回忆：设F是一个域，$A\in M_n(F)$，$f\in F[t]$且$f(A)=0$。再设$f=pq$，其中$p,q\in F[t]$且$\gcd(p,q)=1$.
则
$$sol(p(A)x=0)\oplus sol(q(A)X=0)=F^n,$$
其中$X=(x_1,\dots,x_n)^t$是未知向量。特别地，（矩阵版）.
$$rank(p(A))+rank(q(A))=n.$$

1. Pf：法一：令$f(x)=x^2-1=x(x-1)$，$\gcd(x,x-1)=1$
$$\Rightarrow rank(A)+rank(A-E)=n$$

法二：回忆：$A\in F^{s\times n}$，$B\in F^{s\times n}$，$rank(A+B)\le rank(A)+rank(B)$.（上学期第二章第4次课讲义 例6.13）

（矩阵的秩的不等式）$A\in F^{m\times s}$，$B\in F^{s\times n}$，$rank(AB)\ge rank(A)+rank(B)-s$（上学期第三章第1次课讲义 例10.9）.

$$\Rightarrow rank(A)+rank(A-E)=rank(A)+rank(E-A)\ge rank(A+E-A)=rank(E)=n$$
$$rank(A)+rank(A-E)\le rank(A(A-E))+n=n.$$
$$\Rightarrow rank(A)+rank(A-E)=n.$$

（映射版）设$\phi\in Hom(F^n,F^n)$，$f\in F[t]$且$f(\phi)=\mathcal{O}$，其中$\mathcal{O}$代表从F^n到F^n的零映射，再设$f=pq$，其中$p,q\in F[t]$且$\gcd(p,q)=1$，则
$$ker(p(\phi))\oplus ker(q(\phi))=F^n.$$

例 设ϕ是线性空间F^n上的幂等变换（即$\phi^2=\phi$），从而$F^n=ker(\phi)\oplus ker(\phi-\varepsilon)$ 恒等变换.

2. 证明：法一，$\gcd(f,h)=1\Leftrightarrow\exists u_1,v_1\in F[x]$，s.t $u_1f+v_1h=1$ ①

$\gcd(g,h)=1\Leftrightarrow\exists u_2,v_2\in F[x]$，s.t $u_2g+v_2h=1$ ②

①·②得，$u_1u_2fg+(u_1v_2f+u_2v_1g+v_1v_2h)h=1$.

$\Rightarrow\gcd(fg,h)=1$.

法二：假设$\gcd(fg,h)\ne1$，则存在次数为正的不可约多项式a，使得$a|fg$，$a|h$.

$a|fg\Rightarrow a|f$或者$a|g$，这与$\gcd(f,h)=1=\gcd(g,h)$相矛盾.

$\Rightarrow\gcd(fg,h)=1$.

法三：$F[x]$是UFD，则f,g,h有标准的不可约分解，

$f=u_1p_1^{m_1}\cdots p_l^{m_l}$（$u_1\in U_D$，$p_1,\dots,p_l$是两两互不相伴的不可约元，$m_1,\dots,m_l$为正整数）

$g=v_1q_1^{n_1}\cdots q_s^{n_s}$（$v_1\in U_D$，$q_1,\dots,q_s$为两两互不相伴的不可约元，$n_1,\dots,n_s$为正整数）

$h=w_1r_1^{t_1}\cdots r_e^{t_e}$（$w_1\in U_D$，$r_1,\dots,r_e$为两两互不相伴的不可约元，$t_1,\dots,t_e$为正整数）

1

进而，

由 $\gcd(f,h)=1 \Rightarrow \{p_1,\cdots,p_t\} \cap \{r_1,\cdots,r_e\}=\phi$

由 $\gcd(g,h)=1 \Rightarrow \{q_1,\cdots,q_s\} \cap \{r_1,\cdots,r_e\}=\phi$

3、Eisenstein 判别法 设 D 是 UFD，F 是 D 的分式域，

$$f=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_0\in D[x],\ n>0,\ f_n\neq 0.$$

设 p 是 D 中的不可约元，如果

$$p\nmid f_n,\ p\mid f_{n-1},\ \cdots,\ p\mid f_0,\ p^2\nmid f_0.$$

则 f 在 $F[x]$ 中不可约.

