近世代数 (H) 第四周作业

涂嘉乐 PB23151786

2025 年 3 月 21 日

Exercise 1 写出 $K=\mathbb{R}[x]/(x^2+1)$ 的乘法表，K 是否同构于 $\mathbb{C}$?

Solution 以下 $m,n,a_1,b_1,a_2,b_2\in\mathbb{R},u=\overline{x}\in K$

	m	a_1u+b_1
n	mn	na_1u+nb_1
a_2u+b_2	ma_2u+mb_2	$(a_2b_1+a_1b_2)u+(b_1b_2-2a_1a_2)$

表 1: $\mathbb{R}[x]/(x^2+1)$ 的乘法表

K 同构于 $\mathbb{C}$：首先证明 $\mathbb{R}[x]/(x^2+2)\cong\mathbb{C}$，因为 $\forall\overline{f(x)}\in\mathbb{R}[x]/(x^2+1)$ 都可以写为 $a+bu,a,b\in\mathbb{R}$ 的形式，其中 $u=\overline{x}$，我们考虑映射

$$\begin{aligned}\varphi:\mathbb{R}[x]/(x^2+1)&\longrightarrow\mathbb{C}\\ a+bu&\longmapsto a+bi\end{aligned}$$

下面验证 φ 是同构：

(1). 同态

$(a).\varphi(1)=1$

$(b).\forall a+bu,c+du\in\mathbb{R}[x]/(x^2+1)$

$$\begin{aligned}\varphi\big((a+bu)+(c+du)\big)&=\varphi\big((a+c)+(b+d)u\big)=(a+c)+(b+d)i\\&=(a+bi)+(c+di)=\varphi(a+bu)+\varphi(c+du)\end{aligned}$$

$$\begin{aligned}\varphi\big((a+bu)(c+du)\big)&=\varphi\big(ac+(ad+bc)u+bdu^2\big)=\varphi\big(ac-bd+(ad+bc)u\big)\\&=(ac-bc)+(ad+bc)i=(a+bi)(c+di)=\varphi(a+bu)\varphi(c+du)\end{aligned}$$

(2). 双射

(a). 单射：设 $a+bu\in\mathrm{Ker}\varphi$，则 $\varphi(a+bu)=a+bi=0\Rightarrow a=b=0$，所以 $\mathrm{Ker}\varphi=\{0\}$，故为单射

(b). 满射：对 $\forall a+bi\in\mathbb{C}$，均有原像 $a+bu\in\mathbb{R}[x]/(x^2+1)$

综上 φ 确实是同构，我们要证明 $K\cong\mathbb{C}$，只需证明 $K\cong\mathbb{R}[x]/(x^2+1)$，考虑域同态

$$\begin{aligned}\theta:\mathbb{R}&\longrightarrow\mathbb{R}[x]/(x^2+2)\\ a&\longmapsto a\end{aligned}$$

右边的 a 实际上为 $a+(x^2+2)$，但仍记为 a，我们使用域同态 θ 的泛性质：首先我们还有域同态

$$\begin{aligned}\delta:\mathbb{R}&\longrightarrow\mathbb{R}[x]/(x^2+1)\\ a&\longmapsto a\end{aligned}$$

右边的 a 实际上为 $a+(x^2+1)$，但仍记为 a，在 $\mathbb{R}[x]/(x^2+1)$ 中，$(\sqrt{2}u)^2+2=2(u^2+1)=0\Rightarrow\sqrt{2}u\in$

$\mathrm{Root}_{\mathbb{R}[x]/(x^2+1)}(x^2+2)$，则存在唯一的域同态

$$\delta' : \mathbb{R}[x]/(x^2+2) \longrightarrow \mathbb{R}[x]/(x^2+1)$$
$$a \longmapsto a$$
$$u \longmapsto \sqrt{2}u$$

且 δ' 是同构，只需补充证明双射：

单射：设 $a+bu \in \mathrm{Ker}\delta'$，则 $\delta(a+bu) = a+\sqrt{2}bu = 0 \Rightarrow a=b=0$，即 $\mathrm{Ker}\delta' = \{0\}$

满射：对 $\forall a+bu \in \mathbb{R}[x]/(x^2+1)$，$\delta'(a+\frac{b}{\sqrt{2}}u) = a+bu$，即原像均存在

综上，δ' 确实是域同构，所以 $\mathbb{R}[x]/(x^2+2) \cong \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ □

