第十五次作业

1. R环，$\forall x\in R$，$x^2=x$．证明：R是交换环．

Pf：$\forall x\in R$．$(x+x)^2=x+x=2x$．又 $(x+x)^2=4x^2=4x \Rightarrow 2x=0 \Rightarrow x=-x$

$\forall x,y\in R$．$(x+y)^2=x+y=x^2+xy+yx+y^2=x+y+xy+yx \Rightarrow xy=-yx=yx$

$\therefore R$是交换环．

P_{142}．5．证明任意有限整环R是一个域．

Pf：方法一：只需证 $\forall a\in R\setminus\{0\}$．$\exists b\in R\setminus\{0\}$ s.t. $ab=ba=1$（交换律自然满足）

若 $a=1$，则 $b=1$是a的逆．

若 $a\neq 1$，则由环的乘法封闭性可知 $a,a^2,\dots,a^n,\dots\in R$

$\because card(R)<\infty$ $\therefore \exists i,j\in\mathbb{Z}^+$，$i\neq j$ s.t. $a^i=a^j$，不妨设$i<j$

则 $a^i(1-a^{j-i})=0$ $\because R$是整环，有消去律且 $a\neq 0 \Rightarrow a^{j-i}=1$．

若 $j-i=1$，则 $a=1$，与$a\neq1$矛盾．$\therefore j-i>1$．则 $a^{j-i-1}\cdot a=1$．

令 $b=a^{j-i-1}$，即满足 $ab=ba=1$．

方法二：设 $R=\{r_1,\dots,r_n\}$．

$\forall r_i\in R\setminus\{0\}$．$r_i\cdot r_j\neq r_i\cdot r_k$，$j\neq k$ $\therefore \{r_ir_1,\dots,r_ir_n\}$有$n$个元素且包含于$R$

$\therefore R=\{r_ir_1,\dots,r_ir_n\} \Rightarrow \exists j\in\{1,\dots,n\}$ s.t. $r_ir_j=1$．

6．R交换环，p素数，$\forall x\in R$，$px=0$．证明 $(x+y)^{p^m}=x^{p^m}+y^{p^m}$，$m=1,2,\dots$

Pf：归纳法．$m=1$，$(x+y)^p=x^p+y^p+\sum_{i=1}^{p-1}\binom{p}{i}x^iy^{p-i}$（有交换律）

$\because p\mid\binom{p}{i}$ $\forall i=1,\dots,p-1$．$\therefore (x+y)^p=x^p+y^p$．

[或直接用 Freshman's dream，事实上，$\mathrm{char}R=p$：$\because p\cdot1=0$ $\therefore \underset{\text{加法阶}}{ord(1)}\mid p$

$\because p$是素数 $\therefore ord(1)=1$ or p．若 $ord(1)=1$，则 $1=0$ 矛盾（环中$1\neq0$）$\therefore ord(1)=p$

i.e. $\mathrm{char}R=p$]

假设 $m-1$ 时等式成立，则

$$(x+y)^{p^m} = \left((x+y)^{p^{m-1}}\right)^p = \left(x^{p^{m-1}}+y^{p^{m-1}}\right)^p = \left(x^{p^{m-1}}\right)^p + \left(y^{p^{m-1}}\right)^p = x^{p^m}+y^{p^m}$$

8. 环 R 的非零元 x 称为幂零的，若 $\exists\, n\in\mathbb{N}$ s.t. $x^n=0$. 证明：

(1) 若 x 是幂零元，则 $1-x$ 是可逆元

(2) 环 $\mathbb{Z}_m$ 中含有幂零元 $\Longleftrightarrow$ $\exists\, s\in\mathbb{Z},\ s>1$ s.t. $s^2\mid m$

Pf: (1) $x\neq 0$. $\exists\, n\in\mathbb{N}$ s.t. $x^n=0$. $n>1$

$1=1-x^n=(1-x)(1+x+\cdots+x^{n-1})=(1+x+\cdots+x^{n-1})(1-x)$

$\therefore\ 1-x$ 可逆.

(2) $\Leftarrow$ 设 $m=s^2t$, $m>1$, $t\in\mathbb{Z}^+$ $\because st<m$ $\therefore \overline{st}\neq\overline{0}$ 且

$(\overline{st})^2=\overline{s}^2\overline{t}^2=\overline{m}\cdot\overline{t}=\overline{0}$ $\therefore\ \overline{st}$ 是 $\mathbb{Z}_m$ 中幂零元.

