

高等代数专题

倪兴程¹

2025 年 2 月 20 日

¹Email: 19975022383@163.com

Todo list

辗转相除法在 latex 里面很难搞，不想打了	8
没搞懂	9
倒根变换需要严格证明	13

目录

第一章 多项式	1
1.1 多项式带余除法及整除	1
1.1.1 证明多项式整除性的常用方法	1
1.1.2 例题	1
1.2 最大公因式与互素多项式	6
1.2.1 基本定义与定理	6
1.2.2 题型	6
1.2.3 例题	8
1.3 多项式的根	11
1.3.1 题型	11
1.3.2 例题	12
1.3.3 复根、实根、有理根与整数根	12
1.3.4 三个常用数域上的多项式	14

Chapter 1

多项式

1.1 多项式带余除法及整除

1.1.1 证明多项式整除性的常用方法

1. 定义法

要证 $g(x)|f(x)$, 去构造 $h(x)$, 使得 $f(x) = h(x)g(x)$ 。常常将 $f(x)$ 分解因式分解出 $g(x)$, 剩下的就是 $h(x)$ 。

2. 带余除法定理

要证 $g(x)|f(x)$, 只要证 $g(x)$ 除 $f(x)$ 的余式为 0。

3. 准标准式分解法

要证 $g(x)|f(x)$, 只要证它们的准标准分解式中的同一个不可约因式的方幂前者不大于后者。

4. 根法

要证 $g(x)|f(x)$, 只要证在复数域中 $g(x)$ 的根都是 $f(x)$ 的根, 重根按重数计算。

1.1.2 例题

定理 1.1. $f(x) = (x+1)^{k+n} + 2x(x+1)^{k+n-1} + \cdots + (2x)^k(x+1)^n$, 证明 $x^{k+1} | (x-1)f(x) + (x+1)^{k+n+1}$ 。

证明. 因为:

$$\begin{aligned} f(x) &= (x+1)^{k+n} + 2x(x+1)^{k+n-1} + \cdots + (2x)^k(x+1)^n \\ &= (x+1)^n \left[(x+1)^k + (2x)(x+1)^{k-1} + \cdots + (2x)^k \right] \end{aligned}$$

因为 $x - 1 = [2x - (x + 1)]$, 所以:

$$\begin{aligned}
 (x-1)f(x) + (x+1)^{k+n+1} &= [2x - (x+1)](x+1)^n \left[(x+1)^k + (2x)(x+1)^{k-1} + \cdots + (2x)^k \right] \\
 &\quad + (x+1)^{k+n+1} \\
 &= (x+1)^n [2x - (x+1)] \left[(x+1)^k + (2x)(x+1)^{k-1} + \cdots + (2x)^k \right] \\
 &\quad + (x+1)^{k+n+1} \\
 &= (x+1)^n [(2x)^{k+1} - (x+1)^{k+1}] + (x+1)^{k+n+1} \\
 &= (2x)^{k+1} (x+1)^n
 \end{aligned}$$

显然有 $x^{k+1} | (x-1)f(x) + (x+1)^{k+n+1}$. □

定理 1.2. 证明 $g(x) = 1 + x^2 + \cdots + x^{2n}$ 整除 $f(x) = 1 + x^4 + x^8 + \cdots + x^{4n}$ 的充分必要条件是 n 是偶数。

证明. 显然:

$$g(x) = \frac{1 - (x^2)^{n+1}}{1 - x^2}, \quad f(x) = \frac{1 - (x^4)^{n+1}}{1 - x^4}$$

所以:

$$\begin{aligned}
 g(x)|f(x) &\Leftrightarrow \frac{1 - (x^2)^{n+1}}{1 - x^2} \Big| \frac{1 - (x^4)^{n+1}}{1 - x^4} \\
 &\Leftrightarrow (1 + x^2)[1 - (x^2)^{n+1}] \Big| [1 - (x^4)^{n+1}] \\
 &\Leftrightarrow (1 + x^2) | [1 + (x^2)^{n+1}] \\
 &\Leftrightarrow 1 + x^2 \text{ 的根 } \pm i \text{ 都是 } 1 + (x^2)^{n+1} \text{ 的根} \\
 &\Leftrightarrow 1 + (-1)^{n+1} = 0 \\
 &\Leftrightarrow n \text{ 为偶数}
 \end{aligned}$$
□

定理 1.3. 设 $f(x), g(x)$ 为数域 K 上的多项式, $n \in \mathbb{Z}$. 证明 $f(x)|g(x)$ 的充分必要条件为 $f^n(x)|g^n(x)$.

证明. **(1) 必要性:** 若 $f(x)|g(x)$, 则存在数域 K 上的多项式 $h(x)$ 使得 $g(x) = h(x)f(x)$, 于是 $g^n(x) = h^n(x)f^n(x)$, 所以 $f^n(x)|g^n(x)$.

(2) 充分性: 将 $f(x), g(x)$ 进行标准分解得到:

$$f(x) = ap_1^{r_1}(x) \cdots p_m^{r_m}(x), \quad g(x) = bq_1^{t_1}(x) \cdots q_n^{t_n}(x)$$

于是:

$$f^k(x) = a^k p_1^{kr_1}(x) \cdots p_m^{kr_m}(x), \quad g^k(x) = b^k q_1^{kt_1}(x) \cdots q_n^{kt_n}(x)$$

因为 $f^k(x)|g^k(x)$, 所以 $f(x)$ 标准分解式中的任一元素 $p_i(x)$, $i = 1, 2, \dots, m$ 都是 $g(x)$ 标准分解式中的元素 (记为 q_{n_i}), 同时有 $kr_i \leq kt_{n_i}$, 即 $r_i \leq t_{n_i}$, 于是 $f(x)|g(x)$. □

定理 1.4. $(x^d - 1)|(x^n - 1)$ 的充分必要条件为 $d|n$.

