Abstract Algebra Homework 8

Joe Loser

April 3, 2016

This problem set includes problems $2, 24, 28, 34$, and 38 from section 16.6.

2) Let R be the ring of 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

where $a, b \in \mathbb{R}$. Show that although R is a ring that has no identity, we can find a subring S of R with an identity.

<u>Proof</u>: We first show that R has no identity. Suppose for the sake of contradiction that R has an identity which we denote 1_R. From the definition of R we see that $1_R \in R$ means there exist $a, b \in \mathbb{R}$ such that $1_R = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$. Since the element $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in R$ and 1_R is the identity for R we have that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot 1_R = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

But from the definition of multiplication in R we also have that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot 1_R = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

Thus we see that $a = 1, b = 0$. This means that

$$1_R = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

However, this element 1_R is clearly not the identity for R. For instance, consider another element, say $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in R$. We have that

$$1_R \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \tag{1}$$

Also,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot 1_R = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \tag{2}$$

Since the right hand side of both (1) and (2) do not agree, we see that 1_R cannot be the identity for R which is a contradiction. Thus R is a ring without an identity element.

Even though R has no identity element, we can find a subring S of R which has an identity. We claim that $S = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ where $a \in \mathbb{R}$ is a subring of R. We will use the Subring Test to show that this is indeed a subring.

i) We first see that S is clearly nonempty since a is any real number.

ii) We now show that $rs \in S$ for all $r, s \in S$. Let $r = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ and $s = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$ where $a, b \in \mathbb{R}$. Then we have that

$$\begin{aligned} rs &= \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \\ &\in S \end{aligned}$$

since $ab \in \mathbb{R}$ because a and b are both in $\mathbb{R}$.

iii) Lastly, we show that $r - s \in S$ for all $r, s \in S$. Let r and s be as above in ii). Then

$$\begin{aligned} r - s &= \begin{pmatrix} a-b & 0 \\ 0 & 0 \end{pmatrix} \\ &\in S \end{aligned}$$

since $a - b \in \mathbb{R}$ because both a and b are in $\mathbb{R}$.

Thus we have shown that $S = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is indeed a subring of R by the Subring Test. $\square$

24) Let R be a ring with a collection of subrings $\{R_\alpha\}$. Prove that $\bigcap R_\alpha$ is a subring of R. Give an example to show that the union of two subrings need not be a subring.

Proof: Let S be the intersection of a collection of subrings of the ring R. That is, $S = \bigcap\limits_{i \in I} S_i$ where I is an indexed set and each S_i is a subring of R. We will use the Subring Test to show that S is indeed a subring of R.

We first begin with a claim and its proof to use it later on.

Claim: If S is a subring of a ring R then $0 \in S$.

Proof of Claim: If S is a subring of R then S is nonempty. Let $x \in S$. Then since S is a ring and has closure under additive inverses and addition, we have that $x + (-x) \in S$. By definition of additive inverses, $x + (-x) = 0$. Thus $0 \in S$.

We now check the conditions of the Subring Test hold.

i) To show that S is nonempty, just apply the result from the claim. Since $0 \in S_i$ for each $i \in I$ we have that $0 \in \bigcap_{i\in I} S_i$; i.e. $0 \in S$.

ii) Next we show for all $a, b \in S, a - b \in S$. Let $a, b \in S$. By definition of S we see $a, b \in S_i$ for each $i \in I$. By assumption that each S_i is a subring (and so S_i is a ring), we have that $a - b \in S_i$ for each $i \in I$. Then by definition of intersection, this means that $a - b \in \bigcap_{i\in I} S_i$ for each $i \in I$. That is, $a - b \in S$.

iii) Lastly we show that for all $a, b \in S, ab \in S$. Let $a, b \in S$. By definition of S we see that $a, b \in S_i$ for each $i \in I$. By assumption that each S_i is a subring (and so S_i is a ring), we have that $ab \in S_i$ for each $i \in I$. Then by definition of intersection, this means that $ab \in \bigcap_{i\in I} S_i$ for each $i \in I$. That is, $ab \in S$.