$\Rightarrow$ 设 $\overline{x}\in\mathbb{Z}_m$ 是幂零元 且 $\overline{x}^n=\overline{0}$. $n\in\mathbb{N}$. 即 $m\nmid x$, $m\mid x^n$.

下证 m 可被一个大于1的整数平方整除.

(反证) 假设上述结论不成立，考虑 m 的素分解 $m=p_1p_2\cdots p_s$. p_i 是互不相同的素数

$\because m\mid x^n$. $\therefore \forall i,\ p_i\mid x^n$. $\because p_i$ 是素数 $\therefore p_i\mid x$ $\Rightarrow p_1p_2\cdots p_s\mid x$ i.e. $m\mid x$ 矛盾.

10. R 环. $a,b\in R$. 证：

$(1-ab)c=c(1-ab)=1 \Rightarrow (1-ba)d=d(1-ba)=1$. $d=1+bca$.

i.e. $1-ab$ 可逆 $\Rightarrow$ $1-ba$ 可逆. 元素 $1+adb=?$

Pf: $(1-ab)c=1 \Rightarrow c-abc=1$. ①

$c(1-ab)=1 \Rightarrow c-cab=1$ ②

$(1-ba)d=(1-ba)(1+bca)=1-ba+bca-b(abc)a$ 由①

$=1-ba+bca-b(c-1)a=1$.

$d(1-ba)=(1+bca)(1-ba)=1-ba+bca-b(cab)a$ 由②

$=1-ba+bca-b(c-1)a=1$

$1+adb=1+a(1+bca)b=1+ab+(abc)ab \overset{①}{=} 1+ab+(c-1)ab=1+cab \overset{②}{=} c$

3. 设 $A=\begin{pmatrix}\bar{1} & \bar{2}\\ \bar{3} & \bar{4}\end{pmatrix}\in M_2(\mathbb{Z}_5)$. 求 $A+A^t$, AA^t, $\det(A)$, A^{-1}.

解: $A^t=\begin{pmatrix}\bar{1} & \bar{3}\\ \bar{2} & \bar{4}\end{pmatrix}$.

$$A+A^t=\begin{pmatrix}\bar{1} & \bar{2}\\ \bar{3} & \bar{4}\end{pmatrix}+\begin{pmatrix}\bar{1} & \bar{3}\\ \bar{2} & \bar{4}\end{pmatrix}=\begin{pmatrix}\bar{2} & \bar{0}\\ \bar{0} & \bar{3}\end{pmatrix}$$

$$AA^t=\begin{pmatrix}\bar{1} & \bar{2}\\ \bar{3} & \bar{4}\end{pmatrix}\begin{pmatrix}\bar{1} & \bar{3}\\ \bar{2} & \bar{4}\end{pmatrix}=\begin{pmatrix}\bar{0} & \bar{1}\\ \bar{1} & \bar{0}\end{pmatrix}$$

$$\begin{vmatrix}\bar{1} & \bar{2}\\ \bar{3} & \bar{4}\end{vmatrix}=\bar{4}-\bar{1}=\bar{3}\neq 0 \quad \therefore A \text{ 可逆}.$$

求 A^{-1} 可用以下两种方法:

① $$\begin{pmatrix}\bar{1} & \bar{2} & \bar{1} & \bar{0}\\ \bar{3} & \bar{4} & \bar{0} & \bar{1}\end{pmatrix}\xrightarrow[-\bar{3}=\bar{2}]{r_1\cdot(-\bar{3})+r_2}\begin{pmatrix}\bar{1} & \bar{2} & \bar{1} & \bar{0}\\ \bar{0} & \bar{3} & \bar{2} & \bar{1}\end{pmatrix}\xrightarrow[\bar{3}^{-1}=\bar{2}]{r_2\cdot\bar{3}^{-1}}\begin{pmatrix}\bar{1} & \bar{2} & \bar{1} & \bar{0}\\ \bar{0} & \bar{1} & \bar{4} & \bar{2}\end{pmatrix}$$

$$\xrightarrow[-\bar{2}=\bar{3}]{r_2\cdot(-\bar{2})+r_1}\begin{pmatrix}\bar{1} & \bar{0} & \bar{3} & \bar{1}\\ \bar{0} & \bar{1} & \bar{4} & \bar{2}\end{pmatrix}$$

$$\therefore A^{-1}=\begin{pmatrix}\bar{3} & \bar{1}\\ \bar{4} & \bar{2}\end{pmatrix}$$

