MA 638 - Section 7.3 Homework

INSTRUCTIONS: The solutions to all problems here should be typed up in LaTeX using correct mathematical notation and language. Proofs and explanations must be written in complete sentences using correct grammar and punctuation. Use mathematical displays and *implication* or *if and only if* arrows where appropriate to manipulate equations or to validate steps in a proof or argument. Your completed pdf will be uploaded in Canvas. Be sure to save your pdf file using the naming format "first initial last name underscore section number", i.e. Jane Doe would save her this homework as **jdoe_7-3.pdf**.

1. Find all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/20\mathbb{Z}$. In each case describe the kernel and image.

   Every homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}$ is determined by how it maps 1. This is because, for any other $n \in \mathbb{Z}$ we have

   $$\varphi(n) = \varphi(\overbrace{1 + 1 + \cdots + 1}^{n \text{ times}}) = \overbrace{\varphi(1) + \varphi(1) + \cdots + \varphi(1)}^{n \text{ times}} = n\varphi(1)$$

   However, not every choice of $\varphi(1)$ yields a homomorphism. The following demonstrates a property that any homomorphism must have. Suppose $\varphi(1) = n \in \mathbb{Z}/20\mathbb{Z}$, then

   $$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) \quad \Rightarrow$$

   $$n = n^2$$

   The equation above is, in our case, taken mod 20. So we must select numbers satisfying this equation, and it suffices to compute the square of every number mod 20.

$$\begin{aligned}
\overline{0}^2 &= \overline{0} \\
\overline{1}^2 &= \overline{1} \\
\overline{2}^2 &= \overline{4} \\
\overline{3}^2 &= \overline{9} \\
\overline{4}^2 &= \overline{16} \\
\overline{5}^2 &= \overline{25} = \overline{5} \\
\overline{6}^2 &= \overline{36} = \overline{16} \\
\overline{7}^2 &= \overline{49} = \overline{9} \\
\overline{8}^2 &= \overline{64} = \overline{4} \\
\overline{9}^2 &= \overline{81} = \overline{1} \\
\overline{10}^2 &= \overline{100} = \overline{0} \\
\overline{11}^2 &= \overline{121} = \overline{1} \\
\overline{12}^2 &= \overline{144} = \overline{4} \\
\overline{13}^2 &= \overline{169} = \overline{9} \\
\overline{14}^2 &= \overline{196} = \overline{16} \\
\overline{15}^2 &= \overline{225} = \overline{5} \\
\overline{16}^2 &= \overline{256} = \overline{16} \\
\overline{17}^2 &= \overline{289} = \overline{9} \\
\overline{18}^2 &= \overline{324} = \overline{4} \\
\overline{19}^2 &= \overline{361} = \overline{1}
\end{aligned}$$

The only numbers satisfying the necessary equation are $\overline{0}^2 = \overline{0}, \overline{1}^2 = \overline{1}, \overline{5}^2 = \overline{5}$, and $\overline{16}^2 = \overline{16}$. These four then determine all homomorphisms.

For the homomorphism such that $\varphi(1) = \overline{0}$ this is the zero map, and therefore $\ker\varphi = \mathbb{Z}$ and $\mathrm{Im}\varphi = \{0\}$.

For the homomorphism such that $\varphi(1) = \overline{1}$ this is the identity map and so $\ker\varphi = \{0\}$ and $\mathrm{Im}\varphi = \mathbb{Z}/20\mathbb{Z}$.

If $\varphi(1) = \overline{5}$ then $x \in \ker\varphi$ if $\varphi(x) = \overline{5x} = \overline{0}$ which occurs just in case x has two factors of 2. This then implies $\ker\varphi$ is all multiples of 4. $\mathrm{Im}\varphi$ is all multiples of $\overline{5}$.