证明. (1) 充分性: 由 $d|n$ 可知, 存在正整数 k 使得 $n = dk$ 。于是:

$$x^n - 1 = x^{dk} - 1 = (x^d)^k - 1 = (x^d - 1)[x^{d(k-1)} + \cdots + 1]$$

所以 $(x^d - 1)|(x^n - 1)$ 。

(2) 必要性: 由整数的带余除法定理, 设 $n = dq + r$, 这里 $r = 0$ 或 $0 < r < d$ 。若 $0 < r < d$, 则:

$$x^n - 1 = x^{dq+r} - 1 = x^{dq}x^r - x^r + x^r - 1 = x^r(x^{dq} - 1) + (x^r - 1)$$

由充分性可知 $(x^d - 1)|(x^{dq} - 1)$ 。而 $(x^d - 1)|(x^n - 1)$ 。则 $(x^d - 1)|(x^r - 1)$ 。于是 $d \leq r$, 矛盾。□

定理 1.5. 设 $h(x), k(x), f(x), g(x)$ 是实系数多项式, 且:

$$(x^2 + 1)h(x) + (x + 1)f(x) + (x - 2)g(x) = 0$$

$$(x^2 + 1)k(x) + (x - 1)f(x) + (x + 2)g(x) = 0$$

则 $(x^2 + 1)|f(x)$, 且 $(x^2 + 1)|g(x)$ 。

证明. 要证 $(x^2 + 1)|f(x)$ 和 $(x^2 + 1)|g(x)$, 即证 $\pm i$ 是 $f(x)$ 和 $g(x)$ 的根。将 $x = \pm i$ 代入上式可得:

$$(i + 1)f(i) + (i - 2)g(i) = 0, \quad (i - 1)f(i) + (i + 2)g(i) = 0$$

$$(-i + 1)f(-i) + (-i - 2)g(-i) = 0, \quad (-i - 1)f(-i) + (-i + 2)g(-i) = 0$$

解方程可得:

$$f(i) = g(i) = 0, \quad f(-i) = g(-i) = 0$$

所以 $(x - i)|f(x)$, $(x + i)|f(x)$, $(x - i)|g(x)$, $(x + i)|g(x)$ 。因为 $(x + i, x - i) = 1$, 所以 $(x + i)(x - i)|f(x)$, $(x + i)(x - i)|g(x)$, 即 $(x^2 + 1)|f(x)$, $(x^2 + 1)|g(x)$ 。□

定理 1.6. 对于任意 $n \in \mathbb{N}^+$, 都有 $(x^2 + x + 1) \mid [x^{n+2} + (x + 1)^{2n+1}]$ 。

证明. 方法一: 令 $x^2 + x + 1 = 0$, 求得它在复数域内的两个根分别为 $x_1 = \frac{-1 + \sqrt{3}i}{2}$, $x_2 = \frac{-1 - \sqrt{3}i}{2}$ 。将 x_1, x_2 代入到 $x^{n+2} + (x + 1)^{2n+1}$ 中可得:

$$x^{n+2} + (x + 1)^{2n+1} = x^2 x^n + (x + 1)(x^2)^n = 0$$

于是 x_1, x_2 也是 $x^{n+2} + (x + 1)^{2n+1}$ 的根, 所以 $(x^2 + x + 1) \mid [x^{n+2} + (x + 1)^{2n+1}]$ 。

方法二: 设 α 为 $x^2 + x + 1 = 0$ 的根, 则 $\alpha^2 + \alpha + 1 = 0$, 两边同乘 $\alpha - 1$ 可得 $\alpha^3 = 1$ 且 $\alpha \neq 1$ 。于是:

$$\begin{aligned} \alpha^{n+2} + (\alpha + 1)^{2n+1} &= \alpha^{n+2} + (-\alpha^2)^{2n+1} \\ &= \alpha^{n+2} + (-1)^{2n+1} \alpha^{4n+2} \\ &= \alpha^{n+2} - \alpha^{3n} \alpha^{n+2} \\ &= 0 \end{aligned}$$

于是 α 是 $x^{n+2} + (x+1)^{2n+1} = 0$ 的根, 所以 $(x^2 + x + 1) \mid [x^{n+2} + (x+1)^{2n+1}]$ 。 \square

定理 1.7. 若 $(s, n+1) = 1$, 则 $f(x) = x^{sn} + x^{s(n-1)} + \cdots + x^s + 1$ 可被 $g(x) = x^n + x^{n-1} + \cdots + x + 1$ 整除。

证明. 假设 α 为 $g(x) = 0$ 的根, 因为:

$$g(x) = \frac{1 - x^{n+1}}{1 - x}$$

所以 $\alpha^{n+1} = 1$ 且 $\alpha \neq 1$ 。而:

$$f(x) = \frac{1 - (x^s)^{n+1}}{1 - x^s} = \frac{1 - (x^{n+1})^s}{1 - x^s}$$

代入 $\alpha^{n+1} = 1$ 则显然 $f(x) = 0$, 即 α 也是 $f(x) = 0$ 的根, $g(x) \mid f(x)$ 。但是如果 α 是 $f(x)$ 的根, 此时应有 $\alpha^s \neq 1$ 。若 $\alpha^s = 1$, 因为 $(s, n+1) = 1$, 则存在 $u, v \in \mathbb{N}$, 使得:

$$us + v(n+1) = 1$$

于是 $\alpha = \alpha^{us+v(n+1)} = \alpha^{us}\alpha^{v(n+1)} = \alpha^{us}(\alpha^{n+1})^v = (\alpha^s)^u = 1$, 与 $\alpha \neq 1$ 矛盾, 所以 $\alpha^s - 1 \neq 0$ 。 \square

定理 1.8. 设 $n \in \mathbb{N}^+$, $f_1(x), f_2(x), \dots, f_n(x)$ 都是多项式, 并且有:

$$x^n + x^{n-1} + \cdots + x + 1 \mid f_1(x^{n+1}) + x f_2(x^{n+1}) + \cdots + x^{n-1} f_n(x^{n+1})$$

