答案

1.(1) 解：设 $\alpha=a+bi\in\mathbb{Z}[i]$ 是不可约元(也是素元)

则 $\alpha\mid\alpha\bar{\alpha}=a^2+b^2$，设 $n\in\mathbb{N}$ 是最小的被 α 整除的正整数

则 n 是素数，否则 $n=n_1n_2$，$n_1,n_2<n$，$\alpha\mid n\Rightarrow\alpha\mid n_1$ 或 $\alpha\mid n_2$，与 n 的最小性矛盾.

若 $n=2$，$2=(1+i)(1-i)$，$1\pm i$ 即是不可约元

现在设 $n=p$ 是奇素数，由Fermat小定理，$\forall a\neq 0\in\mathbb{N}$，

$a^{p-1}\equiv 1(\mathrm{mod}\,p)$

若 $p\equiv 1(\mathrm{mod}\,4)$，则 $p-1\equiv 0(\mathrm{mod}\,4)$，存在 $t\in\mathbb{Z}$，$p-1=4t$

$a^{4t}\equiv 1(\mathrm{mod}\,p)$ 令 $b=a^{2t}$，则 $b^2\equiv -1(\mathrm{mod}\,p)$，$p\mid b^2+1=(b+\sqrt{-1})(b-\sqrt{-1})$ (取 $b<p$，即 $b\in\mathbb{Z}_p$)，$p\nmid b\pm\sqrt{-1}$，所以 p 非素元(也非不可约) 因此 $p=\pi_1\pi_2\cdots\pi_n$ π_i 不可约

两边取共轭，得 $p=\bar{\pi}_1\cdot\bar{\pi}_2\cdots\bar{\pi}_n$，相乘，$p^2=(\pi_1\bar{\pi}_1)\cdot(\pi_2\bar{\pi}_2)\cdots$

由于 p 是素数，$n\leq 2$，p 可约 $\Rightarrow n=2$，$p=\pi_1\pi_2$，若 $\pi_1\mid p$，

则 $\bar{\pi}_1\mid p\Rightarrow\pi_2=\bar{\pi}_1$，即 $p=\pi_1\bar{\pi}_1$

若 $p\equiv 3(\mathrm{mod}\,4)$，如上讨论，若 p 可约，则 $p=\pi\bar{\pi}$，π 不可约，

则 $p=a^2+b^2$ $\exists a,b\in\mathbb{Z}$，p 奇，a,b 必一奇一偶，设奇数为 a

则 $a^2\equiv 1(\mathrm{mod}\,4)$ $b^2\equiv 0(\mathrm{mod}\,4)$ $\Rightarrow p\equiv 1(\mathrm{mod}\,4)$ 矛盾，因此

当 $p\equiv 3(\mathrm{mod}\,4)$，$p$ 是不可约元.

(2) 令 $\beta = 81+8i$，则 $\beta\bar{\beta} = 81^2+8^2 = 5^3 \times 53$

$5 = (1+2\sqrt{-1})(1-2\sqrt{-1})$，$53 = (7+2i)(7-2i)$，由(1)，右边均不可约

验证 可得 $81+8i = (1-2i)^3 \cdot (-7-2i)$

(3) 由(1) 当 $p \equiv 1 \pmod 4$，$p = \pi\bar{\pi}$　$\pi = x+yi$ 不可约 $\Rightarrow p = x^2+y^2$，反之，若 $p = x^2+y^2$，容易证 $p=2$ 或 $p \equiv 1 \pmod 4$