② $$AA^{\vee}=|A|E \Rightarrow A^{-1}=\frac{A^{\vee}}{|A|}=\bar{3}^{-1}\begin{pmatrix}\bar{4} & -\bar{2}\\ -\bar{3} & \bar{1}\end{pmatrix}=\bar{2}\begin{pmatrix}\bar{4} & \bar{3}\\ \bar{2} & \bar{1}\end{pmatrix}=\begin{pmatrix}\bar{3} & \bar{1}\\ \bar{4} & \bar{2}\end{pmatrix}$$

赵若旻 54　　　　第十六次作业

1. $fg=(\bar{2}x^2+x+\bar{4})(\bar{3}x^3+\bar{5}x)=\bar{6}x^5+\bar{10}x^3+\bar{3}x^4+\bar{5}x^2+\bar{12}x^3+\bar{20}x$

$=\bar{6}x^5+\bar{3}x^4+\bar{22}x^3+\bar{5}x^2+\bar{20}x$

$=\bar{3}x^4+\bar{4}x^3+\bar{5}x^2+\bar{2}x$

$\therefore \deg(fg)=4 < \deg(f)+\deg(g)$　　$(\because \bar{2}\cdot\bar{3}=\bar{0})$

$gh=(\bar{3}x^3+\bar{5}x)(x+\bar{3})=\bar{3}x^4+\bar{9}x^3+\bar{5}x^2+\bar{15}x=\bar{3}x^4+\bar{3}x^3+\bar{5}x^2+\bar{3}x$

$\therefore \deg(gh)=4 = \deg(g)+\deg(h)$

2. (1) $f(2)=2^2+2-2=4$ ~~(2) $f(\bar{a})=\bar{a}^2$~~　　注：将值代入 x^2+x-2 或 $(x-1)(x+2)$ 都可以

(2) $f(\bar{a})=(\bar{a})^2+\bar{a}-\bar{2}$　　$\because \bar{a}\in\mathbb{Z}_3$

$\therefore$ 当 $\bar{a}=\bar{0}$ 时：$f(\bar{a})=-\bar{2}=\bar{1}$

当 $\bar{a}=\bar{1}$ 时：$f(\bar{a})=\bar{0}$

当 $\bar{a}=\bar{2}$ 时：$f(\bar{a})=\bar{1}$

(3) $f(A)=(A-E)(A+2E)=\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}3&1&0\\0&3&1\\0&0&3\end{pmatrix}=\begin{pmatrix}0&3&1\\0&0&3\\0&0&0\end{pmatrix}$

3. $f=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in F[x]$　$a_n\neq 0$

$\therefore \deg(f(x))=n$

$f(ax+b)=a_n(ax+b)^n+a_{n-1}(ax+b)^{n-1}+\cdots+a_0=a_na^nx^n+$低次项

$\because a_n\neq 0.\ a\neq 0$

$\therefore a_na^n\neq 0$

$\therefore \deg(f(ax+b))=n=\deg(f(x))$ 且 $lc(f(ax+b))=a_na^n$.

4. P161. 1. 第一种：

$$\begin{array}{r}
x^3+2x^2-2x+4 \\
x^2+x+1\,\big)\,\overline{x^5+3x^4+x^3+4x^2-3x-1} \\
\underline{x^5+x^4+x^3} \\
2x^4+4x^2-3x-1 \\
\underline{2x^4+2x^3+2x^2} \\
-2x^3+2x^2-3x-1 \\
\underline{-2x^3-2x^2-2x} \\
4x^2-x-1 \\
\underline{4x^2+4x+4} \\
-5x-5
\end{array}$$

$\therefore g(x)\nmid f(x)$

第二种：

$f(x)=(x^3+\bar{2}x^2-\bar{2}x+\bar{4})g(x)-\bar{5}x-\bar{5}$

$=(x^3+\bar{2}x^2-\bar{2}x+\bar{4})g(x)$.

$\therefore g(x)\mid f(x)$

反过来 在 $\mathbb{Z}_5[x]$ 中 $g\nmid f$. 但在 $\mathbb{Z}[x]$ 中 $g\mid f$ 不可能.

