

回顾 GCD: 在整环中定义,

有 gcd 的例子: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{F}[x], +, \cdot)$, $\mathbb{F}$: 域

无 gcd 的例子: $\mathbb{Z}[\sqrt{5}] = \{x+y\sqrt{5} \mid x, y \in \mathbb{Z}\}$. 整环, 但不是 UFD.

观察到: $9 = 3 \cdot 3 = (2+\sqrt{5})(2-\sqrt{5})$

定义(UFD): 我们称 D 是 UFD, 如果 D 中每个非零非单位的元素 a 都满足下列两个

条件: (1) a 可以写成 D 中有限多个不可约元素积.

$$(2) \text{ 设 } a = p_1 \cdots p_m = q_1 \cdots q_n$$

其中 $p_1, \dots, p_m, q_1, \dots, q_n$ 是 D 中的不可约元, 则 $m=n$ 且适当调整次序

$$p_i \sim q_i, \dots, p_m \sim q_m.$$

D 首先验证. $3, 2+\sqrt{5}, 2-\sqrt{5}$ 不可约. $\left. \begin{array}{l} \text{② 其次 } 3 \text{ 和 } 2+\sqrt{5}, 3 \text{ 和 } 2-\sqrt{5} \text{ 都不相伴.} \end{array} \right\} \Rightarrow \text{不是 UFD.}$

而且 9 没有非平凡的最大因子, 因为 $3, 2+\sqrt{5}, 2-\sqrt{5}$ 之间没有整除关系

$$\text{①: 不可约: } 3 = (m+n\sqrt{5})(k+l\sqrt{5}), m, n, k, l \in \mathbb{Z}.$$

$$3 = (m-n\sqrt{5})(k-l\sqrt{5})$$

$$\Rightarrow 9 = (m^2+5n^2)(k^2+5l^2) \quad m^2+5n^2, k^2+5l^2 \in \mathbb{N}$$

又 $m^2+5n^2 \neq 3$, 所以 $m^2+5n^2 = 9$ 或 1 ,

若 $m^2+5n^2 = 1$, 则 $n=0, m=\pm 1 \Rightarrow 3 = \pm 1 \cdot (k+l\sqrt{5})$, ± 1 是可逆元

若 $m^2+5n^2 = 9$, 则 $k^2+5l^2 = 1 \Rightarrow k=\pm 1, l=0 \Rightarrow 3 = \pm 1 \cdot (m+n\sqrt{5})$

$\Rightarrow 3$ 不可约.

同理, $2 \pm \sqrt{5}$ 也不可约.

②: 怎么证不相伴! 从定义出发.

定义: (相伴): 设 $a, b \in D$, 如果存在 $u, v \in U_D$ 使得 $ua = vb$ 则 a 和 b 在 D 上相伴.

先要刻画出 $\mathbb{Z}[\sqrt{5}]$ 中的所有可逆元:

$$\text{设 } uv = 1, \Rightarrow |u| \cdot |v| = 1 \text{ 故 } |u| \leq 1 \text{ 且 } |v| \leq 1,$$

$$\text{不妨设 } |u| \leq 1, \text{ 设 } u = m + n\sqrt{5}, \text{ 则 } |u| = \sqrt{u \cdot \bar{u}} = \sqrt{m^2 + 5n^2} \leq 1$$

$$\Rightarrow n = 0 \quad m = \pm 1, \text{ 从而 } v = \pm 1.$$

所以 $\mathbb{Z}[\sqrt{5}]$ 中的可逆元只有 ± 1



问题1: $\mathbb{Z}[x]$ 中 GCD 的存在性.

问题2: 若 GCD 存在, $\mathbb{Z}[x]$ 中 Bezant 关系式是否成立.

问题3: $\mathbb{Z}[x]$ 中是否有“辗转相除法”.

回答1: 定理: 如果 R 是一个 UFD, 则 $\forall a, b \in R$ 在 R 中 GCD-是存在.

定理2: 如果 R 是一个 UFD, 则 多项式环 $R[x, \dots, x_n]$ 也是 UFD.

参考文献: $\langle \text{Algebra} \rangle$ — Serge Lang

证明定理1: 设 $a, b \in R \setminus \{0\}$, 且有唯一分解:

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n} \quad b = q_1^{f_1} q_2^{f_2} \dots q_m^{f_m}$$

记 $r_1, \dots, r_s$ 为集合 $\{p_1, \dots, p_n, q_1, \dots, q_m\}$ 中的不同元素, 则 a 和 b 可以

$$\text{重写为: } a = \prod_{i=1}^s r_i^{g_i} \quad \text{and} \quad b = \prod_{i=1}^s r_i^{h_i}$$

其中某些 g_i, h_i 为 0. 则

$$\gcd(a, b) = \prod_{i=1}^s r_i^{\min(g_i, h_i)}$$

若 a 或 b 至少有一个为 0, 不妨设 $a=0$ 则 $\gcd(a, b) = b$.