Exercise 2 求证：$\mathbb{F}_4$ 与 $\mathbb{Z}_4$ 不同构

Proof 为方便表示，设 $\mathbb{Z}_4 = \{0,1,2,3\}, \mathbb{F}_4 = \{\overline{0},\overline{1},u,u+\overline{1}\}$，假设存在环同构 $\theta : \mathbb{Z}_4 \to \mathbb{F}_4$，则 $\theta(1)=\overline{1}, \theta(0)=\overline{0}$，由环同构是双射知，只有两种可能：

$$\begin{cases} \theta_1(2) = u \\ \theta_1(3) = u+\overline{1} \end{cases} \qquad \begin{cases} \theta_2(2) = u+\overline{1} \\ \theta_2(3) = u \end{cases}$$

因为在 $\mathbb{Z}_4$ 中有 $2\cdot 2 = 0$，所以 $\theta(2)\cdot\theta(2) = \theta(0) = \overline{0}$，但对于 θ_1 而言，$\theta^2(2) = u^2 = u+\overline{1} \neq \overline{0}$；对于 θ_2 而言，$\theta^2(2) = (u+\overline{1})^2 = u \neq \overline{0}$，无论那种情况均不是同构，所以 $\mathbb{F}_4$ 与 $\mathbb{Z}_4$ 不同构 □

Exercise 3 在 $\mathbb{F}_3[x]$ 中，求出 $a(x)(\overline{1}+\overline{2}x) + b(x)(x^2+\overline{1}) = 1$ 中的 $a(x), b(x)$

Solution 因为 $(x^2+\overline{1}) = (\overline{2}x+\overline{1})(\overline{2}x+\overline{2})+\overline{2}$，两边同乘 $\overline{2}$ 得

$$\overline{2}(x^2+\overline{1}) + (\overline{2}x+\overline{2})(\overline{2}x+\overline{1}) = 1$$

则 $a(x) = \overline{2}x+\overline{2}, b(x) = \overline{2}$ □

Exercise 4 计算 $\mathbb{F}_9$ 的乘法表

Solution $\mathbb{F}_9 = \{\overline{0},\overline{1},\overline{2},u,\overline{1}+u,\overline{2}+u,\overline{2}u,\overline{1}+2u,\overline{2}+2u\}$，其中 $u^2 = \overline{-1} = \overline{2}$

	$\overline{0}$	$\overline{1}$	$\overline{2}$	u	$\overline{1}+u$	$\overline{2}+u$	$\overline{2}u$	$\overline{1}+\overline{2}u$	$\overline{2}+\overline{2}u$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	u	$\overline{1}+u$	$\overline{2}+u$	$\overline{2}u$	$\overline{1}+\overline{2}u$	$\overline{2}+\overline{2}u$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$	$\overline{2}u$	$\overline{2}+\overline{2}u$	$\overline{1}+\overline{2}u$	u	$\overline{2}+u$	$\overline{1}+\overline{u}$
u	0	u	$\overline{2}u$	$\overline{2}$	$\overline{2}+u$	$\overline{2}+\overline{2}u$	$\overline{1}$	$\overline{1}+u$	$\overline{1}+\overline{2}u$
$\overline{1}+u$	$\overline{0}$	$\overline{1}+u$	$\overline{2}+\overline{2}u$	$\overline{2}+u$	$\overline{2}u$	$\overline{1}$	$\overline{1}+\overline{2}u$	$\overline{2}$	u
$\overline{2}+u$	$\overline{0}$	$\overline{2}+u$	$\overline{1}+\overline{2}u$	$\overline{2}+\overline{2}u$	$\overline{1}$	u	$\overline{1}+u$	$\overline{2}u$	$\overline{2}$
$\overline{2}u$	$\overline{0}$	$\overline{2}u$	u	$\overline{1}$	$\overline{1}+\overline{2}u$	$\overline{1}+u$	$\overline{2}$	$\overline{2}+\overline{2}u$	$\overline{2}+u$
$\overline{1}+\overline{2}u$	$\overline{0}$	$\overline{1}+\overline{2}u$	$\overline{2}+u$	$\overline{1}+u$	$\overline{2}$	$\overline{2}u$	$\overline{2}+\overline{2}u$	u	$\overline{1}$
$\overline{2}+\overline{2}u$	$\overline{0}$	$\overline{2}+\overline{2}u$	$\overline{1}+u$	$\overline{1}+\overline{2u}$	u	$\overline{2}$	$\overline{2}+u$	$\overline{1}$	$\overline{2}u$

表 2: $\mathbb{F}_9$ 的乘法表

Exercise 5 构造域同构 $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+\overline{1}) \xrightarrow{\sim} \mathbb{F}_9'' = \mathbb{F}_3[x]/(x^2+\overline{2}x+\overline{2})$

Solution 考虑域同态

$$\begin{aligned}\theta:\mathbb{F}_3&\longrightarrow\mathbb{F}_3/(x^2+\overline{1})=\mathbb{F}_9\\ a&\longmapsto a\end{aligned}$$