Finally, if $\varphi(1) = \overline{16}$ then $\varphi(x) = \overline{16x} = \overline{0}$ just in case x has a factor of 5 and therefore $\ker\varphi$ is all multiples of 5. $\mathrm{Im}\varphi$ is all multiples of $\overline{16}$, but in this case finding these takes more work. They include

$$\begin{aligned}
\overline{0} \\
\overline{16} \\
\overline{32} = \overline{12} \\
\overline{48} = \overline{8} \\
\overline{64} = \overline{4} \\
\overline{80} = \overline{0}
\end{aligned}$$

All other values repeat after these, so Imφ is all multiples of 4.

2. Suppose that $R = \mathbb{Z}[x]$, (i.e. R is the polynomial ring with integer coefficients)

   (a) Is $\mathbb{Z}[x^2]$ (i.e. the polynomials of which only even powers of x appear) an ideal of the ring R?

   (b) Is the set of polynomials $p(x)$ such that $p'(0) = 0$, where $p'(x)$ is the usual first derivative of $p(x)$ with respect to x, an ideal of R?

   (c) Prove that $I = \{p(x) \in R \mid p(0) = 0\}$ is an ideal of R.

   Part (a) No, because $x \in R$ and $x^2 \in \mathbb{Z}[x^2]$, but yet $x(x^2) = x^3 \notin \mathbb{Z}[x^2]$.

   Part (b) No. Say that $p(0) \neq 0$ like for instance with $p(x) = 1 + x^2$. Now say you have a polynomial $q(x)$ such that $q'(0) \neq 0$ like for instance $q(x) = x$. If the set were an ideal then the polynomial $(p(x)q(x))'$ would have a root at zero. However

$$(p(x)q(x))' = p'(x)q(x) + p(x)q'(x)$$

   and $p'(0)q(0)+p(0)q'(0) = 0+p(0)q'(0) = p(0)q'(0)$. Since $\mathbb{Z}$ is an integral domain, $p(0) \neq 0, q'(0) \neq 0$, then $p(0)q'(0) \neq 0$. With the particular example chosen above, $p(x) = 1 + x^2$ and $q'(x) = 1$, so that $p(0)q'(0) = 1 \cdot 1 = 1$. Hence $p(x)q(x)$ is not in this set, and so the set is not an ideal.

   Part (c) *Proof:* Let $p(x) \in I$ and $q(x) \in R$. Then $q(0)p(0) = q(0) \cdot 0 = 0$ and therefore $q(x)p(x) \in I$. Moreover, I is a subgroup since it is a subset closed under sums and inverses: If $r(x) \in I$ then $p(0) + r(0) = 0 + 0 = 0$ and $p(0) - p(0) = 0 - 0 = 0$. And it is a subring because it is closed under products, which is immediate from the property established at the start of this paragraph. Hence I is an ideal. $\square$

3. Prove that the ring $M_2(\mathbb{R})$ contains a subring that is isomorphic to $\mathbb{C}$.

   Proof: We identify $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ with the number 1, and $M_i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ with the number i. This suggests that the subring of $M_2(\mathbb{R})$ we seek is the set $S = \left\{ M \in M_2(\mathbb{R}) : M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ for any } a, b \in \mathbb{R} \right\}$. We start by constructing a map $\varphi : \mathbb{C} \to S$ defined by

$$\varphi(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

   We show that this map is an isomorphism, starting with injectivity. If $\varphi(a + ib) = \varphi(c + id) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ and therefore $a = b$ and $c = d$, so $a + ib = c + id$. For surjectivity of course if $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in S$ then $\varphi(a + ib) = M$.

   Next we show the homomorphism property, first for sums.

$$\varphi((a + ib) + (c + id)) = \begin{pmatrix} a + c & b + d \\ -(b + d) & a + c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \varphi(a + ib) + \varphi(c + id).$$

   Next for multiplication,

$$\varphi((a+ib)(c+id)) = \varphi((ac-bd)+i(ad+bc))$$

$$= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

$$= \varphi(a+ib)\varphi(c+id).$$

Now that we know φ is a homomorphism then its image is a subring of $M_2(\mathbb{R})$ and since φ is onto, $S = \mathrm{Im}\varphi$ is a subring of $M_2(\mathbb{R})$. Hence we have an isomorphism between $\mathbb{C}$ and S, so the proof is complete. $\square$