

§6 多项式理论

设 R 为任意环, x 为未定元, 则形式和

$$a_0 + a_1x + a_2x^2 + \dots$$

称为 R 上的 **一元多项式**, 其中 $a_i \in R$ ($\forall i \geq 0$) 且 $a_i = 0$ ($\forall i \gg 0$). 一般记作

$$f(x) = a_nx^n + \dots + a_1x + a_0$$

注: 1) $\forall g(x) = b_mx^m + \dots + b_0$. 则 $f(x) = g(x) \Leftrightarrow a_i = b_i \ \forall i$.

2) 若 $a_n \neq 0$, 则

$$f(x) = \underbrace{a_n}_{\text{首项系数}} x^{\underbrace{n}_{\text{次数 } \deg(f) = n}} + \dots + a_1x + \underbrace{a_0}_{\text{常数项}}$$

→ 首项

约定: $\deg(0) = -\infty$

定理: 记 $R[x]$ 为全体 R 上-元多项式组成的集合. $\forall f(x) = \sum_i a_i x^i, g(x) = \sum_i b_i x^i \in R[x]$

$$f(x) + g(x) := \sum_i (a_i + b_i) x^i$$

$$f(x) \cdot g(x) := \sum_i \left(\sum_{s+r=i} a_s b_r \right) \cdot x^i$$

则

- 1) $(R[x], +, \cdot)$ 构成任意环. 称为 R 上的 **一元多项式环**.
- 2) $R[x]$ 为交换环 $\Leftrightarrow R$ 为交换环
- 3) $R[x]$ 为整环 $\Leftrightarrow R$ 为整环

本节主要研究对象: $\mathbb{F}[x]$ 和 $\mathbb{Z}[x]$

(其中 \mathbb{F} 为域, 即 $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ 等)

§6.1 域上多项式理论.

设 F 为域, 则 $F[x]$ 与 \mathbb{Z} 有惊人的相似之处:

- 整除理论 带余除法 \leadsto 贝祖定理 \rightarrow 主理想整环 \rightarrow 唯一分解整环.
- 同余理论 环 $F[x]/f \cdot F[x]$, 中国剩余定理
- 其它性质 不可约判定, 代数基本定理. 韦达定理. 重根判定

§ 整除理论

$$g \mid f \stackrel{\text{def}}{\iff} \exists h \text{ s.t. } f = gh$$

\swarrow \searrow
 f 的因子 g 的倍数

例(平凡因子): $a \in F^\times$ & af 均为 f 的因子.

定理(带余除法): $\forall f, \forall g \neq 0, \exists! (q, r) \text{ s.t.}$

$$f = qg + r \quad \text{其中 } \deg r < \deg g.$$

\nwarrow \swarrow
商 余式

Pf: 存在性: $I := \{ f - ag \mid a \in F[x] \} \neq \emptyset$

$r := I$ 中次数最小的多项式.

$\Rightarrow \deg r < \deg g$. (否则可用 g 消除 r 的最高次项)

唯一性: $f = q'g + r' \Rightarrow g \mid r - r' \Rightarrow r = r' \Rightarrow v.$

注: 若 R 不为域, $R[x]$ 上是否有带余除法?

-6-2- 答: 对一般的 g 没有, 但对首项系数可逆的 g 有.

定义: $\forall f, g \in \mathbb{F}[x]$, 称 $d \in \mathbb{F}[x]$ 为 f 与 g 的 **最大公因子**, 若

1) $d \neq 0$ (保证唯一性)

2) $d|f$ & $d|g$ (公因子)

3) $d'|f$ & $d'|g \Rightarrow \deg d' \leq \deg d$. (最大)

此时记 $d = \gcd(f, g) = (f, g)$. 若 $d=1$, 则称 f 与 g **互素**.

注: 最大公因子存在, 是否唯一呢?

回顾: $(S) \triangleq R$ 为包含 S 的最小理想.

定理 (贝祖定理): $(\gcd(f, g)) = (f, g) \triangleq \mathbb{F}[x]$.