证明 $(x-1)^n \mid f_1(x)f_2(x)\cdots f_n(x)$ 。

证明. 设 $x^{n+1} - 1 = 0$ 的不为 1 的 n 个根分别为 $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$, 此时有 $\varepsilon_i^{n+1} - 1 = 0$, $i = 1, 2, \dots, n$ 。对 $x^{n+1} - 1 = 0$ 作分解可得 $x^n + x^{n-1} + \cdots + x + 1 = (x - \varepsilon_1)(x - \varepsilon_2) \cdots (x - \varepsilon_n)$, 所以:

$$x - \varepsilon_i \mid x^n + x^{n-1} + \cdots + x + 1 \mid f_1(x^{n+1}) + x f_2(x^{n+1}) + \cdots + x^{n-1} f_n(x^{n+1})$$

于是 ε_i , $i = 1, 2, \dots, n$ 是 $f_1(x^{n+1}) + x f_2(x^{n+1}) + \cdots + x^{n-1} f_n(x^{n+1}) = 0$ 的根, 所以:

$$\begin{cases} f_1(\varepsilon_1^{n+1}) + \varepsilon_1 f_2(\varepsilon_1^{n+1}) + \cdots + \varepsilon_1^{n-1} f_n(\varepsilon_1^{n+1}) = 0 \\ f_1(\varepsilon_2^{n+1}) + \varepsilon_2 f_2(\varepsilon_2^{n+1}) + \cdots + \varepsilon_2^{n-1} f_n(\varepsilon_2^{n+1}) = 0 \\ \vdots \\ f_1(\varepsilon_n^{n+1}) + \varepsilon_n f_2(\varepsilon_n^{n+1}) + \cdots + \varepsilon_n^{n-1} f_n(\varepsilon_n^{n+1}) = 0 \end{cases}$$

即:

$$\begin{cases} f_1(1) + \varepsilon_1 f_2(1) + \cdots + \varepsilon_1^{n-1} f_n(1) = 0 \\ f_1(1) + \varepsilon_2 f_2(1) + \cdots + \varepsilon_2^{n-1} f_n(1) = 0 \\ \vdots \\ f_1(1) + \varepsilon_n f_2(1) + \cdots + \varepsilon_n^{n-1} f_n(1) = 0 \end{cases}$$

将 $f_i(1)$, $i = 1, 2, \dots, n$ 看作未知数, 因为 $\varepsilon_i \neq \varepsilon_j$, $i \neq j$, 所以该线性方程组的系数行列式为:

$$\det(A) = \begin{vmatrix} 1 & \varepsilon_1 & \varepsilon_1^2 & \cdots & \varepsilon_1^{n-1} \\ 1 & \varepsilon_2 & \varepsilon_2^2 & \cdots & \varepsilon_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \varepsilon_n & \varepsilon_n^2 & \cdots & \varepsilon_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (\varepsilon_j - \varepsilon_i) \neq 0$$

所以该线性方程组只有零解, 即 $f_i(1) = 0$, 于是 $x - 1 | f_i(x)$, $i = 1, 2, \dots, n$, 所以 $(x - 1)^n | f_1(x)f_2(x)f_n(x)$ 。□

定理 1.9. 求多项式 $f(x)$, 使得 $(x^2 + 1) | f(x)$ 且 $(x^3 + x^2 + 1) | f(x) + 1$ 。

证明. 由整除的定义, 存在多项式 $g(x), h(x)$ 使得

$$\begin{aligned} f(x) &= (x^2 + 1)g(x) \\ f(x) + 1 &= (x^3 + x^2 + 1)h(x) \end{aligned}$$

由条件可知 $\pm i$ 是 $f(x)$ 的根, 将 $\pm i$ 分别代入上第二式可得:

$$1 = -ih(i), \quad 1 = ih(-i)$$

取 $h(x) = x$ 发现可以满足上式要求, 于是 $f(x) = x^4 + x^3 + x - 1$ 。□

定理 1.10. 求 7 次多项式 $f(x)$, 使得 $(x - 1)^4 | f(x) + 1$, 且 $(x + 1)^4 | f(x) - 1$ 。

证明. 因为 $(x - 1)^4 | f(x) + 1$, 所以 1 至少是 $f(x) + 1$ 的四重根, 于是 1 至少是 $f'(x)$ 的三重根, 即 $(x - 1)^3 | f'(x)$ 。同理可得 $(x + 1)^3 | f'(x)$ 。因为 $((x - 1)^3, (x + 1)^3) = 1$, 所以 $(x - 1)^3(x + 1)^3 | f'(x)$ 。因为 $f'(x)$ 是六次多项式, 可设:

$$f'(x) = \alpha(x - 1)^3(x + 1)^3$$

其中 α 为常数。对上式积分可得:

$$f(x) = \alpha \left(\frac{1}{7}x^7 - \frac{3}{5}x^5 + x^3 - x \right) + c$$

因为 $(x - 1)^4 | f(x) + 1$, $(x + 1)^4 | f(x) - 1$, 所以 $f(1) = -1$, $f(-1) = 1$, 代入上式可解得:

$$\begin{cases} a = \frac{35}{16} \\ c = 0 \end{cases}$$

所以:

$$f(x) = \frac{5}{16}x^7 - \frac{21}{16}x^5 + \frac{35}{16}x^3 - \frac{35}{16}x$$

□

1.2 最大公因式与互素多项式

1.2.1 基本定义与定理

定义 1.1. 设 $f(x), g(x), d(x) \in K[x]$, 若:

1. $d(x)|f(x), g(x)$;
2. 若任意的 $\varphi(x)|f(x), g(x)$, 都有 $\varphi(x)|d(x)$;

则称 $d(x)$ 为 $f(x), g(x)$ 的最大公因式。用 $(f(x), g(x))$ 表示 $f(x)$ 和 $g(x)$ 首项系数为 1 的最大公因式。

定理 1.11 (最大公因式定理). $K[x]$ 上的任意两个多项式 $f(x), g(x)$ 都有最大公因式, 并且 $f(x)$ 和 $g(x)$ 的任意一个最大公因式 $d(x)$ 都可以表示为 $f(x)$ 与 $g(x)$ 的一个组合, 即:

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

定理 1.12. 若 $f(x) = g(x)q(x) + r(x)$, $g(x) \neq 0$, 则 $(f(x), g(x)) = (g(x), r(x))$ 。

