# Math 333 Problem Set 6
# Due: 03/28/16

Be sure to list EVERYONE in the that you talk to about the homework!

1. Let $R$ be a ring with identity $1_R$. Set $S = \{n1_R : n \in \mathbb{Z}\}$ where we recall $n1_R = 1_R + \cdots + 1_R$ with $n$-copies of $1_R$ on the right hand side. Show that $S$ is a subring of $R$.

   *Proof.* The first thing one needs to do here is define what we mean by $n1_R$ for those integers not in $\mathbb{Z}_{\geq 1}$ since in those cases the definition given in the problem is not sufficient. If $n \in \mathbb{Z}_{<0}$ we set $n1_R = (-1_R) + (-1_R) + \cdots (-1_R)$ where there are $-n$ copies of $-1_R$. We define $01_R = 0_R$. We clearly have that $S$ is nonempty and contains $0_R$ by definition of $01_R$.

   Closed under addition: Let $m, n \in \mathbb{Z}$. If $m$ and $n$ are positive then $m1_R + n1_R = (m+n)1_R \in S$. If $m > 0$ and $n = 0$ we have $m1_R + 01_R = m1_R + 0_R = m1_R \in S$. Suppose $m > 0$ and $n < 0$. Then we have $m1_R + n1_R = (1_R + \cdots 1_R) + ((-1_R) + \cdots + (-1_R) = (m+n)1_R \in S$. Similarly, if $m$ and $n$ are both negative we have $m1_R + n1_R = (m+n)1_R \in S$. Finally, if $m < 0$ and $n = 0$ we have $m1_R + n1_R = m1_R \in S$.

   Closed under multiplication: Let $m, n \in \mathbb{Z}$. If either $m$ or $n$ is 0 we immediately have $(m1_R)(n1_R) = 0_R = 01_R \in S$. Assume $m$ and $n$ are both positive. Then we have $(m1_R)(n1_R) = \left(\sum_{j=1}^{m} 1_R\right)\left(\sum_{i=1}^{n} 1_R\right) = mn1_R$. Similarly, one obtains the same result in the cases $m$ and $n$ are both negative or one is positive and one is negative.

   Closed under additive inverse: Let $m1_R \in S$. Observe we have $m1_R + (-m)1_R = (m-m)1_R = 01_R = 0_R$, thus the additive inverse of $m1_R$ is $(-m)1_R$, which is in $S$.

   Thus, $S$ is a subring of $R$. $\square$

2. Let $R$ and $S$ be rings. Let $T = \{(r, 0_S) : r \in R\}$ be a subset of $R \times S$. Prove that $T$ is a subring of $R \times S$.

   *Proof.* Observe that since $R$ is a ring we have $0_R \in R$ and so $(0_R, 0_S) \in T$. Moreover, $(0_R, 0_S) = 0_T$ so $T$ is nonempty and contains the identity element. Let $(r_1, 0_S), (r_2, 0_S) \in T$.

Closed under addition: We have $(r_1, 0_S) + (r_2, 0_S) = (r_1 + r_2, 0_S) \in T$, so $T$ is closed under addition.

Closed under multiplication: We have $(r_1, 0_2)(r_2, 0_S) = (r_1 r_2, 0_2) \in T$, so $T$ is closed under multiplication.

Closed under additive inverses: We have an additive inverse $-r_1 \in R$ because $R$ is a ring. Thus, $(-r_1, 0_S) \in T$ is the additive inverse of $(r_1, 0_S)$.

Thus, we see $T$ is a subring of $R \times S$. □

3. Let $S$ and $T$ be subrings of a ring $R$. In (a) and (b), if the answer is "yes," prove it. If the answer is "no," give a counterexample.

(a) Is $S \cap T$ a subring of $R$?

