Homework 4

Madilyn Simons

1. Consider $\mathbb{Z}_4 = 0, 1, 2, 3$. We know 0 is not a zero divisor since a zero divisor is a nonzero element by definition. We know that 1 is not a zero because $1x = x$ for all x and then x must be 0 if $1x = 0$. We know that 2 IS a zero divisor because $2 \cdot 2 = 4 = 0$. We know that 3 is not a zero divisor because 3 and 4 are relatively prime, meaning any zero element of $\mathbb{Z}_4$ must be a multiple of 4, which equals 0. Therefore, there does exist a ring with one zero divisor.

2. First, let us prove that $\cong$ is symmetric. Since $f : R \to S$ is an isomorphism, this means that f is bijective. Let $f(r) = s$ for some $r \in R$ and some $s \in S$. If f is bijective, there exists some function $g : S \to R$ such that $g(s) = g(f(r)) = r$.

   To prove g is injective, let $s, s' \in S$ and $r, r' \in R$ such that $s \neq s'$, $r \neq r'$, $f(s) = r$, and $f(s') = r'$. As such, $g(s) = g(f(r)) = r$ and $g(s') = g(f(r')) = r'$. Since $r \neq r'$, this implies that if $s \neq s'$, then $r \neq r'$ and g must be injective.

   Because Im $f = S$, there is an $r \in R$ for all $s \in S$ such that $s = f(r)$. Because $g(s) = g(f(r)) = r$, Im $g = R$ and g is surjective.

   We can prove that $g(s) + g(s') = g(s + s')$ as such:

   $$g(s)+g(s') = g(f(r))+g(f(r')) = r+r' = g(f(r+r')) = g(f(r)+f(r')) = g(s+s')$$

   We can prove $g(s)g(s') = g(ss')$ as such:

   $$g(s)g(s') = g(f(r))g(f(r')) = rr' = g(f(rr')) = g(f(r)f(r')) = g(ss')$$

   Therefore, g is an isomorphism and $\cong$ is symmetric.

   Next, we prove that $\cong$ is transitive. If f and g are isomorphisms, then there exists $r \in R$, $s \in S$, and $t\ inT$ such that $f(r) = s$ and $g(s) = t$. As such, let $h : R \to T$ be the function such that $h(r) = g(f(r)) = g(s) = t$.

   Let $g(s') = t'$ for some $s' \in S$ and $t' inT$ such that $s \neq s'$ and $t \neq t'$.

We know h is injective because $h(r) = g(f(r)) = g(s) = t$ and $h(r') = g(f(r')) = g(s') = t'$ and $t \neq t'$.

We know h is surjective because the Im f is S and Im g is T. Therefore, for all $t \in T$ there is a solution to $h(r) = t$.

We prove $h(r) + h(r') = h(r + r')$ as such:

$$h(r) + h(r') = g(f(r)) + g(f(r')) = g(f(r + r')) = h(r + r')$$

We prove $h(r)h(r') = h(rr')$ as such:

$$h(r)h(r') = g(f(r))g(f(r')) = g(f(r)f(r')) = g(f(rr')) = h(rr')$$

Therefore h is an isomorphism and $\cong$ is transitive.

3. TODO

4. TODO

5. Let $f : R \to \mathbb{Q}[\sqrt{2}]$ be the function $f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}) = a + b\sqrt{2}$ such that $a, b \in \mathbb{Q}$.

   To prove injection, let $c, d \in \mathbb{Q}$ such that $a \neq c$ and $b \neq d$. Also, assume $f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}) = f(\begin{bmatrix} c & d \\ 2d & c \end{bmatrix})$. As such:

   $$f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}) = f(\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}) a + b\sqrt{2} = c + d\sqrt{2} a - c = \sqrt{2}(d - b)\sqrt{2} = (a - c)/(d - b)$$

   Since $\sqrt{2}$ is an irrational number and $(a - c)/(d - b)$ is a rational number, this is a contradiction. Thus, f is injective.

   We know that f is surjective because Im $f = \mathbb{Q}$.

   We can prove $f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}) + f(\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}) = f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} + \begin{bmatrix} c & d \\ 2d & c \end{bmatrix})$ as such:

   $$\begin{gathered} f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}) + f(\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}) \\ = (a + bi) + (c + di) = (a + c) + (b + d)i \\ = f(\begin{bmatrix} a + c & b + d \\ 2(b + d) & a + c \end{bmatrix}) \end{gathered}$$

$$= f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} + \begin{bmatrix} c & d \\ 2d & c \end{bmatrix})$$

We can prove $f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix})f(\begin{bmatrix} c & d \\ 2d & c \end{bmatrix}) = f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \begin{bmatrix} c & d \\ 2d & c \end{bmatrix})$ as such:

$$f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix})f(\begin{bmatrix} c & d \\ 2d & c \end{bmatrix})$$

$$= (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

$$= f(\begin{bmatrix} ac + 2bd & ad + bc \\ 2(ad + bc) & ac + 2bd \end{bmatrix}) = f(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \begin{bmatrix} c & d \\ 2d & c \end{bmatrix})$$

Therefore, f is an isomorphism and R is isomorphic to $\mathbb{Q}[\sqrt{2}]$.

6. The rings are not isomorphic because $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}$ is a 170-element set and $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$ is an 180-element set and it is not possible to have a surjective function from an 170-element set to an 180-element set.