题2: 不存在: 反例: $2, x^2+1 \in \mathbb{Z}[x]$, 不存在 $u, v \in \mathbb{Z}[x]$, s.t.

$$u \cdot 2 + v(x^2+1) = \gcd(2, x^2+1)$$

反证法: 设 $\exists u, v \in \mathbb{Z}[x]$, s.t. $u \cdot 2 + v(x^2+1) = \gcd(2, x^2+1)$

设 $\gcd(2, x^2+1) = g$, 则 $g|2$, 因为 $g \in \mathbb{Z}[x]$, 所以 $g = \pm 1$ 或 ± 2 .

又因为 g 在 $\mathbb{Z}[x]$ 中, $g|x^2+1$, 所以 $g = \pm 1$. 这里取 $g = 1$

$$u \cdot 2 + v \cdot (x^2+1) = 1$$

代入 $x=1$ $2 \cdot u(1) + v(1) \cdot 2 = 1$

$$2(u(1) + v(1)) = 1 \quad \text{矛盾.} \quad \square$$

题3: 没有. 例: $a = 3x^3 + x^2x + 5$ $b = 5x^2 - 3x + 1$

$$\text{In } \mathbb{Q}[x]: a = b \cdot \left(\frac{3}{5}x + \frac{14}{25}\right) + \frac{52}{25}x + \frac{111}{25}$$

$$\text{In } \mathbb{Z}[x]: \text{设 } 3x^3 + x^2x + 5 = (5x^2 - 3x + 1)(q_1x + q_0) + (r_1x + r_0)$$

$$\Rightarrow 3 = 5q_1, \rightarrow \leftarrow$$

$$\text{伪带余除法: } 5^2 \cdot (3x^3 + x^2x + 5) = (5x^2 - 3x + 1)(15x + 14) + (52x + 111)$$

$\square$

2. Def: (幂等): 环中的非零元 a 称为幂等, 如果它满足 $a^2 = a$.

$$|F|^n = a \cdot |F|^n \oplus (1-a) \cdot |F|^n, \quad a \in F \text{ 为幂等元.}$$

$$a \cdot |F|^n = \{a \cdot \vec{x} \mid \vec{x} \in |F|^n\} \quad (1-a) \cdot |F|^n = \{(1-a) \cdot \vec{x} \mid \vec{x} \in |F|^n\}$$

$$\text{Pf: } \forall \vec{x} \in |F|^n \quad \vec{x} = a \cdot \vec{x} + (1-a) \cdot \vec{x} \Rightarrow |F|^n = a \cdot |F|^n + (1-a) \cdot |F|^n$$

$$\forall \vec{x} \in a \cdot |F|^n \cap (1-a) \cdot |F|^n, \text{ 存在 } \vec{y}, \vec{z} \in |F|^n, \text{ s.t. } \vec{x} = a \cdot \vec{y} \text{ 且 } \vec{x} = (1-a) \cdot \vec{z}$$

$$\text{则 } a \cdot \vec{y} = (1-a) \cdot \vec{z} \Rightarrow a^2 \vec{y} = a \cdot (1-a) \vec{z} \Rightarrow a^2 \vec{y} = \vec{0}$$

因为 $a \neq 0$, 所以 $\vec{y} = \vec{0}$.

□

$$\text{令 } \mathcal{A}: F^n \longrightarrow F^n, \text{ 则 } \mathcal{A}^2 = \mathcal{A} \\ \vec{x} \longmapsto a\vec{x}$$

我们断言: $a \cdot F^n = \text{im}(\mathcal{A})$ $(1-a) \cdot F^n = \text{ker}(\mathcal{A})$ (自验证)

$$\text{pf: } \forall \vec{x} \in (1-a) \cdot F^n, \exists \vec{y} \in F^n, \text{ s.t. } \vec{x} = (1-a) \cdot \vec{y}$$

$$\mathcal{A}(\vec{x}) = \mathcal{A}((1-a)\vec{y}) = a \cdot (1-a)\vec{y} = \vec{0}$$

$$\Rightarrow \vec{x} \in \text{ker}(\mathcal{A})$$

$$\text{反过来, } \forall \vec{x} \in \text{ker}(\mathcal{A}), \mathcal{A}(\vec{x}) = \vec{0}$$

$$\text{i.e. } a \cdot \vec{x} = \vec{0}$$

$$(1-a)\vec{x} = \vec{x} - a\vec{x} = \vec{x}$$

$$\Rightarrow \vec{x} \in (1-a) \cdot F^n$$

$$\text{所以 } F^n = \text{im}(\mathcal{A}) \oplus \text{ker}(\mathcal{A}).$$

□

$$\text{并且 } \text{im}(\mathcal{A}) = \text{ker}(\mathcal{A} - E)$$

$$\forall \vec{x} \in \text{im}(\mathcal{A}), \exists \vec{y} \in F^n \text{ s.t. } \vec{x} = \mathcal{A}(\vec{y}) = a \cdot \vec{y}$$

