Recall：（核核分解）

若 $A\in M_n(F)$　$f\in F[t]$　$f(A)=0$．$f=pq$．

若 $\gcd(p,q)=1$．则

$$\ker(p(A))\oplus\ker(q(A))=F^n.$$

特别地有　$rk(p(A))+rk(q(A))=n$.

HW-1：$A^2=A$　令 $f=x^2-x$　$f=(x-1)\cdot x$

$\gcd(x-1,x)=1\Rightarrow$

$rk(A-E)+rk(A)=n$.

HW-2：

M-1.　"$\gcd(p,q)=1 \Leftrightarrow \exists\, u,v\in F[x].\ up+qv=1.$"

$\gcd(f,h)=\gcd(g,h)=1$

$\Rightarrow \exists\ u_1,v_1,\ u_2,v_2$ s.t.

$u_1f+v_1h=1=u_2f+v_2h$.

$\Rightarrow (u_1f+v_1h)\cdot(u_2f+v_2h)=1$

$=f(u_1u_2f+u_1v_2h)+h(v_1u_2f+v_1v_2h)=1$.

M-2.　$F[x]$，UFD　设 f,g,h 的因子只有 $p_1,\cdots,p_s$

设 $f=u_1p_1^{m_1}\cdots p_s^{m_s}$　$g=u_2q_1^{n_1}\cdots q_t^{n_t}$

$h=u_3\cdot r_1^{d_1}\cdots r_w^{d_w}$

$\gcd(f,h)=1\Rightarrow f,h$ 无公因子，$\gcd(g,h)=1\Rightarrow g,h$ 无公因子.

$\{p_1, \cdots, p_s, q_1, \cdots, q_t\}$ 与 $\{r_1, \cdots, r_w\}$ 不相伴.

$\Rightarrow \gcd(f \cdot g, h) = 1$.

注：若 $a \mid fg \not\Rightarrow a \mid f$ or $a \nmid g$. eg $15 \mid 3 \cdot 5$
$15 \nmid 3$, $15 \nmid g$

可约性判断：

① Eisenstein 判别法、

R UFD, $f = a_n x^n + \cdots + a_0 \in D[x]$

若 $\exists\, p \in D$ 不可约. s.t. $p \mid a_0, \cdots, a_{n-1}$, $p \nmid a_n$
且 $p^2 \nmid a_0$, 则 f 在 $D[x]$ 中不可约

HW3: $f(x) = 3x^2 + 15x + 10 \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$.

$5 \in \mathbb{Z}$ 不可约元.

$5 \mid 10, 15$, $5 \nmid 3$. $5^2 \nmid 10$.

$\square$

注意：p 必须为素元(数).

② 整根测试.

若 R UFD, $f \in R[x] \subset F[x]$, $F = \mathrm{Frac}(R)$.

$x = \frac{p}{q}$ 为 f 的根 $\gcd(p, q) = 1$, $p, q \in R$.

若 $f = a_n x^n + \cdots + a_0$, 则 $q \mid a_n$, $p \mid a_0$.

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

i.e. $a_n \cdot p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n = 0$.

$\Rightarrow p \mid a_0 q^n$, $q \mid a_n p^n$ $\gcd(p, q) = 1$

$\Rightarrow p \mid a_0$, $q \mid a_n$.

$\square$.

Cor：若 $f\in F[x]$, $\deg f=2$ or 3, f 可约 $\Leftrightarrow f$ 有根.

HW4：(i) ✓.

(ii) x^2+4 在 $\mathbb{Q}$上无根. $\Rightarrow x^2+4$ 不可约

x^3+4 在 $\mathbb{Q}$上无根. $\Rightarrow x^3+4$ 不可约

$f(x)=x^4+4$ 在 $\mathbb{Q}$上无根.

若 f 可约，则 f 只有 2次因子.

i.e. $f=p\cdot q$ $\deg p=\deg q=2$.

$f=(x^2+ax+b)\cdot(x^2+cx+d)$

$\Rightarrow f=(x^2-2x+2)(x^2+2x+2)$. □

③约化判别法

$f\in\mathbb{Z}[x]$ 若 $\deg f=\deg\bar{f}$, $\mathrm{cont}(f)=1$, $\bar{f}\in\mathbb{Z}_p[x]$, 由 f 所得.

则 $\bar{f}\in\mathbb{Z}_p[x]$ 不可约 $\Rightarrow f\in\mathbb{Z}[x]$ 不可约.

Pf：若 $f=gh$, $\deg g>0$, $\deg h>0$.

$\Rightarrow \bar{f}=\bar{g}\cdot\bar{h}$ $\Rightarrow \deg\bar{g}>0, \deg\bar{h}>0$ $\Rightarrow \bar{f}$ 可约 矛. □

HW-5 (i) $f(x)=x^p-x-1$, 由于 $\bar{f}=x^p-x-1$ 在 $\mathbb{Z}_p[x]$ 中不可约.

$\Rightarrow f(x)$ 在 $\mathbb{Z}_p$中不可约.

$\bar{g}(x)=\bar{f}$ 在 $\mathbb{Z}_p$中不可约 $\Rightarrow g(x)$ 不可约.

注：$f=2(x^2+1)$ 在 $\mathbb{Z}[x]$ 中可约，但在 $\mathbb{Q}[x]$ 中不可约.

i.e. f 在 $\mathbb{Z}[x]$ 与 $\mathbb{Q}[x]$ 的可约性不等价，若 f 为本原多项式，则这是等价的.

(ii) 设 $f \in \mathbb{Z}_p[x]$ 若 f 可约，则

$f = g_1 \cdot \cdots \cdot g_s$ g_i 为 f 的因子. $\deg f = p$.