3. 取素数 5，$5\nmid 3$，$5\mid 15$，$5\mid 10$，$5^2\nmid 10$，由 Eisenstein 判别法可知 f 在 $Q[x]$ 中不可约.

注意：$f\in\mathbb{Z}[x]$ 在 $\mathbb{Z}[x]$ 中不可约 $\Rightarrow$ f 在 $Q[x]$ 中不可约.

Pf：假设整系数多项式 $f(x)$ 有分解式 $f(x)=g(x)h(x)$，其中 $g(x)$，$h(x)$ 是次数大于 0 的有理系数多项式，令（即 f 在 $Q[x]$ 中可约）

$$f(x)=af_1(x),\ g(x)=rg_1(x),\ h(x)=sh_1(x),$$

这里，$f_1(x),g_1(x),h_1(x)$ 都是本原多项式，$a\in\mathbb{Z}$，$r,s\in Q$ 于是，$af_1(x)=rsg_1(x)h_1(x)$.

由高斯引理，$g_1(x)h_1(x)$ 是本原的，有 $a=\pm rs\in\mathbb{Z}$，从而 $f(x)=\underset{\mathbb{Z}[x]}{(rsg_1(x))}h_1(x)$. 在 $\mathbb{Z}[x]$ 中可约.

例：在 $Q[x]$ 中存在任意次数的不可约多项式.

Pf：任取正整数 n，设 $f(x)=x^n+3$. $3\nmid 1$，$3\mid 3$，$3^2\nmid 3$.

推广的 Eisenstein 判别法 设 D 是 UFD，F 是 D 的分式域，

$$f=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_0\in D[x],\ n>0,$$

设 p 是 D 中的不可约元，如果

$$p\mid f_n,\ p\mid f_{n-1},\ \cdots,\ p\mid f_1,\ p\nmid f_0,\ p^2\nmid f_n.$$

那么 f 在 $F[x]$ 中不可约.

Pf：假设 f 在 $F[x]$ 中可约，则存在两个正次数分别为 n_1，n_2 的多项式 $g_1(x)$，$g_2(x)\in D[x]$（定理3.30），使得

$$f(x)=g_1(x)g_2(x).$$

不定元 x 用 $F(x)$ 中的元素 $\frac{1}{x}$ 代入，从而

$$f(\tfrac{1}{x})=g_1(\tfrac{1}{x})g_2(\tfrac{1}{x}).$$

$$x^nf(\tfrac{1}{x})=x^{n_1}f_1(\tfrac{1}{x})x^{n_2}f_2(\tfrac{1}{x}). \qquad (1)$$

显然 $x^{n_i}f_i(\frac{1}{x})\in D[x]$，且次数为 n_i，$i=1,2$.

$$x^nf(\tfrac{1}{x})=a_n+a_{n-1}x+\cdots+a_1x^{n-1}+a_0x^n.$$

由 Eisenstein 判别法，$x^nf(\frac{1}{x})$ 在 $F[x]$ 中不可约，这就与 (1) 式矛盾，因此 $f(x)$ 在 $F[x]$ 中不可约.

4.(i) 设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbb{Z}[x]$，若 $\alpha=\frac{a}{b}\in\mathbb{Q}$，$\gcd(a,b)=1$ 为其根，证明：$a\mid a_0$，$b\mid a_n$.

Pf：法一：

$f(\frac{a}{b})=a_n(\frac{a}{b})^n+\cdots+a_1(\frac{a}{b})+a_0=0$

$\Rightarrow a_na^n+a_{n-1}a^{n-1}b+\cdots+a_1ab^{n-1}+a_0b^n=0$

$\Rightarrow a_na^n=-a_{n-1}a^{n-1}b-\cdots-a_1ab^{n-1}-a_0b^n$

$\Rightarrow b\mid a_na^n$.