设环同态 φ：$\mathbb{Z}[x]\longrightarrow\mathbb{Z}_5[x]$

$\sum_{i=0}^{n}a_ix^i\longrightarrow\sum_{i=0}^{n}\bar{a_i}x^i$

若 $g\mid f$. 不妨设 $f=gh$ $\therefore \varphi(f)=\varphi(gh)=\varphi(g)\cdot\varphi(h)\Rightarrow\varphi(g)\mid\varphi(f)\rightarrow\leftarrow$

$\therefore$ 不可能

5.(1) 证明：由赋值定理可知 $\exists!$ 环同态 $\phi_{ab}: F[x] \longrightarrow F[x]$. 满足 $\phi_{ab}|_F = id_F$. $\phi_{ab}(x) = ax+b$.

证环同态：法一 有单同态 $\phi: F \longrightarrow F[x]$, $a \longmapsto a$. 由赋值定理，$\exists!$ 环同态 $\phi_{a,b}: F[x] \longrightarrow F[x]$ s.t. $\phi_{a,b}|_F = \phi = id_F$, $\phi_{a,b}(x) = ax+b$

$\therefore \phi_{ab}$ 是环同态.

下证 ϕ_{ab} 是双射.

设 $f = \sum_{i=0}^{n} f_i x^i$ 若 $\phi_{ab}(f) = 0$. 则 $\sum_{i=0}^{n} \phi_{ab}(f_i)\phi_{ab}(x)^i = \sum_{i=0}^{n} f_i(ax+b)^i = 0$

法二：用环同态定义证.
$\forall f, g \in F[x]$, 验证 $\phi_{a,b}(f+g) = \phi_{a,b}(f) + \phi_{a,b}(g)$
$\phi_{a,b}(fg) = \phi_{a,b}(f)\phi_{a,b}(g)$
$\phi_{a,b}(1) = 1$

$\therefore \phi_{ab}(f)$ 的首项系数 $f_n a^n = 0$

$\because a \neq 0$

$\therefore a^n \neq 0 \quad \therefore f_n = 0$

$\therefore f$ 的首项系数为 0 $\therefore f = 0$ $\therefore \phi_{ab}$ 是单的环同态.

对 $\forall g \in F[x]$. 设 $g = \sum_{i=0}^{n} g_i x^i$

令 $g' = \sum_{i=0}^{n} g_i(a^{-1}x - a^{-1}b)^i$ 则 $g' \in F[x]$. 且 $\phi_{ab}(g') = \sum_{i=0}^{n} g_i x^i = g$

$\therefore \phi_{ab}$ 是满射 $\quad \therefore \phi_{ab}$ 是环同构 $\square$.

(2). $\because \sigma: F[x] \longrightarrow F[x]$ 是环同构. 且 $\sigma|_F = id_F$.

法一：不妨设 $\sigma(x) = \sum_{i=0}^{n} a_i x^i$ ~~$(n \geq 1)$~~ 为 n 次多项式

当 $n \geq 2$ 时：对于 $\forall f = f_1 x + f_0 \in F[x]$. 不存在 $f' \in F[x]$. s.t $\sigma(f') = f$

这与 σ 是 $F[x] \longrightarrow F[x]$ 的环同构矛盾.

当 $n=1$ 时：$\sigma(x) = ax+b$ $(a \neq 0)$ 则由(1)可知. $\sigma = \phi_{ab}$. 满足题意

当 $n=0$ 时：$\sigma(x) = k$. 常数.

$\therefore$ 对 $\forall f \in F[x]$, $\sigma(f)$ 为常数 与 σ 是满射矛盾.

综上，只有当 $n=1$ 时 满足题意. 即 $\exists\, a, b \in F$ 且 $a \neq 0$. s.t $\sigma = \phi_{ab}$ $\square$.

法二：令 $f(x) = \sigma(x) \in F[x]$，则 $f(x) \notin F$，否则 σ 不是满射，从而 $\deg f(x) \geq 1$.

设 σ^{-1} 是 σ 的逆映射，且 $g(x) = \sigma^{-1}(x)$. 同理 $\deg g(x) \geq 1$.

设令 $\sigma(x) = f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$，$a_n \neq 0$, $n \geq 1$.