Pf: " \supseteq ": 显然

" \subseteq ": 设 $f \neq 0$ 或 $g \neq 0$. 记 d 为 (f, g) 中次数最小的非零首一多项式

带余除法 $\Rightarrow \left\{ \begin{array}{l} d|f \\ d|g \end{array} \right\} \Rightarrow 0 < \deg d \leq \deg(\gcd(f, g))$
 $d \in (f, g) \Rightarrow \gcd(f, g) | d \Rightarrow \gcd(f, g) = d \Rightarrow \checkmark$

推论: (贝祖等式) 1) $\forall f, g, \exists u, v$ s.t. $\gcd(f, g) = fu + gv$
 特别地, 若 d 为 f 和 g 的公因子, 则 $d | \gcd(f, g)$. (最大公因子唯一!)

2) $\gcd(f, g) = 1 \Leftrightarrow \exists u, v$ s.t. $fu + gv = 1$.

定理: $\mathbb{F}[x]$ 为主理想整环

Pf: 1° $I = 0 \checkmark$

2° $I \neq 0$, 记 f 为次数最小的非零首一多项式.

3° $\forall g \in I$. 带余除法 $\Rightarrow f|g \Rightarrow g \in (f) \Rightarrow I = (f)$.

整数的最大公因子的性质都可推广到多项式上. 例如:

- 命题:
- 1). $a, b \in \mathbb{F}^x \Rightarrow \gcd(af, bg) = \gcd(f, g)$
 - 2). $\gcd(f, g) = \gcd(g, f)$
 - 3). $f \neq 0 \Rightarrow \gcd(f, 0) = \gcd(f, f) = \frac{f}{lc(f)} \leftarrow f \text{ 的首项系数.}$
 - 4). $d|f \text{ \& } d|g \Leftrightarrow d|\gcd(f, g)$.
 - 5). $\forall h \neq 0, \gcd(hf, hg) = h \cdot \gcd(f, g)$.
 - 6). $d = \gcd(f, g) \Rightarrow \gcd\left(\frac{f}{d}, \frac{g}{d}\right) = 1$
 - 7). $\gcd(f, h) = 1 \Rightarrow \gcd(f, gh) = \gcd(f, g)$
 - 8). $h|fg \text{ \& } \gcd(h, f) = 1 \Rightarrow h|g$

Pf: 略.

注: 类似地, 定义 $\gcd(f_1, f_2, \dots, f_n), \text{lcm}(f, g), \text{lcm}(f_1, \dots, f_n)$.

问题: 求 u, v s.t. $\gcd(f, g) = fu + gv$

例: $\gcd(x^4 + x^3, x^4 - 1) = x + 1 = x(x^3 + x^2) - (1 + x)(x^4 - 1)$

	$x^4 + x^3$	1	0
1	$x^4 - 1$	0	1
x	$x^3 + 1$	1	-1
$-x^2 + x - 1$	$-x - 1$	-x	1+x
	0		

例 $\mathbb{F} = \mathbb{F}_2 \Rightarrow \gcd(x^4 + x^2 + x + 1, x^2 + 1) = x + 1 = (x^4 + x^2 + x + 1) - x^2(x^2 + 1)$

	$x^4 + x^2 + x + 1$	1	0
x^2	$x^2 + 1$	0	1
$x - 1$	$x + 1$	1	$-x^2$
	0		

定义: $P \in F[x]$.

1) P 不可约 $\stackrel{\text{def}}{\Leftrightarrow} \begin{cases} \deg(P) \geq 1 \\ P \text{ 仅有平凡因子} \end{cases}$

(素数)

2) P 可约 $\stackrel{\text{def}}{\Leftrightarrow} \begin{cases} \deg(P) \geq 1 \\ P \text{ 有非平凡因子} \end{cases}$

(合数)

例: 一次多项式总是不可约的, 反之不成立 ($x^2+1 \in \mathbb{R}[x]$)

欧几里得引理: P 不可约, 则 $P|fg \Rightarrow P|f$ 或 $P|g$.

