 2 (互素的等价条件)**.**

$$((f(x),g(x))=1) \Leftrightarrow u(x)f(x)+v(x)g(x)=1$$

Remark 6. *This theorem contains a kind of symmetry because both $f(x)$ and $g(x)$ and $u(x)$ and $v(x)$ are coprime.*

Theorem 3. *If $(f(x),g(x))=1$, and $f(x)|g(x)h(x)$, then $f(x)|h(x)$.*

证明. Hint:

$$u(x)f(x)+v(x)g(x)=1$$

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

□

Corollary 1. *If $f_1(x)|g(x)$, $f_2(x)|g(x)$, and $(f_1(x),f_2(x))=1$, then $f_1(x)f_2(x)|g(x)$.*

证明. Hint:

$$(f_1 \mid g) \Rightarrow (g=f_1h_1)$$

$$(f_2 \mid g) \Rightarrow (f_2 \mid f_1h_1) \Rightarrow (f_2 \mid h_1)$$

□

上述结论均可推广到多个多项式。

4 因式分解定理

Definition 7 (不可约多项式)**.**

Example 1. x^2+1 在实数域上是不可约多项式。

Remark 7. *Irreducible* 是一个相对于数域的概念，因为一个多项式在一个数域上不可约，但在更大的数域上可能变为可约多项式。因此我们在讨论不可约多项式时必须指明数域。

Remark 8. 由定义可知，$(p(x)\in P[x]$ is irreducible$) \Leftrightarrow p(x)$ 的因式只有 $c\neq 0$ 和 $cp(x)(c\neq 0)$. 因此，$\forall f(x)\in P[x]$, $(p(x),f(x))=1$ *or* $(p(x),f(x))=p(x)$. *In other words, either $p(x)$ and $f(x)$ are coprime, or $p(x)$ is a divisor of $f(x)$.*

Theorem 4 (不可约多项式作因式)**.** *Suppose $p(x)\in P[x]$ is a irreducible polynomial. Given two polynomials $f(x),g(x)\in P[x]$, if $p(x)\mid f(x)g(x)$, then $p(x)\mid f(x)$ or $p(x)\mid g(x)$.*

证明. If $p(x) \mid f(x)$, then the conclusion holds.

If $p(x) \nmid f(x)$, then $(p(x), f(x)) = 1$, and hence $p(x) \mid g(x)$. The conclusion holds. □

Theorem 5 (因式分解定理)**.**

证明. Hint: 存在性证明利用对被分解的多项式的次数进行数学归纳法。唯一性证明利用对分解的不可约多项式的个数进行数学归纳法。 □

Definition 8 (标准分解式)**.**

5 重因式

Definition 9 (k 重因式、重因式和单因式)**.**

Theorem 6. 如果不可约多项式 $p(x)$ 是 $f(x)$ 的 k 重因式，那么它是 $f'(x)$ 的 $k-1$ 重因式。

证明. Hint: 由于 $p(x)$ 是 $f(x)$ 的 k 重因式, there exists $q(x)$ such that $p(x) \nmid q(x)$ and $f(x) = p^k(x)q(x)$. Since $p(x)$ is irreducible, $(p(x) \nmid q(x)) \Rightarrow ((p(x), q(x)) = 1)$. Then

$$\begin{aligned} f'(x) &= kp^{k-1}(x)p'(x)q(x) + p^k(x)q'(x) \\ &= p^{k-1}(x)(kp'(x)q(x) + p(x)q'(x)) \end{aligned}$$

□

Remark 9 (The necessity of the prerequisite that $p(x)$ is irreducible)**.** *From the proof we can see the prerequisite that $p(x)$ is irreducible is necessary. If $p(x)$ is not irreducible, then $p(x)$ and $q(x)$ might have common divisors, which may result in $p(x)|p'(x)q(x)$, and thus $p(x)$* 至少是 $f(x)$ 的一个 k 重因式。

Remark 10 (The falsity of its converse and a counterexample)**.** 这个定理的逆命题并不成立，即若不可约多项式 $p(x)$ 是 $f'(x)$ 的 k 重因式，并不能推出 $p(x)$ 是 $f(x)$ 的 $k+1$ 重因式。*A counterexample: Given $f(x) = \frac{1}{3}x^3 - x$, then $f'(x) = x^2 - 1$, and $(x-1)$ is a divisor of $f'(x)$, but it is not a divisor of $f(x)$.*

Corollary 2. *A irreducible polynomial* $p(x)$ 是 $f(x)$ 的 k 重因式 $\Leftrightarrow$ $p(x)$ 是 $f(x), f^{(1)}(x), f^{(2)}(x), \ldots,$ $f^{(k-1)}(x)$ 的因式，但不是 $f^{(k)}(x)$ 的因式。

