1. 在扩展的辗转相除法(Extended Euclidean Algorithm)中, 令 $a, b \in F[x]^*, r_0 := a, r_1 := b$, 执行 $r_{i+2} := \mathrm{rem}(r_i, r_{i+1}, x)$, 其中 $i = 0, 1, \ldots$. 设 k 是最小的正整数使得 $r_{k+1} = 0$, 证明 $\gcd(r_i, r_{i+1}) = \gcd(r_{i+1}, r_{i+2})$, 其中 $i = 0, \ldots, k-1$, 因而 $\gcd(a, b) = r_k$.

Q1: 证明 $gcd(r_i, r_{i+1}) = gcd(r_{i+1}, r_{i+2})$

Q2: 证明 $gcd(a,b) = r_k$

证: (Q1): 因为 $r_{i+2} = rem(r_i, r_{i+1}, x)$, 所以 $\exists\, q(x) \in F[x]$, s.t

$$r_i = q_i r_{i+1} + r_{i+2} .$$

设 $gcd(r_i, r_{i+1}) = g \quad gcd(r_{i+1}, r_{i+2}) = d$

$g \mid r_i,\ g \mid r_{i+1} \Rightarrow g \mid r_i - q_i r_{i+1}$, 所以 $\left\langle \begin{array}{l} g \mid r_{i+2} \\ g \mid r_{i+1} \end{array} \right. \Rightarrow g \mid d$

$d \mid r_{i+1},\ d \mid r_{i+2} \Rightarrow d \mid q_i r_{i+1} + r_{i+2}$, 所以 $\left\langle \begin{array}{l} d \mid r_i \\ d \mid r_{i+1} \end{array} \right. \Rightarrow d \mid g.$

$\Rightarrow g \approx d$ 所以 $gcd(r_i, r_{i+1}) = gcd(r_{i+1}, r_{i+2})$

(Q2): $a = r_0,\ b = r_1$, 所以 $gcd(a,b) = gcd(r_0, r_1) = \cdots = gcd(r_k, r_{k+1})$

而 $r_{k+1} = 0 \quad gcd(r_k, r_{k+1}) = r_k$, 所以 $gcd(a,b) = r_k$

2. 设 $a = x^4 - 1$ 和 $b = x^2 + 2x + 1$. 分别在 $\mathbb{Q}[x]$ 和 $\mathbb{Z}_2[x]$ 中求解 $\gcd(a, b)$, $\mathrm{lcm}(a, b)$ 以及多项式 u, v 使得 $ua + vb = \gcd(a, b)$.

解: 法一: $a = x^4 - 1 = (x^2+1)(x^2-1) = (x^2+1)(x-1)(x+1)$

$b = (x+1)^2$

In $\mathbb{Q}[x]$: $gcd(a,b) = x+1 \qquad lcm(a,b) = (x^2+1)(x-1)(x+1)^2$

In $\mathbb{Z}_2[x]$: $a = x^4+1 = (x+1)^4$ $\quad b = (x+1)^2$

$\gcd(a,b) = (x+1)^2 = x^2+1$ $\quad \mathrm{lcm}(a,b) = (x+1)^4 = x^4+1$

$u = \bar{0}$ $\quad v = \bar{1}$ 则 $\bar{0}\cdot(x+1)^4 + \bar{1}\cdot(x+1)^2 = (x+1)^2$

法二：（扩展欧几里得算法）

$\mathbb{Q}[x]$中：$r_0 = a$ $\quad r_1 = b$ $\quad u_0 = 1$ $\quad u_1 = 0$ $\quad v_0 = 0$ $\quad v_1 = 1$

$q_2 = \mathrm{quo}(r_0, r_1, x)$ $\quad r_2 = \mathrm{rem}(r_0, r_1, x)$ i.e. $r_0 = q_2 r_1 + r_2$

$i \geq 2$: $q_i = \mathrm{quo}(r_{i-2}, r_{i-1}, x)$ $\quad r_i = \mathrm{rem}(r_{i-2}, r_{i-1}, x)$ i.e. $r_i = r_{i-2} - q_i r_{i-1}$