$\sigma^{-1}(x) = g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$，$b_m \neq 0$, $m \geq 1$

$\Rightarrow x = \sigma^{-1}(\sigma(x)) = \sigma^{-1}(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = a_n(\sigma^{-1}(x))^n + a_{n-1}(\sigma^{-1}(x))^{n-1} + \cdots + a_0$

$= \underbrace{a_n(b_m x^m + \cdots + b_0)^n + \cdots + a_0}_{\deg = mn}$

$\therefore mn = 1 \Rightarrow m = n = 1 \Rightarrow f(x) = ax+b$, $a \neq 0$

Note：证：$\phi_{a,b}: F[x] \longrightarrow F[x]$，$a,b\in F$，$a\neq 0$ 是环同态有以下两种方法：

$p(x) \longrightarrow p(ax+b)$.

法一：用赋值定理.

首先：$\phi: F \longrightarrow F[x]$ 是单同态 or 嵌入.

$a \longmapsto a$

由赋值定理，$\exists!$ 环同态 $\phi_{a,b}: F[x] \longrightarrow F[x]$ s.t. $\phi_{a,b}|_F = \phi$

$x \longmapsto ax+b$　　$\phi_{a,b}(x) = ax+b$.

法二：用环同态定义证

$\forall p, q \in F[x]$，设 $p(x) = \sum_{i=0}^{n} p_i x^i$，$q(x) = \sum_{j=0}^{m} q_j x^j$，不妨设 $m \leq n$.

$$\phi_{a,b}(p+q) = \phi_{a,b}\left(\sum_{i=m+1}^{n} p_i x^i + \sum_{i=0}^{m} (p_i+q_i) x^i\right)$$

$$= \sum_{i=m+1}^{n} p_i (ax+b)^i + \sum_{i=0}^{m} (p_i+q_i)(ax+b)^i$$

$$= \sum_{i=0}^{n} p_i (ax+b)^i + \sum_{j=0}^{m} q_j (ax+b)^j = \phi_{a,b}(p) + \phi_{a,b}(q)$$

$$\phi_{a,b}(pq) = \phi_{a,b}\left(p \cdot \sum_{j=0}^{m} q_j x^j\right) = \sum_{j=0}^{m} \phi_{a,b}(p q_j x^j)$$

$$= \sum_{j=0}^{m} \phi_{a,b}\left(\sum_{i=0}^{n} p_i x^i \cdot q_j x^j\right) = \sum_{j=0}^{m} \sum_{i=0}^{n} \phi_{a,b}(p_i q_j x^{i+j})$$

$$= \sum_{j=0}^{m} \sum_{i=0}^{n} \cancel{\phi_{a}} p_i q_j (ax+b)^{i+j} = \phi_{a,b}(p)\, \phi_{a,b}(q)$$

$\phi_{a,b}(1) = 1$.

事实上，从一元多项式环到交换环的同态都是赋值同态.

Pf：设 $\varphi: R[x] \longrightarrow S$ 环同态，S交换环且 $\varphi(x)=s$.
$\quad\quad x \longmapsto s$

令 $\psi=\varphi|_R$. 则 $\psi: R \longrightarrow S$ 环同态. 由赋值定理，$\exists !$ 环同态

$\psi_s: R[x] \longrightarrow S$ s.t. $\psi_s(x)=s$，$\psi_s|_R=\psi$.
$\quad\quad x \longmapsto s$

注意到 $\psi_s(x)=\varphi(x)=s$，$\psi_s|_R=\varphi|_R=\psi$. 由赋值定理中同态的唯一性可得 $\varphi=\psi_s$. i.e. φ是赋值同态.

1. 一元多项式　（以下R表示交换环）

R交换环．$\tilde{R}=\{(r_0,r_1,\cdots,r_n,\cdots)\mid r_n\in R$，有限多个非0$\}$

令 $x=(0,1,0,0,\cdots)$．$\tilde{R}=\{\sum_{k=0}^{n} r_k x^k \mid n\in\mathbb{N}, r_k\in R\}:=R[x]$．交换环．

prop：① $p,q\in R[x]$，$\deg(p+q)\le\max(\deg(p),\deg(q))$．当 p,q 次数不同时，等号成立．

② $p,q\in R[x]$，$\deg(pq)\le\deg(p)+\deg(q)$．且 $lc(p)lc(q)\ne 0 \Leftrightarrow$ 等号成立．

