近世代数 (H) 第五周作业

涂嘉乐 PB23151786

2025 年 3 月 19 日

Exercise 1 分别将 60 和 $81+8i$ 在 $\mathbb{Z}[i]$ 中分解为不可约元之积

Solution 在 $\mathbb{Z}$ 上有 $60=2^2 3^1 5^1$，因为 $5=(2+i)(2-i), 2=(1+i)(1-i)$，且 3 为 $4k+3$ 型素数，故为 *Gauss* 素数，所以

$$60=(1+i)(1-i)\cdot 3\cdot(2+i)(2-i)$$

在 $\mathbb{Z}$ 上分解 $N(81+8i)=81^2+8^2=5^3\cdot 53$，因为 $53=49+4=(7+2i)(7-2i), 5=(1+2i)(1-2i)$，所以 $81+8i$ 的因子只能在 $7\pm 2i, 1\pm 2i$ 之间，经过尝试可得

$$81+8i=(7+2i)(11-2i)$$

对 $(11-2i)$ 继续尝试可得

$$11-2i=(1-2i)(3+4i)$$

对 $(3+4i)$ 继续尝试可得

$$3+4i=-(1-2i)^2$$

综上我们有

$$81+8i=-(1-2i)^3(7+2i)$$

$\square$

Exercise 2 设 $p=a^2+b^2$ 是 $4k+1$ 型素数，求证 $\mathbb{Z}[i]/(a+bi)=\mathbb{F}_p$

Proof 易知 $a\pm bi$ 是高斯素数，首先证明 a,b 互素，否则存在素数 $q, \text{s.t. } q\mid \gcd(a,b)$，则在 $\mathbb{Z}[i]$ 中，$a+bi=q\left(\frac{a}{q}+\frac{b}{q}i\right)$，这与 $a+bi$ 是高斯素数矛盾，所以 $\gcd(a,b)=1$

考虑环同态

$$\varphi:\mathbb{Z}\longrightarrow \mathbb{Z}[i]/(a+bi)$$
$$m\longmapsto \overline{m}$$

它是两个环同态 $\mathbb{Z}\hookrightarrow\mathbb{Z}[i]\hookrightarrow\mathbb{Z}[i]/(a+bi)$ 的复合，因此还是环同态，接下来我们证明它是满同态，即证明对 $\forall x+yi\in\mathbb{Z}[i], \exists z\in\mathbb{Z}, \text{s.t. } \overline{x+yi}=\overline{z}$，因为 $\gcd(a,b)=1$，所以 $\exists u,v\in\mathbb{Z}, \text{s.t. } au+bv=1$，故

$$(a+bi)(v+ui)=(av-bu)+(au+bv)i=(av-bu)+i$$

因此在 $\mathbb{Z}[i]/(a+bi)$ 中，$\bar{i}=\overline{bu-av}$，所以

$$\overline{x+yi}=\overline{x+y(bu-av)}=\overline{x+ybu-yav}$$

即对 $\forall x+yi\in\mathbb{Z}[i],\exists x+ybu-yav\in\mathbb{Z},\text{s.t. }\varphi(x+ybu-yav)=\overline{x+yi}$，故 φ 为满射

接下来证明 $\text{Ker}\varphi=(p)$,一方面 $\forall zp\in\mathbb{Z},\varphi(zp)=\varphi(z)\varphi(p)=\bar{0}$,所以 $zp\in\text{Ker}\varphi\Longrightarrow(p)\subseteq\text{Ker}\varphi$;另一方面假设 $z\in\text{Ker}\varphi$，则 $\varphi(z)=\bar{z}=\bar{0}\Longrightarrow a+bi\mid z$，所以 $\exists\alpha\in\mathbb{Z}[i],\text{s.t. }(a+bi)\alpha=z$，故

$$\alpha=\frac{z}{a+bi}=\frac{z(a-bi)}{a^2+b^2}=\frac{za-zbi}{p}\in\mathbb{Z}[i]$$

因此 $p\mid za,p\mid zb$，又因为 $1\leq a,b\leq p$，所以 a,b 中有一者为 1 时显然有 $p\mid z$；$a,b\geq 2$ 时，$p\neq 1$ 时，$p\nmid a,p\nmid b\Rightarrow p\mid z$，所以 $z\in(p)$，所以 $\text{Ker}\varphi\subseteq(p)$