$\because \gcd(a,b)=1$ $\therefore b\mid a_n$

同理，$a_0b^n=-a_na^n-a_{n-1}a^{n-1}b-\cdots-a_1ab^{n-1}$

$\Rightarrow a\mid a_0b^n$

$\because \gcd(a,b)=1$，$\therefore a\mid a_0$

问题. $b\mid a_na^n$，$\because b\nmid a^n$ $\therefore b\mid a_n$ （×）.

（b 为不可约元（这里为素数），上述因果关系才成立）.

法二：若 $\alpha=\frac{a}{b}\in\mathbb{Q}$ 为 $f(x)=0$ 的根，由于 $\gcd(a,b)=1$，故 $bx-a$ 是 $\mathbb{Z}[x]$ 中的本原多项式.

$\boxed{\text{证：设 } f(x), g(x) \text{ 是整系数多项式，且 } g(x) \text{ 是本原多项式，若 } f(x)=g(x)h(x)，h(x)\in\mathbb{Q}[x]，\text{则 } h(x) \text{ 必为整系数多项式.}}$

（$\mathbb{Z}[x]$ 中）

Pf：令 $f(x)=af_1(x)$，$h(x)=ch_1(x)$，其中 $a\in\mathbb{Z}$，$c\in\mathbb{Q}$，$f_1(x)$，$h_1(x)$ 是本原多项式，于是

$af_1(x)=g(x)ch_1(x)=cg(x)h_1(x)$，$c=\pm a\in\mathbb{Z}$，$h(x)=ch_1(x)$ 为整系数多项式.

$\Rightarrow f(x)=(bx-a)g(x)$，其中 $g(x)=g_{n-1}x^{n-1}+\cdots+g_0\in\mathbb{Z}[x]$

$\Rightarrow a_n=b\cdot g_{n-1}$，$a_0=-ag_0$.

$\Rightarrow b\mid a_n$，$a\mid a_0$.

（注意 $\gcd(a,b)=1$，这里保证了 $bx-a$ 是本原的（$\mathbb{Z}[x]$），从而 $g(x)$ 是整系数多项式）.

x^2-2 在有理数域上不可约.

$=(x+\sqrt{2})(x-\sqrt{2})$ 在实数域上可约.

(ii) 判断：$g(x)=x^q+4\in\mathbb{Q}[x]$ 是否可约，其中 $q=2$ 或 3 或 4.

解：$q=2$，$g(x)=x^2+4$，若 $\frac{a}{b}$，$\gcd(a,b)=1$ 是 $g(x)$ 的根，则 $a\mid 4$，$b\mid 1$.

$\Rightarrow a$ 只能为 $\pm1,\pm2,\pm4$，b 只能为 ±1.

$\Rightarrow g(x)$ 的有理根只能为 $\pm1,\pm2,\pm4$，显然这些都不是 $g(x)$ 的有理根，

x^2+4 在 $\mathbb{Q}[x]$ 中可约，则必然在 $\mathbb{Q}$ 中有根，由上述推导中 x^2+4 在 $\mathbb{Q}[x]$ 中不可约.

$q=3$，$g(x)=x^3+4$，若在 $\mathbb{Q}$ 上可约，则 x^3+4 只能分解成一个一次因式和二次因式之积，或一次因式的3次方. 总之，$g(x)$ 在 $\mathbb{Q}$ 上有根 α，易得 α 只能为 $\pm1,\pm2$.

显然 $g(x)$ 在 $\mathbb{Q}$ 中无根，则在 $\mathbb{Q}[x]$ 中不可约.