*Proof.* Note that since $S$ and $T$ are subrings, we have $0_R$ is in each, so is in their intersection. Let $a, b \in S \cap T$. Since $S$ is a ring we have $a+b$ and $ab$ are both in $S$ and similarly $a+b$ and $ab$ are in $T$. Thus, $S \cap T$ is closed under addition and multiplication. Since $S$ is a subring we have an additive inverse $x$ of $a$ in $S$ and since $T$ is a subring there is an additive inverse of $a$ in $T$. Since additive inverses are unique, the additive inverse of $a$ is in $S \cap T$. Thus, $S \cap T$ is a subring of $R$. □

(b) Is $S \cup T$ a subring of $R$?

Consider the subrings $6\mathbb{Z}$ and $8\mathbb{Z}$ of $\mathbb{Z}$. Note that $6 \in 6\mathbb{Z}$ and $8 \in 8\mathbb{Z}$ but $6 + 8 = 14$ is not in $6\mathbb{Z}$ or $8\mathbb{Z}$, so it is not in their union. Thus, the union of $6\mathbb{Z}$ and $8\mathbb{Z}$ is not closed under addition and so not a subring.

4. (a) If $ab$ is a zero divisor in a commutative ring $R$, prove that $a$ or $b$ is a zero divisor.

*Proof.* Let $ab$ be a zero divisor, i.e., there exists a nonzero element $c \in R$ so that $abc = 0_R$. If $bc = 0_R$ we are done as that means $b$ is a zero divisor ($b \neq 0_R$ because if $b = 0_R$, then $ab = 0_R$ which is a contradiction since $ab$ is a zero divisor.) If $bc \neq 0_R$, then $a$ is a zero divisor. Thus, $a$ or $b$ is a zero divisor. □

(b) If $a$ or $b$ is a zero divisor in a commutative ring $R$ and $ab \neq 0_R$, prove that $ab$ is a zero divisor.

*Proof.* Let $a$ or $b$ be a zero divisor and assume $ab \neq 0_R$. If $a$ is a zero divisor, then there exists a nonzero $c \in R$ so that $ac = 0_R = ca$. Thus, $c(ab) = (ca)b = 0_R$ so $ab$ is a zero divisor. Similarly, if $b$ is a zero divisor, then there exists a nonzero $d \in R$ so that $bd = 0_R = db$. Thus, $(ab)d = a(bd) = 0_R$. Thus, $ab$ is a zero divisor. □

5. Assume that $R = \{0_R, 1_R, a, b\}$ is a ring and $a$ and $b$ are units. Write out the multiplication table for $R$.

The main issue here is to determine $a^2, b^2$ and $ab$. Since $a$ is a unit we must have $a^2 = 1_R$ or $ab = 1_R$. Suppose that $a^2 = 1_R$. Since inverses are unique we cannot have $ab = 1_R$; we cannot have $ab = 0_R$ because a unit cannot be a zero divisor, and if $ab = a$ then multiplying both sides by $a$ gives $b = 1_R$, a contradiction. Thus, if $a^2 = 1_R$ we must have $ab = b$. However, this is a contradiction since $b$ is a unit so we obtain $(a - 1_R)b = 0_R$ and so $a = 1_R$ or $b = 0_R$, both of which are contradictions. Thus, we cannot have $a^2 = 1_R$. The same argument shows $b^2$ cannot be $1_R$. Thus, it must be the case that $ab = 1_R = ba$. Thus, we must have $a^2 = b$ and $b^2 = a$. This allows one to fill in the multiplication table.

6. An element $a$ of a ring $R$ is *nilpotent* if $a^n = 0_R$ for some positive integer $n$. Prove that $R$ has no nonzero nilpotent elements if and only if $0_R$ is the only solution of the equation $x^2 = 0_R$.