综上，φ 是满环同态且 $\text{Ker}\varphi=(p)$，由环同态基本定理，我们有环同构

$$\mathbb{Z}/(p)\cong\mathbb{Z}[i]/(a+bi)$$

所以 $\mathbb{F}_p\cong\mathbb{Z}/(p)\cong\mathbb{Z}[i]/(a+bi)$ □

Exercise 3 求证: 设 R 是 UFD, $a=up_1^{n_1}\cdots p_r^{n_r}$ 是 a 的标准分解, 则 a 的因子总形如 $vp_1^{m_1}\cdots p_r^{m_r}$,其中 $v\in U(R)$，$0\leq m_i\leq n_i$

Proof 设 x 为 a 的因子

Case 1. 若 $x\in U(R)$, 则 x 是 p 的平凡因子, 则 $p=vp_1^{m_1}\cdots p_r^{m_r}$, 其中 $v=x,m_1=\cdots=m_r=0$

Case 2. 若 x 是素元，则 $x\mid a\Longrightarrow\exists p_i,1\leq i\leq r,\text{s.t. }x\mid p_i$，又因为 p_i 是不可约元，故 x 与 p_i 相伴，则 $x=vp_i=vp_1^{m_1}\cdots p_r^{m_r}$，其中 $v\in U(R),m_1=\cdots=m_{i-1}=m_{i+1}=\cdots=m_r=0,m_i=1$

Case 3. 若 x 非单位且可约，则 x 存在素因子 q，则 $q\mid x\mid a$，由 *Case 2* 知，$\exists 1\leq i\leq r,\text{s.t. }q,p_i$ 相伴，可不妨设 $q=p_1$，我们固定 $n_2,\cdots,n_r$，对 n_1 归纳

因为 $p_1\mid x,p_1\mid a$，所以 $\exists x_1\in R,a_1\in R,\text{s.t. }x=x_1p_1,a=a_1p_1$，再由 $x\mid a$ 可设 $x\beta=a,\beta\in R$,所以

$$x_1p_1\beta=a_1p_1\Longrightarrow x_1\beta=a_1\Longrightarrow x_1\mid a_1$$

因为 $a=up_1^{n_1}\cdots p_r^{n_r}=a_1p_1$，由整环的消去律知 $a_1=up_1^{n_1-1}\cdots p_r^{n_r}$，由归纳假设知，$a_1$ 的因子 x_1 形如

$$x_1=vp_1^{\tilde{m}_1},\cdots,p_r^{m_r},\quad \tilde{m}_1\leq n_1-1,m_2\leq n_2,\cdots,m_r\leq n_r$$

记 $m_1=\tilde{m}_1+1$ 所以

$$x=x_1p_1=vp_1^{m_1},\cdots,p_r^{m_r},\quad m_1\leq n_1,\cdots,m_r\leq n_r$$

□

Exercise 4 设 R 是 *Noether* 环，则其中理想升链 $I_1 \subset I_2 \subset \cdots$ 稳定，即 $\exists n_0 > 0, \text{s.t.}$

$$I_{n_0} = I_{n_0+1} = \cdots$$

Proof 考虑

$$I = \bigcup_{i=1}^{\infty} I_i$$

下证 $I \lhd R$

①.$\forall a, b \in I, \exists N_1, N_2, \text{s.t. } a \in I_{N_1} \subset I_{N_1+1} \subset \cdots, b \in I_{N_2} \subset I_{N_2+1} \subset \cdots$，取 $N = \max\{N_1, N_2\}$，则 $a, b \in I_N \Longrightarrow a + b \in I_N \subset I$

②.$\forall a \in I, \exists N \in \mathbb{N}^*, \text{s.t. } a \in I_N$，对 $\forall r \in R, ra \in I_N \subset I$

所以 $I \lhd R$，由 R 是 *Noether* 环知 $\exists a_1, \cdots, a_m \in R, \text{s.t. } I = (a_1, \cdots, a_m)$，即 $a_1, \cdots, a_m \in I = \bigcup\limits_{i=1}^{\infty} I_i$，取 N 足够大使得 $a_1, \cdots, a_m \in I_N$，所以 $I \subseteq I_N \subseteq I_{N+1} \subseteq I$，所以

$$I_N = I_{N+1} = I$$

进而 $\forall n \geq N, I_n = I$ □

Exercise 5 设 R 是环，$c \in R$，求证

$$R[x]/(c) \cong \big(R/(c)\big)[x]$$

Proof $c = 0$ 时是平凡的，$c \neq 0$ 时，考虑环同态

$$\begin{gathered} \phi : R[x] \longrightarrow \big(R/(c)\big)[x] \\ a_n x^n + \cdots + a_1 x + a_0 \longmapsto \overline{a}_n x^n + \cdots + \overline{a}_1 x + \overline{a}_0 \end{gathered}$$