$u_i = u_{i-2} - q_i u_{i-1}$ $\quad v_i = v_{i-2} - q_i v_{i-1}$

$q_2 = \mathrm{quo}(x^4-1, x^2+2x+1, x) = x^2-2x+3$ $\quad r_2 = -4x-4$

$$\begin{array}{r|l|l} x^2+2x+1 & x^4-1 & x^2-2x+3 \\ & x^4+2x^3+x^2 & \\ \hline & -2x^3-x^2-1 & \\ & -2x^3-4x^2-2x & \\ \hline & 3x^2+2x-1 & \\ & 3x^2+6x+3 & \\ \hline & -4x-4 & \end{array}$$

u_i, v_i 始终满足

$u_i a + v_i b = r_i$ $\quad i=0$

$1\cdot a + 0\cdot b = a$

$0\cdot a + 1\cdot b = b$ $\quad i=1$

$(u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b = r_{i-2} - q_i r_{i-1}$
$= r_i$

$u_2 = u_0 - q_2 u_1 = 1 - 0 = 1$ $\quad v_2 = 0 - 1\cdot(x^2-2x+3) = -x^2+2x-3$

$q_3 = \mathrm{quo}(r_1, r_2) = \mathrm{quo}(x^2+2x+1, -4x-4) = -\frac{1}{4}x - \frac{1}{4}$

$r_3 = \mathrm{rem}(r_1, r_2) = \mathrm{rem}(x^2+2x+1, -4x-4) = 0$

$$\begin{array}{r|l|l} -4x-4 & x^2+2x+1 & -\frac{1}{4}x-\frac{1}{4} \\ & x^2+x & \\ \hline & x+1 & \\ & x+1 & \\ \hline & 0 & \end{array}$$

$r_3=0 \Longrightarrow \gcd(a,b)=r_2=-4x-4$ 与 $x+1$ 在 $\mathbb{Q}[x]$ 中相伴.

$$u=u_2=1 \qquad v=v_2=-x^2+2x-3$$

命题: $\operatorname{lcm}(a,b)=\dfrac{ab}{\gcd(a,b)}$.

证明: 要证 $\dfrac{ab}{\gcd(a,b)}$ 是 a 和 b 的最小公倍式, 只需证.

① $\dfrac{ab}{\gcd(a,b)}$ 是 a 和 b 的公倍式.

② 任意的 a 和 b 的公倍式 h, 都有 $\dfrac{ab}{\gcd(a,b)} \mid h$

记 $l := \dfrac{ab}{\gcd(a,b)}$, 则 $l=\dfrac{a}{\gcd(a,b)}\cdot b = a\cdot \dfrac{b}{\gcd(a,b)}$

因为 $\dfrac{a}{\gcd(a,b)}\in F[x]$, $\dfrac{b}{\gcd(a,b)}\in F[x]$, 所以我们有 l 是 a 和 b 的公倍式. ①

设 $a=\gcd(a,b)\cdot m \quad b=\gcd(a,b)\cdot n$, 则 m 和 n 互素, 由 Bezout 关系式知道

存在 $u,v\in F[x]$, 使得 $um+vn=1$

设 h 为 a 与 b 的公倍式, 对上式两边同乘 h

则有 $umh+vnh=h$

因为 h 为 a 与 b 的公倍式 所以存在 $c,d\in F[x]$, 使得

$$h=a\cdot c \quad 且 \quad h=b\cdot d$$

则 $$u\cdot m\cdot b\cdot d + v\cdot n\cdot a\cdot c = h$$

因为 $m=\dfrac{a}{\gcd(a,b)} \qquad n=\dfrac{b}{\gcd(a,b)}$

所以 $$u\cdot\frac{ab}{\gcd(a,b)}\cdot d + v\cdot\frac{ab}{\gcd(a,b)}\cdot c = h$$

$$\Longrightarrow \frac{ab}{\gcd(a,b)}(ud+vc)=h$$

$$\Longrightarrow \frac{ab}{\gcd(a,b)} \mid h \quad ② \qquad \square$$

$$\Longrightarrow \operatorname{lcm}(a,b)=\frac{(x^4-1)(x^2+2x+1)}{-4x-4}=-\frac{1}{4}(x^4-1)(x+1)$$

