Homework 3 Solutions

1. ⓐ We use subring criteria, for $a, b, c, d \in \mathbb{Z}$

- $a+bw-(c+dw) = (a-c)+(b-d)w \in \mathbb{Z}[w]$.
- $(a+bw)(c+dw) = ac+adw+bcw+bdw^2$

$$= ac+(ad+bc)w+bdw^2$$

here uses: $w^2+w+1=0$

$$= ac+(ad+bc)w+bd(-w-1)$$

$$= (ac-bd)+(ad+bc-bd)w \in \mathbb{Z}[w].$$

$\Rightarrow$ $\mathbb{Z}[w]$ is a subring of $\mathbb{C}$.

ⓑ · First we show $\mathbb{Q}[w]$ is a field.

By similar argument as above, we know $\mathbb{Q}[w]$ is a subring of $\mathbb{C}$.

Now consider for $\forall\ \underset{\in \mathbb{Q}[w]}{a+bw} \neq 0$, $\frac{1}{a+bw}$.

According to hint, we compute

$$(a+bw)(a+b\bar{w}) = a^2+ab(w+\bar{w})+b^2 w\bar{w}.$$

$$= a^2-ab+b^2 \quad \left(\text{Here we used } w=\tfrac{-1+\sqrt{-3}}{2},\ \bar{w}=\tfrac{-1-\sqrt{-3}}{2} \text{ and get } w+\bar{w}=-1,\ w\bar{w}=1\right)$$

$a^2-ab+b^2 = (a-\frac{b}{2})^2+\frac{3}{4}b^2 \neq 0$ since $a\neq 0$, $b\neq 0$.

$$\Rightarrow \frac{1}{a+bw} = \frac{1}{a+bw}\cdot\frac{a+b\bar{w}}{a+b\bar{w}} = \frac{a+b\bar{w}}{a^2-ab+b^2} = \frac{a+b(-1-w)}{a^2-ab+b^2}$$

$$= \frac{a-b}{a^2-ab+b^2} + \frac{-b}{a^2-ab+b^2}\,w \in \mathbb{Q}[w].$$

$\Rightarrow$ $\mathbb{Q}[w]$ is a field.

- Let $i: \mathbb{Z}[w] \longrightarrow \mathbb{Q}[w]$ be the natural inclusion

$$m+nw \longmapsto m+nw \quad (m,n\in\mathbb{Z})$$

i is injective ring homomorphism.

For any $a+bw \in \mathbb{Q}[w]$

$$a+bw = \frac{k_1}{k_2}+\frac{l_1}{l_2}w = \frac{(k_1l_2+k_2l_1)w}{k_2l_2}, \text{ with } (k_1l_2+k_2l_1)w \in \mathbb{Z}[w]$$

$k_i, l_i \in \mathbb{Z}$, $i=1,2$. $\qquad k_2l_2 \in \mathbb{Z} \subseteq \mathbb{Z}[w]$.

$\Rightarrow$ $\mathbb{Q}[w]$ is the field of fraction of $\mathbb{Z}[w]$

since $R = \langle 1 \rangle$

2. ⓐ $\langle u \rangle = R \iff \langle u \rangle = \langle 1 \rangle \iff 1 \in \langle u \rangle \iff \exists\, v \in R$ s.t. $uv = 1$

$\iff u \in U(R)$

ⓑ $\langle a \rangle = \langle b \rangle \Rightarrow a = bu$ for $u, u' \in R$

$b = au'$

here we assume $a \neq 0$.

$\Rightarrow a = bu = au'u \Rightarrow 1 = u'u$ since R is integral domain.

$\Rightarrow u$ is unit $\Rightarrow a = bu$ with $u \in U(R)$

If $a = 0$. $\langle a \rangle = \langle b \rangle = \langle 0 \rangle \Rightarrow b \in \langle 0 \rangle \Rightarrow b = 0. \Rightarrow a = 1b$, with $1 \in U(R)$.

On the other hand.

$$\left.\begin{array}{l} a = bu \Rightarrow a \in \langle b \rangle. \\ u \text{ is unit} \Rightarrow au^{-1} = b \Rightarrow b \in \langle a \rangle \end{array}\right\} \Rightarrow \langle a \rangle = \langle b \rangle.$$

3. Let $I_1 = \{ x \in R_1,$ s.t. $(x, 0) \in I \}$

Let $I_2 = \{ y \in R_2,$ s.t. $(0, y) \in I \}$.