首先由定义可以看出它是一个满环同态，接下来证明 $\text{Ker}\phi = (c)$，设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$

$$\begin{aligned} f(x) \in \text{Ker}\phi &\iff \phi\big(f(x)\big) = 0 \iff \overline{a}_n = \cdots = \overline{a}_0 = \overline{0} \\ &\iff a_n, \cdots, a_0 \in (c) \iff c \mid a_i, 0 \leq i \leq n \\ &\iff c \mid f(x) \iff f(x) \in (c) \end{aligned}$$

且 ϕ 是满环同态，由环同态基本定理，我们有环同构

$$R[x]/(c) \cong \big(R/(c)\big)[x]$$

□

Exercise 6 设 R 是 *UFD*，$K = \text{Frac}(R)$，若 $f(x) \in R[x]$ 本原，证明

$$f(x)\text{在}R[x]\text{中不可约} \iff f(x)\text{在}K[x]\text{中不可约}$$

Proof $(\Longrightarrow)$: 证明逆否命题，假设 f 在 $K[x]$ 中可约，则 f 在 $K[x]$ 中存在非平凡分解 $f=gh$，其中 $g,h\in K[x]$，则通过谨慎通分，g,h 有本原分解，即 $\exists c_g,c_h\in K,g_0,h_0$ 本原，使得

$$g(x)=c_g g_0(x),h(x)=c_h h_0(x)\Longrightarrow f(x)=c_g c_h g_0(x)h_0(x)$$

由高斯引理知 g_0h_0 本原，又由 f 本原知 $c_gc_h\sim 1$，可不妨设 $c_gc_h=1$，所以 $f(x)=g_0(x)h_0(x)$，故 $f(x)$ 在 $R[x]$ 中可约

$(\Longleftarrow)$: 证明逆否命题，假设 f 在 $R[x]$ 中可约，则 f 在 $R[x]$ 中有非平凡分解 $f=gh$，其中 $g,h\in R[x]$，由 f 本原知，g,h 不是常值多项式，故 $\deg g,\deg h\geq 1$，此时 g,h 在 $K[x]$ 中非单位，因此在 $K[x]$ 中也有 $f=gh$，故 f 在 $K[x]$ 中也可约 $\square$

Exercise 7 设 R 是 *UFD*，$b\in R,g(x)=a_nx^n+\cdots+a_1x+a_0\in R[x]$，定义 $g(x+b)=a_n(x+b)^n+\cdots+a_1(x+b)+a_0$ 展开后视为 x 的多项式，则有

1. $g(x)$ 本原 $\Longleftrightarrow$ $g(x+b)$ 本原

2. $g(x)$ 在 $R[x]$ 中不可约 $\Longleftrightarrow$ $g(x+b)$ 在 $R[x]$ 中不可约

Proof 考虑环同态（嵌入）$\psi:R\hookrightarrow R[x],r\mapsto r$，由多项式环的泛性质知，存在唯一环同态 $\tilde{\psi}:R[x]\to R[x]$，满足 $\tilde{\psi}|_R=\psi,\tilde{\psi}(x)=x+b$，即

$$\begin{aligned}\tilde{\psi}:R[x]&\longrightarrow R[x]\\ r&\longmapsto r\\ x&\longmapsto x+b\end{aligned}$$

实际上，$\forall f(x)=a_nx^n+\cdots+a_1x+a_0\in R[x],\tilde{\psi}\big(f(x)\big)=a_n(x+b)^n+\cdots+a_1(x+b)+a_0=f(x+b)$，即 $\tilde{\psi}$ 将 $f(x)$ 打到 $f(x+b)$，接下来证明它是环同构，只需证明 $\tilde{\psi}$ 是双射即可

再次利用多项式环的泛性质，存在唯一环同态 $\theta:R[x]\to R[x]$，满足 $\theta|_R=\psi,\theta(x)=x-b$，即

$$\begin{aligned}\theta:R[x]&\longrightarrow R[x]\\ r&\longmapsto r\\ x&\longmapsto x-b\end{aligned}$$

实际上，$\forall f(x)=a_nx^n+\cdots+a_1x+a_0\in R[x],\theta\big(f(x)\big)=a_n(x-b)^n+\cdots+a_1(x-b)+a_0=f(x+b)$，即 $\tilde{\psi}$ 将 $f(x)$ 打到 $f(x-b)$

因为 $\tilde{\psi}\circ\theta(x)=\tilde{\psi}(x-b)=x-b+b=x,\tilde{\psi}\circ\theta(r)=r,\forall r\in R$，所以 $\tilde{\psi}\circ\theta=\mathrm{Id}_{R[x]}$，同理 $\theta\circ\tilde{\psi}=\mathrm{Id}_{R[x]}$，因此 $\tilde{\psi}$ 是双射，且 $\tilde{\psi}^{-1}=\theta$