右边的 a 实际上为多项式同余类 $a+(x^2+1)$，但为方便表示仍记为 a，我们使用域同态 θ 的泛性质：首先我们还有域同态

$$\begin{aligned}\delta:\mathbb{F}_3&\longrightarrow\mathbb{F}_3/(x^2+\overline{2}x+\overline{2})=\mathbb{F}_9''\\ a&\longmapsto a\end{aligned}$$

右边的 a 实际上为多项式同余类 $a+(x^2+\overline{2}x+\overline{2})$，但为方便表示仍记为 a，我们需要在 $\mathbb{F}_9''$ 中找到元素 a, s.t. $a\in\mathrm{Root}_{\mathbb{F}_9''}(x^2+\overline{1})$，因为在 $\mathbb{F}_9''$ 中，我们有

$$(x^2+1)=(x+u+1)(x+2u+2)$$

所以 $\mathrm{Root}_{\mathbb{F}_9''}(x^2+\overline{1})=\{u+1,2u+2\}$，所以我们有两个域同态：

$$\begin{aligned}\delta_1:\mathbb{F}_9&\longrightarrow\mathbb{F}_9''\\ \overline{0},\overline{1},\overline{2}&\longmapsto\overline{0},\overline{1},\overline{2}\\ u&\longmapsto u+1\end{aligned}$$

$$\begin{aligned}\delta_2:\mathbb{F}_9&\longrightarrow\mathbb{F}_9''\\ \overline{0},\overline{1},\overline{2}&\longmapsto\overline{0},\overline{1},\overline{2}\\ u&\longmapsto 2u+2\end{aligned}$$

我们还需证明 δ_1,δ_2 是域同构，即证明它们是双射

单射：设 $a+bu\in\mathrm{Ker}\delta_1$，则 $\delta_1(a+bu)=(a+b)+bu=\overline{0}$，故 $b=\overline{0}\Rightarrow a=\overline{0}$，所以 $\mathrm{Ker}\delta_1=\{0\}$，$\delta_1$ 是单射

设 $c+du\in\mathrm{Ker}\delta_2$，则 $\delta_2(c+du)=(c+2d)+2du=\overline{0}$，故 $d=\overline{0}\Rightarrow c=\overline{0}$，所以 $\mathrm{Ker}\delta_2=\{0\}$，$\delta_2$ 是单射

满射：对 $\forall a+bu\in\mathbb{F}_9''$，因为 $\delta_1(a-b+bu)=a+bu,\delta_2(a+2b+2bu)=a+bu$，故 δ_1,δ_2 是满射

综上，δ_1,δ_2 确实是域同构 $\square$

Exercise 6 证明：$\mathbb{Z}[\sqrt{-2}]$ 是 *ED*，进而是 *PID*

Proof 考虑 *size function*

$$\begin{aligned}N:\mathbb{Z}[\sqrt{-2}]^\times&\longrightarrow\mathbb{N}\\ a+b\sqrt{-2}&\longmapsto a^2+2b^2\end{aligned}$$

首先我们有

$$\begin{aligned}N\big((a+b\sqrt{-2})(c+d\sqrt{-2})\big)&=N\big(ac-2bd+(ad+bc)\sqrt{-2}\big)\\ &=(ac-2bd)^2+2(ad+bc)^2=(ac)^2-4abcd+4(bd)^2+2(ad)^2+2(bc)^2+4abcd\\ &=(ac)^2+2(ad)^2+2(bc)^2+4(bd)^2=(a^2+2b^2)(c^2+2d^2)\\ &=N(a+b\sqrt{-2})N(c+d\sqrt{-2})\end{aligned}$$

对 $\forall x,y\in\mathbb{Z}[\sqrt{-2}]^\times$，则 $\exists\alpha,\beta\in\mathbb{Q}$, s.t.

$$\frac{x}{y}=\alpha+\beta\sqrt{-2}$$

则 $\exists m,n\in\mathbb{Z}$, s.t. $|m-\alpha|\le\frac{1}{2},|n-\beta|\le\frac{1}{2}$，则

$$\frac{x}{y}=\alpha+\beta\sqrt{-2}=(\alpha-m)+(\beta-n)\sqrt{-2}+m+n\sqrt{-2}$$

即
$$x=(m+n\sqrt{-2})y+[(\alpha-m)+(\beta-n)\sqrt{-2}]y$$
记 $r=[(\alpha-m)+(\beta-n)\sqrt{-2}]y=x-(m+n\sqrt{-2})y\in\mathbb{Z}[\sqrt{-2}]$，因为

$$\begin{aligned}N(r)&=N\big((\alpha-m)+(\beta-n)\sqrt{-2}\big)N(y)\\&=\left[(\alpha-m)^2+2(\beta-n)^2\right]N(y)\\&\le\frac{3}{4}N(y)<N(y)\end{aligned}$$

