Solutions to Midterm Exam 2

Math 401

1. (25 points) Consider the following commutative rings with four elements:

(i) $\mathbb{Z}_4$

(ii) $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(iii) $\mathbb{Z}_2[x]/(x^2)$

(iv) $\mathbb{Z}_2[y]/(y^2+1)$

(v) $\mathbb{Z}_2[z]/(z^2+z)$

(vi) $\mathbb{Z}_2[w]/(w^2+w+1)$

Show that:

(a) Show that (ii) is isomorpic to (v).
Hint: Consider the map $\varphi\colon \mathbb{Z}_2[z] \to \mathbb{Z}_2 \times \mathbb{Z}_2$ defined by $\varphi(f) = (f(0), f(1))$.

Solution: First we check that φ is a homomorphism:

$$\begin{aligned}\varphi(f+g) &= (f(0)+g(0), f(1)+g(1)) \\ &= (f(0), f(1)) + (g(0), g(1)) \\ &= \varphi(f) + \varphi(g)\end{aligned}$$

$$\begin{aligned}\varphi(fg) &= (f(0)g(0), f(1)g(1)) \\ &= (f(0), f(1)) \cdot (g(0), g(1)) \\ &= \varphi(f)\varphi(g)\end{aligned}$$

$$\varphi(1) = (1,1).$$

Next we observe that φ is surjective:

$$\varphi(0) = (0,0) \qquad \varphi(1) = (1,1) \qquad \varphi(z) = (0,1) \qquad \varphi(z+1) = (1,0)$$

Last we show that $\ker\varphi = (z^2+z)$. We have $\varphi(f) = (0,0)$ if and only if $f(0) = 0$ and $f(1) = 0$, which is true if and only if f is divisible by $z(z-1) = z^2+z$.

Now by the first isomorphism theorem (which Shifrin calls the fundamental homomorphism theorem) we have $\mathbb{Z}_2[z]/(z^2+z) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Show that (iii) is isomorphic to (iv).
Hint: Consider the map $\varphi\colon \mathbb{Z}_2[x] \to \mathbb{Z}_2[y]/(y^2+1)$ given by $\varphi(f) = \overline{f(y+1)}$. Observe that $y^2+1 = (y+1)^2$.

Solution: It is straightforward to check that φ is a homomorphism. Next we observe that φ is surjective:

$$\varphi(0) = 0 \qquad \varphi(1) = 1 \qquad \varphi(x) = \overline{y+1} \qquad \varphi(x+1) = \overline{y}.$$

It it remains to show that $\ker\varphi = (x^2)$. First, $\varphi(x^2) = \overline{(y+1)^2} = \overline{y^2+1} = 0$, so $x^2 \in \ker\varphi$, so $(x^2) \subset \ker\varphi$. Conversely, if $\overline{f(y+1)} = 0$ in $\mathbb{Z}_2[y]/(y^2+1)$ then there is a $g \in \mathbb{Z}_2[y]$ such that $f(y+1) = (y^2+1)g(y)$. Substituting $y = x+1$ we get $f(x) = x^2 g(x+1)$. Thus $\ker\varphi \subset (x^2)$.

(c) Show that (i) is not isomorphic to any of the others.
Hint: In (i) we have $1+1 \neq 0$.

Solution: Let R be any of the rings (ii)–(vi). Then we have $1+1 = 0$ in R. If $\varphi\colon \mathbb{Z}_4 \to R$ is any homomorphism then $\varphi(2) = \varphi(1+1) = \varphi(1)+\varphi(1) = 1+1 = 0$, so φ is not injective. Thus there is no bijective homomorphism from $\mathbb{Z}_4$ to R.

(d) Show that (ii) is not isomorpic to (iii).
Hint: In (ii) there is no non-zero element a with $a^2 = (0,0)$.

Solution: Let $\varphi\colon \mathbb{Z}_2[x]/x^2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ be any homomorphism. Then we have $\varphi(\bar{x})^2 = \varphi(\bar{x}^2) = \varphi(0) = (0,0)$. But every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ satisfies $a^2 = a$:

$$(0,0)^2 = (0,0) \quad (1,0)^2 = (1,0) \quad (0,1)^2 = (0,1) \quad (1,1)^2 = (1,1).$$

Thus $\varphi(\bar{x}) = \varphi(\bar{x})^2 = (0,0)$, so φ is not injective, and in particular not an isomorphism.

(e) Show that (vi) is not isomorphic to any of the others.
Hint: w^2+w+1 is irreducible, so (vi) is a field.