pf: 若 $P|f, P|g \Rightarrow \gcd(f, P) = \gcd(g, P) = 1 \Rightarrow \gcd(fg, P) = 1 \Rightarrow P \nmid fg$ \square

唯一分解定理: $\deg f \geq 1$ 则 f 的首项系数

$$f \doteq C P_1(x) \cdots P_r(x)$$

首-不可约
不计顺序下唯一-

pf: 略 \square

推论: $\gcd(C_1 P_1^{\alpha_1} \cdots P_s^{\alpha_s}, C_2 P_1^{\beta_1} \cdots P_s^{\beta_s}) = P_1^{\min(\alpha_1, \beta_1)} \cdots P_s^{\min(\alpha_s, \beta_s)}$

§ 同余理论

设 $\deg(m) \geq 1$ (i.e. m 不为常值多项式)

$$f \equiv g \pmod{m} \stackrel{\text{def}}{\iff} m \mid f - g$$

称 f 与 g 模 m 同余. “ \equiv ” 为等价关系.

$$[r] := r \text{ 所在模 } m \text{ 等价类} = \{r + mf \mid f \in \mathbb{F}[x]\}$$

$$\bar{r}, r \bmod m, r + m\mathbb{F}[x], r + (m).$$

$$\mathbb{F}[x]/(m) = \mathbb{F}[x]/m\mathbb{F}[x] = \{[r] \mid r \in \mathbb{F}[x]\}$$

$$[r_1] + [r_2] := [r_1 + r_2], \quad [r_1] \cdot [r_2] := [r_1 \cdot r_2].$$

定理: 1) $\mathbb{F}[x]/m\mathbb{F}[x]$ 为交换环.

2) $\mathbb{F}[x]/m\mathbb{F}[x]$ 中的元素都可唯一地表示为 $[r]$, 其中 $r=0$ 或 $\deg r < \deg m$.

3) $(\mathbb{F}[x]/m\mathbb{F}[x])^\times = \{[a] \mid \gcd(a, m) = 1, \deg(a) < \deg m\}$

4) $\mathbb{F}[x]/m\mathbb{F}[x] \stackrel{\text{①}}{=} \text{整环} \iff \mathbb{F}[x]/m\mathbb{F}[x] \stackrel{\text{②}}{=} \text{域} \iff m \stackrel{\text{③}}{=} \text{不可约}.$

→ 常用来构造有限域.

Pf: 1) 直接验证. 2) 带余除法 3) 贝祖等式

4) ③ \Rightarrow ②: $\forall [a] \neq [0] \Rightarrow \gcd(a, m) = 1 \Rightarrow [a]$ 可逆

② \Rightarrow ①: \checkmark

① \Rightarrow ③: 若 $m = pf$, 则 $pf \equiv 0 \pmod{m}$

$\mathbb{F}[x]/m = \text{整} \Rightarrow p=0 \text{ 或 } f=0 \Rightarrow m \mid p \text{ 或 } m \mid f \Rightarrow m \text{ 不可约}.$

推论: 若 $\mathbb{F} = \mathbb{F}_p$, $\deg(m) = d > 0$. 则

1) $\#(\mathbb{F}_p[x]/m\mathbb{F}_p[x]) = p^d$

2) m 不可约 $\Rightarrow \mathbb{F}_p[x]/m\mathbb{F}_p[x]$ 为 p^d 元域

例: $x^2 + x + 1 \in \mathbb{F}_2[x]$ 不可约. $\Rightarrow \mathbb{F}_4 := \mathbb{F}_2[x]/(x^2 + x + 1)$ 为 4 元域.

$\mathbb{F}_4 = \{0, 1, \bar{x}, \bar{x}+1\}$, $\bar{x}^2 = \bar{x}+1$, $\overline{x+1}^2 = \bar{x}$, $\bar{x} \cdot \overline{x+1} = 1$.