4. $g(x)=x^4+4$

法一：观察法，$g(x)=x^4+4+4x^2-4x^2=(x^2+2)^2-(2x)^2=(x^2+2x+2)(x^2-2x+2)$

法二：(待定系数法) $x^4+4=(x^2+ax+b)(x^2+cx+\frac{4}{b})$

(由于$g(x)$无有理根,若可约,只能分解成2个2次多项式的乘积)

$$=x^4+(a+c)x^3+(ac+b+\frac{4}{b})x^2+(\frac{4a}{b}+bc)x+4$$

$$\Rightarrow\begin{cases}a+c=0 & ①\\ ac+b+\frac{4}{b}=0 & ②\\ \frac{4a}{b}+bc=0 & ③\end{cases}$$

由①得 $c=-a$，由③得 $\frac{4a}{b}-ab=0$

(i) $a=0$，$c=0$，b无解

(ii) $b=2$，代入②得 $ac+4=0$，即：$-a^2+4=0$，即 $a=\pm2$

$$\begin{cases}a=2,\ c=-2,\\ a=-2,\ b=2,\ c=2\end{cases}\Rightarrow x^4+4=(x^2-2x+2)(x^2+2x+2)$$

(iii) $b=-2$，代入②得 $ac-4=0\Rightarrow -a^2-4=0\Rightarrow$ 无解。

5. (i) 利用 $f(x)=x^p-x-1$ 在 $\mathbb{Z}_p[x]$ 中不可约，其中p为素数。证明：$f(x)=x^p-x-1$与$g(x)=x^p+(p-1)x+(p-1)$ 在$\mathbb{Q}[x]$中不可约。

pf: $f\in\mathbb{Z}[x]$ (约化算法)，$\phi:\mathbb{Z}[x]\mapsto\mathbb{Z}_p[x]$ 注意到 $deg(\phi(f))\leq deg(f)$.

$$a_0+a_1x+\cdots+a_nx^n\mapsto\bar{a}_0+\bar{a}_1x+\cdots+\bar{a}_nx^n$$

若 $deg(\phi(f))=deg(f)$，则 f 在 $\mathbb{Z}[x]$中可约 $\Rightarrow\phi(f)\in\mathbb{Z}_p[x]$中 可约.

pf: 若$\exists$ g，$h\in\mathbb{Z}[x]$且 $deg(g)\geq1$，$deg(h)\geq1$，s.t $f=gh$.

$\Rightarrow\phi(f)=\phi(gh)=\phi(g)\phi(h)$

$deg(\phi(f))=deg(f)\Rightarrow deg(\phi(g))=deg(g)$，$deg(\phi(h))=deg(h)$.

$\Rightarrow\phi(f)$ 在 $\mathbb{Z}_p[x]$中可约.

反例：$\phi:\mathbb{Z}[x]\to\mathbb{Z}_2[x]$

$f=(2x-1)(x+1)$. $\phi(f)=(\bar{2}x-\bar{1})(x+\bar{1})=-(x+\bar{1})$.

f在$\mathbb{Z}[x]$中可约，但在$\mathbb{Z}_2[x]$中不可约.

$f(x)=x^p-x-1\in\mathbb{Z}[x]$，$\phi(f(x))=x^p-x-1$ 在 $\mathbb{Z}_p[x]$中不可约，则 $f(x)$在$\mathbb{Z}[x]$中不可约

$g(x)=x^p+(p-1)x+(p-1)$，$\phi(g(x))=x^p-x-1$在$\mathbb{Z}_p[x]$中不可约，则$f(x)$在$\mathbb{Z}[x]$中不可约.

注意到 $f(x)$与$g(x)$在$\mathbb{Z}[x]$中是本原的，从而 $f(x)$，$g(x)$ 在$\mathbb{Z}[x]$中的可约性$\Leftrightarrow f(x),g(x)$在$\mathbb{Q}[x]$中的可约性

从而$f(x)$，$g(x)$在$\mathbb{Q}[x]$中不可约.

例 $f=2(x^2+1)\in\mathbb{Z}[x]$. 在 $\mathbb{Z}[x]$ 中可约，注意到 2 是不可约元.