最后一步小于号是因为 $y\neq0\Rightarrow N(y)>0$，由 x,y 的任意性知，$\mathbb{Z}[\sqrt{-2}]$ 是 *ED*，而 *ED* 是 *PID*，故 $\sqrt{-2}$ 是 *PID* $\square$

Exercise 7 证明：在 $\mathbb{Z}[\sqrt{-3}]$ 中，$(2,1+\sqrt{-3})=(2)+(1+\sqrt{-3})$ 是素理想，但不是主理想

Proof 因为 $(2,1+\sqrt{-3})$ 的素理想 $\iff$ $\mathbb{Z}[\sqrt{-3}]/(2,1+\sqrt{-3})$ 是整环，下面证明 $\mathbb{Z}[\sqrt{-3}]/(2,1+\sqrt{-3})$ 是整环，记 $(2,1+\sqrt{-3})=(p)$，设 $a+b\sqrt{-3}+(p)\in\mathbb{Z}[\sqrt{-3}]/(p)$，其中 $a,b\in\mathbb{Z}$，则

$$a+b\sqrt{-3}+(p)=(a-b)+b(1+\sqrt{-3})+(p)=a-b+(p)$$

用 $(a-b)'$ 表示 $a-b$ 被 2 除的余数（即为 $0,1$），所以

$$a-b+(p)=(a-b)'+(p)$$

因此 $\mathbb{Z}[\sqrt{-3}]\subseteq\{(p),1+(p)\}$，且显然有 $\{(p),1+(p)\}\subseteq\mathbb{Z}[\sqrt{-3}]/(p)$，所以 $\mathbb{Z}[\sqrt{-3}]/(p)=\{(p),1+(p)\}\cong\mathbb{F}_2$，故为整环，所以 $(2,1+\sqrt{-3})$ 为素理想

假设 $(2,1+\sqrt{-3})$ 为主理想，则 $\exists x\in\mathbb{Z}[\sqrt{-3}],\text{s.t. }(x)=(2,1+\sqrt{-3})$，则 $\exists m\in\mathbb{Z}[\sqrt{-3}],\text{s.t. }xm=2$，两边同时取模长得
$$|x|^2\cdot|m|^2=4$$
设 $x=u+v\sqrt{-3}$，则 $|x|^2=u^2+3v^2\le4$

若 $u^2=v^2=1$，则在相伴意义下 $x=1+\sqrt{-3},1-\sqrt{-3}$，则 $m=\frac{1\pm\sqrt{-3}}{2}\notin\mathbb{Z}[\sqrt{-3}]$，矛盾！

若 $u^2=1,v^2=0$，则在相伴意义下 $x=1$，但由上分析知 $1\notin(2,1+\sqrt{-3})$，矛盾！

若 $u^2=0,v^2=1$，则在相伴意义下 $x=\sqrt{-3}$，进而 $x(1+\sqrt{-3})-x=1\in(2,1+\sqrt{-3})$，矛盾！

若 $u^2=v^2=0$，则 $(0)=(2,1+\sqrt{-3})$ 显然矛盾！

综上，$(2,1+\sqrt{-3})$ 是素理想，但不是主理想 $\square$

Exercise 8 证明：$\mathrm{Frac}(\mathbb{Z}[\omega])\xrightarrow{\sim}\mathbb{Q}(\sqrt{-3})$，其中 $\omega=e^{\frac{2}{3}\pi i}$

Proof 首先，对 $\forall x\in\mathrm{Frac}(\mathbb{Z}[\omega]),\exists a,b,c,d\in\mathbb{Z},\text{s.t. }x=\frac{a+b\omega}{c+d\omega}$，因为 $\overline{\omega}=\omega^2=-\omega-1\in\mathbb{Z}[\omega]$，考虑映射

$$\begin{aligned}\varphi:\mathrm{Frac}(\mathbb{Z}[\omega])&\longrightarrow\mathbb{Q}(\sqrt{-3})\\\frac{a+b\omega}{c+d\omega}&\longmapsto\frac{a+b\omega}{c+d\omega}=\frac{\left(a-\frac{b}{2}\right)+\frac{b\sqrt{-3}}{2}}{\left(c-\frac{d}{2}\right)+\frac{d\sqrt{-3}}{2}}\end{aligned}$$

下面验证 φ 确实是合理的，即 $\frac{\left(a-\frac{b}{2}\right)+\frac{b\sqrt{-3}}{2}}{\left(c-\frac{d}{2}\right)+\frac{d\sqrt{-3}}{2}}\in\mathbb{Q}(\sqrt{-3})$，这是因为

$$\frac{\left(a-\frac{b}{2}\right)+\frac{b\sqrt{-3}}{2}}{\left(c-\frac{d}{2}\right)+\frac{d\sqrt{-3}}{2}}=\frac{2(ac+bd)-(ad+bc)}{2(c^2+d^2-cd)}+\frac{bc-ad}{2(c^2+d^2-cd)}\sqrt{-3}\in\mathbb{Q}(\sqrt{-3})$$