定义 1.2. 设 $f(x), g(x) \in K[x]$, 若 $(f(x), g(x)) = 1$, 则称 $f(x)$ 和 $g(x)$ 互素。

定理 1.13. $(f(x), g(x)) = 1$ 的充分必要条件为:

$$\exists u(x), v(x) \in K[x], u(x)f(x) + v(x)g(x) = 1$$

定理 1.14. 若 $(f(x), g(x)) = 1$, 且 $f(x)|g(x)h(x)$, 则 $f(x)|h(x)$ 。

定理 1.15. 若 $(f(x), g(x)) = 1$, 且 $f(x)|h(x)$, $g(x)|h(x)$, 则 $f(x)g(x)|h(x)$ 。

定理 1.16. 若 $(f(x), g(x)) = 1$, $(f(x), h(x)) = 1$, 则 $(f(x), g(x)h(x)) = 1$ 。

定理 1.17. 数域的扩张不影响最大公因式和互素。

1.2.2 题型

求具体多项式最大公因式

1. 辗转相除法

(a) 计算 $f(x)$ 除以 $g(x)$, 得到商 $q(x)$ 和余数 $r(x)$, 即:

$$f(x) = g(x) \cdot q(x) + r(x)$$

其中, $r(x)$ 是多项式的余数, 且满足 $\deg(r(x)) < \deg(g(x))$ 。

(b) 如果余数 $r(x) = 0$, 则 $g(x)$ 就是 $f(x)$ 和 $g(x)$ 的最大公因式。

(c) 如果余数 $r(x) \neq 0$, 则将 $f(x)$ 赋值为 $g(x)$, 将 $g(x)$ 赋值为 $r(x)$, 然后返回第 1 步。

2. 因式分解法

如果求得 $f(x), g(x)$ 在数域 K 上的标准分解式:

$$f(x) = ap_1^{r_1}(x) \cdots p_m^{r_m}(x), \quad g(x) = bq_1^{t_1}(x) \cdots q_n^{t_n}(x)$$

二者最大的公共部分即为 $f(x), g(x)$ 的最大公因式。

证明最大公因式

1. 定义法

要证 $d(x)$ 是 $f(x), g(x)$ 的最大公因式, 只要证:

(a) $d(x)$ 是 $f(x), g(x)$ 的公因式;

(b) 以下二者的任意一条:

- 找到 $u(x), v(x)$ 使得 $u(x)f(x) + v(x)g(x) = d(x)$;
- 对 $f(x), g(x)$ 的任意公因式 $\varphi(x)$, 有 $\varphi(x)|d(x)$ 。

2. 标准分解式法

从标准分解式中找最大公因式。

3. 利用最大公因式的性质和等式

证明多项式的互素

1. 定义法

证明 $(f(x), g(x)) = 1$ 。

2. 只要证明:

$$\exists u(x), v(x) \in K[x], \quad u(x)f(x) + v(x)g(x) = 1$$

3. 根法

证明在复数域上 $f(x)$ 的根都不是 $g(x)$ 的根 (重根按重数计算)。

4. 反证法

若 $(f(x), g(x)) = d(x) \neq 1$, 则可以由:

- $f(x), g(x)$ 有公共根
- $d(x)|f(x)$, 则 $d(x)|g(x)$

推出矛盾。

5. 互素的性质及等式

性质 6、7、8。

1.2.3 例题

求具体多项式的最大公因式

定理 1.18. 设 $f(x) = 3x^5 + 5x^4 - 4x^3 - 16x^2 - 5x - 6$, $g(x) = 3x^4 - 4x^3 - x^2 - x - 2$, 求:

1. $(f(x), g(x))$;

2. 多项式 $u(x), v(x)$ 使得 $u(x)f(x) + v(x)g(x) = (f(x), g(x))$ 。

辗转相除法
在 latex 里
面很难搞,
不想打了

证明. (1) $(f(x), g(x)) = x + \frac{2}{3}$ 。

(2) 将辗转相除法的过程倒推即可求得:

$$u(x) = -\frac{1}{3}(x^2 - x - 1), v(x) = \frac{1}{3}(x^3 + 2x^2 - 5x - 4) \quad \square$$

证明最大公因式

定理 1.19. 证明: $(f(x)h(x), g(x)h(x)) = (f(x), g(x))h(x)$, 其中 $h(x)$ 是首项系数为 1 的多项式。

证明. 令 $d(x) = (f(x), g(x))$, 则有 $d(x)|f(x)$, $d(x)|g(x)$, 从而 $d(x)h(x)|f(x)h(x)$, $d(x)h(x)|g(x)h(x)$, 所以 $(f(x)h(x), g(x)h(x))$ 是 $f(x)h(x), g(x)h(x)$ 的一个公因式。

因为 $d(x) = (f(x), g(x))$, 所以

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

于是 $u(x)h(x)f(x) + v(x)h(x)g(x) = d(x)f(x)$, $d(x)h(x)$ 是 $f(x)h(x), g(x)h(x)$ 的最大公因式。因为 $d(x) = (f(x), g(x))$, 所以它的首项系数为 1, 而 $h(x)$ 的首项系数也是 1, 于是 $(f(x)h(x), g(x)h(x)) = (f(x), g(x))h(x)$ 。 \square

定理 1.20. 设 $f_1(x) = af(x) + bg(x)$, $g_1(x) = cf(x) + dg(x)$, 且有 $ad - bc \neq 0$ 。证明 $(f(x), g(x)) = (f_1(x), g_1(x))$ 。

证明. 令 $d(x) = (f(x), g(x))$, 则有 $d(x)|f(x)$, $d(x)|g(x)$, 于是 $d(x)|af(x) + bg(x)$, $cf(x) + dg(x)$, 即 $d(x)|f_1(x), g_1(x)$, 于是 $(f(x), g(x))$ 是 $f_1(x), g_1(x)$ 的一个公因式。

因为 $d(x) = (f(x), g(x))$, 所以

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

因为 $ad - bc \neq 0$, 所以关于 $f(x), g(x)$ 的方程组:

$$\begin{cases} af(x) + bg(x) = f_1(x) \\ cf(x) + dg(x) = g_1(x) \end{cases}$$

有唯一解, 可解得:

$$f(x) = \frac{1}{ad-bc}[df_1(x) - bg_1(x)], \quad g(x) = \frac{1}{ad-bc}[-cf_1(x) + ag_1(x)]$$

