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 $\gcd(a, b) = r_k$.

证明: 设 $i = 0, 1, \ldots, k+1$. $r_i = q_{i+2} \cdot r_{i+1} + r_{i+2}$ (*)

其中 $\deg(q_{i+2}) + \deg(r_{i+1}) = \deg(r_i)$, $\deg(r_{i+2}) < \deg(r_{i+1})$.

设 $g_i = \gcd(r_i, r_{i+1})$, 只需证明 $g_i \sim g_{i+1}$ 即 (1) $g_i \mid g_{i+1}$. (2) $g_{i+1} \mid g_i$

因而, $\gcd(a,b) = g_0 = g_1 = \cdots = g_{k+1} = \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k$

(1) 由 $g_i \mid r_i$, $g_i \mid r_{i+1}$ 及(*)式, 可得: $g_i \mid r_{i+2}$

那么 g_i 是 r_{i+1} 和 r_{i+2} 的公因式. $g_i \mid \gcd(r_{i+1}, r_{i+2})$.

(2) 由 $g_{i+1} \mid r_{i+1}$, $g_{i+1} \mid r_{i+2}$ 及(*)式可得: $g_{i+1} \mid r_i$.

那么 g_{i+1} 是 r_i 和 r_{i+1} 的公因式. 那么 $\gcd(r_i, r_{i+1}) \mid a_{i+1}$. □

注: 1. 设 $g = \gcd(a,b)$. $a = n \cdot g$, $b = m \cdot g$ $\gcd(n, m) = 1$.

2. 在F[x]中. $a \mid b$ 且 $b \mid a$ 则 $a \sim b$. 在$\mathbb{Z}$中 $a \le b$ 且 $a \not\sim b$ 则 $a = b$.

3. 复习命题5.3.(1). 整除关系的传递性: $a \mid b$ 且 $b \mid c$ 则 $a \mid c$.

(2) $a|f$ 且 $a|g$ 则 $a|u\cdot f+v\cdot g$.

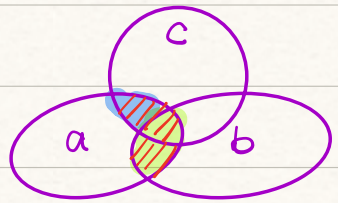
4. $a,b\in D^*$ $\forall u,v\in D$

(1) $\gcd(a,b+u\cdot a)=\gcd(a,b)$.

$\gcd(a+vb,b)=\gcd(a,b)$

(2) ~~$\gcd(a,b\cdot c)=\gcd(a,b)\cdot\gcd(a,c)/\gcd(b,c)$~~.

$$\gcd(a,b\cdot c)=\gcd(a,b)\gcd\left(\frac{a}{\gcd(a,b)},c\right)$$



(3) $\gcd(a,b)=1$ 且 $a|bc\Rightarrow a|c$.

5 数学归纳法：$\forall n\in\mathbb{N}$，存在某个命题 $P(n)$

(1) $P(1)$ 成立 (2) $\forall k\in\mathbb{N}$. 由 $P(k)$ 成立总能推出 $P(k+1)$ 成立则对所有 $n\in\mathbb{N}$，$P(n)$ 成立.

比较讲义中的数学归纳法和上述证明方法.

6. 反证法：正确做出反设. 分析反设和命题关系

典型：证明素数有无限多个.

$a_1,\cdots,a_N$ $n=a_1\cdots a_N+1$ $a_i\nmid N$.

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: $r_0 := a$ $r_1 := b$. $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$.

$\mathbb{Q}[x]$: $r_0 = q_2 \cdot r_1 + r_2$, $q_2 = x^2 - 2x + 3$, $r_2 = -4x - 4$.

$u_2 = u_0 - q_2 \cdot u_1 = 1$, $v_2 = v_0 - q_2 \cdot v_1 = -x^2 + 2x - 3$.

$r_1 = q_3 \cdot r_2 + r_3$, $q_3 = -\frac{1}{4}x - \frac{1}{4}$, $r_3 = 0$.

可不算: $u_3 = u_1 - q_3 \cdot u_2 = \frac{1}{4}x + \frac{1}{4}$, $v_3 = v_1 - q_3 \cdot v_2 = 1 + (\frac{1}{4}x + \frac{1}{4})(-x^2 + 2x - 3) = \frac{1}{4}(-x^3 + x^2 - x + 1)$

$\gcd(a, b) = r_2 = -4x - 4$, $u = 1$, $v = -x^2 + 2x - 3$. 书写规范: 注明 u, v

可化为首一: 分 $x + 1$ $-\frac{1}{4}$ $\frac{1}{4}(x^2 - 2x + 3)$

$$\mathrm{lcm}(a, b) = \frac{a \cdot b}{\gcd(a, b)} = x^5 + x^4 - x - 1.$$

$\mathbb{Z}_2[x]$: 环同态 $\varphi : \mathbb{Q}[x] \to \mathbb{Z}_2[x]$.