2.(1) 设 $\mathbb{Z}[\sqrt{D}]$ 是一个 UFD，$\alpha = a+b\sqrt{D}$ 是一个不可约元（因而是素元），则 $\alpha \mid \alpha\bar{\alpha} = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2-Db^2$ 取 α 整除的最小正整数 p，正如1(1)，p 是一个素数，即不可约元是素数因子，正如1(1)，若 p 可约，则 $p = \pi\cdot\bar{\pi}$，π 不可约，令 $\pi = x+y\sqrt{D}$，则 $p = |x^2-Dy^2|$ 即 $x^2 \equiv Dy^2 \pmod p$ 在 $\mathbb{Z}_p$ 中，$x, y \neq 0$ 因而可逆，得 $\left(\frac{x}{y}\right)^2 \equiv x^2y^{-2} \equiv D \pmod p$

即存在 $u = \frac{x}{y} \in \mathbb{Z}_p$　$u^2 \equiv D \pmod p$

反之，若 $\exists u \in \mathbb{Z}_p$，$u^2 \equiv D \pmod p$，则 $p \mid u^2 - D = (u-\sqrt{D})(u+\sqrt{D})$，因此若 p 是素元则 $p \mid u+\sqrt{D}$ 或 $p \mid u-\sqrt{D}$，即 $\frac{u \pm \sqrt{D}}{p} \in \mathbb{Z}[\sqrt{D}]$

显然 $\frac{1}{p} \notin \mathbb{Z}$. $\Rightarrow p$ 不是素元，$\Rightarrow p$ 可约，设 $p = \alpha\beta$，正如(1)的讨论 $p = \alpha\bar{\alpha}$　α 不可约，令 $\alpha = x+y\sqrt{D}$，$p = |x^2-Dy^2|$

(2) 若$\mathbb{Z}[\sqrt{D}]$是一个UFD，由(1)，任一素数p，

$$p=|x^2-Dy^2| \Longleftrightarrow D\equiv x^2 \pmod p \quad x\in\mathbb{Z}.$$

特别地，令$p=2$，任意$D<-2$，$D\equiv 0^2 \pmod 2$或$D\equiv 1^2 \pmod 2$ 但是不存在x,y，使得$2=|x^2-Dy^2|$

$(x,y\in\mathbb{Z})$

(3) $\forall\, x+y\sqrt{D}\in\mathbb{Z}[\sqrt{D}]$ $D=-2$

定义$\delta(x+y\sqrt{D})=|x^2-Dy^2|$ 这个定义可扩充到$\mathbb{Q}(\sqrt{D})$

设$\alpha=x_1+y_1\sqrt{D}\neq 0$ $\beta=x_2+y_2\sqrt{D}\neq 0$，需要$q,r\in\mathbb{Z}[\sqrt{D}]$

使$\alpha=\beta q+r$, $\delta(r)<\delta(\beta)$.

$$\Updownarrow$$

$\alpha\beta^{-1}=q+r\beta^{-1}$ 令$\alpha\beta^{-1}=x+y\sqrt{D}$，$x,y\in\mathbb{Q}$，

$\exists\, r,s\in\mathbb{Z}$ $|r-x|,|s-y|\leq\frac{1}{2}$ 令$q=r+s\sqrt{D}$

$\cancel{\delta(\alpha\beta^{-1}-q)=|(r-x)}$

$$\delta(\alpha-\beta q)=\delta(\beta)\,\delta(\alpha\beta^{-1}-q)=\delta(\beta)\,|(r-x)^2-D(s-y)^2|$$

$$\leq(|r-x|^2+|D||s-y|^2)\,\delta(\beta)\leq\frac{|D|+1}{4}\cdot\delta(\beta)$$

若$D=-2$，则$\frac{|D|+1}{4}<1$，即$\delta(r)<\delta(\beta)$.