Solution: The polynomial $f = w^2+w+1 \in \mathbb{Z}_2[w]$ is a quadratic with no roots – indeed, $f(0) = f(1) = 1$ – so it is irreducible. Thus $\mathbb{Z}_2[w]/(w^2+w+1)$ is a field, by a theorem we proved in lecture. If it were isomorphic to any of the rings (i)–(v) then they too would be fields, but we will show that they are not even integral domains:

In (i) we have $2 \cdot 2 = 0$. In (ii) we have $(1,0)\cdot(0,1) = (0,0)$. In (iii) we have $\bar{x}\cdot\bar{x} = 0$. We have seen that (iv) is isomorphic to (iii) and (v) is isomorphic to (ii).

3. (25 points) Let R be a commutative ring and $I, J \subset R$ two ideals. Recall that IJ is the ideal generated by elements of the form ij where $i \in I$ and $j \in J$:

$$IJ = \{i_1 j_1 + i_2 j_2 + \cdots + i_k j_k : \\ i_1, \ldots, i_k \in I,\ j_1, \ldots, j_k \in J,\ k \text{ is allowed to vary}\}.$$

(a) Show that $IJ \subset I \cap J$.

Solution: Let $x = i_1 j_1 + \cdots + i_k j_k$ be an arbitrary element of IJ. Because I is an ideal, we have $i_l j_l \in I$ for all l, so x is a sum of elements in I, hence is in I. Because J is an ideal, we have $i_l j_l \in J$, so $x \in J$. Thus $x \in I \cap J$, as desired.

(b) Give an example with $R = \mathbb{Z}$ where IJ is a proper subset of $I \cap J$, that is, where they are not equal.

Solution: Take $I = J = (2)$. Then $I \cap J = I \cap I = I = (2)$, but $IJ = (4)$.

(c) Show that if $I + J = (1)$ then $IJ = I \cap J$.

Solution: We have seen that $IJ \subset I \cap J$, so it remains to show that $I \cap J \subset IJ$. Since $I + J = (1)$, there are elements $i \in I$ and $j \in J$ such that $i + j = 1$. Let $k \in I \cap J$, and multiply $i + j = 1$ through by k to get $ki + kj = k$. Write this more suggestively as

$$k = ik + kj.$$

The first term is in IJ because $k \in J$, and the second term is in IJ because $k \in I$, so $k \in IJ$ as desired.

(d) Show that the converse of part c holds when $R = \mathbb{Z}$ and $I, J \neq (0)$. (Hint: This isn't meant to be hard. Use the well-known description of the gcd and lcm of two integers in terms of their prime factorizations.)

Solution: Because $R = \mathbb{Z}$, we can write $I = (a)$ and $J = (b)$ for some positive integers a and b. Let $p_1, \ldots, p_n$ be the primes dividing either a or b, and write

$$a = p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n} \qquad\qquad b = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n},$$

where $i_1, \ldots, i_n, j_1, \ldots, j_n \geq 0$. Then the greatest common divisor of a and b is

$$d = p_1^{\min(i_1, j_1)} p_2^{\min(i_2, j_2)} \cdots p_n^{\min(i_n, j_n)},$$

and the least common multiple of a and b is

$$m = p_1^{\max(i_1, j_1)} p_2^{\max(i_2, j_2)} \cdots p_n^{\max(i_n, j_n)}.$$

But we have $i_l + j_l = \min(i_l, j_l) + \max(i_l, j_l)$, so $ab = dm$.

Now we have $IJ = (ab)$ and $I \cap J = (m)$ and $I + J = (d)$, and if $ab = m$ then $d = 1$.

(You can just assert that $ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$, but it's important to be clear that this is something that works in $\mathbb{Z}$ and not in an arbitrary commutative ring.)

(e) Show that the converse of part c does not hold in general by taking $R = \mathbb{Z}[x]$, $I = (2)$, and $J = (x)$.

Solution: We have $IJ = (2x)$. First I claim that $I \cap J = (2x)$ as well. We know that $IJ \subset I \cap J$, so it remains to show that $I \cap J \subset IJ$. Let $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$ be arbitrary. If $f \in I$ then $2 \mid f$, so all of the a_i are even. If $f \in J$ then $x \mid f$, so $a_0 = 0$. Thus if $f \in I \cap J$ then $a_0 = 0$ and the remaining a_i are even, so f is a multiple of $2x$, so $f \in IJ$.

Next I claim that $I + J = (2, x)$ is different from (1), and in fact that $1 \notin I + J$. Suppose we could write $1 = 2f + xg$ for some $f, g \in \mathbb{Z}[x]$. Plugging in $x = 0$, we get $1 = 2f(0) + 0g(0)$, but the left-hand side is odd while the right-hand side is even.