若 $m(x) \mid n(x)$, $\mathbb{R}[x]$ $f \equiv g \pmod{n} \Rightarrow f \equiv g \pmod{m}$

从而有环满同态: $\mathbb{R}[x]/m\mathbb{R}[x] \twoheadrightarrow \mathbb{R}[x]/n\mathbb{R}[x]$.

中国剩余定理: 若 m_1, \dots, m_s 两两互素, $m = m_1 m_2 \dots m_s$. $\mathbb{R}[x]$

1) 有环同构:

$$\mathbb{R}[x]/m\mathbb{R}[x] \cong \mathbb{R}[x]/m_1\mathbb{R}[x] \times \dots \times \mathbb{R}[x]/m_s\mathbb{R}[x]$$

2) 它诱导群同构:

$$\mathbb{R}[x]/m\mathbb{R}[x]^\times \cong \left(\mathbb{R}[x]/m_1\mathbb{R}[x]\right)^\times \times \dots \times \left(\mathbb{R}[x]/m_s\mathbb{R}[x]\right)^\times$$

Pf: 单 \checkmark

$$\begin{aligned} \text{满: } \hat{m}_i &:= \frac{m}{m_i}, \quad \gcd(m_i, \hat{m}_i) = 1 \Rightarrow \exists s_i, t_i \text{ s.t. } s_i m_i + t_i \hat{m}_i = 1 \\ &\Rightarrow \mathbb{R}(t_i \hat{m}_i) = (0, \dots, 0, \underset{i}{1}, 0, \dots, 0) \\ &\Rightarrow \text{至满.} \end{aligned}$$

定理: 若 $m(x) = m_1(x) \cdot m_2(x) \cdot \dots \cdot m_s(x)$, m_i 两两互素, $a_1, \dots, a_s \in \mathbb{R}[x]$. $\mathbb{R}[x]$

$$\begin{cases} f \equiv a_1 \pmod{m_1} \\ f \equiv a_2 \pmod{m_2} \\ \vdots \\ f \equiv a_s \pmod{m_s} \end{cases}$$

有解, 且解集为模 m 的一个同余类.

§ 其它性质

性质: 设 $\deg(m) \geq 1$. 记 $\Sigma_m := \{n \in \mathbb{N}[x] \mid n|m \text{ 且 } n \notin \mathbb{F}\} \neq \emptyset$ 则

1) Σ_m 中次数最小者不可约.

2) $\deg(m)=2$ 或 3 , 则

m 不可约 $\Leftrightarrow m$ 在 \mathbb{F} 上无零点.

定理(代数学基本定理): $\forall f \in \mathbb{C}[x] \setminus \mathbb{C}, \Rightarrow f$ 有复根.

证明(后续课程) Gauss thesis.

推论: 若 $f \in \mathbb{C}[x] \setminus \mathbb{C}$, 则

1) $\deg f = n \Rightarrow f$ 恰有 n 个复根(计重数) $\left(\begin{array}{l} \text{i.e. } f(x) = (x-x_1)^{\alpha_1} \cdots (x-x_s)^{\alpha_s} \\ n = \alpha_1 + \alpha_2 + \cdots + \alpha_s \end{array} \right)$

2) f 不可约 $\Leftrightarrow \deg(f)=1$.

推论: 1) $\forall f \in \mathbb{R}[x] \setminus \mathbb{R}, \Rightarrow \exists p_1, \dots, p_s$ 不可约且 $\deg(p_i)=1$ 或 2 , 使得 $f = p_1 p_2 \cdots p_s$.

2) $p = ax^2 + bx + c \in \mathbb{R}[x]$ 不可约 $\stackrel{\text{aff}}{\Leftrightarrow} b^2 - 4ac < 0$.

§ 韦达定理

余数定理: $\forall f \in \mathbb{F}[x], \forall a \in \mathbb{F}, \exists! q \in \mathbb{F}[x], \text{ s.t.}$

$$f(x) = q(x)(x-a) + f(a)$$

推论: $f(a)=0 \Leftrightarrow x-a \mid f$

多项式的拉格朗日定理: $\deg f = n \Rightarrow f$ 的零点数 $\leq n$.