3.(1) 回忆 R 是整环 $\iff$ x^3-y^2 是不可约多项式

设 $x^3-y^2=f(x,y)g(x,y)$　令 $x=t^2$, $y=t^3$, 则 $\forall t\in\mathbb{F}$ 令

$f(t^2,t^3)=0$ 或 $g(t^2,t^3)=0$，不妨设 $f(t^2,t^3)=0$

$f(x,y)=(y^2-x^3)h(x,y)+a(x)y+b(x)$ (关于 y 的带余除法)，代入 $x=t^2$, $y=t^3$，则 $a(t^2)t^3+b(t^2)=0$

分离奇、偶次数 $\Rightarrow a=b=0$　　$\forall t\in\mathbb{F}$

(2) $R/P_0\cong\dfrac{\mathbb{F}[x,y]}{(x,y)}\cong\mathbb{F}$　因此 P_0 是极大理想.

R_{P_0} 是 R 关于 P_0 的局部化，即

$$R_{P_0}=\left\{\frac{r}{s}\,\middle|\, r\in R,\ s\in R-P_0\right\}\Big/\sim \;=\; \frac{R\times(R-P_0)}{\sim}.$$

"$\sim$": $\dfrac{r}{s}\sim\dfrac{r'}{s'}\iff rs'=r's$ 或 $(r,s)\sim(r',s')\iff rs'=r's$

$$\begin{aligned} R &\longrightarrow R_{P_0} \\ r &\longmapsto \frac{r}{1} \end{aligned}$$

是一个嵌入，$P_0\cdot R_{P_0}$ 是 R_{P_0} 的唯一极大理想，因为 (a) $P_0R_{P_0}$ 是 R_{P_0} 的极大理想：

若 $\frac{r}{s}\notin P_0R_{P_0}$，则 $r\notin P_0$，$\exists\, u\in R$, $y\in P_0$，$ur+y=1_R$，$\cancel{\Rightarrow\frac{usr}{s}}$

在 $R_{P_0}/P_0R_{P_0}$ 中 $\overline{\frac{r}{s}}$ 的逆是 $\overline{us}$ $\Rightarrow$ $\dfrac{R_{P_0}}{P_0R_{P_0}}$ 是一个域.

(b) 它是唯一的极大理想

因为若 $x \notin P_0R_{P_0}$，$x=\frac{r}{s} \Rightarrow r \notin P_0$，$\Rightarrow r$ 在 R_{P_0} 中可逆

即 x 在 R_{P_0} 中可逆 $x^{-1}=\frac{s}{r}$

一般地，设 R 整区，$\mathfrak{m}$ 是极大理想，$\Rightarrow R/\mathfrak{m}$ 是一个域.

$\mathfrak{m}/\mathfrak{m}^2$ 可看作 $R/\mathfrak{m}$ 上的向量空间. 设 $x_1,\cdots,x_n \in \mathfrak{m}$ 生成元

~~代表~~则 $\forall\ y \in \mathfrak{m}/\mathfrak{m}^2$ $\quad \bar{y}=a_1\bar{x}_1+\cdots+a_n\bar{x}_n \quad a_i \in R/\mathfrak{m}$.

回到本题 $P_0R_{P_0}=\mathfrak{m}=(\tilde{x},\tilde{y}) \quad \tilde{x}=\bar{x}+\mathfrak{m}^2$.

$\tilde{y}=\bar{y}+\mathfrak{m}^2$ 则 $\forall\ v \in \mathfrak{m}/\mathfrak{m}^2 \quad v=c_1\tilde{x}+c_2\tilde{y}$ ~~$c_1,c_2\in R_{P_0}/P_0$~~

$c_1,c_2 \in \frac{R_{P_0}}{P_0R_{P_0}} \cong \mathbb{F}$.