接下来证明 φ 是同态

(a). 同构

(i). $1_{\mathrm{Frac}(\mathbb{Z}[\omega])}=\frac{1+0\omega}{1+0\omega},\varphi(1_{\mathrm{Frac}(\mathbb{Z})[\omega]})=\frac{1}{1}=1$

(ii). 对任意 $\frac{a_1+b_1\omega}{c_1+d_1\omega},\frac{a_2+b_2\omega}{c_2+d_2\omega}\in\mathrm{Frac}(\mathbb{Z}[\omega])$，由于左右两侧通分规则完全一致，所以

$$\varphi\left(\frac{a_1+b_1\omega}{c_1+d_1\omega}+\frac{a_2+b_2\omega}{c_2+d_2\omega}\right)=\frac{a_1+b_1\omega}{c_1+d_1\omega}+\frac{a_2+b_2\omega}{c_2+d_2\omega}=\varphi\left(\frac{a_1+b_1\omega}{c_1+d_1\omega}\right)+\varphi\left(\frac{a_2+b_2\omega}{c_2+d_2\omega}\right)$$

(iii). 对任意 $\frac{a_1+b_1\omega}{c_1+d_1\omega},\frac{a_2+b_2\omega}{c_2+d_2\omega}\in\mathrm{Frac}(\mathbb{Z}[\omega])$

$$\varphi\left(\frac{a_1+b_1\omega}{c_1+d_1\omega}\cdot\frac{a_2+b_2\omega}{c_2+d_2\omega}\right)=\frac{a_1+b_1\omega}{c_1+d_1\omega}\cdot\frac{a_2+b_2\omega}{c_2+d_2\omega}=\varphi\left(\frac{a_1+b_1\omega}{c_1+d_1\omega}\right)\varphi\left(\frac{a_2+b_2\omega}{c_2+d_2\omega}\right)$$

(b). 双射

单射：因为 $\varphi\left(\frac{a+b\omega}{c+d\omega}\right)=\frac{\left(a-\frac{b}{2}\right)+\frac{b\sqrt{-3}}{2}}{\left(c-\frac{d}{2}\right)+\frac{d\sqrt{-3}}{2}}=0\iff a=b=0\iff\frac{a+b\omega}{c+d\omega}=0$，所以 $\mathrm{Ker}\varphi=\{0\}$

满射：对任意 $\frac{b}{a}+\frac{d}{c}\sqrt{-3}\in\mathbb{Q}(\sqrt{-3})$，其中 $a,b,c,d\in\mathbb{Z},a,c\neq0$，且 $(a,b)=(c,d)=1$，我们有

$$\frac{b}{a}+\frac{d}{c}\sqrt{-3}=\frac{bc+ad\sqrt{-3}}{ac}=\frac{-3ad+bc\sqrt{-3}}{ac\sqrt{-3}}=\frac{\left(-3ad+bc-\frac{2bc}{2}\right)+\frac{2bc\sqrt{-3}}{2}}{\left(ac-\frac{2ac}{2}\right)+\frac{2ac\sqrt{-3}}{2}}$$

所以我们有

$$\varphi\left(\frac{-3ad+bc+2bc\omega}{ac+2ac\omega}\right)=\frac{b}{a}+\frac{d}{c}\sqrt{-3}$$

故满射得证，则 φ 确实是同构 □

Exercise 9 证明：$\mathbb{Z}[\omega]$ 是 *ED*，进而是 *PID*

Proof 考虑 *size function*（其实还是复数模长的平方）

$$\begin{aligned}N:\mathbb{Z}[\omega]&\longrightarrow\mathbb{N}\\a+b\omega&\longmapsto a^2+b^2-ab\end{aligned}$$

又因为

$$\frac{a+b\omega}{c+d\omega}=\frac{(ac+bd-ad)+(bc-ad)\omega}{c^2+d^2-cd}$$

所以对 $\forall x,y\in\mathbb{Z}[\omega]^\times,\exists\alpha,\beta\in\mathbb{Q},\text{s.t.}$

$$\frac{x}{y}=\alpha+\beta\omega$$

则 $\exists m,n\in\mathbb{Z},\text{s.t.}\ |m-\alpha|\leq\frac{1}{2},|n-\beta|\leq\frac{1}{2}$，则

$$\frac{x}{y}=(m+n\omega)+[(\alpha-m)+(\beta-n)\omega]$$

即

$$x=(m+n\omega)y+[(\alpha-m)+(\beta-n)\omega]y$$

记 $r=[(\alpha-m)+(\beta-n)\omega]y$，则

$$\begin{aligned}N(r)&=N\big([(\alpha-m)+(\beta-n)\omega]\big)N(y)\\&=[(\alpha-m)^2+(\beta-n)^2-(\alpha-m)(\beta-n)]N(y)\\&\leq\left[(\alpha-m)^2+(\beta-n)^2+\frac{(\alpha-m)^2+(\beta-n)^2}{2}\right]N(y)\\&\leq\frac{3}{4}N(y)<N(y)\end{aligned}$$