首一 首一 $\sum_{i=1}^{n} a_i x^i \mapsto \sum_{i=1}^{n} \overline{a}_i x^i$.

$\varphi(r_0) = \varphi(q_2)\varphi(r_1) + \varphi(r_2)$, $\varphi(q_2) = x^2 + 1$, $\varphi(r_2) = 0$. $\therefore \varphi(r_2) = \mathrm{rem}(\varphi(r_0), \varphi(r_1), x)$.

因此: $\gcd(a, b) = b$, 即 $u = 0$, $v = 1$.

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

另：$a = x^4-1 = (x^2-1)(x^2+1) = (x+1)(x-1)(x^2+1)$　$b = x^2+2x+1 = (x+1)^2$

存在 u, v $\begin{cases}\deg(u) < \deg(\frac{b}{g}) \\ \deg(v) < \deg(\frac{a}{g})\end{cases}$ 使得 $u\cdot a + v\cdot b = \gcd(a,b) = x+1$

待定系数法 设 $u_0, v_0, v_1, v_2 \in \mathbb{Q}$ s.t. $u_0\cdot a + (v_0+v_1x+v_2x^2)\cdot b = x+1$.

$u_0(x^4-1) + (v_0+v_1x+v_2x^2)(x^2+2x+1) = x+1$

线性方程组：

$$\begin{cases} u_0 + v_2 = 0 \\ v_1 + 2v_2 = 0 \\ v_0 + 2v_1 + v_2 = 0 \\ 2v_0 + v_1 = 1 \\ v_0 - u_0 = 1 \end{cases}$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 2 & 1 & 0 \\ -1 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} u_0 \\ v_0 \\ v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

"overdetermined system."

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & -\frac{1}{4} \\ 0 & 0 & 1 & 2 & 0 & -\frac{1}{2} \\ 0 & 1 & 2 & 1 & 0 & \frac{3}{4} \\ 0 & 2 & 1 & 0 & 1 & 1 \\ -1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & -\frac{1}{4} \\ 0 & 0 & 1 & 2 & 0 & -\frac{1}{2} \\ 0 & 1 & 2 & 1 & 0 & \frac{3}{4} \\ 0 & 0 & -3 & -2 & 1 & \frac{1}{2} \\ 0 & 1 & 1 & 1 & 0 & \frac{1}{4} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & -\frac{1}{4} \\ 0 & 0 & 1 & 2 & 0 & -\frac{1}{2} \\ 0 & 1 & 2 & 1 & 0 & \frac{3}{4} \\ 0 & 0 & 1 & \frac{2}{3} & -\frac{1}{3} & -\frac{1}{6} \\ 0 & 0 & -1 & -1 & 0 & -\frac{1}{4} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & -\frac{1}{4} \\ 0 & 0 & 1 & 2 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & -\frac{1}{3} & \frac{2}{3} & \frac{5}{12} \\ 0 & 0 & 1 & \frac{2}{3} & -\frac{1}{3} & -\frac{1}{6} \\ 0 & 0 & 0 & -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{12} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & -\frac{1}{4} \\ 0 & 0 & 1 & 2 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & -\frac{1}{3} & \frac{2}{3} & \frac{5}{12} \\ 0 & 0 & 1 & \frac{2}{3} & -\frac{1}{3} & -\frac{1}{6} \\ 0 & 0 & 0 & 1 & 1 & \frac{1}{4} \end{pmatrix}$$

$u_0 = -\frac{1}{4}$, $v_0 = \frac{3}{4}$, $v_1 = -\frac{1}{2}$, $v_2 = \frac{1}{4}$

$u = -\frac{1}{4}$　$v = \frac{1}{4}(x^2-2x+3)$.

注：若 $\gcd(a,b) = 1$，则 $\exists u, v$. $\deg(u) < \deg(b)$, $\deg(v) < \deg(a)$ s.t. $u\cdot a + v\cdot b = 1$.

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：由命题5.7和 $a \sim b$ 和 $c \sim d$ 可得：$a \mid b$ 且 $b \mid a$. $c \mid d$ 且 $d \mid c$

由命题5.3得：$ac \mid bd$ 且 $bd \mid ac$.

综上：$ac \sim bd$. 注：U_D 是一个乘法群. 设 $ua = vb$, $mc = nd$. 其中 $u, v, m, n \in U_D$

那么 $umac = vnbd$, $um, vn \in U_D$. 因此 $ac \sim bd$.