于是:

$$u(x)\frac{1}{ad-bc}[df_1(x) - bg_1(x)] + v(x)\frac{1}{ad-bc}[-cf_1(x) + ag_1(x)] = d(x)$$

化简可得:

$$\frac{du(x) - cv(x)}{ad-bc}f_1(x) + \frac{av(x) - bu(x)}{ad-bc}g_1(x) = d(x)$$

即 $d(x) = (f(x), g(x))$ 是 $f_1(x), g_1(x)$ 的最大公因式。因为 $(f(x), g(x))$ 首项系数为 1, 所以 $(f(x), g(x)) = (f_1(x), g_1(x))$ 。□

定理 1.21. 设 $f(x), g(x) \in K[x]$, 且 $(f(x), g(x)) = 1$, 又 $\varphi(x) = (x^3 - 1)f(x) + (x^3 - x^2 + x - 1)g(x)$, $\psi(x) = (x^2 - 1)f(x) + (x^2 - x)g(x)$, 则 $(\varphi(x), \psi(x)) = x - 1$ 。

证明. 由因式分解可得:

$$\begin{aligned}\varphi(x) &= (x-1)[(x^2+x+1)f(x) + (x^2+1)g(x)] \\ \psi(x) &= (x-1)[(x+1)f(x) + xg(x)]\end{aligned}$$

所以 $x-1$ 是 $\varphi(x)$ 和 $\psi(x)$ 的一个公因式。由定理 1.19 可知:

$$(\varphi(x), \psi(x)) = ((x^2+x+1)f(x) + (x^2+1)g(x), (x+1)f(x) + xg(x))(x-1)$$

接下来只需证明 $((x^2+x+1)f(x) + (x^2+1)g(x), (x+1)f(x) + xg(x)) = 1$ 。

考虑以 $f(x), g(x)$ 为自变量的方程组:

$$\begin{cases} \varphi(x) = (x^3-1)f(x) + (x^3-x^2+x-1)g(x) \\ \psi(x) = (x^2-1)f(x) + (x^2-x)g(x) \end{cases}$$

其系数行列式为 $-x^3 - x^2 + 2x + 1$, 由 Cramer 法则可知 □ 没搞懂

定理 1.22. 设 $f(x), g(x)$ 是两个不全为 0 的多项式, 则 $\forall n \in N$, 有 $(f(x), g(x))^n = (f^n(x), g^n(x))$ 。

证明. 令 $d(x) = (f(x), g(x))$, 则存在 $f_1(x), g_1(x) \in K[x]$, 使得:

$$f(x) = d(x)f_1(x), \quad g(x) = d(x)g_1(x)$$

同时有 $(f_1(x), g_1(x)) = 1$, 从而 $(f_1^n(x), g_1^n(x)) = 1$, 所以:

$$\begin{aligned}(f^n(x), g^n(x)) &= (d^n(x)f_1^n(x), d^n(x)g_1^n(x)) \\ &= (f_1^n(x), g_1^n(x))d^n(x) \\ &= (f(x), g(x))^n\end{aligned}$$

其中第一行到第二行利用到了定理 1.19。□

证明多项式的互素

定理 1.23. 设 $f_1(x), f_2(x), \dots, f_m(x), g_1(x), g_2(x), \dots, g_n(x) \in K[x]$, 则:

$$(f_1(x)f_2(x) \cdots f_m(x), g_1(x)g_2(x) \cdots g_n(x)) = 1 \Leftrightarrow (f_i(x), g_j(x)) = 1$$

其中 $i = 1, 2, \dots, m, j = 1, 2, \dots, n$ 。

证明. (1) **必要性:** 因为 $(f_1(x)f_2(x) \cdots f_m(x), g_1(x)g_2(x) \cdots g_n(x))$, 所以 $\exists u(x), v(x) \in K[x]$ 使得:

$$u(x)f_1(x)f_2(x) \cdots f_m(x) + v(x)g_1(x)g_2(x) \cdots g_n(x) = 1$$

即:

$$f_i(x)[u(x)f_1(x) \cdots f_{i-1}(x)f_{i+1}(x) \cdots f_m(x)] + g_j(x)[v(x)g_1(x) \cdots g_{j-1}(x)g_{j+1}(x) \cdots g_n(x)] = 1$$

所以 $(f_i(x), g_j(x)) = 1$, 其中 $i = 1, 2, \dots, m, j = 1, 2, \dots, n$ 。

(2) **充分性:** 取 $f_1(x)$, 因为 $(f_1(x), g_j(x)) = 1, i = 1, 2, \dots, n$, 由定理 1.16 可得, $(f_1(x), g_1(x) \cdots g_n(x)) = 1$ 。同理可得对任意的 $i = 1, 2, \dots, m$, 都有 $(f_i(x), g_1(x) \cdots g_n(x)) = 1$, 再利用定理 1.16 即可得到 $(f_1(x)f_2(x) \cdots f_m(x), g_1(x)g_2(x) \cdots g_n(x)) = 1$ 。□

定理 1.24. 对 $\forall n \in \mathbb{N}^+$, 令 $f_n(x) = x^{n+2} - (x+1)^{2n+1}$, 有 $(x^2 + x + 1, f_n(x)) = 1$ 。

证明. 设 α 是 $x^2 + x + 1 = 0$ 的根, 则 $\alpha^2 + \alpha + 1 = 0, \alpha^3 = 1$ 。于是:

$$\begin{aligned} f_n(\alpha) &= \alpha^{n+2} - (\alpha+1)^{2n+1} \\ &= \alpha^{n+2} - (-\alpha^2)^{2n+1} \\ &= \alpha^{n+2} + \alpha^{4n+2} \\ &= \alpha^{n+2} + \alpha^{3n}\alpha^{n+2} \\ &= 2\alpha^{n+2} \end{aligned}$$