Pf: 设 a_1, \dots, a_s 为 f 的不同零点.

$$\Rightarrow f(x) = f_1(x) \cdot (x-a_1) \cdot \dots \cdot f_s(x) \text{ 且 } f_1(a_2) = \dots = f_s(a_s) = 0$$

$$\text{归纳} \Rightarrow \deg(f_1) \geq s-1 \Rightarrow \deg f = \deg(f_1) + 1 \geq s.$$

注: 此处系数环需要为域. 一般的环不成立. eg. $\mathbb{Z}/8\mathbb{Z}$ 中 $\bar{3}^2 = \bar{5}^2 = \bar{7}^2 = \bar{1}$
 \mathbb{H} 中 $i^2 = j^2 = k^2 = -1$.

定理(韦达): $\mathbb{F} = \text{域}, f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{F}[x] (a_n \neq 0)$.

1) 若 f 有 n 个不同的根 x_1, \dots, x_n , 则

$$f(x) = a_n (x-x_1)(x-x_2) \cdots (x-x_n).$$

2) 若 $f(x) = a_n (x-x_1)(x-x_2) \cdots (x-x_n)$, (可有重根) 则

$$\sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}$$

$$\text{特别地, } x_1 + x_2 + \dots + x_n = -\frac{a_{n-1}}{a_n} \quad \& \quad x_1 x_2 \cdots x_n = (-1)^n \frac{a_0}{a_n}$$

Pf: i) 对 n 归纳. $n=1$ \checkmark 若 $n-1$ \checkmark

$$\left. \begin{array}{l} f(x_1)=0 \Rightarrow f(x) = f_1(x)(x-x_1) \\ f(x_2)=\dots=f(x_n)=0 \end{array} \right\} \Rightarrow f_1(x_2)=\dots=f_1(x_n)=0$$

$$\text{归纳} \Rightarrow f_1(x) = a_n (x-x_2) \cdots (x-x_n)$$

$$\Rightarrow f = a_n (x-x_1) \cdots (x-x_n)$$

ii) 比较系数. \square

1例) 1) $n=2$: $x^2 + bx + c = (x-x_1)(x-x_2) \Rightarrow \begin{cases} x_1 + x_2 = -b \\ x_1 x_2 = c \end{cases}$

2) $n=3$: $x^3 + bx^2 + cx + d = (x-x_1)(x-x_2)(x-x_3)$

$$\Rightarrow \begin{cases} x_1 + x_2 + x_3 = -b \\ x_1 x_2 + x_2 x_3 + x_3 x_1 = c \\ x_1 x_2 x_3 = -d \end{cases}$$

1例: $\mathbb{F} = \mathbb{F}_p \Rightarrow x^p - x = \prod_{a \in \mathbb{F}_p} (x-a)$

性质: $\forall f \in \mathbb{F}[x] \not\equiv 0, \forall a \in \mathbb{F}, \exists! m \in \mathbb{N}, \& g \in \mathbb{F}[x] \text{ s.t. } g(a) \neq 0 \&$

$$f(x) = (x-a)^m \overbrace{g(x)}^{\text{重数}} \begin{cases} \text{单根} & m=1 \\ \text{重根} & m \geq 2 \end{cases}$$

定义: $\forall f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{F}[x]$, 记

$$f'(x) := n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1 \in \mathbb{F}[x]$$

称 $f'(x)$ 为 f 的 形式微商 (formal derivative)

性质: 1) $(cf)' = c \cdot f'$

2) $(f+g)' = f' + g'$

3) $(fg)' = f'g + f \cdot g'$

性质: 1) $(x-a)^m \parallel f \xRightarrow{m \geq 1} (x-a)^{m-1} \parallel f' \quad (\text{反之不正确!})$

2) $\gcd(f, f') = 1 \Leftrightarrow f \text{ 无重根}$

3) $(x-a) \parallel f \Leftrightarrow \begin{cases} f(a) = 0 \\ f'(a) \neq 0 \end{cases}$
i.e. a 为 f 单根.