$\mathbb{Z}_2[x]$: $\quad a=x^4-1 \quad b=x^2+2x+1=(x+1)^2=x^2+1$

$\gcd(a,b)=x^2+1 \qquad 0-\frac{b}{g}=0-\frac{x^2+1}{x^2+1}=-1=1$

或 $u=0 \quad v=1$

也可取 $u=1 \quad v=-x^2$ 则 $\qquad 1+\frac{a}{g}=1+\frac{x^4-1}{x^2+1}=1+x^2+1=x^2=-x^2$

$$1\cdot(x^4-1)-x^2(x^2+1)=-x^2-1=x^2+1=\gcd(a,b)$$

也就是说 使得 $ua+vb=\gcd(a,b)$ 的 u 和 v 不唯一.

若 $u,v\in F[x]$ 使得 $ua+vb=g$, 则

$$\left(u-q\cdot\frac{b}{g}\right)a+\left(v+q\cdot\frac{a}{g}\right)b=g \qquad \forall q\in F[x]$$

若加条件: ① $\deg(u)<\deg(\frac{b}{g})$, 且 ② $\deg(v)<\deg(\frac{a}{g})$, 则 (u,v) 被唯一确定.

否则 存在 u_1, v_1, $\deg(u_1)<\deg(\frac{b}{g})$ $\deg(v_1)<\deg(\frac{a}{g})$ 使得

$$\begin{aligned} u_1a+v_1b&=g \\ ua+vb&=g \end{aligned} \Longrightarrow (u_1-u)a+(v_1-v)b=0$$

因为 $\deg(u)<\deg(\frac{b}{g})=\deg(b)-\deg(g)$ 且 $\deg(u_1)<\deg(b)-\deg(g)$

所以 $\deg(u_1-u)\le\max\{\deg(u_1),\deg(u)\}<\deg(b)-\deg(g)$

$\Longrightarrow \deg((u_1-u)a)<\deg(a)+\deg(b)-\deg(g)$

又因为 $\mathrm{lcm}(a,b)=\frac{ab}{\gcd(a,b)}$, 所以 $\deg(\mathrm{lcm}(a,b))=\deg(a)+\deg(b)-\deg(g)$

$\Longrightarrow \deg((u_1-u)a)<\deg(\mathrm{lcm}(a,b))$

另一方面, $(u_1-u)a$ 是 a 的倍式, $(u_1-u)a=-(v_1-v)b$ 也是 b 的倍式, 所以 $(u_1-u)a$ 是 a 与 b 的公倍式, 则有 $\mathrm{lcm}(a,b)\mid(u_1-u)a$

与 $\deg((u_1-u)a)<\deg(\mathrm{lcm}(a,b))$ 矛盾. $\square$

By the way, 扩展欧几里得算法给出的是满足次数条件的解.

3. 设 D 是整环, $a, b, c, d \in D$. 证明 $a \approx b$ 和 $c \approx d$ 蕴含 $ac \approx bd$.

证明: 因为 $a \approx b$, $c \approx d$. 所以存在 $u, v, s, t \in U_D$, 使得

D中可逆元集合

$ua = vb$ 且 $sc = td$

则有 $uasc = vbtd$, 由整环的交换性可知

$usac = vtbd$

又因为 $u \cdot s \in U_D$ 且 $vt \in U_D$, 所以 $ac \approx bd$.

方法二: ① 若 $a, b, c, d \in D^*$

整除运算除数 $\neq 0$

则由 $a \approx b$, $c \approx d$, 可知

$a | b$ 且 $b | a$ $\quad$ $c | d$ 且 $d | c$

$\Rightarrow ac | bd$ 且 $bd | ac$

$\Rightarrow ac \approx bd$

② 若至少有1个为0, 不妨设 $a = 0$ 则由 $a \approx b \Rightarrow b = 0$

则 $ac = 0$ $bd = 0$ $\Rightarrow ac \approx bd$.

4. 设 $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ 是 $\mathbb{Q}^3$ 的标准基, 线性映射 $\mathcal{A}\colon \mathbb{Q}^3 \to \mathbb{Q}^3$ 由

$$\mathcal{A}(\mathbf{e}_1) = \mathbf{e}_2,\ \mathcal{A}(\mathbf{e}_2) = \mathbf{e}_3,\ \mathcal{A}(\mathbf{e}_3) = \mathbf{e}_1$$

确定.

