MATH 333 — MIDTERM EXAM 2

April 20, 2016

NAME: Solutions

1. (3 points each) You do not need to give full proofs; short justifications are fine.

   (a) Give an example of a ring that is not an integral domain.

   The ring $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain because it has the zero divisor $[2]_4$.

   (b) Give an example of an integral domain that is not a field.

   The ring $\mathbb{Z}$ is an integral domain but not a field as 2 does not have a multiplicative inverse in $\mathbb{Z}$.

   (c) Give an example of a field with finitely many elements.

   The ring $\mathbb{Z}/3\mathbb{Z}$ is a field with only 3 elements.

   (d) Give an example of a ring that is not commutative.

   The ring $\mathrm{Mat}_2(\mathbb{Z})$ is not commutative. For instance, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$ while $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$.

   (e) Give an example of a ring R and an element $a \in R$ with $a \neq 1_R$ but $a^2 = 1_R$.

   Let $R = \mathbb{Z}/3\mathbb{Z}$. Then $a = [2]_3$ is such an example.

   (f) Give an example of a ring homomorphism that is not an isomorphism.

   Let $\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be defined by $[a]_4 \mapsto [a]_2$. This cannot be an isomorphism because the rings have different numbers of elements (so no bijection can exist between them), but we saw in class this is a ring homomorphism.

2. (12 points) Let F be a field. Show that $x - 1_F$ divides $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $F[x]$ if and only if $a_n + a_{n-1} + \cdots + a_1 + a_0 = 0_F$.

   Proof. Recall we showed that $x - a$ divides f if and only if a is a root of f, i.e., if the polynomial function evaluated at a is 0_F. Translating this to our problem, we have $x - 1_F$ divides f if and only if $f(1_F) = 0_F$. However, observe that $f(1_F) = a_n + \cdots + a_1 + a_0$. Thus, we have $x - 1_F$ divides f if and only if $a_n + \cdots + a_1 + a_0 = 0_F$, as claimed. $\square$

3. (5 points each)

(a) Let R and S be rings and $\varphi : R \to S$ a ring homomorphism. Show that $\ker \varphi = \{r \in R : \varphi(r) = 0_S\}$ is a subring of R.

Proof. First, observe that $0_R \in \ker(\varphi)$ as we showed in class that $\varphi(0_R) = 0_S$ for any ring homomorphism φ. Let $r_1, r_2 \in \ker \varphi$. We have

$$\begin{aligned}\varphi(r_1 + r_2) &= \varphi(r_1) + \varphi(r_2)\\ &= 0_S + 0_S\\ &= 0_S\end{aligned}$$

so $r_1 + r_2 \in \ker \varphi$ and

$$\begin{aligned}\varphi(r_1 r_2) &= \varphi(r_1)\varphi(r_2)\\ &= 0_S 0_S\\ &= 0_S\end{aligned}$$

so $r_1 r_2 \in \ker \varphi$. Finally, we have $-r_1$ is the additive inverse of r_1 and we showed in class $\varphi(-r_1) = -\varphi(r_1)$, so $\varphi(-r_1) = -0_S = 0_S$, so $-r_1 \in \ker \varphi$. Thus, $\ker \varphi$ is a subring of R. □

(b) Let $n \in \mathbb{Z}_{>1}$. Define a function $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\varphi(a) = [a]_n$. Show φ is a ring homomorphism. (You must use bracket notation for elements of $\mathbb{Z}/n\mathbb{Z}$ here so I can tell you know what you are doing.)

Proof. Let $a, b \in \mathbb{Z}$. Observe we have

$$\begin{aligned}\varphi(a + b) &= [a + b]_n\\ &= [a]_n + [b]_n\\ &= \varphi(a) + \varphi(b)\end{aligned}$$

and

$$\begin{aligned}\varphi(ab) &= [ab]_n\\ &= [a]_n[b]_n\\ &= \varphi(a)\varphi(b).\end{aligned}$$

Thus, φ is a ring homomorphism. □

(c) Show that $\ker \varphi = n\mathbb{Z} = \{m \in \mathbb{Z} : n \mid m\}$. Use this to conclude that $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.