First we show $I_1 \times I_2 = I$.

$\forall (x, y) \in I_1 \times I_2, \quad (x, y) = (x, 0) + (0, y) \in I. \Rightarrow I_1 \times I_2 \subset I.$

$\forall (x, y) \in I$, want to show $x \in I_1, y \in I_2$.

$$\left.\begin{array}{l} (x, y)(1_{R_1}, 0) = (x, 0) \Rightarrow x \in I_1 \text{ by the definition of } I_1. \\ (x, y) \cdot (0, 1_{R_2}) = (0, y) \Rightarrow y \in I_2 \text{ by the definition of } I_2. \end{array}\right\} \Rightarrow I_1 \times I_2 \supset I.$$

So $I_1 \times I_2 = I$.

Now we show $I_1 \triangleleft R_1$, $I_2 \triangleleft R_2$.

Let $x_1, x_2 \in I_1$, $r \in R_1$.

$x_1 - x_2 \in I_1$ since $(x_1 - x_2, 0) = (x_1, 0) - (x_2, 0) \in I.$

$rx_1 \in I_1$ since $(rx_1, 0) = (r, 0)(x_1, 0) \in I$

$\Rightarrow I_1 \triangleleft R_1$.

Similarly we can show that $I_2 \triangleleft R_2$.

4. Assume by contradiction that $\langle 2, x \rangle$ is a principal ideal.

Then $\exists\, f(x) \in \mathbb{Z}[x]$ s.t. $\langle 2, x \rangle = \langle f(x) \rangle$.

- $2 \in \langle f(x) \rangle \Rightarrow 2 = f(x) \cdot g(x)$ with $g(x) \in \mathbb{Z}[x]$

  $\deg f(x) + \deg g(x) = 0$ while $\deg f(x) \geq 0$, $\deg g(x) \geq 0$

  $\Rightarrow \deg f(x) = \deg g(x) = 0 \Rightarrow f(x) \equiv m,\ g(x) \equiv n,\ m, n \in \mathbb{Z}$.

  $\Rightarrow 2 = m \cdot n \Rightarrow f(x) \equiv m = \pm 1$ or ± 2.

- Also, $x \in \langle f(x) \rangle$

  Suppose $f(x) = \pm 2$, $x = \pm 2 \cdot g(x) \Rightarrow g(x) = \pm \frac{x}{2} \notin \mathbb{Z}[x]$.

  $\Rightarrow$ The only possibilities for $f(x)$ are ± 1.

- Suppose $f(x) = \pm 1$.

  $\Rightarrow \langle 2, x \rangle = \langle \pm 1 \rangle = \langle 1 \rangle$

  $\Rightarrow 1 \in \langle 2, x \rangle$.

  i.e. $\exists\, h_1(x), h_2(x) \in \mathbb{Z}[x]$, s.t. $1 = 2h_1(x) + x\,h_2(x)$.

  But the constant term of RHS is an even number

  $\Rightarrow f(x) = \pm 1$ is also impossible.

$\Rightarrow$ Our assumption is wrong.

$\Rightarrow \langle 2, x \rangle$ is not principal ideal in $\mathbb{Z}[x]$.

5. (a). $102459087 = 10^8 + 2 \times 10^6 + 4 \times 10^5 + 5 \times 10^4 + 9 \times 10^3 + 8 \times 10 + 7$. (mod 9)

$102459087 \pmod 9 = 1^8 + 2 \times 1^6 + 4 \times 1^5 + 5 \times 1^4 + 0 \times 1^3 + 8 \times 1 + 7$

$= 0 \pmod 9$.

$\Rightarrow$ the remainder is 0.

(b). Similarly, $102459087 \pmod{11} = (-1)^8 + 2 \times (-1)^6 + 4 \times (-1)^5 + 5 \times (-1)^4$

$+ 9 \times (-1)^3 + 8 \times (-1) + 7 \pmod{11} = 5 \pmod{11}$.