但 f 在 $\mathbb{Q}[x]$ 中不可约.

(ii) 证明：$f(x)=x^p-x-1$ 在 $\mathbb{Z}_p[x]$ 中不可约.

假设 $f(x)=x^p-x-1$ 在 $\mathbb{Z}_p[x]$ 中可约，则存在 $\mathbb{Z}_p[x]$ 中不可约元 $g_1,\cdots,g_s$，使得

$$f(x)=g_1(x)\cdots g_s(x).$$

首先注意到 $g_1,\cdots,g_s$ 不可能为一次因式，若存在 g_i 使得 g_i 为一次因式，则 f 在 $\mathbb{Z}_p$ 中有根，

$\forall \bar{a}\in\mathbb{Z}_p$，则 $f(\bar{a})=\underbrace{\bar{a}^p-\bar{a}}-1=-1\neq 0$ $\rightarrow\leftarrow$

$\bar{a}^p\equiv\bar{a} \bmod p$

从而 $0<s<p$

$f(x+\bar{i})=(x+\bar{i})^p-(x+\bar{i})-1=x^p+\bar{i}-x-\bar{i}-1=x^p-x-1$

$f(x)=g_1(x)\cdots g_s(x)$

$f(x+\bar{1})=g_1(x+\bar{1})\cdots g_s(x+\bar{1})$

$f(x+\bar{2})=g_1(x+\bar{2})\cdots g_s(x+\bar{2})$

$\vdots$

$f(x+\overline{p-1})=g_1(x+\overline{p-1})\cdots g_s(x+\overline{p-1})$

注意到这些多项式都是首一的，

由 UFD 定义中的第(ii)条可知，$g_1(x)=g_{m_1}(x+\bar{1})=g_{m_2}(x+\bar{2})=\cdots$
$=g_{m_{p-1}}(x+\overline{p-1})$

由 $0<s<p$ 可知，$\exists\, i,j$，$i\neq j$，s.t $m_i=m_j$，

即 $g_{m_i}(x+\bar{i})=g_{m_j}(x+\bar{j})$.

$\Rightarrow g_{m_i}(x)=g_{m_j}(x\underbrace{-\bar{i}+\bar{j}}_{=n})$

设 $g_{m_i}(x)=x^m+a_{m-1}x^{m-1}+\cdots+a_0$，$1\leq m<p$

$g_{m_i}(x+\bar{n})=(x+\bar{n})^m+a_{m-1}(x+\bar{n})^{m-1}+\cdots+a_0=x^m+(m\bar{n}+a_{m-1})x^{m-1}+\cdots$

$\Rightarrow a_{m-1}=m\bar{n}+a_{m-1}$ $\Rightarrow m\bar{n}=0$，$m\neq\bar{0}$ $\Rightarrow \bar{n}=0$. $\Rightarrow i=j$ $\rightarrow\leftarrow$

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

6. 设 R 是整环. 如果存在 $d:R\setminus\{0\}\to\mathbb{N}$ 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 为欧几里德整环.

(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.

(ii) 尽可能多的列举你知道的欧几里德环.

$\mathbb{Z}[i]=\{m+ni \mid m,n\in\mathbb{Z}, i^2=-1\}$. $\forall m_1+n_1 i,\ m_2+n_2 i\in\mathbb{Z}[i]$.

$+$: $m_1+n_1 i+m_2+n_2 i=(m_1+m_2)+(n_1+n_2)i$

$\cdot$: $(m_1+n_1 i)(m_2+n_2 i)=(m_1m_2-n_1n_2)+(m_1n_2+m_2n_1)i$

$\mathbb{Z}[i]$关于"+"和"·"构成一个整环.