$$\forall f: 1) f = (x-a)^m g \Rightarrow f' = m(x-a)^{m-1}g + (x-a)^m g' \Rightarrow (x-a)^{m-1} | f'$$

$$2) \Rightarrow: \underline{\text{反例}} \quad (x-a)^2 | f \Rightarrow (x-a) | \gcd(f, f') \Rightarrow \gcd(f, f') \neq 1. \quad \text{错}$$

$$\Leftarrow: \underline{\text{反例}} \quad \exists a \quad \left\{ \begin{array}{l} x-a | f \Rightarrow f = (x-a)g \\ x-a | f' \end{array} \right\} \Rightarrow x-a | g \Rightarrow (x-a)^2 | f \quad \text{错}$$

$$3) \Rightarrow: f = (x-a)g \quad (g(a) \neq 0) \quad f' = g + (x-a)g' \Rightarrow \checkmark$$

$$\Leftarrow): \exists g \text{ s.t. } f = (x-a)g \quad \& \quad \left\{ \begin{array}{l} 0 \neq f'(a) = g(a) + (a-a)g'(a) \end{array} \right\}$$

$$\Rightarrow x-a \nmid f.$$

例: $\mathbb{F} = \mathbb{F}_p, f = x^p - x, f' = -1 \Rightarrow f$ 无重根.

§ 整系数多项式环 $\mathbb{Z}[x]$

$\mathbb{Q}[x]$ 与 $\mathbb{Z}[x]$ 不同之处:

整除性 $\begin{cases} \text{在 } \mathbb{Q}[x] \text{ 中: } 2x+1 \mid 4x+2 & \& 4x+2 \mid 2x+1 \\ \text{在 } \mathbb{Z}[x] \text{ 中: } 2x+1 \mid 4x+2 & \& 4x+2 \nmid 2x+1 \end{cases}$

带余除法 $\begin{cases} \text{在 } \mathbb{Q}[x] \text{ 中: } x^2 = (\frac{1}{2}x - \frac{1}{4})(2x+1) + \frac{1}{4} \\ \text{在 } \mathbb{Z}[x] \text{ 中: } \nexists q(x), r(x) \in \mathbb{Z}[x] \text{ s.t. } x^2 = q(x)(2x+1) + r(x). \end{cases}$

主理想 $\begin{cases} \text{在 } \mathbb{Q}[x] \text{ 中: } \forall I \triangleleft \mathbb{Q}[x] \text{ 都为主理想.} \\ \text{在 } \mathbb{Z}[x] \text{ 中: } I = (2, x) \triangleleft \mathbb{Z}[x] \text{ 不为理想.} \end{cases}$

定理(带余除法) $g \in \mathbb{Z}[x]$ 首一. 则 $\forall f \in \mathbb{Z}[x], \exists! q, r \in \mathbb{Z}[x]$ s.t.

$$f = q \cdot g + r \quad (\deg r < \deg g)$$

pf: 唯一性同 $\mathbb{Q}[x]$.

存在性: $I := \{f - ag \mid a \in \mathbb{Z}[x]\} \neq \emptyset$

设 $r(x) \in I$ 有最低次数. 则 $\deg(r) < \deg g$.

(否则 $r_1(x) = r(x) - \frac{lc(r)}{lc(g)} g(x) \cdot x^{\deg(r) - \deg(g)} \in I$
的次数小于 $r(x)$ 的次数 \nexists)

$\Rightarrow \checkmark$

注: $p \in \mathbb{F}[x]$ 不可约 $\Leftrightarrow \mathbb{F}[x]/(p) = \text{域}$

定义: 设 R 为整环. 称 $r \in R$ 为不可约元若

- 1) $r \notin R^\times$
- 2) $r = gh \Rightarrow g \in R^\times$ 或 $h \in R^\times$

注: $\mathbb{Z}[x]^\times = \{\pm 1\}$ 例. $2, 2x+1, x^2+1 \in \mathbb{Z}[x]$ 不可约

注: $f \in \mathbb{Z}[x]$ 不可约 $\Rightarrow f$ 的全体系数的公因子为 1.