最后一步不等号要求 $N(y)>0$，因为 $N(a+b\omega)=0$ 时，$a^2+b^2-ab=0$，若 $b\neq 0$，则 $\left(\frac{a}{b}\right)^2-\frac{a}{b}+1=0$，但该方程无实数解；若 $b=0$，则 $a=b=0$，则 $\omega=0$，因此 $y\neq 0$ 时，$N(y)>0$

综上，$\mathbb{Z}[\omega]$ 是 *ED*，进而是 *PID* $\square$

Exercise 10 证明：(1). $2\in\mathbb{Z}[\omega]$ 是素元；(2). $U(\mathbb{Z}[\omega])=\{\pm 1,\pm\omega,\pm\omega^2\}$

Proof

(2). 首先注意到 $1^2=1,(-1)^2=1,\omega\cdot\omega^2=1,(-\omega)\cdot(-\omega^2)=1$，所以 $\{\pm 1,\pm\omega,\pm\omega^2\}\subseteq\mathbb{Z}[\omega]$；其次对 $\forall 0\neq x\in\mathbb{Z}[\omega]\backslash\{\pm 1,\pm\omega,\pm\omega^2\}$，我们证明 x 不可能是单位，这就证明了我们想要的结果

假设 $\exists a,b\in\mathbb{Z}[\omega],\text{s.t. } ab=1$，则 $|a|^2\cdot|b|^2=1$，由任意 $m+n\omega\in\mathbb{Z}[\omega]$ 的模平方为 $m^2+n^2-mn\in\mathbb{Z}$ 知，只能是 $|a|=|b|=1$，因为 $1+\omega=\frac{1+\sqrt{-3}}{2}=-\omega^2,-1-\omega=\omega^2$，我们排除这两种情况

Case 1.$x=1-\omega,-1+\omega$，即 $x=\pm\frac{3-\sqrt{-3}}{2}$，则 $|x|^2=3>1$，故不是单位

Case 2.$x=m+n\omega,m,n\neq\pm 1$，则 $|x|^2=m^2+n^2-mn$，不妨设 $m\geq n$，则 $m^2+n^2-mn\geq n^2>1$，故也不是单位

综上 $\forall 0\neq x\in\mathbb{Z}[\omega]\backslash\{\pm 1,\pm\omega,\pm\omega^2\}$ 均不是单位，所以

$$U(\mathbb{Z}[\omega])=\{\pm 1,\pm\omega,\pm\omega^2\}$$

(1). 因为上题得出 $\mathbb{Z}[\omega]$ 是 *PID*，*PID* 中素元与不可约元等价，所以只需证明 $2\in\mathbb{Z}[\omega]$ 不可约，假设 $a,b\notin U(\mathbb{Z}[\omega]),\text{s.t. } 2=ab$，取模长可得 $|a|^2\cdot|b|^2=4$，所以只需对 $|a|$ 讨论即可，我们将模长平方 <4 的 $\mathbb{Z}[\omega]$ 中的元素全部列出（等于 4 时，$|b|=1$ 为单位，故为平凡分解），即

$$0,\pm 1,\pm 2,1+\omega,-1-\omega,1-\omega,-1+\omega,2+\omega,-2-\omega,1+2\omega,-1-2\omega$$

Case 1. $a=0,\pm 1,\pm 2$：$a=0$ 时矛盾，$a=\pm 1,\pm 2$ 时为平凡分解

Case 2. $a=1+\omega,-1-\omega$：它们两个是单位，故为平凡分解

Case 3. $a=1-\omega,-1+\omega,1+2\omega,-1-2\omega$：它们的模长平方均为 3，但是 $|a|^2|b|^2=4\Rightarrow|a|^2\mid 4$，矛盾！

综上，$2\in\mathbb{Z}[\omega]$ 没有非平凡分解，即它是不可约元，也是素元 $\square$

Exercise 11 设 $F=\mathbb{Q}(\sqrt{-3})$，求 $\mathcal{O}_F$

Proof 因为 $\omega=\frac{-1+\sqrt{-3}}{2}\in\mathbb{Q}(\sqrt{-3})$，且 ω 是 $x^2+x+1=0$ 的解，所以 $\omega\in\mathcal{O}_F$，且 1 是 $x-1=0$ 的解，所以 $1\in\mathcal{O}_F$，由环对加法、乘法封闭知 $\forall m+n\omega\in\mathbb{Z}[\omega],m+n\omega\in\mathcal{O}_F$，即 $\mathbb{Z}[\omega]\subseteq\mathcal{O}_F$