验证: $\forall a_1,a_2\in R$, $d(a_1a_2)=d(a_1)d(a_2)$

$a_1=m_1+n_1 i$, $a_2=m_2+n_2 i$, $d(a_1)=m_1^2+n_1^2$ $d(a_2)=m_2^2+n_2^2$

$a_1a_2=(m_1m_2-n_1n_2)+(m_1n_2+m_2n_1)i$

$d(a_1a_2)=(m_1m_2-n_1n_2)^2+(m_1n_2+m_2n_1)^2=m_1^2m_2^2+n_1^2n_2^2-2m_1\cancel{m_2}n_1n_2+m_1^2n_2^2+m_2^2n_1^2+2n_1n_2\cancel{m_1}m_2$

$=m_1^2(m_2^2+n_2^2)+n_1^2(n_2^2+m_2^2)=(m_1^2+n_1^2)(n_2^2+m_2^2)$

$=d(a_1)d(a_2)$.

$\forall a,b\in R$, $b^{-1}\in Q[i]=\{q_1+q_2 i \mid q_1,q_2\in Q, i^2=-1\}$.

令 $ab^{-1}=q_1+q_2 i$, $q_1,q_2\in Q$

我们取 $u,v\in\mathbb{Z}$, 使得 $\varepsilon=q_1-u$ 和 $\eta=q_2-v$ 满足 $|\varepsilon|\le\frac{1}{2}$, $|\eta|\le\frac{1}{2}$, 于是

$$a=b(q_1+q_2 i)=b((\varepsilon+u)+(\eta+v)i)=b(u+vi)+b(\varepsilon+\eta i)$$

令 $r=b(\varepsilon+\eta i)$ $r=a-b(u+vi)\in R$.

$d(r)=d(b)d(\varepsilon+\eta i)=(\varepsilon^2+\eta^2)d(b)\le\frac{1}{2}d(b)<d(b)$.

(i) ① 整数环 $\mathbb{Z}$, $d(a)=|a|$, $\forall a\in\mathbb{Z}$

($\forall a,b\in\mathbb{Z}$, $a=qb+r$, $r=0$ 或 $|r|<|b|$).

② 域F上一元多项式环 $F[x]$ 是一个欧几里德整环, $d(f(x))=\deg(f(x))$).

环R的子集S叫做R的理想，是指满足如下两个条件：

(1) 如果 $a,b\in S$，则 $a\pm b\in S$

(2) 如果 $r\in R, a\in S$，则 $ar, ra\in S$

例 整数环 $\mathbb{Z}$ 的子环均有形式 $m\mathbb{Z}(m\geq 0)$，它也是 $\mathbb{Z}$ 的全部理想。

由一个元素 $x\in R$ 生成的理想 (x) 叫做环R的主理想，如果R是整环，并且R的每个理想都是主理想 $(x)=xR$，则R叫做主理想整环。

若R为UFD，则R具有下面性质：

性质1. R中不存在无限的元素序列 $a_1,a_2,\cdots,a_n,\cdots$，使得每个 a_{i+1} 都是 a_i 的真因子

性质2. R中不可约元必为素元

性质3. R中任意两个非零元素 a 和 b 都有最大公因子

Pf：设 a_1 为 r 个不可约元素之积：$a_1=p_1\cdots p_r$，由于 a_2 是 a_1 的真因子，从而 $a_1=a_2x$，$x\neq 0$，$x\notin U(R)$，

令 a_2 和 x 分别是 t 和 λ 个不可约元之积，$a_2=q_1\cdots q_t$，$x=l_1\cdots l_\lambda$，则 $\lambda\geq 1$，并且

$$p_1\cdots p_r=q_1\cdots q_t l_1\cdots l_\lambda.$$

由分解唯一性可知

$$r=t+\lambda>t$$

即 a_2 分解成不可约因子个数 t 要小于 a_1 的不可约因子个数 r，这个过程显然不能无限下去，从而证明了性质1.