在复数域内求解方程 $x^2 + x + 1 = 0$ 可得:

$$x_1 = \frac{-1 + \sqrt{3}i}{2}, x_2 = \frac{-1 - \sqrt{3}i}{2}$$

所以 $f_n(\alpha) = 2\alpha^{n+2} \neq 0$, 即 α 不是 $f_n(x)$ 的根。由上我们得到 $x^2 + x + 1 = 0$ 的根都不是 $f_n(x)$ 的根, 所以 $(x^2 + x + 1, f_n(x)) = 1$ 。□

定理 1.25. $f(x) = x^{m-1} + x^{m-2} + \cdots + x + 1, g(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$, 其中 $m, n \in \mathbb{N}$, 则有:

$$(m, n) = 1 \Leftrightarrow (f(x), g(x)) = 1$$

证明. (1) 充分性: 若 $(m, n) = d \neq 1$, 设 $m = ds$, $n = dt$, 则:

$$\begin{aligned} f(x) &= \frac{x^m - 1}{x - 1} = \frac{x^{ds} - 1}{x - 1} \\ &= \frac{x^d - 1}{x - 1} [x^{d(s-1)} + x^{d(s-2)} + \cdots + x^d + 1] \\ &= (x^{d-1} + \cdots + x + 1) [x^{d(s-1)} + x^{d(s-2)} + \cdots + x^d + 1] \end{aligned}$$

而:

$$\begin{aligned} g(x) &= \frac{x^n - 1}{x - 1} = \frac{x^{dt} - 1}{x - 1} \\ &= \frac{x^d - 1}{x - 1} [x^{d(t-1)} + x^{d(t-2)} + \cdots + x^d + 1] \\ &= (x^{d-1} + \cdots + x + 1) [x^{d(t-1)} + x^{d(t-2)} + \cdots + x^d + 1] \end{aligned}$$

可以发现 $f(x)$ 与 $g(x)$ 有次数大于 0 的公因式 $x^{d-1} + \cdots + x + 1$, 与 $(f(x), g(x)) = 1$ 矛盾, 所以 $(m, n) = 1$ 。

(2) 必要性: 若 $(f(x), g(x)) = d(x) \neq 1$, 则 $f(x), g(x)$ 有公共根 α 。由 n 次方差公式可得:

$$\begin{aligned} \alpha^m - 1 &= (\alpha - 1)(\alpha^{m-1} + \alpha^{m-2} + \cdots + \alpha + 1) = 0 \\ \alpha^n - 1 &= (\alpha - 1)(\alpha^{n-1} + \alpha^{n-2} + \cdots + \alpha + 1) = 0 \end{aligned}$$

于是 $\alpha^m = \alpha^n = 1$, 且有 $\alpha \neq 1$ 。由 $(m, n) = 1$ 可知, 存在 $u, v \in \mathbb{N}$ 使得 $um + vn = 1$, 于是:

$$\alpha = \alpha^{um+vn} = (\alpha^m)^u (\alpha^n)^v = 1$$

矛盾, 所以 $(f(x), g(x)) = 1$ 。□

1.3 多项式的根

定理 1.26. 若 $f(x) = ap_1^{r_1}(x)p_2^{r_2}(x) \cdots p_s^{r_s}(x)$, 则:

$$\frac{f(x)}{(f(x), f'(x))} = ap_1(x)p_2(x) \cdots p_s(x)$$

1.3.1 题型

重根的证明

1. 互素法

- 若 $f(x)$ 是一个复多项式, 则 $f(x)$ 无重根的充分必要条件是 $(f(x), f'(x)) = 1$ 。
- 若 $f(x)$ 是一般数域 K 上的多项式, 若 $(f(x), f'(x)) = 1$, 则 $f(x)$ 无重因式, 自然无重根。

2. 反证法

1.3.2 例题

定理 1.27. 如果 $f'(x)|f(x)$, 证明: $f(x)$ 有 n 重根, 其中 $n = \deg f(x)$

证明. 由 $f'(x)|f(x)$, 所以 $f'(x) = (f(x), f'(x))$ 。因为 $\deg f'(x) = n - 1$, 则:

$$\varphi(x) = \frac{f(x)}{(f(x), f'(x))}$$

是一次多项式, 设 $\varphi(x) = a(x - b)$, $a \neq 0$ 。由定理 1.26 可得 $f(x)$ 与 $\varphi(x)$ 有相同的不可约因式, 又因为 $\deg f(x) = n$, 所以 $f(x) = a(x - b)^n$, $f(x)$ 有 n 重根。□

定理 1.28. 设 $f(x)$ 是复数域中的 n 次多项式, 且 $f(0) = 0$, 令 $g(x) = xf(x)$, 若 $f'(x)|g'(x)$, 则 $g(x)$ 有 $n + 1$ 重零根。

证明. 由 $f(0) = 0$ 可知 0 是 $f(x)$ 的根。因为 $g(x) = xf(x)$, 所以 $g'(x) = f(x) + xf'(x)$ 。因为 $f'(x)|g'(x)$, 所以 $f'(x)|f(x)$ 。由上一题的结论, $f(x)$ 有 n 重根, 又因为 0 是 $f(x)$ 的根, 所以 0 就是 $f(x)$ 的 n 重根。设 $f(x) = ax^n$, 于是 $g(x) = ax^{n+1}$, 即 $g(x)$ 有 $n + 1$ 重零根。□

1.3.3 复根、实根、有理根与整数根

定理 1.29. 设 $f(x)$ 为整系数多项式:

1. 证明: 若 $f(1 + \sqrt{2}) = 0$, 则 $f(1 - \sqrt{2}) = 0$;

2. 推测结论 (1) 的推广形式 (不需要证明)。

证明. (1) $f(x)$ 有因式:

$$[x - (1 + \sqrt{2})][x - (1 - \sqrt{2})] = x^2 - 2x - 1 \in \mathbb{Z}[x]$$

作带余除法, 设:

$$f(x) = (x^2 - 2x - 1)q(x) + ax + b$$

其中 $a, b \in \mathbb{Z}$ 。由 $f(1 + \sqrt{2}) = 0$ 可知, $a(1 + \sqrt{2}) + b = 0$, 于是 $a = b = 0$, 所以 $f(x) = (x^2 - 2x - 1)q(x)$, 显然 $f(1 - \sqrt{2}) = 0$ 。

