ASSIGNMENT 4

MATH 235

QUESTION 1

Part (1): Let R, S be commutative rings. Define the ring $R \times S$ with the following operations:

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2) \quad \text{and} \quad (r_1, r_2) \cdot (s_1, s_2) = (r_1 s_1, r_2 s_2)$$

with $\mathbb{0} := (\mathbb{0}_R, \mathbb{0}_S)$ and $\mathbb{1} := (\mathbb{1}_R, \mathbb{1}_S)$.

We've seen in class that this is indeed a ring.

Let $I \triangleleft R$ and $J \triangleleft S$. We have then that $I \subseteq R$ and $J \subseteq S$, so $I \times J \subseteq R \times S$.

1. Since $\mathbb{0}_R \in I$ and $\mathbb{0}_S \in J$, $(\mathbb{0}_R, \mathbb{0}_S) \in I \times J$.
2. Let $r_1, r_2 \in I$, $s_1, s_2 \in J \implies r_1 + r_2 \in I$ and $s_1 + s_2 \in J$.

   $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \in I \times J$, since $r_1 + r_2 \in I$, $s_1 + s_2 \in J$.
3. Let $(r_1, s_1) \in I \times J$, $(r_2, s_2) \in R \times S$. Then $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$. Since $r_1 \in I$ and $r_2 \in R$, $r_1 r_2 \in I$. Similarly, $s_1 s_2 \in J$. Thus $(r_1 r_2, s_1 s_2) \in I \times J$

We conclude that $I \times J \triangleleft R \times S$.

Part (2): Let Q be some ideal of $R \times S$. We do not know a priori that Q is a Cartesian product. Let I be the left coordinates of Q, i.e. $\{i : (i, \alpha) \in Q \text{ for some } \alpha\}$, and similarly define J to be the right coordinates of Q. We see immediately that $Q \subseteq I \times J$. To show that these are ideals of R and S, respectively:

1. Since $Q \triangleleft R \times S$, we know that $(\mathbb{0}_R, \mathbb{0}_S) \in Q$, so $\mathbb{0}_R \in I$ and $\mathbb{0}_S \in J$
2. Let $a, b \in I$. Consider (a, α_a) and (b, α_b), members of Q, where α_a, α_b are the unknown right coordinates relative to a and b. Then, $(a, \alpha_a) + (b, \alpha_b) = (a + b, \alpha_a + \alpha_b) \in Q$.

   $\implies a + b \in I$, since this is a left coordinate of an element in Q. Similarly, one sees that $c, d \in J \implies c + d \in J$
3. Let $a \in I$, and define $(a, \alpha_a) \in Q$ as above. Furthermore, let $(r, s) \in R \times S$. Then $(a, \alpha_a)(r, s) = (ar, \alpha_a r) \in Q$, and thus $ar \in I$. One shows $b \in J \implies br \in J$ the same way.

Now let $(i, \alpha_i), (\alpha_j, j) \in Q$, where $i \in I$, $j \in J$, and α_i, α_j are the unknown coordinates respective to i, j, as above. $(i, \alpha_i)(\mathbb{1}_R, \mathbb{0}_S) = (i, \mathbb{0}_S) \in Q$ and $(\alpha_j, j)(\mathbb{0}_R, \mathbb{1}_S) = (\mathbb{0}_R, j) \in Q$

$\implies (i, \mathbb{0}_S) + (\mathbb{0}_R, j) = (i, j) \in Q$. This is the same as saying $I \times J \subseteq Q$. But $Q \subseteq I \times J$, so $Q = I \times J$, and also $I \triangleleft R$ and $J \triangleleft S$ from above.