(a) 求非零多项式 $f \in \mathbb{Q}[t]$ 使得 $f(\mathcal{A}) = \mathcal{O}$, 其中 $\mathcal{O}$ 代表从 $\mathbb{Q}^3$ 到 $\mathbb{Q}^3$ 的零线性映射.

(b) 求解 $\dim(\ker(\mathcal{A}^2 + \mathcal{A} + \mathcal{I}))$, 其中 $\mathcal{I}$ 代表从 $\mathbb{Q}^3$ 到 $\mathbb{Q}^3$ 的恒等线性映射.

定义(特征多项式)：给定线性算子 $\mathcal{A}$，设 A 是 $\mathcal{A}$ 在标准基下的矩阵，则 $P(t)=\det(tE-A)$ 为线性算子 $\mathcal{A}$ 的特征多项式.

定理(Hamilton-Cayley定理)：设 $P(t)$ 为 $\mathcal{A}$ 的特征多项式 则 $P(\mathcal{A})=0$.
零映射

$P(A)=0$ → 零矩阵

证明：$p(t)=|tE-A|=t^n+a_1t^{n-1}+\cdots+a_{n-1}t+a_n$

$$P(A)=A^n+a_1A^{n-1}+\cdots+a_{n-1}A+a_nE$$

设 B 是 $tE-A$ 的伴随矩阵，则

$$(tE-A)\cdot B=|tE-A|\cdot E=p(t)\cdot E$$

因为伴随矩阵中的每个元素都是 A 中元素的代数余子式，所以 B 中的元素次数不超过 $n-1$ 的关于 t 的多项式，则 B 可以写成：

$$B=B_0+B_1t+\cdots+B_{n-1}t^{n-1}$$

则 $p(t)\cdot E=(tE-A)\cdot B$

$$=(tE-A)\cdot\sum_{i=0}^{n-1}t^iB_i$$

$$=\sum_{i=0}^{n-1}t^{i+1}B_i-\sum_{i=0}^{n-1}t^iAB_i$$

$$=t^nB_{n-1}+\sum_{i=1}^{n-1}t^i(B_{i-1}-AB_i)-AB_0$$

又因为 $p(t)E=t^nE+a_1t^{n-1}E+\cdots+a_{n-1}tE+a_nE$

所以比较两边的系数，得到

$$\begin{cases}B_{n-1}=E\\ B_{i-1}-AB_i=a_{n-i}E\quad\forall\,1\le i\le n-1\\ -AB_0=a_nE\end{cases}\Longrightarrow\begin{cases}A^nB_{n-1}=A^n\\ A^i(B_{i-1}-AB_i)=a_{n-i}A^i\quad(\star)\\ -AB_0=a_nE\end{cases}$$

对($\star$)式两边相加得 $A^nB_{n-1}+A^{n-1}B_{n-2}-A^nB_{n-1}+A^{n-2}B_{n-3}-A^{n-1}B_{n-2}+\cdots-AB_0$

$$=0=A^n+a_{n-1}A^1+a_{n-2}A^2+\cdots+a_1A^{n-1}+a_nE=P(A)$$ ▯

(a) $tE-A=\begin{pmatrix} t & & \\ & t & \\ & & t \end{pmatrix}-\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

$$=\begin{pmatrix} t & 0 & -1 \\ -1 & t & 0 \\ 0 & -1 & t \end{pmatrix}$$

所以 $\det(tE-A)=t^3+1\cdot(-1)=t^3-1$.

解: (1) $\mathcal{A}(\vec{e}_1,\vec{e}_2,\vec{e}_3)=(e_1,e_2,e_3)\underbrace{\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}}_{A}$

$A^2=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ $\quad A^3=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}=E$

所以取 $f=t^3-1$ 此时 $f(\mathcal{A})=\mathcal{A}^3-I=O$

Or $A^4=A$, 所以取 $f=t^4-t$ 也可以.

