Homework 5 Solutions

①

$$\langle x^2+\bar{1}\rangle = \{ \bar{0}\cdot(x^2+\bar{1}),\ \bar{1}\cdot(x^2+\bar{1}),\ \bar{2}\cdot(x^2+\bar{1}),$$
$$x\cdot(x^2+\bar{1}),\ (\bar{1}+x)(x^2+\bar{1}),\ (\bar{2}+x)(x^2+\bar{1}),$$
$$\bar{2}x\cdot(x^2+\bar{1}),\ (\bar{1}+\bar{2}x)(x^2+\bar{1}),\ (\bar{2}+\bar{2}x)(x^2+\bar{1}),\ldots\}$$

infinitely many more polynomials

②

(a) $S=\{(a,a)\mid a\in\mathbb{Z}\}$ is not an ideal of $\mathbb{Z}\times\mathbb{Z}$. For example, $(1,1)\in S$ and $(2,0)\in\mathbb{Z}\times\mathbb{Z}$ but

$$(2,0)\cdot(1,1)=(2,0)\notin S.$$

(b) Let $S=\{(2a,3b)\mid a,b\in\mathbb{Z}\}$. We show that S is an ideal of $\mathbb{Z}\times\mathbb{Z}$.

First we show that S is a subgroup of $\mathbb{Z}\times\mathbb{Z}$.

- Note that $(0,0)=(2\cdot 0,3\cdot 0)\in S$.
- Let $x,y\in S$. Then $x=(2a_1,3b_1)$ and $y=(2a_2,3b_2)$ where $a_1,a_2,b_1,b_2\in\mathbb{Z}$.

Then $x-y=(2(a_1-a_2), 3(b_1-b_2)) \in S$.

So, S is a subgroup of $\mathbb{Z}\times\mathbb{Z}$.

Let $r \in \mathbb{Z}\times\mathbb{Z}$ and $i \in S$. Then $r=(c,d)$ and $i=(2e,3f)$ where $c,d,e,f \in \mathbb{Z}$.

So,

$$ir = (2e,3f)(c,d) = (2ec, 3fd) \in S$$

and

$$ri = (c,d)(2e,3f) = (2ec, 3fd) \in S.$$

Thus, S is an ideal of $\mathbb{Z}\times\mathbb{Z}$.

(c) Let $S=\{(a,0) \mid a \in \mathbb{Z}\}$. We show that S is an ideal of $\mathbb{Z}\times\mathbb{Z}$.

- $(0,0) \in S$ (set $a=0$)
- Let $(a,0),(b,0) \in S$ where $a,b \in \mathbb{Z}$. Then $(a,0)-(b,0)=(a-b,0) \in S$.
- Let $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ and $(c,0) \in S$. Then

$$(x,y)(c,0) = (xc,0) \in S$$

and $(c,0)(x,y) = (cx,0) \in S$.

(d) $S = \{(a, -a) \mid a \in \mathbb{Z}\}$ is not an ideal of S. For example $(1,-1) \in S$ and $(5,0) \in \mathbb{Z} \times \mathbb{Z}$, but

$$(1,-1)(5,0) = (5,0) \notin S.$$

---

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

$I = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2})\}$.

We show that $I = \langle(\bar{0},\bar{1})\rangle$ and hence is an ideal of $\mathbb{Z}_2 \times \mathbb{Z}_3$.

$$\begin{aligned}\langle(\bar{0},\bar{1})\rangle &= \{(\bar{0},\bar{0})(\bar{0},\bar{1}), (\bar{0},\bar{1})(\bar{0},\bar{1}), (\bar{0},\bar{2})(\bar{0},\bar{1}), \\ &\qquad (\bar{1},\bar{0})(\bar{0},\bar{1}), (\bar{1},\bar{1})(\bar{0},\bar{1}), (\bar{1},\bar{2})(\bar{0},\bar{1})\} \\ &= \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2})\} \\ &= I\end{aligned}$$

④

(a) By 455 we know that every subgroup of $\mathbb{Z}_n$ is cyclic since $\mathbb{Z}_n$ is cyclic. Thus, every subgroup is of the form

$$\langle \bar{k} \rangle = \{ \bar{0}, \bar{k}, \overline{2k}, \overline{3k}, \ldots, \overline{(n-1)k} \}.$$

Furthermore, if $\bar{x} \in \mathbb{Z}_n$ and $\overline{ak} \in \langle \bar{k} \rangle$ where $x, a \in \mathbb{Z}$, then

$$\bar{x} \cdot \overline{ak} = \overline{xak} \in \langle \bar{k} \rangle$$

and $$\overline{ak} \cdot \bar{x} = \overline{xak} \in \langle \bar{k} \rangle,$$

Hence $\langle \bar{k} \rangle$ is an ideal and every ideal of $\mathbb{Z}_n$ is of this form.

(b) $\langle \bar{0} \rangle = \{ \bar{0} \}$

$\langle \bar{1} \rangle = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \} = \langle \bar{5} \rangle$

$\langle \bar{2} \rangle = \{ \bar{0}, \bar{2}, \bar{4} \} = \langle \bar{4} \rangle$

$\langle \bar{3} \rangle = \{ \bar{0}, \bar{3} \}$

(c) $\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\} = \langle \bar{3} \rangle = \langle \bar{5} \rangle = \langle \bar{7}$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} = \langle \bar{6} \rangle$

$\langle \bar{4} \rangle = \{\bar{0}, \bar{4}\}$

(d)

$\langle \overline{13} \rangle = \{\bar{0}, \overline{13}\}$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}\}$

---

5 (a) $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \,\middle|\, a \in \mathbb{R} \right\}$

is not an ideal of $M_2(\mathbb{R})$. For example,

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$ and $\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \in S$ but

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 0 \end{pmatrix} \notin S.$$

(5) (b) $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \; a, b \in \mathbb{R} \right\}$ is not an ideal of $M_2(\mathbb{R})$.

