1. Bézout's identity (Bezout's Lemma)

$\mathbb{Z}$：设整数 a b 的最大公因子是 d，那么存在整数 x、y 使得 $x\cdot a+y\cdot b=d$。

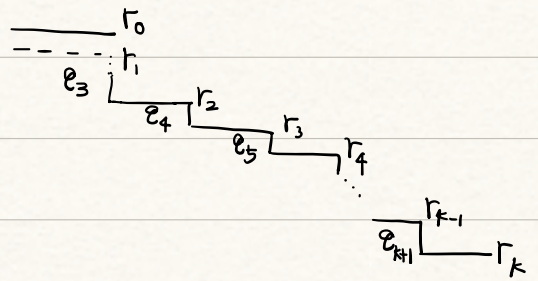
$F[x]$：设 $F[x]$ 中多项式 a、b 的最大公因式为 g，那么存在多项式 u、v 使得 $u\cdot a+v\cdot b=g$。

我们称 (u,v) 为 (a,b) 的 Bezout 系数。如何计算？

回顾多项式环上的扩展欧几里德算法 (Extended Euclidean Algorithm)

不妨假设 $\deg(a)\geq\deg(b)$，　$r_0\leftarrow a$　$r_1\leftarrow b$；　$u_0\leftarrow 1$，$v_0\leftarrow 0$，$u_1\leftarrow 0$，$v_1\leftarrow 1$.

由欧几里德除法：$r_0=q_2\cdot r_1+r_2$



$\deg r_0=\deg q_2+\deg r_1$，　$\deg(r_2)<\deg(r_1)$

$u_2\leftarrow u_0-q_2\cdot u_1$，　$v_2\leftarrow v_0-q_2\cdot v_1$

⋮

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

$u_{i+2}\leftarrow u_i-q_{i+2}\cdot u_{i+1}$，　$v_{i+2}\leftarrow v_i-q_{i+2}\cdot v_{i+1}$　　$u_i\cdot a+v_i\cdot b=r_i$，$i\geq 0$

⋮

$r_{k-1}=q_{k+1}\cdot r_k+0$　循环终止

输出 u_k、v_k

1.1 见讲义 命题5.11， $f_1,\cdots,f_n \in F[x]$, $\gcd(f_1,\cdots,f_n)=g$. 存在 $a_1,\cdots,a_n \in F[x]$ 使得

$$a_1f_1+\cdots+a_nf_n=g.$$ 如何计算 $a_1,\cdots,a_n$.

注意到 $g=\gcd(f_1,\gcd(f_2,\cdots,f_n))$, $\gcd(f_2,\cdots,f_n)=\bar{g}$

由EEA: $a,b\in F[x]$ s.t. $a\cdot f_1+b\cdot\bar{g}=g$.

递归地计算: $\bar{a}_2,\cdots,\bar{a}_n\in F[x]$ s.t. $\bar{a}_2f_2+\cdots+\bar{a}_nf_n=\bar{g}$ 作为 $n-1$ 个元素的计算问题.

$$\Rightarrow\quad a\cdot f_1+b\cdot\bar{a}_2\cdot f_2+\cdots+b\bar{a}_n\cdot f_n=g.$$

a_1 a_2 a_n

1.2 解的存在性✓. 如何计算✓. 解的结构？

解不唯一！ 注意到 若 $u_0,v_0\in F[x]$ 使得 $u_0a+v_0b=g$. 则 $(x_0-k\cdot\frac{b}{g},\ y_0+k\cdot\frac{a}{g})$

$|x_0|<|\frac{b}{g}|$, $|y_0|<|\frac{a}{g}|$

那么 $(u_0-q\cdot b/g)\cdot a+(v_0+q\cdot a/g)\cdot b=g$, $\forall q\in F[x]$.