注：对于R中每个无限序列 $a_1,a_2,\cdots,a_n,\cdots$，如果 $a_{i+1}\mid a_i\ (i=1,2,\cdots)$ 均成立，则必有正整数N使得

$a_N\sim a_{N+1}\sim\cdots$. (性质1')

设R为整环，则下列三个命题彼此等价：

(1) R为UFD；

(2) R满足性质1和3；

(3) R满足性质1和2

Pf：(1)⇒(2) 已证

(2)⇒(3) 若R中任意两个非零元素 a 和 b 均存在最大公因子，则每个不可约元都为素元，设 p 为不可约元，如果 $p\nmid a$，$p\nmid b$，$a,b\in R$，易证 $\gcd(p,a)\approx 1$，$\gcd(p,b)\approx 1$，从而 $\gcd(p,ab)\approx 1$. 于是 $p\nmid ab$.

(3)⇒(1) 由性质1证明R中每个非零元素 $a\notin U_R$ 均可分解成有限个不可约元之积. 如果 a 不可约则证毕，否则 $a=a_1b_1$，a_1 和 b_1 均是 a 的真因子. 如果 a_1 和 b_1 均不可约则完毕，否则 a_1 或 b_1 又要有真因子，根据性质1这样下去不可能无休止地进行下去，因此 a 必可分解成有限个不可约元之积.

再由性质2证明分解的唯一性：设 $a=p_1\cdots p_s=q_1\cdots q_t$，其中 p_i,q_j 均为 R 中不可约元.
根据性质2，它们也是素元，由于 $p_1|a=q_1\cdots q_t$，由素元定义可知 $p_1|q_j$，不妨设 $p_1|q_1$，于是 $q_1=p_1u$.
由 q_1 不可约可知 $u\in U_R$. 因此 $p_1\approx q_1$，从而 $p_2\cdots p_s=uq_2\cdots q_t\approx q_2\cdots q_t$. 这样继续下去可知 $s=t$，并且存在 $\{1,2,\cdots,s\}$ 的一个置换 σ，使得 $p_i\approx q_{\sigma(i)}$ $(1\le i\le s)$，这就证明分解的唯一性.

定理 每个主理想整环都是UFD

证：我们证明每个主理想整环 R 都有性质1'和性质3. 设 $a_1,a_2,\cdots,a_n,\cdots$ 是 R 中元素的无限序列，并且 $a_{i+1}|a_i$ $(i=1,2,3,\cdots)$. 则为 $(a_1)\subseteq(a_2)\subseteq\cdots\subseteq(a_n)\subseteq\cdots$. 令 $I=\bigcup_{n=1}^{\infty}(a_n)$.
则 I 是 R 的理想，由于 R 为主理想整环，从而 $I=(a)$，$a\in R$. 由于 $a\in I$，从而 a 必然属于某个 (a_k)，由此推出 $(a)\subseteq(a_k)\subseteq(a_{k+1})\subseteq\cdots\subseteq I=(a)$
于是 $(a_k)=(a_{k+1})=\cdots$，即 $a_k\sim a_{k+1}\sim\cdots$.
再证性质3. 设 $a,b\in R\setminus\{0\}$. 令 I 为理想 $(a)+(b)$. 由于 R 是主理想整环，从而 $I=(d)$，$d\in R$
下证 $d=\gcd(a,b)$. 由于 $a=a+0\in(a)+(b)=(d)$，从而 $d|a$，同样 $d|b$，即 d 是 a 和 b 的公因子. 如果 d' 也是 a 和 b 的公因子，则 $d'|a$，$d'|b$. 于是 $a\in(d')$，$b\in(d')$，从而 $(d)=(a)+(b)\subseteq(d')$，于是 $d'|d$. 这就表明 d 是 a 和 b 的最大公因子.

定理 每个欧几里德整环均为主理想整环

证：设 $I\subseteq R$ 为理想，下证 I 为主理想，
若 $I\neq\{0\}$，则 $\exists\, 0\neq a\in I$, 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 $d(a)$ 极小性矛盾，从而 $r=0$
故对 $\forall\, b\in I$，$b\in(a)$. 即 $I\subseteq(a)$
$(a)\subseteq I$ 显然.
$\Rightarrow I=(a)$.