(2)（法一）$f = t^3 - 1 = (t-1)(t^2+t+1)$

因 $\gcd(t-1, t^2+t+1) = 1$，由核桎分解可知

$$\mathbb{F}^3 = \ker(\mathcal{A} - I) \oplus \ker(\mathcal{A}^2 + \mathcal{A} + I)$$

进而 $\dim(\ker(\mathcal{A} - I)) + \dim(\ker(\mathcal{A}^2 + \mathcal{A} + I)) = 3$

$$\dim(\ker(\mathcal{A} - I)) = \dim(\mathrm{sol}((A-E)\vec{v} = \vec{0}))$$
$$= 3 - \dim(A-E)$$

$$A - E = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \end{pmatrix} \longrightarrow \begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$\Longrightarrow \dim(A-E) = 2 \Longrightarrow \dim(\ker(\mathcal{A} - I)) = 1$

所以 $\dim(\ker(\mathcal{A}^2 + \mathcal{A} + I)) = 3 - 1 = 2$.

（法二） 由对偶定理可知：

$$\dim(\ker(\mathcal{A}^2 + \mathcal{A} + I)) + \dim(\mathrm{im}(\mathcal{A}^2 + \mathcal{A} + I)) = 3$$

$$\dim(\mathrm{im}(\mathcal{A}^2 + \mathcal{A} + I)) = \dim(\mathrm{rank}(A^2 + A + E))$$

而 $A^2 + A + E = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

所以 $\dim(\mathrm{rank}(A^2 + A + E)) = 1$

$\Rightarrow \dim(\ker(\mathscr{A}^2+\mathscr{A}+\mathcal{I}))=3-1=2.$ $\square$

5. 设 $\mathbb{Z}[\sqrt{-1}]=\{x+y\sqrt{-1} \mid x,y\in\mathbb{Z}\}$. 求 5 在 $\mathbb{Z}[\sqrt{-1}]$ 中的不可约分解.

首先找到所以 $\mathbb{Z}[\sqrt{-1}]$ 中的可逆元

设 $a+b\sqrt{-1}$ 可逆，则存在 $c+d\sqrt{-1}$, $a,b,c,d\in\mathbb{Z}$ 使得

$(a+b\sqrt{-1})(c+d\sqrt{-1})=1$
$(a-b\sqrt{-1})(c-d\sqrt{-1})=1$ $\Rightarrow (a^2+b^2)(c^2+d^2)=1$

则 $a=\pm1$ $b=0$ 或 $a=0$ $b=\pm1$

$\Downarrow$ $\qquad\qquad$ $\Downarrow$

$a+b\sqrt{-1}=\pm1$ $\qquad$ $a+b\sqrt{-1}=\pm\sqrt{-1}$

$\Downarrow$ $\qquad\qquad$ $\Downarrow$

$c+d\sqrt{-1}=\pm1$ $\qquad$ $c+d\sqrt{-1}=\pm\sqrt{-1}$

所以不可约元只有 $\pm1, \pm\sqrt{-1}$.

设 $5=(a+b\sqrt{-1})(c+d\sqrt{-1})$ $\quad a,b,c,d\in\mathbb{Z}$.

则 $5=(a-b\sqrt{-1})(c-d\sqrt{-1})$

$\Rightarrow 25=(a^2+b^2)(c^2+d^2)$

两种可能: ① 25×1 或 ② 5×5

①: 不妨设 $a^2+b^2=1$ 则 $a=\pm1$ $b=0$ 或 $b=\pm1$ $a=0$

$\Rightarrow 25=\pm1(c^2+d^2)$ 或 $25=\pm\sqrt{-1}(c^2+d^2)$

不符合不可约分解这一条件.

② $a^2+b^2=c^2+d^2=5$

则 $a=\pm 2$ $b=\pm 1$ 或 $a=\pm 1$, $b=\pm 2$

$\Rightarrow$ $a+b\sqrt{-1}=\pm 2\pm\sqrt{-1}$ 或 $\pm 1\pm 2\sqrt{-1}$

对应的 $c+d\sqrt{-1}$ 为 $\pm 2\mp\sqrt{-1}$ 或 $\pm 1\mp 2\sqrt{-1}$

$\Rightarrow$ $5=(2+\sqrt{-1})(2-\sqrt{-1})$

$=(-2-\sqrt{-1})(-2+\sqrt{-1})$

$=(1+2\sqrt{-1})(1-2\sqrt{-1})$

$=(-1-2\sqrt{-1})(-1+2\sqrt{-1})$

下证 上述因子不可约. 以 $2+\sqrt{-1}$ 为例.