Thm：D是整环，则 $D[x]$ 是整环．特别地，F是域时，$F[x]$ 是整环．

赋值定理：R，S交换环，$\varphi: R\to S$ 环同态，且 $s\in R$，则∃！环同态

$\varphi_s: R[x]\to S$ s.t. ① $\varphi_s|_R=\varphi$，$\varphi_s(x)=s$．

注：$\varphi_s(\sum_{k=0}^{n} r_k x^k)=\sum_{k=0}^{n}\varphi(r_k)s^k$

eg：① $\pi_{\bar{m}}: \mathbb{Z}[x]\to\mathbb{Z}_n$　是环同态

$f(x)\longmapsto f(\bar{m})$，$\bar{m}\in\mathbb{Z}_n$

② $\varphi_A: F[x]\to F[A]$　是环同态

$f(x)\longmapsto f(A)$，$A\in M_n(F)$

多项式的除法：

$f,g\in R[x]$，$g\ne 0$，$lc(g)$ 可逆，存在唯一 $q,r\in R[x]$ s.t.

$f=qg+r$，$\deg(r)<\deg(g)$

Thm：F域，$f,g\in F[x]$，$g\ne 0$，∃！$q,r\in F[x]$ s.t.

$f=qg+r$，$\deg(r)<\deg(g)$．

2. 整环中的gcd和lcm.

记号：D整环，$D^*=D\setminus\{0\}$. U_D是D中所有可逆元的集合（U_D关于乘法是交换群）
F域

整除：$a\in D^*$, $b\in D$. 若$\exists c\in D$ s.t. $b=ca$. 则称a是b的因子，b是a的倍式，
称a在D中整除b. 记为$a|b$

prop：$a,b\in D^*$, $c,f,g\in D$.
① $a|b$, $b|c\Rightarrow a|c$
② $a|f$, $a|g\Rightarrow\forall u,v\in D$. $a|(uf+vg)$

相伴：$a,b\in D$. 若$\underbrace{\exists\, u,v\in U_D \text{ s.t. } ua=vb}_{\Updownarrow}$. 则称$a$和$b$在$D$上相伴. 记为$a\approx b$.
"≈"是等价关系. ($\exists u\in U_D$ s.t. $a=ub$)

eg：$U_{\mathbb{Z}}=\{1,-1\}$. $a\approx b\Leftrightarrow a=\pm b$. $a,b\in\mathbb{Z}$.
$U_{F[x]}=F^*$ $f\approx g\Leftrightarrow\exists\, a\in F^*$ s.t. $f=ag$. $f,g\in F[x]^*$
$\Leftrightarrow f,g$的$\underbrace{\text{首一部分}}_{lc(f)^{-1}f,\ lc(g)^{-1}g}$相同.

gcd：$a,b_1,\cdots,b_n\in D^*$. 若$g|b_1,\cdots,g|b_n$（g是$b_1,\cdots,b_n$的公因子）
且对$b_1,\cdots,b_n$任意公因子a，有$a|g$. 则称g是$b_1,\cdots,b_n$
的一个最大公因子. 如果$b_1,\cdots b_n$最大公因子存在 记为$\gcd(b_1,\cdots,b_n)$

lcm：$c,d_1,\cdots,d_n\in D^*$. 若l是$d_1,\cdots,d_n$的公倍式 且对$d_1,\cdots,d_n$任意公倍式
c有$l|c$. 则称l是$d_1,\cdots,d_n$的一个最小公倍式.
如果$d_1,\cdots,d_n$最小公倍式存在 记为$\mathrm{lcm}(d_1,\cdots,d_n)$.

prop：$b_1,\cdots,b_n\in D^*$
① g是$b_1,\cdots,b_n$最大公因子. 则$h\in D^*$也是$b_1,\cdots,b_n$最大公因子$\Leftrightarrow h\approx g$.
② l是$b_1,\cdots,b_n$最小公倍式；则$h\in D^*$也是$b_1,\cdots,b_n$最小公倍式$\Leftrightarrow h\approx l$

注：gcd, lcm在相伴意义下是唯一的.

prop：$f_1,\cdots,f_n\in F[x]$ 不全为零，则 $f_1,\cdots,f_n$ 最大公因子存在，设 $g=\gcd(f_1,\cdots,f_n)$

则 $\exists\ a_1,\cdots,a_n\in F[x]$ s.t.

$$a_1f_1+\cdots+a_nf_n=g$$

Thm：$f,g\in F[x]$，f,g 互素 $\Leftrightarrow \exists\ u,v\in F[x]$ s.t. $uf+vg=1$.

