Mathematics 103B Homework 2
Due: Wednesday 14 April 2021

Instructions: Please write clearly and fully explain your solutions. It is OK to work with others to solve the problems, but if you do so, you should write your solutions up separately. Copying solutions from your peers or a solutions manual will be deemed academic misconduct. Chapter and problem numbers refer to Contemporary Abstract Algebra, ninth edition, by Joseph A. Gallian. Please feel free to reach out to me or the TA if you have any questions.

1. Chapter 12, number 40.

Proof. The set $R$ is not a subring. It is not closed under multiplication. For example,

\[
\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}
\]

is not of the form \( \begin{pmatrix} a & a + b \\ a + b & b \end{pmatrix} \), even though \( \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \) and \( \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \) are of this form.

2. Chapter 12, number 41.

Proof. The set $R$ is a subring. It is easy to see that $R$ is nonempty and closed under subtraction. The interesting part is that $R$ is also closed under multiplication. Indeed,

\[
\begin{pmatrix} a & a - b \\ a - b & b \end{pmatrix} \begin{pmatrix} c & c - d \\ c - d & d \end{pmatrix} = \frac{ac + (a - b)(c - d)}{(a - b)c + b(c - d)} \cdot \frac{a(c - d) + d(a - b)}{bd + (a - b)(c - d)}
\]

\[
= \begin{pmatrix} ac - bd & ac - bd \\ ac - bd & bd + (a - b)(c - d) \end{pmatrix}
\]

is of the desired form.

3. Chapter 13, number 5.

Proof. Suppose $m$ is an integer, and consider the image of $m$ in $\mathbb{Z}/n\mathbb{Z}$. If $m$ is relatively prime to $n$, then $m$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. Indeed, because $n, m$ are relatively prime, there exists integers $x, y$ so that $mx + ny = 1$, and thus $mx = 1$ in $\mathbb{Z}/n\mathbb{Z}$. (You might also recall directly from 103A that if $m$ is relatively prime to $n$, then it has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$.) Conversely, suppose $m$ is not 0 in $\mathbb{Z}/n\mathbb{Z}$ and that $m$ shares a common factor with $n$. Then we can write $m = dm'$ and $n = dn'$ for a positive integer $d > 1$. Then $n'm = dnn' = nm'$ is 0 in $\mathbb{Z}/n\mathbb{Z}$, but neither $m$ nor $n'$ is 0 in $\mathbb{Z}/n\mathbb{Z}$, so $m$ is a zero-divisor.


Proof. For example, take $R = \mathbb{Z}/12\mathbb{Z}$, $a = 4$ and $b = 3$. Then $4 \cdot 3 = 0$ in $R$, so that both 4 and 3 are zero-divisors in $R$. However, $4 + 3 = 7$ is a not a zero divisor in $R$ because 7 is relatively prime to 12 (see the previous problem.)
5. Chapter 13, number 18. Also, find all the idempotents in \( \mathbb{Z}/6\mathbb{Z} \).

Proof. Suppose \( R \) is an integral domain, and \( a^2 = a \) in \( R \). Then \( a^2 - a = 0 \), so \( a(a - 1) = 0 \). Because \( R \) is an integral domain, we obtain \( a = 0 \) or \( a - 1 = 0 \). In other words, that \( a = 0 \) or \( a = 1 \).

For the second part, one can test all the elements of \( \mathbb{Z}/6\mathbb{Z} \) to see that 0, 1, 3, 4 are the idempotents in \( \mathbb{Z}/6\mathbb{Z} \). \( \square \)