这就证明了 $\tilde{\psi}$ 是双射，进而 $\tilde{\psi}$ 是环同构，回到本题：

(1).$(\Longrightarrow)$: 考虑逆否命题：假设 $g(x+b)$ 不是本原多项式，则 $\exists$ 素元 p，使得 p 是 $g(x+b)$ 所有系数的公因子，因此 $\exists g_1(x)\in R[x],\text{s.t. } g(x+b)=pg_1(x)$，前面已证 $\tilde{\psi}^{-1}=\theta$，所以

$$g(x)=\tilde{\psi}^{-1}\big(g(x+b)\big)=\theta(pg_1(x))=pg_1(x-b)$$

所以 $p \mid g(x)$，这与 $g(x)$ 本原矛盾！所以 $g(x+b)$ 是本原多项式

$(\Longleftarrow)$: 考虑逆否命题：假设 $g(x)$ 不是本原多项式，则 $\exists$ 素元 p，使得 p 是 $g(x)$ 所有系数的公因子，因此 $\exists g_2(x) \in R[x], \text{s.t. } g(x) = pg_2(x)$，所以

$$g(x+b) = \tilde{\psi}(pg_2(x)) = pg_2(x+b)$$

所以 $p \mid g(x+b)$，这与 $g(x+b)$ 是本原多项式矛盾！所以 $g(x)$ 是本原多项式

(2).$(\Longrightarrow)$: 考虑逆否命题：假设 $g(x+b)$ 在 $R[x]$ 中可约，则 $\exists m(x), n(x) \in R[x], \text{s.t. } g(x+b) = m(x)n(x)$，所以

$$g(x) = \tilde{\psi}^{-1}(g(x+b)) = \theta\big(m(x)n(x)\big) = m(x-b)n(x-b)$$

则 $g(x)$ 在 $R[x]$ 中可约

$(\Longleftarrow)$: 考虑逆否命题：假设 $g(x)$ 在 $R[x]$ 中可约，则 $\exists m(x), n(x) \in R[x], \text{s.t. } g(x) = m(x)n(x)$，所以

$$g(x+b) = \tilde{\psi}\big(m(x)n(x)\big) = m(x+b)n(x+b)$$

则 $g(x+b)$ 在 $R[x]$ 中可约 $\square$

Exercise 8 设 k 是域，$R = k[t]$，令 $S = \{f(t) \in R | f(t)\text{的}t^1\text{项系数为零}\} \subset R$，证明

1. $S \cong k[x,y]/(y^3 - x^2)$

2. $\operatorname{Frac}(S) = k(t)$

Proof (1). 首先我们有 $k[x,y] \cong k[y][x]$，只需将 $f(x,y) \in k[x,y]$ 视为系数属于 $k[y]$ 的 x 的一元多项式即可，考虑环同态

$$\begin{aligned} \phi : k[x,y] &\longrightarrow S \\ x &\longmapsto t^3 \\ y &\longmapsto t^2 \\ r &\longmapsto r, \forall r \in k \end{aligned}$$

即 ϕ 将 $\forall f(x,y) \in k[x,y]$ 映为 $f(t^3, t^2)$，首先它是满环同态，只需证明 $\forall n \geq 2, t^n$ 均有原像：因为 $t^2 = \phi(y), t^3 = \phi(x), \forall n = 2k, t^n = \phi(y^k), \forall n = 2k+1, t^n = \phi(xy^{k-1})$，故 ϕ 是满同态，下面证明 $\operatorname{Ker}\phi = (y^3 - x^2)$

设 $f(x,y) \in (y^3 - x^2)$，则 $\exists g(x,y) \in k[x,y], \text{s.t. } f(x,y) = g(x,y)(y^3 - x^2)$，所以

$$\phi\big(f(x,y)\big) = \phi\big(g(x,y)\big)\phi\big(y^3 - x^2\big) = \phi\big(g(x,y)\big) \cdot (t^6 - t^6) = 0$$

所以 $f(x,y) \in \operatorname{Ker}\phi$，进而 $(y^3 - x^2) \subseteq \operatorname{Ker}\phi$