$$\mathcal{A} - E(\vec{x}) = \mathcal{A}\vec{x} - \vec{x} = \mathcal{A}(\mathcal{A}(\vec{y})) - \vec{x} = \mathcal{A}\vec{y} - \vec{x} = \vec{0}$$

$$\text{反过来: } \forall \vec{x} \in \text{ker}(\mathcal{A} - E), \mathcal{A} - E(\vec{x}) = 0 \text{ i.e. } \mathcal{A}\vec{x} = \vec{x}$$

$$\Rightarrow \vec{x} \in \text{im} \mathcal{A} \quad \square$$

3. 一元多项式的无平方部分

设 F 是域; 则 $F[x]$ 是 UFD. 设 $f \in F[x]$ 且次 ≥ 1 , 则有唯一分解

$$f = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \quad p_i \in \text{Irr.} \quad p_i \text{ 互素.}$$

$$J = p_1 \cdots p_n, \quad p_i = \dots, \quad 1 \leq i \leq n.$$

称 p_i 是 f 的 i 重因子, $i=1, \dots, n$.

特别地, 当 $i=1$ 时, p_i 称为 f 的单因子.

$p_1 \cdot p_2 \cdots p_n$ 称为 f 的无平方部分.

问题: 怎么判断 f 是不是只有单因子.

定义: (形式导数):

设 $f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_1 x + f_0 \in F[x]$, 定义 f 关于 x 的导数为

$$f' = n f_n x^{n-1} + (n-1) f_{n-1} x^{n-2} + \cdots + f_1$$

性质: (1) $(f+g)' = f' + g'$

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

$$f = \sum_{i=0}^n f_i x^i \quad g = \sum_{j=0}^m g_j x^j$$

$$f \cdot g = \sum_{l=0}^{n+m} \left(\sum_{i=0}^l f_i g_{l-i} \right) x^l$$

$$\Rightarrow \boxed{(f \cdot g)' = \sum_{l=0}^{n+m-1} \left(\sum_{i=0}^l f_i g_{l-i} \cdot l \right) x^{l-1}}$$

$$\boxed{f'g + fg' = \left(\sum_{i=1}^n i f_i x^{i-1} \right) \left(\sum_{j=0}^m g_j x^j \right) + \left(\sum_{i=0}^n f_i x^i \right) \left(\sum_{j=1}^m j g_j x^{j-1} \right)}$$

$$= \sum_{l=0}^{n+m-1} \left(\sum_{i=0}^l i f_i g_{l-i} \right) x^l + \sum_{l=0}^{n+m-1} \left(\sum_{i=0}^l f_i g_{l-i+1} \cdot (l-i+1) \right) x^l$$

$$= \sum_{l=0}^{n+m-1} \left(\sum_{i=0}^l \left(i f_i g_{l-i+1} + f_i g_{l-i+1} (l-i+1) \right) \right) x^l$$

$$= \sum_{l=0}^{n+m-1} \left(\sum_{i=0}^l (l+1) g_{l-i+1} f_i \right) x^l$$

$$l \rightarrow l'-1$$

$$0 \leq l \leq n+m-1 \Rightarrow$$

$$1 \leq l' = l+1 \leq n+m$$

$$\Rightarrow f'g + fg' = \sum_{e'=1}^{m+n} \left(\sum_{i=0}^{e'} e' g_{e'-i} f_i \right) x^{e'-1}$$

$$\text{所以 } (fg)' = f'g + fg'$$

□

Thm. 设 F 是特征为 0 的域, $f \in F[x] \setminus F$, 则 f 的互素多项式在本域上与 $\frac{f}{\gcd(f, f')}$ 相伴.

Pf. 设 $f = p_1^{e_1} \cdots p_n^{e_n}$

$$\begin{aligned} f' &= \sum_{i=1}^n p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} \cdot e_i p_i^{e_i-1} \cdot p_{i+1}^{e_{i+1}} \cdots p_n^{e_n} \\ &= p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \cdot \underbrace{(e_1 p_1' p_2 \cdots p_n + p_1 e_2 p_2' \cdots p_n + \cdots + p_1 \cdots e_n p_n')}_{:= q} \end{aligned}$$

$$\text{下证 } \gcd(p_1^{e_1} \cdots p_n^{e_n}, q) = 1$$

反设: 设 $\gcd(p_1^{e_1} \cdots p_n^{e_n}, q) \neq 1$, 则一定存在 $p_j \ 1 \leq j \leq n$ 且 $p_j | q$

不妨设 $p_j = p_1$

$$p_1 | p_1 e_2 p_2 \cdots p_n + \cdots + p_1 \cdots e_n p_n'$$

$$\text{且 } p_1 | q \Rightarrow p_1 | e_1 p_1' p_2 \cdots p_n \Rightarrow p_1 | e_1 p_1'$$

与 $\deg(p_1') < \deg(p_1)$ 矛盾

$$\Rightarrow \gcd(f, f') = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

$$\frac{f}{\gcd(f, f')} = p_1 p_2 \cdots p_n$$

□.

推论: f 只有单因子当且仅当 $\gcd(f, f') = 1$.