定义: 若 $f \in \mathbb{Z}[x]$ 的全体系数的公因子为 1, 则称 f 为 **本原多项式**.

引理: $\forall a \in \mathbb{Q}[x] \setminus \{0\}$, $\exists! c \in \mathbb{Q} \ \& \ a_1 \in \mathbb{Z}[x] \text{ s.t.}$

$$a = c a_1$$

a 的零度 (content)

其中 a_1 为首项系数为正的**本原多项式**

Pf: 取 $N \in \mathbb{Z} \setminus \{0\}$ s.t. $Na = \sum_{i=0}^n \alpha_i x^i \in \mathbb{Z}[x]$ 且 $\alpha_n > 0$.

$$\alpha := \gcd(\alpha_0, \alpha_1, \dots, \alpha_n) \in \mathbb{Z}$$

$\Rightarrow a_1 = \frac{Na}{\alpha}$ 为首项系数为正的**本原多项式**

$\Rightarrow a = \frac{\alpha}{N} \cdot a_1$ 满足要求.

唯一性: 若 $a = c_2 a_1 = c_1 a_2$, 则 $\exists M \in \mathbb{N}$ s.t. $M a_1, M a_2 \in \mathbb{Z}[x]$

$$d := \gcd(M a_1, M a_2) \text{ 则}$$

$$\frac{M c_2}{d} a_1 = \frac{M c_1}{d} a_2 \text{ 其中 } \gcd\left(\frac{M c_1}{d}, \frac{M c_2}{d}\right) = 1.$$

$\Rightarrow \frac{M c_2}{d}$ 整除 a_1 所有系数 $\xrightarrow{a_1 \text{ 本原}} \frac{M c_2}{d} = \pm 1$

$\Rightarrow a_1 = \pm a_2 \xrightarrow{a_1, a_2 \text{ 首项系数为正}} a_1 = a_2 \Rightarrow c_1 = c_2. \quad \square$

注: $\varphi_p: \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$ 为环映射.

$$f = \sum_{i=0}^n a_i x^i \mapsto \bar{f} := \sum_{i=0}^n \bar{a}_i x^i$$

引理: 设 $f, g, h \in \mathbb{Z}[x] \setminus \{0\}$. 若 $f = gh$, 则

$$f = \text{本原} \iff g \ \& \ h = \text{本原}.$$

pf: \Rightarrow : 反证. 否则不妨设 $g \neq \text{本原}$. $\Rightarrow g = cg_1$ ($c \in \mathbb{Z} \setminus \{1, 0\}$)

$\Rightarrow c|g \Rightarrow c|f \Rightarrow c|f$ 的所有系数 $\Rightarrow f \neq \text{本原}$ 也.

\Leftarrow : 假设 $f \neq \text{本原} \Rightarrow \exists$ 素数 p s.t.

$$\varphi_p(f) = 0 \in \mathbb{F}_p[x]$$

$$\Rightarrow \varphi_p(g) \cdot \varphi_p(h) = \varphi_p(f) = 0 \in \mathbb{F}_p[x]$$

$$\Rightarrow \varphi_p(g) = 0 \in \mathbb{F}_p[x] \text{ 或 } \varphi_p(h) = 0 \in \mathbb{F}_p[x].$$

$$\Rightarrow p|g \text{ 或 } p|h \Rightarrow g \neq \text{本原} \text{ 或 } f \neq \text{本原} \square$$

定理: $f \in \mathbb{Z}[x]$ 本原. 则

f 在 $\mathbb{Z}[x]$ 中不可约 $\Leftrightarrow f$ 在 $\mathbb{Q}[x]$ 中不可约.