证明. $\Rightarrow$: Use mathematical induction on k

$\Leftarrow$: Use proof by contradiction. 如果 $p(x)$ 是 $f(x)$ 的 $n(n > k)$ 重因式，则 $p(x)$ 是 $f^{(k)}$ 的因式，这与条件相矛盾。如果 $p(x)$ 是 $f(x)$ 的 $n(n < k)$ 重因式，则 $p(x)$ 不是 $f^{(k-1)}(x)$ 的因式，这与条件相矛盾。 □

Corollary 3. $p(x)$ 是 $f(x)$ 的重因式 $\Leftrightarrow$ $p(x)$ 是 $f(x)$ 和 $f'(x)$ 的公因式

Corollary 4. $f(x)$ 没有重因式 $\Leftrightarrow$ $f(x)$ 和 $f'(x)$ 互素

Remark 11. 这个推论给出了一个判别一个多项式 $f(x)$ 是否有重因式的方法，即判断 $f(x)$ 和 $f'(x)$ 是否互素，具体方法是 *Euclid's Algorithm. The process is even mechanical.*

6 多项式函数

Definition 10 (多项式函数的根和零点).

Theorem 7 (The polynomial remainder theorem). 用一次多项式 $x-\alpha$ 去除多项式 $f(x)$，所得的余式是一个常数，这个常数等于 $f(\alpha)$。

Corollary 5. *The polynomial remainder theorem relates a root of a polynomial to a divisor of the polynomial as follows:*

$$(x=\alpha \text{ is a root of } f(x)) \Leftrightarrow ((x-\alpha) \mid f(x))$$

Definition 11 (重根和单根).

Theorem 8 (非零多项式根的个数的最大值). *A non-zero polynomial $f(x) \in P[x]$ with the degree of $n(n \geq 0)$ has at most n roots.*

Theorem 9 (多项式共点定理). 如果多项式 $f(x), g(x)$ 的次数都不超过 n，而它们对 $n+1$ 个不同的数 $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ 有相同的值，即 $f(\alpha_i) = g(\alpha_i), i = 1, 2, \ldots, n+1$，则 $f(x) = g(x)$。

证明. □

Example 2 (Lagrange Interpolating Polynomial).

7 复系数与实系数多项式的因式分解

7.1 复系数多项式

Theorem 10 (Fundamental Theorem of Algebra). 每个次数大于等于 *1* 的复系数多项式在复数域中有一根。

Theorem 11 (复系数多项式因式分解定理). 每一个次数大于等于 *1* 的复系数多项式在复数域上都可以唯一地分解为一次因式的乘积。

7.2 实系数多项式

Lemma 2 (实系数多项式根的共轭性). 在复数域上，若 $x=\alpha$ 是一个实系数多项式的根，则其共轭 $\bar{x}=\bar{\alpha}$ 也是这个实系数多项式的一个根。

Theorem 12 (实系数多项式因式分解定理). 每一个次数大于等于 *1* 的实系数多项式在实数域上都可以唯一地分解为一次因式和二次不可约因式的乘积。

证明. □

8 有理系数多项式

Definition 12 (本原多项式). 如果一个非零整系数多项式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ 的系数 $a_n, a_{n-1}, \ldots, a_1, a_0$ 是互素的，则我们称这样的多项式为 *primitive polynomial.*

Remark 12. *For all non-zero polynomial $p(x) \in \mathbb{Q}[x]$, it can be expressed as $r \cdot g(x)$ in which $r \in \mathbb{Q}$ and $g(x)$ is a primitive polynomial. This expression is unique up to a $\pm$ sign.*

Example 3.

$$f(x) = \frac{5}{4} = \frac{5}{4} \cdot 1 = -\frac{5}{4} \cdot (-1)$$

$$f(x) = \frac{2}{3}x = \frac{2}{3} \cdot (x) = -\frac{2}{3} \cdot (-x)$$

$$f(x) = \frac{2}{3}x^4 - 2x^2 + \frac{4}{5} = \frac{2}{15}(5x^4 - 15x^2 + 6) = -\frac{2}{15}(-5x^4 + 15x^2 - 6)$$

Theorem 13 (Gauss's Lemma)**.** *The product of two primitive polynomials is still a primitive polynomial.*

证明. □

Theorem 14. 如果一个非零的整系数多项式能够分解为两个次数较低的有理系数多项式的乘积，那么它一定能分解成两个次数较低的整系数多项式的乘积。

Corollary 6. *Suppose $f(x), g(x) \in \mathbb{Z}[x]$, and $g(x)$ is a primitive polynomial. If $f(x) = g(x)h(x)$, in which $h(x) \in \mathbb{Q}[x]$, then we can conclude that $h(x) \in \mathbb{Z}[x]$.*

证明. □

Remark 13. *If $g(x)$ is not a primitive polynomial,*

Theorem 15 (A necessary condition of rational roots of a polynomial with integer coefficients)**.** *Suppose $f(x) \in \mathbb{Z}[x]$ where $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. If $\frac{r}{s}$ is a rational root of $f(x)$ and r, s are coprime, then*

$$s \mid a_n, r \mid a_0$$

Especially if $a_n = 1$, then all rational roots of $f(x)$ are integers, and divisors of a_0.