*Proof.* First, suppose that $R$ has no nonzero nilpotent elements. If $a$ is a solution to $x^2 = 0_R$, then $a = 0_R$ for otherwise $a$ would be a nonzero nilpotent element. Now suppose $0_R$ is the only solution to the equation $x^2 = 0_R$. Suppose $a \in R$ is a nonzero nilpotent element, i.e., $a^n = 0_R$ for some positive integer $n$ and assume $n$ is the smallest such positive integer. If $n$ is even, say $n = 2k$ for some $k \in \mathbb{Z}$, then $0_R = a^{2k} = (a^k)^2$. This contradicts our assumption that $0_R$ is only solution to the equation $x^2 = 0_R$ as $a^k \neq 0_R$ by our assumption $n$ is minimal positive integer so that $a^n = 0_R$. If $n$ is odd, say $n = 2k + 1$

for some $k \in \mathbb{Z}$. Then we have $a^{2k+1} = 0_R$. Multiplying both sides by $a$ gives $a^{2k} = 0_R$ and we are in the case we just handled. Thus, we cannot have a nonzero nilpotent element as claimed. $\square$

7. Let $R$ be a ring with identity. If there is a smallest integer $n$ so that $n1_R = 0_R$, then $R$ is said to have characteristic $n$. If no such $n$ exists, $R$ is said to have characteristic zero.

   (a) Show that $\mathbb{Z}$ has characteristic zero and $\mathbb{Z}/n\mathbb{Z}$ has characteristic $n$.

   It is clear that $\mathbb{Z}$ has characteristic zero because $m1 \neq 0$ for all integers $m > 0$.

   We clearly have $n[1]_n = [n]_n = [0]_n$. However, to see that the characteristic of $\mathbb{Z}/n\mathbb{Z}$ is $n$ we have to show there is no smaller positive integer $m$ so that $m[1]_n = [0]_n$. If $m[1]_n = [0]_n$, then $[m]_n = [0]_n$, i.e., $n \mid m$. This can only happen if $m = 0$ or $m \geq n$. Thus, $n$ is the characteristic of $\mathbb{Z}/n\mathbb{Z}$.

   (b) What is the characteristic of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

   Set $R = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. It is easy to $121_R = 0_R$. Suppose that $m1_R = 0_R$ for some positive integer $m$. Then we must have $m[1]_4 = [0]_4$ and $m[1]_6 = [0]_6$. This means that $4 \mid m$ and $6 \mid m$, i.e., the least common multiple of 4 and 6 must divide $m$. This gives $12 \mid m$ as desired.

8. (a) Show that $R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in \mathrm{Mat}_2(\mathbb{R}) \right\}$ is a subring of $\mathrm{Mat}_2(\mathbb{R})$.

   *Proof.* We have $0_{\mathrm{Mat}_2(\mathbb{R})} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$. This gives $R$ is nonempty and contains the additive identity. Let $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in R$. We have $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} a+c & 0 \\ 0 & b+d \end{bmatrix} \in R$ and $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} =$

$\begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in R$. Thus, $R$ is closed under addition and multiplication. Finally, the additive inverse of $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ in $\mathrm{Mat}_2(\mathbb{R})$ is $\begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix}$, which is clearly in $R$. Thus, $R$ is a subring of $\mathrm{Mat}_2(\mathbb{R})$. □

(b) Show that $R$ is isomorphic to $\mathbb{R} \times \mathbb{R}$.

*Proof.* Define $\varphi : R \to \mathbb{R} \times \mathbb{R}$ by $\varphi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right) = (a, b)$. One can show this is bijective by checking injective and surjective, but in this case it is easy to define an inverse function $\psi : \mathbb{R} \times \mathbb{R} \to R$ by $\psi(a, b) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$. It is clear that $\varphi \circ \psi$ is the identity map on $\mathbb{R} \times \mathbb{R}$ and $\psi \circ \varphi$ is the identity on $R$. Thus, we have $\varphi$ is bijective.

Let $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in R$. We have

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

and

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

Thus, $\varphi$ is an isomorphism between $R$ and $\mathbb{R} \times \mathbb{R}$. □