对 $\forall\alpha\in\mathcal{O}_F\subseteq\mathbb{Q}(\sqrt{-3})$，由于 $\mathbb{Q}(\sqrt{-3})\cong\mathrm{Frac}(\mathbb{Z}[\omega])$，可设 $\alpha=\frac{p}{q}$，其中 $p,q\in\mathbb{Z}[\omega]$，由 $\mathbb{Z}[\omega]$ 是 *ED*⇒*PID*⇒*UFD*，我们可以在相伴意义下设 $\gcd(p,q)=1$，因为 $\alpha\in\mathcal{O}_F$，所以存在

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{Z}[x]$$

满足 $f(\alpha)=0$，代入方程，两边同时乘以 q^n 得

$$p^n+a_{n-1}p^{n-1}q+\cdots+a_1pq^{n-1}+a_0q^n=0$$

若 $q\notin U(\mathbb{Z}[\omega])$，则 $\exists p'\in\mathbb{Z}[\omega]$ 素元，使得 $p'\mid q$，所以 $p'\mid q\mid p^n\Rightarrow p'\mid p$，因此 $p'\mid\gcd(p,q)$，这与我们假设 $\gcd(p,q)=1$ 矛盾！所以 $q\in U(\mathbb{Z}[\omega])$，因此 $\alpha=\frac{p}{q}=pq^{-1}\in\mathbb{Z}[\omega]$，故 $\mathcal{O}_F\subseteq\mathbb{Z}[\omega]$ $\square$

Exercise 12 证明

$$\begin{aligned}\sigma:\mathbb{Q}(\sqrt{2})&\longrightarrow\mathbb{Q}(\sqrt{2})\\ a+b\sqrt{2}&\longmapsto a-b\sqrt{2}\end{aligned}$$

是域同构

Proof

(1). 同态

(i). $\sigma(1)=1$

(ii). 设 $a+b\sqrt{2}, c+d\sqrt{2}\in\mathbb{Q}(\sqrt{2})$，则

$$\begin{aligned}\sigma\big((a+b\sqrt{2})+(c+d\sqrt{2})\big)&=\sigma\big((a+c)+(b+d)\sqrt{2}\big)=(a+c)-(b+d)\sqrt{2}\\&=(a-b\sqrt{2})+(c-d\sqrt{2})=\sigma(a+b\sqrt{2})+\sigma(c+d\sqrt{2})\end{aligned}$$

(iii) 设 $a+b\sqrt{2}, c+d\sqrt{2}\in\mathbb{Q}(\sqrt{2})$，则

$$\begin{aligned}\sigma\big((a+b\sqrt{2})(c+d\sqrt{2})\big)&=\sigma\big((ac+2bd)+(ad+bc)\sqrt{2}\big)=(ac+2bd)-(ad+bc)\sqrt{2}\\&=(a-b\sqrt{2})(c-d\sqrt{2})=\sigma(a+b\sqrt{2})\sigma(c+d\sqrt{2})\end{aligned}$$

(2). 双射

单射：设 $a+b\sqrt{2}\in\mathrm{Ker}\sigma$，则 $\sigma(a+b\sqrt{2})=a-b\sqrt{2}=0\Rightarrow a=b=0\Rightarrow\mathrm{Ker}\sigma=\{0\}$

满射：对 $\forall a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$，我们有 $\sigma(a-b\sqrt{2})=a+b\sqrt{2}$

综上所述，σ 为同构 $\square$

Exercise 13 证明：$\mathbb{Z}(\sqrt{2})$ 是 *ED*

Proof 考虑 *size function*

$$\begin{aligned}N:\mathbb{Z}[\sqrt{2}]&\longrightarrow\mathbb{N}\\a+b\sqrt{2}&\longmapsto|(a+b\sqrt{2})\cdot\sigma(a+b\sqrt{2})|=|a^2-2b^2|\end{aligned}$$

