Homework #1 Solutions

(1)

(a) $R = \mathbb{Z}^+ = \{1, 2, 3, 4, \ldots\}$

R is not a ring. It has no additive identity element x with $x+y = y+x = y$ for all $x \in R$. (0 is missing)

(1) (b) $\mathbb{Z}[i]$ is a ring.

It is a group under addition:

- If $a, b, c, d \in \mathbb{Z}$ then $(a+bi)+(c+di) = (a+c)+(b+d)i \in \mathbb{Z}[i]$ since $a+c$ and $b+d$ are in $\mathbb{Z}$.
- The additive identity is $0 = 0 + 0i$.
- $\mathbb{C}$ is associative under addition and $\mathbb{Z}[i] \subseteq \mathbb{C}$. Thus $\mathbb{Z}[i]$ is associative under addition.
- The additive inverse of $a+bi$ is $(-a)+(-b)i$.
- Addition is commutative because it is in $\mathbb{C}$.

$\mathbb{Z}[i]$ is closed under multiplication:

- If $a, b, c, d \in \mathbb{Z}$, then

$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i \in \mathbb{Z}[i]$$

since $ac-bd$ and $ad+bc$ are integers.

$\mathbb{Z}[i]$ satisfies the distributive and associative laws involving multiplication because $\mathbb{C}$ does and $\mathbb{Z}[i] \subseteq \mathbb{C}$.

Further answers about $\mathbb{Z}[i]$:

(a) $\mathbb{Z}[i]$ is a commutative ring since

$$(a+bi)(c+di) = (c+di)(a+bi)$$

(b) $1 = 1+0i$ is the mult. identity

(c) Let $a+bi \in \mathbb{Z}[i]$ where $a,b \in \mathbb{Z}$.

Then $\dfrac{1}{a+bi} = \dfrac{1}{a+bi} \cdot \dfrac{a-bi}{a-bi} = \dfrac{a}{a^2+b^2} - \dfrac{b}{a^2+b^2}\, i$.

The only way for $\frac{1}{a+bi}$ to be in $\mathbb{Z}[i]$ is if $\frac{a}{a^2+b^2} \in \mathbb{Z}$ and $\frac{b}{a^2+b^2} \in \mathbb{Z}$. That is we need a^2+b^2 to divide a and b simultaneously. Since $|a^2+b^2| \geq |a|$ and $|a^2+b^2| \geq |b|$ this can only happen if $(a,b) = (\pm 1, 0)$ or $(a,b) = (0, \pm 1)$.

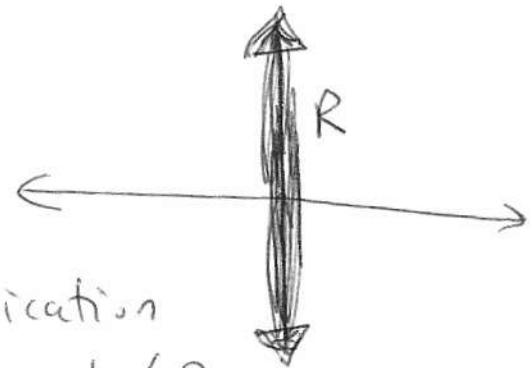
So, $\underset{a+bi=}{\boxed{1, -1, i, -i}}$ are the units of $\mathbb{Z}[i]$.

(d) $\mathbb{Z}[i]$ is not a field since, for example,

$$\frac{1}{2i} = \frac{i}{2i(i)} = \frac{i}{-2} = -\frac{1}{2} i \notin \mathbb{Z}[i].$$

That is $2i$ has no multiplicative inverse in $\mathbb{Z}[i]$.

(1) (c) $R = \{ix \mid x \in \mathbb{R}\}$



R is not closed under multiplication since $i \in R$ but $i \cdot i = -1 \notin R$.

~~(d) You can do this one. Answer is that $\mathbb{Q}(\sqrt{2})$ is a field.~~

(1) (d) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Let's show that $\mathbb{Q}(\sqrt{2})$ is a subring of $\mathbb{R}$. Certainly $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ since $\sqrt{2} \in \mathbb{R}$.