若 $\deg(u_0)<\deg(b/g)$ 且 $\deg(v_0)<\deg(a/g)$. 则 (u_0,v_0) 是极小的且被唯一确定。

否则 $(u_0-\bar{u}_0)\cdot a+(v_0-\bar{v}_0)\cdot b=0$.

$$\Rightarrow \deg((u_0-\bar{u}_0)\cdot a)<\deg(a)+\deg(b)-\deg(g)=\deg(\mathrm{lcm}(a,b))\Longleftarrow\Longleftarrow$$

$(u_0-\bar{u}_0)\cdot a$ 是 a,b 的公倍式

已知 (u,v). $u_0=\mathrm{rem}(u,b/g,x)$. $u_0=u-q\cdot b/g$. $v_0=v+q\cdot b/g$.

注1：EEA 输出的是极小解：

$r_i = q_{i+2} \cdot r_{i+1} + r_{i+2}$，$\deg(q_{i+2}) = \deg(r_i) - \deg(r_{i+1})$

$u_{i+2} = u_i - q_{i+2} \cdot u_{i+1}$

$u_2 = u_0 - q_2 \cdot u_1 = 1$，$u_3 = u_1 - q_3 \cdot u_2 = 0 - q_3$，$u_4 = u_2 - q_4 \cdot u_3 = 1 + q_4 \cdot q_3$，…

$u_5 = u_3 - q_5 \cdot u_4 = -q_3 - q_5 - q_3 q_4 q_5$

……

$\deg u_k = \deg q_3 + \cdots + \deg q_k$　注意到 $\deg q_3 + \cdots + \deg q_{k+1} = \deg(b) - \deg(g)$

$k \geq 3$　　$q_{k+1} > 0$

$< \deg(b) - \deg(g)$　□.

若 $k=2$，则 $\deg(u_2) = 0$ 显然满足极小解的条件.

注2：EEA 同时可以输出 $\mathrm{lcm}(a,b)$：　$\mathrm{lcm}(a,b) = \frac{a \cdot b}{\gcd(a,b)}$

① $\deg u_{k+1} = \deg(b) - \deg(g) \Rightarrow \deg(u_{k+1} \cdot a) = \deg(\mathrm{lcm}(a,b))$

② $u_{k+1} \cdot a + v_{k+1} \cdot b = r_{k+1} = 0 \Rightarrow \mathrm{lcm}(a,b) \mid u_{k+1} \cdot a$

综合①②　$u_{k+1} \cdot a \sim v_{k+1} \cdot b \sim \mathrm{lcm}(a,b)$

计算：　例：$f(x)=2x^3-3x+4$，$g(x)=x^2-2x+3$.

r_0　$u_0=1, v_0=0$　　r_1　$u_1=0$, $v_1=1$

$$\begin{array}{r|l} x^2-2x+3 & 2x^3-3x+4 \\ & 2x^3-4x^2+6x \\ \hline & 4x^2-9x+4 \\ & 4x^2-8x+12 \\ \hline & r_2=-x-8 \end{array} \qquad q_2=2x+4$$

$u_2=u_0-q_2u_1=1$，$v_2=v_0-q_2v_1=-2x-4$

$$\begin{array}{r|l} -x-8 & x^2-2x+3 \\ & x^2+8x \\ \hline & -10x+3 \\ & -10x-80 \\ \hline & r_3=83 \end{array} \qquad q_3=-x+10$$

$u_3=u_1-q_3u_2=x-10$

$v_3=v_1-q_3v_2=1+(x-10)(-2x-4)$

$=-2x^2+16x+41$

$\Rightarrow \frac{x-10}{83}\cdot f+\frac{-2x^2+16x+41}{83}\cdot g=1.$

$-x-8=(-\frac{1}{83}x-\frac{8}{83})\cdot 83+0.$　　$u_4=u_2-q_4u_3=1+(\frac{1}{83}x+\frac{8}{83})(x-10)=\frac{1}{83}(x^2-2x+3).$