(2) 若 $f(a + b\sqrt{2}) = 0$, 则 $f(a - b\sqrt{2}) = 0$, 其中 $a, b \in \mathbb{Z}$ 。□

定理 1.30. 已知整系数多项式 $f(x)$ 满足 $f(2)f(21) = 505$, 证明 $f(x)$ 无整数根。

证明. 因为 $f(2)f(21) = 505$, 所以 $f(2)$ 和 $f(21)$ 都是奇数。假设 α 是 $f(x)$ 的整数根, 则 $f(x) = (x - \alpha)q(x)$, 其中 $q(x) \in \mathbb{Z}[x]$, 则 $2 - \alpha, 21 - \alpha$ 中至少有一个是偶数, 于是 $f(2)$ 与 $f(21)$ 中至少有一个是偶数, 矛盾, 所以 $f(x)$ 无整数根。□

定理 1.31. 求一个一元多项式, 使它的各根分别等于 $f(x) = 5x^4 - 6x^3 + x^2 + 4$ 的各根减 1。

证明. 令 $y = x - 1$, 则 $x = y + 1$ 。

$$g(y) = 5(y+1)^4 - 6(y+1)^3 + (y+1)^2 + 4$$

$g(y)$ 即为所求多项式。 \square

定理 1.32. 求一个一元多项式, 使它的各根分别等于 $f(x) = 15x^4 - 2x^3 + 11x^2 - 21x + 13$ 的倒数。

证明. 因为 $f(0) = 13$, 所以 0 不是 $f(x)$ 的根。令 $y = \frac{1}{x}$, 则 $x = \frac{1}{y}$ 。

$$\begin{aligned} y^4 f(x) &= y^4 \left[15 \left(\frac{1}{y} \right)^4 - 2 \left(\frac{1}{y} \right)^3 + 11 \left(\frac{1}{y} \right)^2 - 21 \left(\frac{1}{y} \right) + 13 \right] \\ &= 13y^4 - 21y^3 + 11y^2 - 2y + 15 \\ &= g(y) \end{aligned}$$

$g(y)$ 即为所求多项式。 \square

定理 1.33. 设 $f(x)$ 为有理数域 \mathbb{Q} 上 $n(n \geq 2)$ 次多项式, 并且它在 \mathbb{Q} 上不可约, 如果 $f(x)$ 的一个根 α 的倒数 $\frac{1}{\alpha}$ 仍是 $f(x)$ 的根, 证明 $f(x)$ 每一个根的倒数也是 $f(x)$ 的根。

倒根变换需要严格证明

证明. 假设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, 其中 $a_n \neq 0$ 。由 $f(x)$ 不可约可得 $a_0 \neq 0$, 于是 0 不是 $f(x)$ 的根。对 $f(x)$ 作倒根变换, 得到多项式:

$$g(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

由 $\frac{1}{\alpha}$ 使 $f(x)$ 的根, 则 α 是 $g(x)$ 的根。因为 α 也是 $f(x)$ 的根, 所以 $(f(x), g(x)) \neq 1$ 。因为 $f(x)$ 不可约, 所以 $f(x) | g(x)$ 。任取 $f(x)$ 的根 β , 则 β 也是 $g(x)$ 的根, 于是 $\frac{1}{\beta}$ 是 $f(x)$ 的根。 \square

定理 1.34. 求以 $\sqrt{2} + \sqrt{3}$ 为根的有理系数不可约多项式。

证明. 设 $f(x) \in \mathbb{Q}[x]$ 且以 $\sqrt{2} + \sqrt{3}$ 为根, 则 $\sqrt{2} - \sqrt{3}, -\sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}$ 也是 $f(x)$ 的根。令

$$f(x) = [x - (\sqrt{2} + \sqrt{3})][x - (\sqrt{2} - \sqrt{3})][x + (\sqrt{2} + \sqrt{3})][x + (\sqrt{2} - \sqrt{3})] = x^4 - 10x^2 + 1$$

接下来证明 $f(x)$ 在 $\mathbb{Q}[x]$ 上不可约。

如果 $f(x)$ 有有理根, 必为 ± 1 。但 ± 1 都不是 $f(x)$ 的根, 所以 $f(x)$ 不能分解一个一次多项式与一个三次多项式的乘积。其次, 如果 $f(x)$ 在 $\mathbb{Q}[x]$ 上分解为两个二次多项式的乘积, 则 $f(x)$ 必可在整系数多项式上分解为两个二次多项式的乘积, 即:

$$f(x) = x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

其中 $a, b, c, d \in \mathbb{Z}$ 。比较两边系数可得：

$$\begin{cases} a + c = 0 \\ b + d + ac = -10 \\ ad + bc = 0 \\ bd = 1 \end{cases}$$

因为 $bd = 1$ 且 $bd \in \mathbb{Z}$ ，所以 $b = d = -1$ 或 $b = d = 1$ 。

当 $b = d = 1$ 时， $a = -c$ ， $c^2 = 12$ ，但是 $c \in \mathbb{Z}$ ，矛盾。

当 $b = d = -1$ 时， $c^2 = 8$ ，但是 $c \in \mathbb{Z}$ ，矛盾。

所以 $f(x)$ 无法分解为两个二次多项式的乘积。

综上， $f(x)$ 既无法分解为一个一次多项式与一个三次多项式的乘积，也无法分解为两个二次多项式的乘积，所以 $f(x)$ 不可约。 $f(x)$ 即为所求。 \square

1.3.4 三个常用数域上的多项式

复数域

代数基本定理任何 n 次多项式在复数域中恰好有 n 个根。每个次数大于 0 的多项式在复数域上都可以唯一分解为一次因式的乘积。韦达定理

实数域

虚根的共轭也是虚根次数大于 2 的实系数多项式在实数域上是可约的实多项式分解定理

有理数域

如果能够分解为有理系数多项式的乘积则一定可以分解为整系数多项式的乘积根与系数的关系

定理 1.35. 设 $f(x) = a_n x^n + \cdots + a_0$ 是一个整系数多项式，而 $\frac{r}{s}$ 是一个有理数，其中 r, s 互素，则