Let's use the subring criteria:

- $0 = 0 + 0 \cdot \sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
- Let $a + b\sqrt{2},\ c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ where $a, b, c, d \in \mathbb{Q}$. Then,

$$(a+b\sqrt{2}) - (c + d\sqrt{2}) = (a-c) + (b-d)\sqrt{2}$$

and

$$(a+b\sqrt{2}) \cdot (c+d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

are in $\mathbb{Q}(\sqrt{2})$ since $a-c$, $b-d$, $ac+2bd$, and $ad+bc$ are in $\mathbb{Q}$.

- Thus, $\mathbb{Q}(\sqrt{2})$ is a subring of $\mathbb{R}$.

(a) Since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ and $\mathbb{R}$ is commutative we know that $\mathbb{Q}(\sqrt{2})$ is commutative.

(b) $1 = 1 + 0 \cdot \sqrt{2} \in \mathbb{Q}(\sqrt{2})$, Thus $\mathbb{Q}(\sqrt{2})$ has a multiplicative identity.

(c) Let $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ with $a, b \in \mathbb{Q}$ and $a+b\sqrt{2} \neq 0$. Then,

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}.$$

Note that $a^2-2b^2 \neq 0$ since if it was then either $a=0=b$ which isn't true since $a+b\sqrt{2} \neq 0$, OR $a^2-2b^2=0$ would give that $\left(\frac{a}{b}\right)^2 = 2$ which can't happen because $\sqrt{2} \notin \mathbb{Q}$.

Thus, $\frac{a}{a^2-2b^2}$ and $\frac{b}{a^2-2b^2}$ are in $\mathbb{Q}$. Hence if $a+b\sqrt{2} \neq 0$ then $\frac{1}{a+b\sqrt{2}} \in \mathbb{Q}(\sqrt{2})$.
So every non-zero element of $\mathbb{Q}(\sqrt{2})$ is a unit.

(d) $\mathbb{Q}(\sqrt{2})$ is a field by (a)-(c) above.

(2) We use the subring criteria.

(a) $R_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$

- $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R_1$
- Let $\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \in R_1$ where $a_1, a_2, b_1, b_2 \in \mathbb{Z}$.

Then $a_1 - a_2, b_1 - b_2, a_1 a_2, b_1 b_2 \in \mathbb{Z}$. Hence

$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} - \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & 0 \\ 0 & b_1 - b_2 \end{pmatrix} \in R_1$$

and $$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{pmatrix} \in R_1$$

Thus, R_1 is a subring of $M_2(\mathbb{R})$.

(b) R_2 is not a subring of $M_2(\mathbb{R})$.

Note that $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ does not satisfy determinant equal to 1. Thus, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin R_2$.

(3) (a) $(1,1)$ is the mult. identity of $\mathbb{Z}\times\mathbb{Z}$.
Suppose that $a,b,c,d\in\mathbb{Z}$ with

$$(a,b)(c,d)=(1,1).$$

[That is, (a,b) and (c,d) are units and they are mult. inverses of each other.]

Then $(ac,bd)=(1,1)$.

So, $ac=1$ and $bd=1$.

Since $a,b,c,d\in\mathbb{Z}$ we must have one of the following:

$(a,b)=(1,1)$ and $(c,d)=(1,1)$
$(a,b)=(-1,1)$ and $(c,d)=(-1,1)$
$(a,b)=(1,-1)$ and $(c,d)=(1,-1)$
or $(a,b)=(-1,-1)$ and $(c,d)=(-1,-1)$.

So, the units of $\mathbb{Z}\times\mathbb{Z}$ are

$$(1,1),\ (-1,1),\ (1,-1),\ (-1,-1).$$

(b) $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{1},\bar{0}),(\bar{1},\bar{1}),(\bar{1},\bar{2})\}$

The units are $(\bar{1},\bar{1})$ and $(\bar{1},\bar{2})$.

[They are units since $(\bar{1},\bar{1})$ is the mult. identity and $(\bar{1},\bar{1})\cdot(\bar{1},\bar{1})=(\bar{1},\bar{1})$ and $(\bar{1},\bar{2})(\bar{1},\bar{2})=(\bar{1},\bar{4})=(\bar{1},\bar{1})$]

inverses of each other

inverses of each other

The other elements have $\bar{0}$'s in a component which makes it so they can't have an inverse.

Another way: Let R_1 and R_2 be commutative rings with identities. Let $(a,b) \in R_1 \times R_2$. Then (a,b) is a unit in $R_1 \times R_2$ iff a is a unit in R_1 and b is a unit in R_2.