Proof. Let $a \in \ker \varphi$, i.e., $\varphi(a) = [0]_n$. Thus, $[a]_n = [0]_n$, which is equivalent to $n \mid a$. Thus, $a \in n\mathbb{Z}$. Conversely, let $m \in n\mathbb{Z}$. Then $m = nb$ for some $b \in \mathbb{Z}$. We have $\varphi(m) = [m]_n = [nb]_n = [n]_n[b]_n = [0]_n[b]_n = [0]_n$. Thus, $m \in \ker \varphi$. Hence, $\ker \varphi = n\mathbb{Z}$. Since $n\mathbb{Z}$ is the kernel of a ring homomorphism with domain $\mathbb{Z}$, part (a) shows it is a subring of $\mathbb{Z}$. □

4. (15 points) Let R, S, and T be rings. Let $\varphi : R \to S$ and $\psi : S \to T$ be isomorphisms. Prove that $\psi \circ \varphi : R \to T$ is an isomorphism.

Proof. Let $r_1, r_2 \in R$. We have

$$\begin{aligned}(\psi \circ \varphi)(r_1 + r_2) &= \psi(\varphi(r_1 + r_2)) \\ &= \psi(\varphi(r_1) + \varphi(r_2)) \quad \text{(because } \varphi \text{ is a homomorphism)} \\ &= \psi(\varphi(r_1)) + \psi(\varphi(r_2)) \quad \text{(because } \psi \text{ is a homomorphism)} \\ &= (\psi \circ \varphi)(r_1) + (\psi \circ \varphi)(r_2)\end{aligned}$$

and

$$\begin{aligned}(\psi \circ \varphi)(r_1 r_2) &= \psi(\varphi(r_1 r_2)) \\ &= \psi(\varphi(r_1)\varphi(r_2)) \quad \text{(because } \varphi \text{ is a homomorphism)} \\ &= \psi(\varphi(r_1))\psi(\varphi(r_2)) \quad \text{(because } \psi \text{ is a homomorphism)} \\ &= (\psi \circ \varphi)(r_1)(\psi \circ \varphi)(r_2).\end{aligned}$$

Thus, $\psi \circ \varphi$ is a ring homomorphism.

Let $r \in \ker \psi \circ \varphi$, i.e., $\psi(\varphi(r)) = 0_T$. Since ψ is injective and a ring homomorphism, we have $\ker \psi = \{0_S\}$, so we must have $\varphi(r) = 0_S$. Now we use that φ is a ring homomorphism and injective to conclude that $\ker \varphi = \{0_R\}$, so $r = 0_R$. Thus, $\ker \psi \circ \varphi = \{0_R\}$ and so $\psi \circ \varphi$ is injective.

Let $t \in T$. Since ψ is surjective there exists $s \in S$ so that $\psi(s) = t$. The fact that φ is surjective gives $r \in R$ so that $\varphi(r) = s$. Thus, $\psi(\varphi(r)) = \psi(s) = t$ and so $\psi \circ \varphi$ is surjective.

Combining these results gives $\psi \circ \varphi$ is an isomorphism as claimed. □

5. (10 points) Let F be a field and $f, g \in F[x]$. Prove that if $f \mid g$ and $g \mid f$ then $f = cg$ for some $c \in F$.

Proof. Let $f, g \in F[x]$ with $f \mid g$ and $g \mid f$. Since $f \mid g$ there exists $c \in F[x]$ so that $g = cf$ and since $g \mid f$ there exists $d \in F[x]$ so that $f = dg$. Observe this gives $f = dg = d(cf) = dcf$. This gives that $\deg(dc) = 0$, so we must have $d, c \in F$ as claimed. □

6. (10 + 10 + 5+ 5 points) Let $R = \left\{ \begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix} \in \mathrm{Mat}_2(\mathbb{Z}/9\mathbb{Z}) \right\}$.

(a) Show that R is a subring of $\mathrm{Mat}_2(\mathbb{Z}/9\mathbb{Z})$.