证明. Since $x = \frac{r}{s}$ is a rational root of $f(x)$, there exists $g(x) \in \mathbb{Q}[x]$ such that

$$f(x) = (sx - r)g(x)$$

□

Theorem 16 (Eisenstein's Criterion)**.** *Suppose $f(x) \in \mathbb{Z}[x]$ where $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. If there is a prime number p such that*

- $p \nmid a_n$
- $p \mid a_{n-1}, a_{n-2}, \ldots, a_0$
- $p^2 \nmid a_0$

then $f(x)$ is irreducible in $\mathbb{Q}$.

Remark 14. 使用 *Eisenstein's Criterion* 有一个技巧：换元法。如果经过变量替换后的整系数多项式在有理数域上不可约，则原整系数多项式在有理数域上不可约。

证明. □

Example 4. *Determine whether the polynomial $f(x) = x^p + px + 1$ where p is an odd prime number is reducible in $\mathbb{Q}$.*

Let $x = g(y) = y - 1$ then

$$\begin{aligned} f(x) &= f(g(y)) \\ &= (y-1)^p + p(y-1) + 1 \\ &= \Sigma_{k=0}^{p} \binom{p}{k} y^{p-k}(-1)^k + py - p + 1 \end{aligned}$$

Since p is an odd number,

$$\Sigma_{k=0}^{p} \binom{p}{k} y^{p-k}(-1)^k = y^p + \Sigma_{k=1}^{p-2} \binom{p}{k} y^{p-k}(-1)^k + py - 1$$

Hence

$$\begin{aligned} f(x) &= f(g(y)) \\ &= y^p + \Sigma_{k=1}^{p-2} \binom{p}{k} y^{p-k}(-1)^k + 2py - p \end{aligned}$$

Example 5. *$\forall n \in \mathbb{N}^+$, the polynomial $x^n + 2$ is irreducible in $\mathbb{Q}$, since with a prime number $p = 2$, $p \nmid a_n = 1$, $p \mid a_{n-1} = 0, a_{n-2} = 0, \ldots, a_1 = 0, a_0 = 2$, and $p^2 \nmid a_0 = 2$. Therefore, in $\mathbb{Q}$ there is at least one irreducible polynomial with any degree.*

9 多元多项式

Definition 13 (单项式、同类项、n 元多项式、单项式和多项式的次数)**.**

Remark 15 (字典排序法)**.**

Theorem 17. *If $f(x_1, x_2, \cdots, x_n) \neq 0$, $g(x_1, x_2, \cdots, x_n) \neq 0$, the first term of $f(x_1, x_2, \cdots, x_n)g(x_1, x_2, \cdots, x_n)$ is the product of the first term of $f(x_1, x_2, \cdots, x_n)$ and the first term of $g(x_1, x_2, \cdots, x_n)$.*

Corollary 7. *If $f_i(x_1, x_2, \cdots, x_n) \neq 0, i = 1, 2, \ldots, m$, then the first term of $f_1 f_2 \cdots f_m$ is the product of the first term of every polynomial $f_i (i = 1, 2, \ldots, m)$.*

Corollary 8. *If $f(x_1, x_2, \cdots, x_n) \neq 0$, $g(x_1, x_2, \cdots, x_n) \neq 0$, then $f(x_1, x_2, \cdots, x_n)g(x_1, x_2, \cdots, x_n) \neq 0$.*

Remark 16. 这个推论指出了多元多项式环中没有非 *0* 零因子。

10 对称多项式

Definition 14 (Symmetric Polynomials)**.**

Definition 15 (Elementary Symmetric Polynomials)**.** *n 元多项式环中有一类特殊的对称多项式*

$$\begin{cases} \sigma_1 = x_1 + x_2 + \cdots + x_n \\ \sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n \\ \sigma_3 = x_1x_2x_3 + x_1x_2x_4 + \cdots + x_1x_2x_n + x_1x_3x_4 + \cdots + x_1x_{n-1}x_n + x_2x_3x_4 + \cdots + x_{n-2}x_{n-1}x_n \cdots \\ \sigma_n = x_1x_2 \cdots x_{n-1}x_n \end{cases} \tag{2}$$

Theorem 18. *对于任意一个 n 元对称多项式 $f(x_1, x_2, \cdots, x_n)$，都存在一个 n 元多项式 $\phi(x_1, x_2, \cdots, x_n)$，使得*

$$f(x_1, x_2, \cdots, x_n) = \phi(\sigma_1, \sigma_2, \cdots, \sigma_n)$$