若 $\exists g_i$ s.t. $\deg g_i = 1 \Rightarrow f$ 在 $\mathbb{Z}_p$ 中有根

但 $f(\bar{a}) = 0$ $\forall a \in \mathbb{Z}_p$.

$\Rightarrow \deg g_i \geq 2$.

$\Rightarrow 1 < s < p$.

$$
\begin{aligned}
f(x) &= g_1(x) \cdot \cdots \cdot g_s(x) \\
&\parallel \\
f(x+\bar{1}) &= g_1(x+1) \cdot \cdots \cdot g_s(x+1) \\
&\parallel \\
&\vdots \\
&\parallel \\
f(x+\overline{p-1}) &= g_1(x+\overline{p-1}) \cdot \cdots g_s(x+\overline{p-1})
\end{aligned}
$$

$\Rightarrow g_1(x) = g_{n_1}(x+\bar{1}) = g_{n_2}(x+\bar{2}) = \cdots = g_{n_{p-1}}(x+\overline{p-1})$

$\{1, n_1, \cdots, n_{p-1}\} \subset \{1, \cdots, s\}$

$\Rightarrow \exists$ $i \neq j$ s.t. $n_i = n_j$.

i.e. $g_{n_i}(x+\bar{i}) = g_{n_j}(x+\bar{j})$

WLOG $n_i = n_j = 1$ $g_1(x+\bar{i}) = g_1(x+\bar{j})$ $\bar{i} \neq \bar{j} \in \mathbb{Z}_p$.

若 $g_1 = x^m + \alpha_1 x^{m-1} + \cdots$

$g_1(x+\bar{i}) = x^m + (C_m^1 \cdot \bar{i} + \alpha_1) x^{m-1} + \cdots$

$\parallel$

$g_1(x+\bar{j}) = x^m + (C_m^1 \cdot \bar{j} + \alpha_1) \cdot x^{m-1}$

$$\Rightarrow C_m'\cdot\bar{i}+\alpha_1 = C_m'\cdot\bar{j} = \alpha_1$$

$$\Rightarrow C_m'\cdot\bar{i} = C_m'\cdot\bar{j} \Rightarrow \bar{i}=\bar{j} \text{ 矛 } \square.$$

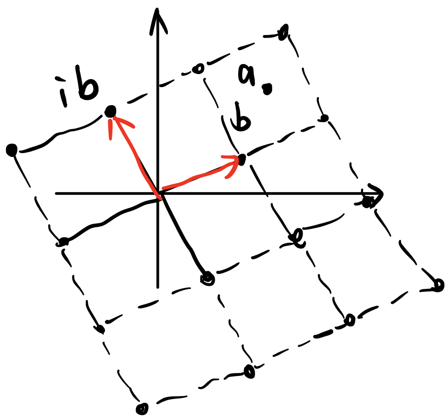
注：$f\in\mathbb{Z}[X]$，f作为函数为常值 $\not\Rightarrow f=c$.

HW-6（选做）

R, $d: R\setminus\{0\}\longrightarrow\mathbb{N}$，$\forall\, a,b\in R$，$b\neq 0$.

$a=qb+r$，$\exists\, q,r$ s.t. $d(r)<d(b)$ or $r=0$.

(i) $\forall b=m_0+n_0 i\in\mathbb{Z}[i]$



$ib=-n_0+m_0 i$

则 $ib\perp b$，$|ib|=b$.

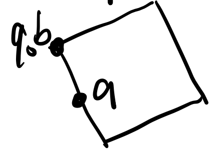
$\forall q\in\mathbb{Z}[i]$ $q=q_0+q_1 i$

$q\cdot b=q_0 b+q_1\cdot(ib)$

i.e. $\{q\cdot b \mid q\in\mathbb{Z}[i]\}$ 为复平面上的一些方格顶点.

$a\in\mathbb{Z}[i]$，则 a 必在某个方格顶点或边上或内部.

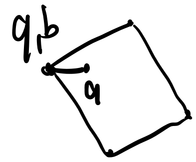
- 若 a 在顶点上，$a=qb$
- 若 a 在边上，



$a=q_0 b+r$

$d(r)=|q_0 b-a|^2 < d(b)$

- 在内部



,

若 a 距 $q_1 b$ 最近，则 $a = q_1 b + r$,
$d(r) < d(b)$.

(ii) $\mathbb{Z}$, $d: \mathbb{Z}\setminus\{0\} \longrightarrow \mathbb{N}$
$n \longmapsto |n|$.

$F[X]$, $d: F[X]\setminus\{0\} \longrightarrow \mathbb{N}$.
$f \longmapsto \deg(f)$.

$\mathbb{Z}[w] = \{ a+bw \mid a,b\in\mathbb{Z} \}$ $\quad w = e^{\frac{2\pi i}{3}}$.

$d: a+bw \longmapsto a^2-ab+b^2$

DVR : Discrete valuation ring.

(iii) 我们证明 ED $\Longrightarrow$ PID. (参考上次习题课讲义)

需要证明：$\forall\, I \subset R$ 为理想，$I = (a) = \{ r_0 \cdot a \mid r_0 \in R\}$
for some $a \in R$.

若 $I \neq \{0\}$，则 $\exists\, a \in I$ s.t. $d(a) = \min\{ d(r) \mid r\in R\}$.

$\forall\ b\in I$，则 $\exists\, q, r$ s.t. $b = q\cdot a + r$
$d(r) < d(a)$ or $r = 0$.

若 $r \neq 0$，则 $d(r) < d(a)$，与 $d(a)$ 最小矛盾.
$\Rightarrow r = 0$

i.e. $\forall\, b \in I$ $\ b = q\cdot a \in (a) \Rightarrow I \subset (a)$

注意到 $a\in I \Rightarrow (a) \subset I$. $\Rightarrow I = (a)$ $\quad\square$