↓ q_4　　↓ r_4

$v_4=v_2-q_4v_3=(-2x-4)+(\frac{1}{83}x+\frac{8}{83})(-2x^2+16x+41)$

$=\frac{-1}{83}(2x^3-3x+4)$

1.3 Bézout's 关系式并不一定对多项式总成立

e.g. $\mathbb{Z}[x]$ ($a,b\in\mathbb{Z}[x]$, $\gcd(a,b)$总存在)　(UFD)

$\gcd(2x,x^2)=x$.　在$\mathbb{Q}[x]$中，$\frac{1}{2}\cdot 2x+0\cdot x^2=x$

不存在 $u,v\in\mathbb{Z}[x]$ 使得 $u\cdot(2x)+v\cdot x^2=x$.

e.g. $F[x,y]$. $\gcd(x,y)=1$. 但是不存在 $u,v\in F[x,y]$ st. $ux+vy=1$.

如果存在，取值 $x=0$, $y=0$ 等式左边为0 →←.

2. 核核分解和应用

$A: F^n \to F^n$ 线性变换. 维数公式: $\dim\ker(A) + \dim\mathrm{Im}(A) = n$

定理: $A \in \mathrm{Hom}(F^n, F^n)$ 若 $A^2 = A$, 则 $\ker(A) \oplus \mathrm{Im}(A) = F^n$. 核像分解.

证明: $\ker(A) \oplus \ker(A-E) = F^n$

$\forall\ v \in F^n$; $(A-E)(Av) = A^2 v - Ev = 0 \Rightarrow \mathrm{Im}(A) \subseteq \ker(A-E)$

$\forall v \in \ker(A-E)$, $Av = v \Rightarrow v \in \mathrm{Im}(A) \Rightarrow \ker(A-E) \subseteq \mathrm{Im}(A)$

综上: $\mathrm{Im}(A) = \ker(A-E)$

投影变换 A 在适当的基下有坐标表示:

$$A: (x_1, \cdots, x_n) \mapsto (x_1, \cdots, x_r, 0, \cdots, 0)$$

$r = \dim \mathrm{Im}A$

反之不成立 e.g. $A: \mathbb{Q}^3 \to \mathbb{Q}^3$ $\quad A = \begin{pmatrix} 0 & & \\ & 2 & \\ & & 2 \end{pmatrix}$

3. 多项式的形式求导以及重因子的判定.

$f(x) \in F[x]$ $\quad f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$f(x)$ 的导数: $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1$

$f(x)$ 的 k 阶导数: $f^{(k)}(x) = (f^{(k-1)}(x))'$

性质: (1) $(af(x) + bg(x))' = af'(x) + bg'(x)$

(2) $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$

(3) $(f^m(x))' = m f^{m-1}(x) \cdot f'(x)$.

设 $f(x) = c \cdot P_1^{m_1} \cdots P_k^{m_k}$ 是 $f(x)$ 在 $F[x]$ 中的不可约分解. $c \in F$, P_i 不可约, $P_i \nsim P_j$

若 $m_i > 1$, 则称 P_i 为 $f(x)$ 的重因式.

定理: $\mathrm{char}(F) = 0$, $f(x) \in F[x]$ 有重因式 $\Leftrightarrow \gcd(f(x), f'(x)) \neq 1$.

$$f'(x) = c \cdot m_1 P_1^{m_1 - 1} \cdot P_1' \cdots P_k^{m_k} + \cdots + c \cdot m_k P_1^{m_1} \cdots P_k^{m_k - 1} \cdot P_k'$$

$\gcd(P_i, P_i') = 1$

$\gcd(f(x), f'(x)) = P_1^{m_1 - 1} \cdots P_k^{m_k - 1}$

$\exists i$ s.t. $m_i > 1 \Leftrightarrow \gcd(f(x), f'(x)) \neq 1$.

注: $\mathrm{char}(F) = p$ 结论不成立