求 gcd：辗转相除法.

核核分解：

设 $\mathcal{A}\in Hom(F^n,F^n)$，$f\in F[x]$ 且 $f(\mathcal{A})=0$，再设 $f=pq$，$p,q\in F[x]$ 且 $\gcd(p,q)=1$，则

$$\ker(p(\mathcal{A}))\oplus\ker(q(\mathcal{A}))=F^n$$

Cor：$A\in M_n(F)$，$f\in F[x]$，$f(A)=0$，再设 $f=pq$，$p,q\in F[x]$ 且 $\gcd(p,q)=1$，则

$$sol(p(A)\vec{x}=\vec{0})\oplus sol(q(A)\vec{x}=\vec{0})=F^n.$$

特别地：$rank(p(A))+rank(q(A))=n$.

注：$p(\mathcal{A}):F^n\longrightarrow F^n$

$$\vec{x}\longmapsto p(A)\vec{x}$$

3. 唯一因子分解整环 (UFD)

D 整环，$D^*=D\setminus\{0\}$，F 域.

素元：$a\in D^*$ 不可逆，若 $\forall\ b,c\in D^*$，$a|bc\Rightarrow a|b$ or $a|c$，称 a 是素元

不可约元：$a\in D^*$ 不可逆，若不 $\exists$ 非可逆元 $b,c\in D^*$ s.t. $a=bc$，称 a 是不可约元

(or，若 a 是不可约元，且 $a=bc$，则 b,c 中只有一个是可逆元，另一个与 a 相伴)

prop：① D 中素元都是不可约元.

② $\mathbb{Z}$，$F[x]$ 中 素元 = 不可约元

③ $a\in D^*$ 不可约元/素元 且 $\tilde{a}\simeq a$，则 $\tilde{a}$ 也是不可约元/素元

UFD：$\forall a\in D^*$ 不可逆满足

① $a=p_1\cdots p_m$，p_i 是 D 不可约元

② $a=p_1\cdots p_m=q_1\cdots q_n$，$p_i, q_j$ 是 D 不可约元，则 $m=n$ 且适当调整下标后有

$$p_1\approx q_1, \cdots, p_m\approx q_m.$$

prop：D 满足①，则 D 是 UFD $\Longleftrightarrow$ D 中不可约元是素元 (i.e. 不可约 = 素元)

注：UFD 中 不可约 = 素元

Thm：(算术基本定理)

设 $n\in\mathbb{Z}\setminus\{0,1,-1\}$，$\exists!$ 两两不同的素数 $p_1,\cdots,p_m$，正整数 $i_1,\cdots,i_m$ s.t.

$$n=\pm p_1^{i_1}p_2^{i_2}\cdots p_m^{i_m}$$

Thm：$f\in F[x]$，$\exists$ 两两互素的不可约多项式 $p_1,\cdots,p_m\in F[x]$，$i_1,\cdots,i_m\in\mathbb{Z}^+$，$u\in F^*$ s.t.

$$f=up_1^{i_1}p_2^{i_2}\cdots p_m^{i_m}$$

$p_1,\cdots,p_m$ 在相伴意义下唯一，$i_1,\cdots,i_m$ 唯一。

重数：D 是 UFD，$a\in D^*$，$p\in D^*$ 不可约元，如果 $m\in\mathbb{N}$ s.t. $p^m\mid a$ 但 $p^{m+1}\nmid a$，称 m 是 p 在 a 中的重数。

prop：D 是 UFD，$a\in D^*$，$p_1,\cdots,p_k\in D^*$ 是两两互不相伴的不可约元且在 a 中重数是 $m_1,\cdots,m_k$，则 $p_1^{m_1}\cdots p_k^{m_k}\mid a$.

prop：D 是 UFD，$a,b\in D^*$，则它们的最大公因子和最小公倍式都存在。

注：$a=up_1^{i_1}\cdots p_m^{i_m}$，$b=vp_1^{j_1}\cdots p_m^{j_m}$，$u,v\in U_D$，$p_i$ 不可约元，$i_1,\cdots,i_m,j_1,\cdots,j_m\in\mathbb{N}$

则 $\gcd(a,b)=p_1^{\min(i_1,j_1)}\cdots p_m^{\min(i_m,j_m)}$

$\operatorname{lcm}(a,b)=p_1^{\max(i_1,j_1)}\cdots p_m^{\max(i_m,j_m)}$