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.

解：(a) 容易验证：$\mathcal{A}^3(e_1) = \mathcal{A}^2(e_2) = \mathcal{A}(e_3) = e_1$, $\mathcal{A}^3(e_2) = e_2$, $\mathcal{A}^3(e_3) = e_3$

也就是说：$\mathcal{A}^3(x) = x$, $\forall x \in \mathbb{Q}^3$, $\mathcal{A}^3 - \mathcal{I} = \mathcal{O}$

$f = t^3 - 1$.

(b) $f = t^3-1 = (t-1)(t^2+t+1)$ $\gcd(t-1, t^2+t+1) = 1$.

由核核分解. $\ker(A-I) \oplus \ker(A^2+A+I) = \mathbb{Q}^3$.

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

A 的矩阵表示 $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ $A-I = \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$

$\mathrm{rank}(A-I) = 2$.

另: 复习线性映射的矩阵表示.

$$A^2+A+I = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

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

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.

解:

注意到 $\mathbb{Z}[\sqrt{-1}]$ 是整环(无零因子的交换幺环)

* $\mathbb{Z}[\sqrt{-1}]$ 中的可逆元是 $\{1, -1, \sqrt{-1}, -\sqrt{-1}\}$

5 在 $\mathbb{Z}$ 上不可约. $5 = 4-(-1) = (2+\sqrt{-1})(2-\sqrt{-1})$

下面证明 $2\pm\sqrt{-1}$ 在 $\mathbb{Z}[\sqrt{-1}]$ 中不可约.

假设: $2+\sqrt{-1} = (m+n\sqrt{-1})(k+l\sqrt{-1})$ $\quad m,n,k,l\in\mathbb{Z}$.

两边取共轭: $2-\sqrt{-1} = (m-n\sqrt{-1})(k-l\sqrt{-1})$

$$5 = (m^2+n^2)(k^2+l^2)$$

$m^2+n^2 = 1$ 或 5.

若 $m^2+n^2=1$ 则 $m=\pm1, n=0$ 或 $m=0, n=\pm1$ 对应 $m+n\sqrt{-1}$ 为可逆元.

若 $m^2+n^2=5$ 则 $k+l\sqrt{-1}$ 是可逆元.

同理可证: $2-\sqrt{-1}$ 是不可约元.

$25 = 5\cdot5 = (2^2+1^2)(2^2+1^2)$.

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

同一个分解.

$2+\sqrt{-1} \not\sim 1-2\sqrt{-1}$

$2-\sqrt{-1} \not\sim 1+2\sqrt{-1}$

注: $\mathbb{Z}[\sqrt{-1}]$ Gaussian integer 高斯整数环 UFD.

2. (Gauss引理) 设 $f, g \in \mathbb{Z}[x]^*$ 都是本原多项式，则 $f \cdot g$ 也是本原多项式.

$f(x) \in \mathbb{Z}[x]$ 在 $\mathbb{Q}[x]$ 上不可约 $\not\Rightarrow$ 在 $\mathbb{Z}[x]$ 上不可约 eg. $2x$.

$\deg(f) > 0$. 在 $\mathbb{Z}[x]$ 上不可约 $\Rightarrow$ 在 $\mathbb{Q}[x]$ 上不可约

由定理 6.3.2 ↗ 如果 $f(x)$ 在 $\mathbb{Z}[x]$ 中不能写成两个正次数多项式之积，则 f 在 $\mathbb{Q}[x]$ 不可约.

在 $\mathbb{Z}[x]$ 上的分解：$f = \mathrm{cont}(f)\,\mathrm{pp}(f)$，$\mathrm{pp}(f)$ 为本原多项式.

若本原多项式可以分解为两个有理系数多项式的乘积，那么它一定可以分解为两个整系数多项式的乘积

若本原多项式在 $\mathbb{Q}[x]$ 中不可约，那么它一定在 $\mathbb{Z}[x]$ 中不可约.

↑ 结合 Eisenstein 不可约判别法

3. C-Finite 序列.

Fibonacci 数列：$F_0 = 0$，$F_1 = 1$，$F_n = F_{n-1} + F_{n-2}$ $(n \geq 2)$. （第 n 个月兔子）

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}$$

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \cdot \begin{pmatrix} F_1 \\ F_0 \end{pmatrix}$$

1、1、2、3、5、8、… OEIS

公元1150年.

由 $a_n = a_{n-1} + a_{n-2}$ $(n \geq 2)$ 确定 $(a_n)_{n \geq 0}$

只需固定 a_0 和 a_1 即可. 解空间是 $\mathbb{Q}$ 上的 2 维线性空间.