pf: \Rightarrow : 设 $f = gh$ (其中 $g = c_1 g'$, $h = c_2 h' \in \mathbb{Q}[x]$), 则

$$f = (c_1 c_2) \cdot g' h'$$

分解唯一性 $\xrightarrow{f \text{ 本原}} c_1 c_2 = \pm 1 \Rightarrow f = -g' h' \Rightarrow g' = \pm 1 \text{ 或 } h' = \pm 1$

$$\Rightarrow g' = 1 \text{ 或 } h' = 1 \Rightarrow g = c_1 \in \mathbb{Q}^\times \text{ 或 } h = c_2 \in \mathbb{Q}^\times.$$

$$\Rightarrow f \text{ 在 } \mathbb{Q}[x] \text{ 中不可约}$$

\Leftarrow : 设 $f = gh$ (其中 $g, h \in \mathbb{Z}[x]$) 则 $g, h \neq \text{本原}$

$$f \text{ 在 } \mathbb{Q}[x] \text{ 中不可约} \Rightarrow g \in \mathbb{Q}^\times \text{ 或 } h \in \mathbb{Q}^\times$$

$$\Rightarrow g = \pm 1 \text{ 或 } h = \pm 1$$

$$\Rightarrow f \text{ 在 } \mathbb{Z}[x] \text{ 中不可约.}$$

推论: $f \in \mathbb{Z}[x]$ 不可约 $\Leftrightarrow \pm f$ 为素数 或 $\begin{cases} f \text{ 本原} \\ f \text{ 在 } \mathbb{Q}[x] \text{ 中不可约} \end{cases}$

定理(UFD): $\forall f \in \mathbb{Z}[x] \setminus \{0\}$, 则 f 可唯一地 (不记不可约元的顺序) 写成

$$f = \epsilon \pi_1 \pi_2 \cdots \pi_r$$

其中 $\epsilon = \pm 1$, π_1, \dots, π_r 为首项系数为正的不可约元.

命题: $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ 为 n 次多项式 ($n \geq 1$). $\alpha = p/q$ ($(p, q) = 1$).

$$f(\alpha) = 0 \Rightarrow p | a_0 \text{ 且 } q | a_n$$

$$\text{pf: } a_n \left(\frac{p}{q}\right)^n + \cdots + a_1 \left(\frac{p}{q}\right) + a_0 = 0$$

$$\Rightarrow a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

$$\Rightarrow \begin{cases} q | a_n p^n \\ p | a_0 q^n \end{cases} \Rightarrow \begin{cases} q | a_n \\ p | a_0 \end{cases}$$

例: 证明 $3x^3 + x + 7$ 在 $\mathbb{Z}[x]$ 中不可约.

判定不可约性常见方法.

定理 (艾森斯坦 (Eisenstein) 判别法) $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ ($a_n \neq 0$)

$$\left. \begin{array}{l} p = \text{素数}, p \nmid a_n \\ p \mid a_i \ (i=0, 1, \dots, n-1) \\ p^2 \nmid a_0 \end{array} \right\} \Rightarrow f \text{ 在 } \mathbb{Q}[x] \text{ 中不可约.}$$

Pf: 反证: 若 f 在 $\mathbb{Q}[x]$ 可约, 则 $f = g \cdot h$ ($0 < \deg g < n$)

分解唯一性 $\Rightarrow f = c g_1 h_1$ ($c \in \mathbb{Z} \setminus \{0\}$, g_1, h_1 本原)

$$\Rightarrow \bar{a}_n x^n = \varphi_p(f) = \varphi_p(c) \cdot \varphi_p(g_1) \varphi_p(h_1)$$

$$\Rightarrow \varphi_p(g_1) = \bar{a}_1 x^{d_1} \text{ 且 } \varphi_p(h_1) = \bar{a}_2 x^{d_2} \quad \begin{array}{l} d_1, d_2 \geq 1 \\ d_1 + d_2 = n \end{array}$$

$\Rightarrow g_1$ 和 h_1 的常数项被 p 整除

$$\Rightarrow p^2 \mid a_0 \quad \downarrow$$

例: $f(x) = x^4 + 2x + 6 \in \mathbb{Q}[x]$

例: $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ (p 次分圆多项式)