4. 证明：$R[x]$ 和 $F_R[x]$ 均是唯一分解整区，因为

$f(\frac{b}{a})=0 \Rightarrow (ax-b)\,|\,f(x)$ 设 $f(x)=(ax-b)(\sum_{i=0}^{n-1}b_ix^i)$

$f(x)=\sum_{i=0}^{n}a_ix^i \in R[x]$，则有 $a_n=ab_{n-1}$，$a_0=b(-b_0)$

$ax-b$ 是本原的，令 $\sum_{i=0}^{n-1}b_ix^i=\frac{t}{s}h_1(x)$ $(s,t)=1$，$h_1(x)$ 本原

(在 $R[x]$ 中) $\quad f(x)=(ax-b)\frac{t}{s}h_1(x)=\frac{t}{s}[(ax-b)h_1(x)]$

$(ax-b)h_1(x) \in R[x]$ 是本原的，$s\,|\,(ax-b)h_1(x) \Rightarrow s$ 是

单位. 即 $\sum_{i=0}^{n-1}b_ix^i \in R[x]$

令 $x=\pm 1$ 代入

$f(1)=(a-b)(b_{n-1}+\cdots+b_0)$ $f(-1)=(a+b)(\cdots)$

5. $\forall f(x)=\sum_{i=0}^{\infty} a_i x^i \in \mathbb{F}[[x]]$，$f(x)$是单位 $\Leftrightarrow a_0 \neq 0$（见课程文件：环的定义），因此，若$f(x)$不是单位，则 $f(x)$形如 $x^k\left(\sum_{j=k}^{\infty} a_j x^{j-k}\right)$，$a_k \neq 0$，$k$称为$f(x)$的尾次数．设$I$是$\mathbb{F}[[x]]$的一个$(\neq(0))$理想，取$f(x)\neq 0 \in I$，使得它的尾次数在$I$中最小，$\forall g(x)\in I$，尾次数为$l$，$l\geq k$

$f(x)=x^k f_1(x)$，$g(x)=x^l g_1(x)$．$f_1(x)$，$g_1(x)$首项均非零，因此可逆，$g(x)=x^l g_1(x)=[f_1^{-1}(x)g_1(x)]x^l f_1(x)$
$=[f_1^{-1}(x)g_1(x)]x^{l-k}f(x) \Rightarrow g(x)\in(f(x))=(x^k)$

6. $\mathbb{R}[x,y]$是含幺交换整环．令I是$\mathbb{R}[x,y]$中常数项为零的多项式全体．I是一个理想．若I是主理想，则存在 $f(x,y)\in\mathbb{R}[x,y]$，$I=(f(x,y))$，$x\in I$，则存在$g(x,y)$
$x=g(x,y)f(x,y)$ 比较两边x,y的次数：

$$0=\deg_y g(x,y)+\deg_y f(x,y)$$

$$1=\deg_x g(x,y)+\deg_x f(x,y)$$

因此 $\deg_y g(x,y)=\deg_y f(x,y)=0$

因为$f(x,y)$无常数项，且$f(x,y)\neq 0$，$\Rightarrow \deg_x f(x,y)=1$，$\deg_x g(x,y)=0$，则有$g(x,y)=g_0\in\mathbb{R}$，$f(x,y)=a_1x$ $a_1\neq 0\in\mathbb{R}$，同理 $y\in(f(x,y))\Rightarrow f(x,y)=b_1y$ $b_1\neq 0\in\mathbb{R}$

这不可能，从而$\mathbb{R}[x,y]$不是PID.

7. 关于n作归纳

令$a_1=a$，$a_2=b$

$n=2$，$(a_1)+(a_2)$是D的理想，因为D是PID，存在d

$(a)+(b)=(d)$，$\Rightarrow a,b\in(d)\Rightarrow d|a$，$d|b$. $\forall c|a, c|b$

$(a)+(b)\subseteq(c)\Rightarrow(d)\subseteq(c)\Rightarrow c|d$. $\Rightarrow d$是最大公约元

因为$(a)+(b)=(d)$，存在$x,y\in D$，$xa+yb=d=d_2$

令$A_2=\begin{pmatrix}a_1 & a_2\\ -y & x\end{pmatrix}$ $\quad\det(A_2)=a_1x+ya_2=d_2$