设 $2+\sqrt{-1}=(a+b\sqrt{-1})(c+d\sqrt{-1})$

则 $2-\sqrt{-1}=(a-b\sqrt{-1})(c-d\sqrt{-1})$

$\Rightarrow$ $5=(a^2+b^2)(c^2+d^2)$ $\quad 5=5\times 1$

不妨设 $a^2+b^2=1$ 则 $a=\pm 1$ $b=0$ 或 $a=0$ $b=\pm 1$

$\Rightarrow$ $2+\sqrt{-1}=1\cdot(2+\sqrt{-1})=(-1)(-2-\sqrt{-1})=(\sqrt{-1})(-2\sqrt{-1}+1)=(-\sqrt{-1})(2\sqrt{-1}-1)$

由于 ± 1, $\pm\sqrt{-1}$ 均可逆 $\Rightarrow$ $2+\sqrt{-1}$ 不可约.

$\square$

例:(函数线性空间) $\mathbb{R}[x]^{(n)} = \{ f \in \mathbb{R}[x] \mid \deg f < n \}$

设 $D: \mathbb{R}[x]^{(n)} \longrightarrow \mathbb{R}[x]^{(n)}$

由 $D(f) = f'$ 定义。求 D 在 $1, x, \cdots, x^{n-1}$ 下的矩阵

$$D(1, x, x^2, \cdots x^{n-1}) = (0, 1, 2x, \cdots (n-1)x^{n-2})$$

$$(0, 1, 2x, \cdots (n-1)x^{n-2}) = (1, x, x^2, \cdots, x^{n-1}) \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & & & n-1 \\ 0 & 0 & 0 & & & 0 \end{pmatrix}$$

定义 0.1 设R是整环。如果存在$d: R \to \mathbb{N}^+$满足:对任意$a, b \in R$, 存在$q, r \in R$满足

$$a = qb + r, \quad r = 0 \text{ 或 } d(r) < d(b),$$

则称R为**欧几里德环**(*Euclidean Domain, ED*)。

尝试完成:

(i) 令$R = \mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}, i^2 = -1\}$, 证明: $d: m + ni \mapsto m^2 + n^2$使得$R$成为欧几里德整环。

Pf: 对于 $\alpha, \beta \in R$, $\beta \neq 0$ 令 $\frac{\alpha}{\beta} = t + s\sqrt{-1}$, $t, s \in \mathbb{Q}$.

eg: $\frac{3+2\sqrt{-1}}{2+\sqrt{-1}} = \frac{(3+2\sqrt{-1})(2-\sqrt{-1})}{(2+\sqrt{-1})(2-\sqrt{-1})} = \frac{6+\sqrt{-1}+2}{5} = \frac{8+\sqrt{-1}}{5} = \frac{8}{5} + \frac{1}{5}\sqrt{-1}$

取整数 u, v s.t. $|t-u| \le \frac{1}{2}$, $|s-v| \le \frac{1}{2}$, 令

$q = u + v\sqrt{-1}$ $\quad r_1 = (t-u) + (s-v)\sqrt{-1}$ 于是

$$\frac{\alpha}{\beta} = q + r_1$$

$\Longrightarrow \quad \alpha = q\beta + r_1\beta, \quad r_1\beta = \alpha - q\beta \in R.$

并且 $d(\gamma_1)=N(\gamma_1)=(t-u)^2+(s-v)^2\le\frac{1}{4}+\frac{1}{4}=\frac{1}{2}<1$

则 $d(\gamma_1\beta)=N(\gamma_1\beta)=N(\gamma_1)\cdot N(\beta)<N(\beta)=d(\beta)$

取 $\gamma=\gamma_1\beta$ 则有 $\alpha=q\beta+\gamma$ 且 $d(\gamma)<d(\beta)$.

$\square$