$\Rightarrow$ the remainder is 5.

(c). · $3 \times 4 = 12 = 1$ in $\mathbb{Z}_{11}$. $\Longrightarrow$ $3^{-1} = 4$ in $\mathbb{Z}_{11}$.

$\Longrightarrow$ $2/3 = 2 \times 4 = 8$ in $\mathbb{Z}_{11}$.

· $11 \times 7 = 77 = 1$ in $\mathbb{Z}_{19}$ $\Longrightarrow$ $7^{-1} = 11$ in $\mathbb{Z}_{19}$.

$\Longrightarrow$ $2/7 = 2 \times 11 = 22 = 3$ in $\mathbb{Z}_{19}$.

· $-5 \times 9 = -45 = 1$ in $\mathbb{Z}_{23}$ $\Longrightarrow$ $9^{-1} = -5 = 18$ in $\mathbb{Z}_{23}$.

$\Longrightarrow$ $2/9 = 2 \times 18 = 36 = 13$ in $\mathbb{Z}_{19}$.

Remark: A general way to find m^{-1} in $\mathbb{Z}_n$ when $(m,n)=1$ is to use Euclidean algorithm.

As an example, we compute 7^{-1} in $\mathbb{Z}_{19}$. $(7,19)=1$.

$19 = 2 \times 7 + 5$.

$7 = 1 \times 5 + 2$ $\Longrightarrow$

$5 = 2 \times 2 + 1$

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2 \times (7 - 5) \\ &= 3 \times 5 - 2 \times 7 \\ &= 3 \times (19 - 2 \times 7) - 2 \times 7 \\ &= 3 \times 19 - 8 \times 7. \quad (☆) \end{aligned}$$

$\Longrightarrow$ in $\mathbb{Z}_{19}$, $(☆) \Rightarrow 1 = -8 \times 7$

$\Longrightarrow$ $7^{-1} = -8 = 11$.

6. ⓐ. $a, b, c, d \in \mathbb{Z}$

· $f((a+bi)+(c+di)) = f((a+c)+(b+d)i) = \overline{a+c} \oplus 2(\overline{b+d})$

$= \bar{a} \oplus \bar{c} \oplus 2\bar{b} \oplus 2\bar{d}$.

$f(a+bi) \oplus f(c+di) = \bar{a} \oplus 2\bar{b} \oplus \bar{c} \oplus 2\bar{d}$

$\Longrightarrow$ $f((a+bi)+(c+di)) = f(a+bi) \oplus f(c+di)$.

$\cdot\ f((a+bi)(c+di)) = f((ac-bd)+(ad+bc)i)$

$= \overline{ac-bd} \oplus 2(\overline{ad+bc})$

$= \overline{ac} \ominus \overline{bd} \oplus 2(\overline{ad}) \oplus 2\overline{bc}$

$= (\bar{a}\odot\bar{c}) \ominus (\bar{b}\odot\bar{d}) \oplus 2(\bar{a}\odot\bar{d}) \oplus 2(\bar{b}\odot\bar{c})$

$= (\bar{a}\odot\bar{c}) \oplus 2(\bar{a}\odot\bar{d}) \oplus 2(\bar{b}\odot\bar{c}) \oplus 4(\bar{b}\odot\bar{d})$ ($-1=4$ in $\mathbb{Z}_5$)

$f(a+bi)\odot f(c+di) = (\bar{a}\oplus 2\bar{b})\odot(\bar{c}\oplus 2\bar{d})$

$= (\bar{a}\odot\bar{c}) \oplus 2(\bar{a}\odot\bar{d}) \oplus 2(\bar{b}\odot\bar{c}) \oplus 4(\bar{b}\odot\bar{d})$

$\Rightarrow f((a+bi)(c+di)) = f(a+bi)\odot f(c+di)$

$\Rightarrow f$ is a ring homomorphism.

ⓑ To show $\langle -2+i\rangle \subset \ker f$.

Enough to show $-2+i \in \ker f$, i.e. $f(-2+i) = \bar{0}$.

$f(-2+i) = \overline{-2} \oplus \bar{2} = \overline{2-2} = \bar{0} \in \mathbb{Z}_5$

i.e. $-2+i \in \ker f$.