That is, $(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$.

Try to prove this for more practice. It's not that bad.

Then do this:

Units of $\mathbb{Z}_2$ are $\bar{1}$

Units of $\mathbb{Z}_3$ are $\bar{1}$ and $\bar{2}$

So units of $\mathbb{Z}_2 \times \mathbb{Z}_3$ are $(\bar{1},\bar{1})$ and $(\bar{1},\bar{2})$.

(c) $\mathbb{Z}[i]$. We did this in problem 1.

Answer: $1, -1, i, -i$.

④ Let R be a ring with multiplicative identity. Suppose that 1_1 and 1_2 are both multiplicative identities. Then

$$1_1 \underset{\boxed{\text{since } 1_2 \text{ is a mult. identity}}}{=} 1_1 \cdot 1_2 \underset{\boxed{\text{since } 1_1 \text{ is a mult. identity}}}{=} 1_2$$

Thus, $1_1 = 1_2$. So mult. identities are unique.

---

⑤ Suppose that y_1 and y_2 are mult. inverse for x and 1 is the mult. identity of R. Then

$$xy_1 = y_1 x = 1$$

and

$$xy_2 = y_2 x = 1.$$

Then

$$y_1 = y_1 \cdot 1 = y_1(xy_2) = (y_1 x)y_2 = 1 \cdot y_2 = y_2$$

So mult. inverses are unique.

$I_a = \{x \in R \mid ax = 0\}$.

(6) We use the subring criteria.

- Note that $a \cdot 0 = 0$. Hence $0 \in I_a$.
- Let $x, y \in I_a$. Then $ax = 0$ and $ay = 0$.

So,

$$a(x-y) = ax - ay = 0 - 0 = 0$$

and

$$a(xy) = (ax)(y) = 0(y) = 0.$$

Thus $x - y \in I_a$ and $xy \in I_a$.

So, I_a is a subring of R.

---

(7) Again we use the subring criteria.

- $0 = n \cdot 0 \in n\mathbb{Z}$.
- Let $x, y \in n\mathbb{Z}$. Then $x = nk_1$ and $y = nk_2$ for some $k_1, k_2 \in \mathbb{Z}$. So,

$$x - y = nk_1 - nk_2 = n(k_1 - k_2) \in n\mathbb{Z}$$

and

$$xy = (nk_1)(nk_2) = n(k_1 n k_2) \in n\mathbb{Z}.$$

So, $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.

(8) R = commutative ring with identity $1 \neq 0$.
$R^\times$ = set of units of R.

<u>Prove:</u> $R^\times$ is a group under mult.

- Let $a, b \in R^\times$. Then a and b are units. Hence a^{-1} and b^{-1} exist and $aa^{-1} = 1$ and $bb^{-1} = 1$ and $a^{-1}, b^{-1} \in R^\times$. Then $ab \in R^\times$ since $a^{-1}b^{-1} = (ab)^{-1}$ because

$$(ab)(a^{-1}b^{-1}) = aba^{-1}b^{-1} \underset{\text{R is commutative}}{=} aa^{-1}bb^{-1} = 1 \cdot 1 = 1.$$

So, $R^\times$ is closed under multiplication.

- $R^\times$ is associative under mult, since R is a ring and $R^\times \subseteq R$.
- 1 is a unit, Hence $1 \in R^\times$.
- As above, if $a \in R^\times$, then that means that a is a unit and a^{-1} exists with $aa^{-1} = a^{-1}a = 1$. So, a^{-1} is also a unit and $a^{-1} \in R^\times$.

- Thus, $R^\times$ is a group under mult.

(9) Let R and S be subrings of a ring T. Then $R \cap S$ is a subring of T.

<u>proof:</u>

- Since R and S are subrings of T we know that $0 \in R$ and $0 \in S$. Thus $0 \in R \cap S$.

- Let $x, y \in R \cap S$. Since $x, y \in R$ and R is a subring we know that $x - y \in R$ and $xy \in R$. Since $x, y \in S$ and S is a subring we know that $x - y \in S$ and $xy \in S$.

Thus

$x - y \in R \cap S$ and $xy \in R \cap S$.

- So, by the subring criteria, $R \cap S$ is a subring of T.