Part (3): Let W be the set of ideals of $\mathbb{Z} \times \mathbb{Z}$. From class, $\mathbb{Z}$ is a principal ideal ring with distinct ideals $(0), (1), (2), \ldots$. Thus, any ideal of $\mathbb{Z} \times \mathbb{Z}$ is of the form $(i) \times (j)$, so $W \subseteq \{(i) \times (j)\}$

over all $i, j \geq 0$. Further, by part (1), if (i) and (j) are ideals of $\mathbb{Z}$, then $(i) \times (j)$ is an ideal of $\mathbb{Z} \times \mathbb{Z}$, so $\{(i) \times (j)\} \subseteq W$. Thus, the ideals of $\mathbb{Z} \times \mathbb{Z}$ are exactly

$$W = \left\{ \underset{i,j \geq 0}{(i) \times (j)} \right\}$$

QUESTION 2

Part (1): Let $f : R \to S$ be a surjective homomorphism and I be an ideal of R. Define $f(I) := \{f(r) : r \in I\}$.

1. $\mathbb{0}_S \in f(I)$, since $f(\mathbb{0}_R) = \mathbb{0}_S$
2. Let $a, b \in f(I)$. Then $\exists a', b' \in I$ with $f(a') = a$ and $f(b') = b$. Note also that $a' + b' \in I$ Then $f(a' + b') = f(a') + f(b') = a + b$, so $a + b \in f(I)$.
3. Let $a \in f(I)$, $b \in S$. Since f is surjective, $\exists\ b' \in R : f(b') = b$. Also, $\exists\ a' \in I : f(a') = a$ and $a'b' \in I$ since $I \triangleleft R$. We have then that $f(a'b') = f(a')f(b') = ab \implies ab \in f(I)$

   $\implies f(I) \triangleleft S$

Part (2): Let $f : \mathbb{Q} \to \mathbb{R}$ be the identity function $f(x) = x$. f is not surjective since, for example, $\nexists\ q \in \mathbb{Q} : f(q) = \sqrt{2}$. However, f is a homomorphism:

In the text of the question, $\mathbb{Q} := R$ and $\mathbb{R} := S$

$$f(\mathbb{1}_{\mathbb{Q}}) = \mathbb{1}_{\mathbb{Q}} = 1 = \mathbb{1}_{\mathbb{R}} \qquad f(x+y) = x+y = f(x)+f(y) \qquad f(xy) = xy = f(x)f(y)$$

Now let $I \triangleleft \mathbb{Q}$ and $f(I) = \{f(q) : q \in I\}$. Note that, since $I \subseteq \mathbb{Q}$, its members are rational, and further $f(I) = I$. Pick $\sqrt{2} \in \mathbb{R}$ and $q \in f(I)$. $\sqrt{2}q$ is irrational, so $\sqrt{2}q \notin I = f(I)$, and we conclude that $f(I)$ is not an ideal of $\mathbb{Q}$.

QUESTION 3

Part (1): Let R be a ring and $I \triangleleft R, J \triangleleft R$. Consider $I \cap J := \{r : r \in I, r \in J\}$.

1. Since $\mathbb{0}_R \in I$ and $\mathbb{0}_R \in J$, $\mathbb{0}_R \in I \cap J$.
2. Let $a, b \in I \cap J$. Then $a, b \in I$, $a, b \in J$. Thus $a+b \in I$ and $a+b \in J \implies a+b \in I \cap J$.
3. Let $a \in I \cap J$, $r \in R$. Then $a \in I$ and $a \in J$, and we have $ar \in I$ and $ar \in J \implies ar \in I \cap J$

Thus, $I \cap J$ is an ideal of R.

Part (2): Let $I + J := \{i + j : i \in I, j \in J\}$. Again we check the axioms:

1. Since $\mathbb{0}_R \in I$ and $\mathbb{0}_R \in J$, $\mathbb{0}_R + \mathbb{0}_R = \mathbb{0}_R \in I + J$
2. Let $a, b \in I + J$. Then $\exists\ i_a, i_b \in I$ and $j_a, j_b \in J$ such that $i_a + j_a = a$ and $i_b + j_b = b$. Then $a + b = \underbrace{i_a + i_b}_{\in I} + \underbrace{j_a + j_b}_{\in J} \implies a + b \in I + J$
3. Let $a \in I + J$, $r \in R$. Then again $\exists\ i \in I, j \in J : i + j = a$. We have $ar = (i + j)r = \underbrace{ir}_{\in I} + \underbrace{jr}_{\in J} \implies ar \in I + J$

Part (3): The ideals of $\mathbb{Z}$ are $i\mathbb{Z}$ for $i \geq 0$. Thus, consider $a \in i\mathbb{Z} \cap j\mathbb{Z}$. Then $a \in i\mathbb{Z}$, so $i|a$, and similarly $j|a$. We conclude that a is a common multiple of i and j.