对 $\forall x,y\in\mathbb{Z}(\sqrt{2}),\exists\alpha,\beta\in\mathbb{Q},\text{s.t.}$

$$\frac{x}{y}=\alpha+\beta\sqrt{2}$$

取 $m,n\in\mathbb{Z},\text{s.t.}\ |m-\alpha|\le\frac{1}{2},|n-\beta|\le\frac{1}{2}$，则

$$x=y(m+n\sqrt{2})+y[(\alpha-m)+(\beta-n)\sqrt{2}]$$

取 $r=y[(\alpha-m)+(\beta-n)\sqrt{2}]$，则 $r=x-y(m+n\sqrt{2})\in\mathbb{Z}(\sqrt{2})$，且

$$\begin{aligned}N(r)=N(y[(\alpha-m)+(\beta-n)\sqrt{2}])&=N(y)N([(\alpha-m)+(\beta-n)\sqrt{2}])\\&\le N(y)|(\alpha-m)^2-2(\beta-n)^2|\\&\le N(y)\max\{(\alpha-m)^2,2(\beta-n)^2\}\\&\le\frac{1}{2}N(y)<N(y)\end{aligned}$$

所以 $\mathbb{Z}(\sqrt{2})$ 是 *ED* $\square$

Exercise 14 验证环同态

$$\begin{aligned}\mathbb{Z}[i]&\xrightarrow{\phi}\mathbb{F}_2\\m+ni&\longmapsto\overline{m+n}\end{aligned}$$

并求 $\mathrm{Ker}\phi$

Proof

(1). $\phi(1)=\overline{1}$

(2). $\forall a+bi, c+di \in \mathbb{Z}[i]$

$$\begin{aligned}\phi\big((a+bi)+(c+di)\big) &= \phi\big((a+c)+(b+d)i\big) = \overline{a+c+b+d} \\ &= \overline{a+b}+\overline{c+d} = \phi(a+bi)+\phi(c+di)\end{aligned}$$

(3). $\forall a+bi, c+di \in \mathbb{Z}[i]$

$$\begin{aligned}\phi\big((a+bi)(c+di)\big) &= \phi\big((ac-bd)+(ad+bc)i\big) = \overline{ac-bd+ad+bc} \\ &= \overline{ac+bd+ad+bc} = \overline{a+b}\cdot\overline{c+d} = \phi(a+bi)\phi(c+di)\end{aligned}$$

因此 ϕ 是环同态，且

$$\begin{aligned}m+ni \in \mathrm{Ker}\phi &\iff \overline{m+n} = 0 \\ &\iff \overline{m} = \overline{n}\end{aligned}$$

即 $\mathrm{Ker}\phi = \{m+ni : m, n\text{同奇偶}\}$，进一步观察可以发现 $\mathrm{Ker}\phi = (1+i)$

一方面 $\forall x \in (1+i), \exists r \in \mathbb{Z}[i], \text{s.t. } x = r(1+i) \Rightarrow \phi(x) = \phi(r)\phi(1+i) = \overline{0} \Rightarrow x \in \mathrm{Ker}\phi \Rightarrow (1+i) \subseteq \mathrm{Ker}\phi$

另一方面，因为 $\forall m+ni \in \mathrm{Ker}\phi$，则 $\exists k \in \mathbb{Z}, \text{s.t. } m = n+2k$，所以 $m+ni = (n+2k)+ni = 2k+n(1+i)$，因为 $2 = (1-i)(1+i) \in (1+i)$，所以

$$m+ni = 2k+n(1+i) \in (1+i)$$

故 $\mathrm{Ker}\phi \subseteq (1+i)$

综上我们有 $\mathrm{Ker}\phi = (1+i)$，由环同态基本定理，存在唯一环同构

$$\mathbb{Z}[i]/(1+i) \cong \mathbb{F}_2$$

□

Exercise 15 $\forall p \in \mathrm{Spec}(\mathbb{Z}[i])$，求证 $p \cap \mathbb{Z} \in \mathrm{Spec}(\mathbb{Z})$

Proof

(1). 加法封闭性：$\forall a, b \in p \cap \mathbb{Z}$，则 $a, b \in \mathbb{Z}, a, b \in p$，所以 $a+b \in \mathbb{Z}, a+b \in p \Rightarrow a+b \in p \cap \mathbb{Z}$

(2). 倍元封闭性：$\forall r \in \mathbb{Z}, a \in p \cap \mathbb{Z}$，则 $a \in p, a \in \mathbb{Z}$，因为 $r \in \mathbb{Z} \subseteq \mathbb{Z}[i]$，所以 $ra \in p$，且 $ra \in \mathbb{Z}$，所以 $ra \in p \cap \mathbb{Z}$

综上，$p \cap \mathbb{Z} \lhd \mathbb{Z}$，下证明它是素理想：对 $\forall a, b \in \mathbb{Z}$，若 $ab \in p \cap \mathbb{Z}$，则 $ab \in p$，由 $p \in \mathrm{Spec}(\mathbb{Z}[i])$ 知，$a \in p$ 或 $b \in p$，则 $a \in p \cap \mathbb{Z}$ 或 $b \in p \cap \mathbb{Z}$，即 $p \cap \mathbb{Z} \in \mathrm{Spec}(\mathbb{Z})$ □