For example, $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{R})$ and $\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \in S$

but $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 5 \\ 1 & 5 \end{pmatrix} \notin S$.

---

(6) Let 0 and $0'$ be the additive identities of R and R'.

(a) • Note that $\varphi(0) = 0'$. Hence $0 \in \ker(\varphi)$.

• Let $x, y \in \ker(\varphi)$. Then $\varphi(x) = 0'$ and $\varphi(y) = 0'$.
Hence $\varphi(x-y) = \varphi(x) - \varphi(y) = 0' - 0' = 0'$.

• Let $r \in R$ and $z \in \ker(\varphi)$. Then $\varphi(z) = 0'$.
And $\varphi(rz) = \varphi(r)\varphi(z) = \varphi(r) \cdot 0' = 0'$
and $\varphi(zr) = \varphi(z)\varphi(r) = 0' \cdot \varphi(r) = 0'$.

(b) • $0' = \varphi(0) \in \varphi(R)$.

• Let $a, b \in \varphi(R)$. Then $a = \varphi(x)$ and $b = \varphi(y)$ where $x, y \in R$. Since R is a ring $x - y \in R$.
Hence $a - b = \varphi(x) - \varphi(y) = \varphi(x-y) \in \varphi(R)$

• Let $c \in \varphi(R)$ and $r' \in R'$, so $c = \varphi(z)$ for some $z \in R$. Since φ is onto there exists $r \in R$ with $\varphi(r) = r'$. Hence,

$$r' \cdot c = \varphi(r)\varphi(z) = \varphi(rz) \in \varphi(R)$$

and $c \cdot r' = \varphi(z)\varphi(r) = \varphi(zr) \in \varphi(R)$

since $rz, zr \in R$.

(7) $\{0\}$ and R are subgroups of R by Math 455. Let $r \in R$. Then

$$r \cdot 0 = 0 \in \{0\}$$

and $0 \cdot r = 0 \in \{0\}$.

Hence $\{0\}$ is an ideal of R.

Let $x \in R$. Then

$$r \cdot x \in R$$

and $x \cdot r \in R$.

So, R is an ideal of R.

---

(8) Let I be an ideal of R.

Then $0 \in I$ and $x - y \in I$ if $x, y \in I$.

Let $a, b \in I$. Then $a \cdot b \in I$ by

The definition of ideal.

Hence by the subgroup criteria, I is a ~~subgroup~~ subring of R.

⑨

- $0 = 0 \cdot a \in \langle a \rangle$.
- Let $x, y \in \langle a \rangle$. Then $x = ar_1$ and $y = ar_2$. Hence $x - y = ar_1 - ar_2 = a \cdot (r_1 - r_2)$ which is in $\langle a \rangle$ since $r_1 - r_2 \in R$.
- Let $z \in \langle a \rangle$ and $w \in R$. Then $z = ar_3$ where $r_3 \in R$. Thus $wr_3 \in R$.

So,

$$wz = war_3 = a(wr_3) \in \langle a \rangle$$

and

$$zw = ar_3w = a(r_3w) \in \langle a \rangle.$$

---

⑩ Claim: $I = \langle (\bar{2}, \bar{2}) \rangle$

proof:

$$\langle (\bar{2},\bar{2}) \rangle = \{ (\bar{0},\bar{0})(\bar{2},\bar{2}), (\bar{0},\bar{1}),(\bar{2},\bar{2}), (\bar{0},\bar{2})(\bar{2},\bar{2}), (\bar{0},\bar{3})(\bar{2},\bar{2}),$$
$$(\bar{1},\bar{0})(\bar{2},\bar{2}), (\bar{1},\bar{1})(\bar{2},\bar{2}), (\bar{1},\bar{2})(\bar{2},\bar{2}), (\bar{1},\bar{3})(\bar{2},\bar{2}),$$
$$(\bar{2},\bar{0})(\bar{2},\bar{2}), (\bar{2},\bar{1})(\bar{2},\bar{2}), (\bar{2},\bar{2})(\bar{2},\bar{2}), (\bar{2},\bar{3})(\bar{2},\bar{2}),$$
$$(\bar{3},\bar{0})(\bar{2},\bar{2}), (\bar{3},\bar{1})(\bar{2},\bar{2}), (\bar{3},\bar{2})(\bar{2},\bar{2}), (\bar{3},\bar{3})(\bar{2},\bar{2}) \}$$

$$= \{ (\bar{0},\bar{0}), (\bar{0},\bar{2}), (\bar{0},\bar{0}), (\bar{0},\bar{2}),$$
$$(\bar{2},\bar{0}), (\bar{2},\bar{2}), (\bar{2},\bar{0}), (\bar{2},\bar{2}),$$
$$(\bar{0},\bar{0}), (\bar{0},\bar{2}), (\bar{0},\bar{0}), (\bar{0},\bar{2}),$$
$$(\bar{2},\bar{0}), (\bar{2},\bar{2}), (\bar{2},\bar{0}), (\bar{2},\bar{2}) \} = I.$$