Proof. Observe that $0_{\mathrm{Mat}_2(\mathbb{Z}/9\mathbb{Z})} = \begin{bmatrix} [0]_9 & [0]_9 \\ [0]_9 & [0]_9 \end{bmatrix} \in R$. Let $\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix}$ and $\begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix}$ be elements of R. We have

$$\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix} + \begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix} = \begin{bmatrix} [a+c]_9 & [0]_9 \\ [b+d]_9 & [0]_9 \end{bmatrix} \in R$$

and

$$\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix} \begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix} = \begin{bmatrix} [ac]_9 & [0]_9 \\ [bd]_9 & [0]_9 \end{bmatrix} \in R.$$

Moreover, the inverse of $\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix}$ is $\begin{bmatrix} [-a]_9 & [0]_9 \\ [-b]_9 & [0]_9 \end{bmatrix}$, which is in R. Thus, R is a subring of $\mathrm{Mat}_2(\mathbb{Z}/9\mathbb{Z})$. □

(b) Define a map $\varphi : R \to \mathbb{Z}/3\mathbb{Z}$ by $\varphi\left(\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix}\right) = [a]_3$. Show that φ is a well-defined ring homomorphism.

Proof. First we must show that φ is well defined. Let $\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix} = \begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix}$, i.e., $9 \mid (a-c)$ and $9 \mid (b-d)$. Thus, there exists $t \in \mathbb{Z}$ so that $a = c + 9t$. We have

$$\begin{aligned}
\varphi\left(\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix}\right) &= [a]_3 \\
&= [c+9t]_3 \\
&= [c]_3 + [9t]_3 \\
&= [c]_3 \\
&= \varphi\left(\begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix}\right).
\end{aligned}$$

Thus, the map is well-defined.

We have for any $\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix}, \begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix} \in R$ that

$$\begin{aligned}
\varphi\left(\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix} + \begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix}\right) &= \varphi\left(\begin{bmatrix} [a+c]_9 & [0]_9 \\ [b+d]_9 & [0]_9 \end{bmatrix}\right) \\
&= [a+c]_3 \\
&= [a]_3 + [c]_3 \\
&= \varphi\left(\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix}\right) + \varphi\left(\begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix}\right)
\end{aligned}$$

and

$$\begin{aligned}
\varphi\left(\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix} \begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix}\right) &= \varphi\left(\begin{bmatrix} [ac]_9 & [0]_9 \\ [bd]_9 & [0]_9 \end{bmatrix}\right) \\
&= [ac]_3 \\
&= [a]_3[c]_3 \\
&= \varphi\left(\begin{bmatrix} [a]_9 & [0]_9 \\ [b]_9 & [0]_9 \end{bmatrix}\right) \varphi\left(\begin{bmatrix} [c]_9 & [0]_9 \\ [d]_9 & [0]_9 \end{bmatrix}\right).
\end{aligned}$$

Thus, φ is a well-defined ring homomorphism. □

(c) Is φ surjective? If not, find its image.

The map is surjective as

$$\varphi\left(\begin{bmatrix}[0]_9 & [0]_9\\ [0]_9 & [0]_9\end{bmatrix}\right) = [0]_3$$
$$\varphi\left(\begin{bmatrix}[1]_9 & [0]_9\\ [0]_9 & [0]_9\end{bmatrix}\right) = [1]_3$$
$$\varphi\left(\begin{bmatrix}[2]_9 & [0]_9\\ [0]_9 & [0]_9\end{bmatrix}\right) = [2]_3.$$

(d) Is φ injective? If not, find its kernel.

The map is not injective. Note that $\begin{bmatrix}[a]_9 & [0]_9\\ [b]_9 & [0]_9\end{bmatrix} \in \ker\varphi$ if and only if $[a]_3 = [0]_3$, i.e., if $3 \mid a$. Thus, the kernel is given by

$$\ker\varphi = \left\{\begin{bmatrix}[a]_9 & [0]_9\\ [b]_9 & [0]_9\end{bmatrix} : [a]_9 = [0]_9, [3]_9, [6]_9\right\}.$$