设 $f(x,y) \in \operatorname{Ker}\phi$，则 $f(t^3, t^2) = 0$，我们可以将 $f(x,y)$ 视为系数属于 $k[x]$ 的 y 的一元多项式，因为 $x^2 - y^3$ 对 x 来说是首一多项式，所以可以对 $x^2 - y^3$ 做带余除法

$$f(x,y) = q(x,y)(x^2 - y^3) + r(x,y)$$

其中 $r(x,y)$ 对 x 的系数为 $0,1$，可设 $r(x,y)=r_1(y)x+r_0(y)$，由 $f(t^3,t^2)=0$ 知，$r_1(t^2)t^3+r_0(t^2)=0$，但是 $r_1(t^2)t^3$ 是 t 的奇数次幂，$r_0(t^2)$ 是 t 的偶数次幂，因此二者加起来等于零只能是 r_1,r_0 的系数为零，即 $r(x,y)=0$，所以 $f(x,y)=q(x,y)(x^2-y^3)\in(y^3-x^2)$，进而 $\mathrm{Ker}\phi\subseteq(y^3-x^2)$，故 $\mathrm{Ker}\phi=(y^3-x^2)$，结合 ϕ 是满同态，由环同态基本定理知

$$\begin{aligned}\tilde{\phi}:k[x,y]/(y^3-x^2)&\longrightarrow S\\ f(x,y)+(y^3-x^2)&\longmapsto f(t^3,t^2)\end{aligned}$$

(2). 考虑典范同态 $S\overset{\mathrm{can}}{\hookrightarrow}\mathrm{Frac}(S)$ 关于环单同态（嵌入）$\pi:S\hookrightarrow k(t),f(t)\mapsto f(t)=\frac{f(t)}{1}$ 的泛性质：存在唯一的域嵌入 $\tilde{\pi}:\mathrm{Frac}(S)\to k(t)$，满足 $\tilde{\pi}\left(\frac{f(t)}{g(t)}\right)=\pi\big(f(t)\big)\pi\big(g(t)\big)^{-1}$

$$\begin{tikzcd} S \arrow[rr, hook, "\pi"] \arrow[dr, hook, "\mathrm{can}"'] & & k(t) \\ & \mathrm{Frac}(S) \arrow[ur, "\tilde{\pi}"'] & \end{tikzcd}$$

则 $\tilde{\pi}$ 是单射，下证明 $\tilde{\pi}$ 是满射：显然有 $\tilde{\pi}|_k=\mathrm{Id}_k$，因为

$$\tilde{\pi}\left(\frac{t^3}{t^2}\right)=\pi(t^3)\pi(t^2)^{-1}=\frac{t^3}{t^2}=t\Longrightarrow t^n=\frac{t^{3n}}{t^{2n}}=\pi(t^{3n})\pi(t^{2n})^{-1}=\tilde{\pi}\left(\frac{t^{3n}}{t^{2n}}\right)$$

所以 $\forall\frac{f(t)}{g(t)}\in k(t)$，设 $f(t)=a_nt^n+\cdots+a_1t+a_0,g(t)=b_mt^m+\cdots+b_1t+b_0\in k[t]$ ，则

$$\begin{aligned}f(t)&=\tilde{\pi}\left(a_n\frac{t^{3n}}{t^{2n}}+\cdots+a_1\frac{t^3}{t^2}+a_0\right)\\&=\tilde{\pi}\left(\frac{a_nt^{3n}+\cdots+a_1t^{2n+1}+a_0t^{2n}}{t^{2n}}\right)\\&=\pi(a_nt^{3n}+\cdots+a_1t^{2n+1}+a_0t^{2n})\pi(t^{2n})^{-1}\end{aligned}$$

同理

$$g(t)=\pi(b_mt^{3m}+\cdots+b_1t^{2m+1}+b_0t^{2m})\pi(t^{2m})^{-1}$$

所以

$$\begin{aligned}\frac{f(t)}{g(t)}&=f(t)g(t)^{-1}\\&=\pi(a_nt^{3n}+\cdots+a_1t^{2n+1}+a_0t^{2n})\pi(t^{2m})\pi(b_mt^{3m}+\cdots+b_1t^{2m+1}+b_0t^{2m})^{-1}\pi(t^{2n})^{-1}\\&=\pi(a_nt^{3n+2m}+\cdots+a_1t^{2n+2m+1}+a_0t^{2n+2m})\pi(b_mt^{3m+2n}+\cdots+b_1t^{2m+2n+1}+b_0t^{2m+2n})^{-1}\end{aligned}$$

即 $\forall\frac{f(x)}{g(x)}\in k(t)$，均可以写为 $\pi(a)\pi(x)^{-1}=\tilde{\pi}\left(\frac{a}{x}\right)$，故 $\tilde{\pi}$ 是满射，所以 $\tilde{\pi}$ 是同构！即

$$\mathrm{Frac}(S)\cong k(t)$$

$\square$