Conversely, consider the set L of common multiples of i and j. If $l \in L$, then $l = n_1 i$ and $l = n_2 j$ for integers n_1, n_2. Thus, $l \in i\mathbb{Z}$ and $j\mathbb{Z} \implies l \in i\mathbb{Z} \cap j\mathbb{Z}$. We conclude that $i\mathbb{Z} \cap j\mathbb{Z}$ is precisely the set of common multiples of i and j, i.e. $\operatorname{lcm}(i, j)k$ for integer k, or

$$\operatorname{lcm}(i, j)\mathbb{Z}$$

Now consider the sum of two ideals of $\mathbb{Z}$, $i\mathbb{Z} + j\mathbb{Z} = \{n_1 + n_2 : n_1 \in i\mathbb{Z}, n_2 \in j\mathbb{Z}\}$. We can re-write this as $\{in_1 + jn_2 : n_1, n_2 \in \mathbb{Z}\}$. We know that $\gcd(i, j)$ is in this set, where n_1 and n_2 are fixed according to Bezout's identity. Even more, for any integer k, $k\gcd(i, j) = in_1k + jn_2k$ is in this set as well. $\implies \gcd(i, j)\mathbb{Z} \subseteq i\mathbb{Z} + j\mathbb{Z}$.

Now consider an element $a \in i\mathbb{Z} + j\mathbb{Z}$, and write $a = in_1 + jn_2$. We have that $\gcd(i, j)|i$, so $\gcd(i, j)|in_1$. Similarly, $(i, j)|jn_2$. Thus $(i, j)|in_1 + jn_2$. We can then say $a = (i, j)k$ for some integer k, or $a \in (i, j)\mathbb{Z}$. Thus, $i\mathbb{Z} + j\mathbb{Z}$ is the set

$$\gcd(i, j)\mathbb{Z}$$

QUESTION 4

Define the relation $R \sim S$ if there exists a bijective homomorphism $f : R \to S$. This is an equivalence relation:

$R \sim R$ Let R be a ring and define $f : R \to R$ by $f(r) = r$. This is a bijection. To show it is a homomorphism:

(a) $f(\mathbb{1}_R) = \mathbb{1}_R$ ✓

(b) $f(r_1 + r_2) = r_1 + r_2 = f(r_1) + f(r_2)\ \forall r_1, r_2 \in R$ ✓

(c) $f(r_1 r_2) = r_1 r_2 = f(r_1)f(r_2)$ ✓

$R \sim S \implies S \sim R$ Let $f : R \to S$ be a bijective homomorphism. Then consider $f^{-1} : S \to R$, which is also a bijection. This is a homomorphism:

(a) Since $f(\mathbb{1}_R) = \mathbb{1}_S$, $f^{-1}(\mathbb{1}_S) = \mathbb{1}_R$ ✓

(b) For any $s_1, s_2 \in S$ where $f(r_1) = s_1$ and $f(r_2) = s_2$ for $r_1, r_2 \in R$, we have $f^{-1}(s_1 + s_2) =$

$$f^{-1}[f(r_1) + f(r_2)] = f^{-1}[f(r_1 + r_2)] = r_1 + r_2 = f^{-1}(s_1) + f^{-1}(s_2) \checkmark$$

(c) Similarly, $f^{-1}(s_1 s_2) = f^{-1}[f(r_1)f(r_2)] = f^{-1}[f(r_1 r_2)] = r_1 r_2 = f^{-1}(s_1)f^{-1}(s_2)$ ✓

$\sim R, R \sim S \implies Q \sim S$ Let Q, R, S be rings with $f : Q \to R$ and $g : R \to S$ both be bijective homomorphisms. Consider the function $g \circ f : Q \to S$. Since the composition of two bijective functions is bijective, this is bijective. This is also a homomorphism between Q and S:

(a) $g \circ f(\mathbb{1}_Q) = g(\mathbb{1}_R) = \mathbb{1}_S$ ✓

(b) $g[f(q_1 + q_2)] = g[f(q_1) + f(q_2)] = g[f(q_1)] + g[f(q_2)]$ ✓

(c) $g[f(q_1 q_2)] = g[f(q_1)f(q_2)] = g[f(q_1)]g[f(q_2)]$ ✓

Question 5

Note that $\mathbb{0}_{\mathbb{Z}} = 0$ and $\mathbb{0}_{\mathbb{Z}/5\mathbb{Z}} = \overline{0}$

Part (1): Suppose there was a homomorphism $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}$. Then $f(\overline{5}) = f(\overline{0}) = 0$. However, we can write

$$f(\overline{5}) = f(\overline{1}) + f(\overline{1}) + f(\overline{1}) + f(\overline{1}) + f(\overline{1}) = 1 + 1 + 1 + 1 + 1 = 5$$

We have $5 = 0$, which is a contradiction $\lightning$

Part (2): Now let $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ be a homomorphism. Then

$$f(\overline{5}) = f(\overline{1}) + ... + f(\overline{1}) = 5(1 \bmod 7) = 5 \bmod 7$$

But also $f(\overline{5}) = f(\overline{0}) = 0 \bmod 7$, which establishes the contradiction.

Part (3): Let $f : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ be an isomorphism, i.e. a bijective homomorphism. Let s be an element in $\mathbb{Z}/4\mathbb{Z}$. Then $\exists r \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with $f(r) = s$. Consider $s + s$. This is $f(r) + f(r) = f(2r) = f[(2i, 2j)] = f[(0, 0)] = 0 \bmod 4$ for $i, j \in \mathbb{Z}/2\mathbb{Z}$.

For the contradiction, one can take, for instance, $s = 1$ to find that $2(1) = 2 \bmod 4 = 0$ $\lightning$

Part (5): Part (4) is on the next page, since it's lengthy.

No, there is not a homomorphism from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$. Suppose there was one. Then $f[(2, 2)] = f[(0, 0)]$, which must map to $0 \bmod 4$. However, $f[(2, 2)] = f[(1, 1) + (1, 1)] = f[(1, 1)] + f[(1, 1)]$, each of which must map to $1 \bmod 4$, so $2 \bmod 4$.

We conclude that $0 \equiv 2 \bmod 4$, which is a contradiction.

Part (4): Let $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ be defined as:

$$f(x) = \begin{cases} (1,1) & \text{if } x \text{ is odd} \\ (0,0) & \text{if } x \text{ is even} \end{cases}$$

noting that the co-domain $(1,1)$ and $(0,0)$ are defined in mod 2. We'll show that this is a homomorphism:

$$f(1 \bmod 4) = (1 \bmod 2, 1 \bmod 2) \qquad \text{1 maps to 1}$$

$$f(a+b) = \begin{cases} (0,0) & \text{if } a,b \text{ same parity} = \begin{cases} \overbrace{(0,0)+(0,0) = f(a)+f(b)}^{\text{for } a,b \text{ even}} \\ \underbrace{(2,2) = (1,1)+(1,1) = f(a)+f(b)}_{\text{for } a,b \text{ odd}} \end{cases} \\ (1,1) & \text{if } a,b \text{ opposite parity} = (0,0)+(1,1) = f(a)+f(b) \end{cases} \qquad f(a+b) = f(a)+f(b)$$

$$f(ab) = \begin{cases} (0,0) & \text{if } a,b \text{ even} = (0,0)(0,0) = f(a)f(b) \\ (0,0) & \text{if } a,b \text{ opposite parity} = (1,1)(0,0) = f(a)f(b) \\ (1,1) & \text{if } a,b \text{ odd} = (1,1)(1,1) = f(a)f(b) \end{cases} \qquad f(ab) = f(a)f(b)$$

and we are done.