定理 1.36 (艾森斯坦判别法). 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 是整系数多项式，若存在素数 p ，使得：

1. $p \nmid a_n$;
2. $p \mid a_{n-1}, a_{n-2}, \dots, a_1, a_0$;
3. $p^2 \nmid a_0$;

则 $f(x)$ 在有理数域上不可约。

定理 1.37. 若 $f(x)$ 是 $n(n > 0)$ 次整系数多项式, 令 $x = y + a$, $a \in \mathbb{Z}$, 得整系数多项式 $g(y) = f(y + a)$, 则 $f(x)$ 在 \mathbb{Q} 上可约的充分必要条件是 $g(x)$ 在 \mathbb{Q} 上可约。

定理 1.38. 次数大于 1 的复多项式都是可约的。次数大于 2 的实多项式都是可约的。次数等于 1 的多项式都是不可约的。

题型

1. 整系数多项式在有理数域上可约性的判别

(a) 方法一:

艾森斯坦判别法或对多项式作变换后再使用艾森斯坦判别法

(b) 方法二:

适合抽象的整系数多项式证明不可约

(c) 方法三:

讨论有理根。判断二次或三次有理多项式不可约只需证明它没有有理根, 当次数大于 3 时, 此结论不再成立。

例题

定理 1.39. 设 p 为素数, 则

$$f(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^p}{p!}$$

在有理数域上不可约。

证明. 令 $g(x) = p!f(x)$, 则 $g(x)$ 的可约性与 $f(x)$ 的可约性是一样的。而:

$$g(x) = x^p + px^{p-1} + \cdots + \frac{p!}{2!} + p!x + p!$$

显然 $g(x)$ 是一个整系数多项式。对于素数 p , 有 $p \nmid a_n = 1$, $p | a_{n-1}, a_{n-2}, \dots, a_1, a_0$, $p^2 \nmid a_0 = p!$. \square

定理 1.40. 判别多项式 $f(x) = x^5 - 5x + 1$ 在有理数域上是否可约。

证明. 令 $x = y - 1$, 则 $g(y) = f(y - 1)$, 即:

$$g(y) = y^5 - 5y^4 + 10y^3 - 10y^2 + 5$$

取 $p = 5$, 由艾森斯坦判别法, 该多项式在有理数域上不可约。 \square

定理 1.41. 关于任意素数 p , 多项式:

$$f(x) = px^4 + 2px^3 - px + 3p - 1$$

在有理数域上不可约。

证明. 因为 p 是一个素数, 所以 $3p - 1 \neq 0$. 令 $y = \frac{1}{x}$, 则:

$$f(y) = (3p - 1)y^4 - py^3 + 2px + p$$

取素数 p , 由艾森斯坦判别法, 该多项式在有理数域上不可约. \square

定理 1.42. 设 n 是大于 1 的整数, 证明 $\sqrt[n]{2008}$ 是无理数.

证明. 令 $f(x) = x^n - 2008$, 取素数 $p = 251$, 由艾森斯坦判别法, 该多项式在有理数域上不可约, 即 $f(x)$ 在有理数域上没有根, 而 $\sqrt[n]{2008}$ 是 $f(x)$ 的根, 所以 $\sqrt[n]{2008}$ 是无理数. \square

定理 1.43. 设 $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) - 1$, 其中 a_1, a_2, \dots, a_n 是两两互不相同的整数, 证明 $f(x)$ 在有理数域上不可约.

证明. 假设 $f(x)$ 可约, 则可设:

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

其中 $g(x), h(x)$ 为整系数多项式, 并且有 $\deg g(x) < \deg f(x) = n$, $\deg h(x) < \deg f(x) = n$. 因为 $f(a_i) = -1$, 所以 $g(a_i)h(a_i) = -1$, $i = 1, 2, \dots, n$, 此时有 $g(a_i) = 1, h(a_i) = -1$ 或 $g(a_i) = -1, h(a_i) = 1$. 无论是哪种情况, 都有 $g(a_i) + h(a_i) = 0$, 即 $g(x) + h(x)$ 有 n 个互不相等的根 a_1, a_2, \dots, a_n , 但是 $\deg(g(x) + h(x)) < n$, 矛盾, 所以 $f(x)$ 不可约. \square

定理 1.44. 设 a_1, a_2, \dots, a_n 是两两互不相同的整数, 证明 $f(x) = (x - a_1)^2(x - a_2)^2 \cdots (x - a_n)^2 + 1$ 在有理数域上不可约.

证明. 假设 $f(x)$ 可约, 则存在次数大于 0 的首项系数为 1 的整系数多项式 $g(x), h(x)$ 使得:

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

因为 $f(a_i) = g(a_i)h(a_i) = 1$, 则 $g(a_i) = h(a_i) = 1$ 或 $g(a_i) = h(a_i) = -1$, $i = 1, 2, \dots, n$. 若 $g(a_i) = -1$, 由 $g(x)$ 是首项系数为 1 的多项式, 则存在充分大的 c , 使得 $g(c) = 0$, 从而 $g(x)$ 有实根. 这与 $f(x)$ 无实根矛盾, 故 $g(a_i) \neq -1$. 若 $g(a_i) = 1$, 因为 a_1, a_2, \dots, a_n 是 $g(x) - 1, h(x) - 1$ 的 n 个互不相同的根, 则 $\deg(g(x) - 1) \geq n$, $\deg(h(x) - 1) \geq n$. 因为 $\deg f(x) = \deg g(x) + \deg h(x)$ 且有 $\deg f(x) = 2n$, 于是 $\deg(g(x) - 1) = \deg(h(x) - 1) = n$, 所以:

$$g(x) - 1 = h(x) - 1 = (x - a_1)(x - a_2) \cdots (x - a_n)$$

所以:

$$f(x) = [(x - a_1)(x - a_2) \cdots (x - a_n) + 1]^2$$

与 $f(x)$ 的表达式矛盾, 所以 $f(x)$ 不可约. \square

1.3.5 多项式的分解

定理 1.45. 求多项式 $x^n - 1$ 在复数域上和实数域上的标准分解式。

证明. 实数域:

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

复数域:

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

□