假设结论对于$n-1$个元素成立，即$a_1\neq 0,\cdots,a_{n-1}\neq 0\in D$，$d_{n-1}$是它们的最大公约元，则存在$A_{n-1}=\begin{pmatrix}a_1 & \cdots & a_{n-1}\\ * & & *\end{pmatrix}$，$\det A_{n-1}=d_{n-1}$

现在给定$a_1\neq 0,\cdots,a_{n-1}\neq 0$，$a_n\neq 0\in D$，令$d_{n-1}=(a_1,\cdots,a_{n-1})$

$d_n=(a_1,\cdots,a_{n-1},a_n)=(d_{n-1},a_n)$，如上讨论，存在$x,y\in D$

$$xd_{n-1}+ya_n=d_n$$

$$令\ A_n=\left(\begin{array}{ccc|c} & A_{n-1} & & \begin{matrix}a_n\\0\\\vdots\\0\end{matrix}\\ \hline -\frac{a_1y}{d_{n-1}} & \cdots & -\frac{a_{n-1}y}{d_{n-1}} & x\end{array}\right)$$

按最后一列展开

$\det(A_n) = a_n(-1)^{n+1}B_{n-1} + x\det(A_{n-1})$

容易检查 $(-1)^{n-3}y\det(A_{n-1}) = d_{n-1}\det(B_{n-1})$

$\Rightarrow d_{n-1}\det(A_n) = a_n y d_{n-1} + x d_{n-1}^2 = d_{n-1}\cdot d_n$

D 整区，消去 $d_{n-1}\neq 0$，得 $\det(A_n) = d_n$

8. 注意：$\begin{pmatrix} m & n \\ -3n & m \end{pmatrix}\begin{pmatrix} m & -n \\ 3n & m \end{pmatrix} = \begin{pmatrix} m^2+3n^2 & 0 \\ 0 & m^2+3n^2 \end{pmatrix}$

D的分式域 $= \left\{ \begin{pmatrix} m & n \\ -3n & m \end{pmatrix}\begin{pmatrix} d & \\ & d \end{pmatrix}^{-1} \middle| \begin{array}{l} m,n\in\mathbb{Z},\ d\in\mathbb{N} \\ 0\neq d = x^2+3y^2,\ x,y\in\mathbb{Z} \end{array} \right\}$

9. $f(\bar{0}) = \bar{-1}$，$f(\bar{1}) = \bar{1}$，$f(\bar{-1}) = \bar{-1}$，$f(x)$ 在 $\mathbb{Z}_3$ 中无根，

$\Rightarrow f(x)$ 不可约（若可约，可分解为两个一次因式，必有根）

同理，x^2+1 也不可约（在 $\mathbb{Z}_3$ 中）

$\dfrac{\mathbb{Z}_3[x]}{(x^2+1)} = \{a+bi \mid a,b\in\mathbb{Z}_3\}$，$x^2+x-1=0$ 在 $\mathbb{C}$ 中的根为

$\frac{1}{2}(-1\pm\sqrt{5})$，~~在 $\mathbb{Z}_3$ 中，$\sqrt{5}$~~ 令 $F = \dfrac{\mathbb{Z}_3[x]}{(x^2+1)}$（可看作 $\mathbb{Z}_3$ 的扩域）

在 $\mathbb{Z}_3$ 中，$5\equiv -1 \pmod 3 \Rightarrow \sqrt{5}$ 能被替换成 $\sqrt{-1}$，令 $\alpha^2=-1$（在

$\mathbb{F}$ 中）$\frac{1}{2} = 2^{-1} = 2$（在 $\mathbb{Z}_3$ 中），$\Rightarrow 2(-1\pm\alpha)$ 是根，验证：

$= -2\pm 2\alpha = 1\pm\alpha$（在 $\mathbb{Z}_3$ 中）

$(1+\alpha)^2 + (1+\alpha) - 1 = 1+2\alpha+\alpha^2+1+\alpha-1 = \alpha^2+1 = 0$.