Thus S is a subring by the Subring Test.

To give an example to show that the union of two subrings need not be a subring, consider the following:

$$R = \mathbb{Z} \quad S = \{2n \mid n \in \mathbb{Z}\} \quad T = \{3n \mid n \in \mathbb{Z}\}.$$

Note that R is a ring and S and T are subrings of R (one can easily verify this – see Example 16.9 in the text). We will show that $S \cup T$ is not a subring of R. Consider two elements: $2 \in S, 3 \in T$. Clearly both are in $S \cup T$. However $2 + 3 = 5 \notin S \cup T$. So $S \cup T$ is not a ring (and hence not a subring of R). □

28) A ring R is a Boolean ring if for every $a \in \mathbb{R}, a^2 = a$. Show that every Boolean ring is a commutative ring.

Proof: We know that R is a commutative ring if $ab = ba$ for all $a, b \in R$.

Let $a, b \in R$. Notice that since R is a Boolean ring and $a, b \in R$ we have that

$$\begin{aligned} a + b &= (a + b)^2 \\ &= (a + b)(a + b) \\ &= a(a + b) + b(a + b) \\ &= a^2 + ab + ba + b^2 \\ &= a + ab + ba + b^2 \quad \because a^2 = a \quad \text{and} \quad b^2 = b. \end{aligned}$$

By subtracting $a + b$ from both sides we have that $0 = ab + ba$. So $-ab = ba$. We are almost done since we want to show that $ab = ba$. To conclude, we will show that for all $c \in R$, $-c = c$. Let $c \in R$. Then

$$\begin{aligned} -c &= (-c)^2 \\ &= (-c)(-c) \\ &= -c(-c) \\ &= -(-c^2) \\ &= c^2 \\ &= c \quad \because \text{R is boolean.} \end{aligned}$$

Thus $-ab = ba \implies ab = ba$ since $-c = c$ for all $c \in R$ and both a and b are arbitrary elements in R as well. □

34) Let p be prime. Prove that

$$Z_{(p)} = \left\{ \frac{a}{b} \middle| a, b \in \mathbb{Z} \text{and } \gcd(b, p) = 1 \right\}$$

is a ring.

Proof: To show that $Z_{(p)}$ is a ring, we can verify directly by checking all of the properties of a ring using the definition of a ring. Or, better yet, we can show that $Z_{(p)}$ is a subring of a known ring and hence is a ring itself. We will show the latter.

Notice that as sets, $Z_{(p)} \subset \mathbb{Q}$ and $\mathbb{Q}$ is a well-known ring. We will show that $Z_{(p)}$ is a subring of $\mathbb{Q}$ by using the Subring Test.

i) To show that $Z_{(p)}$ is nonempty, simply take $a = 1, b = 1$ which is an element of $Z_{(p)}$ since $\gcd(b, p) = 1$ for any p prime.

ii) Next we show that for all $r,s \in Z_{(p)}, rs \in Z_{(p)}$. Let $r,s \in Z_{(p)}$ So $r = \frac{a}{b}, s = \frac{c}{d}$ for some $a,b,c,d \in \mathbb{Z}$ and $\gcd(b,p) = \gcd(d,p) = 1$. Then we have that

$$\begin{aligned} rs &= \frac{a}{b} \cdot \frac{c}{d} \\ &= \frac{ac}{bd}. \end{aligned}$$

Notice that $ac \in \mathbb{Z}, bd \in \mathbb{Z}$. Also $\gcd(bd,p) = 1$ since $\gcd(b,p) = \gcd(d,p) = 1$. Thus $rs = \frac{ab}{cd} \in Z_{(p)}$.

iii) Lastly we show that for all $r,s \in Z_{(p)}, r-s \in Z_{(p)}$. Let $r,s \in Z_{(p)}$ as before in ii). Then

$$\begin{aligned} r-s &= \frac{a}{b} - \frac{c}{d} \\ &= \frac{ad-bc}{bd}. \end{aligned}$$

Notice that $ad-bc \in \mathbb{Z}, bd \in \mathbb{Z}$ and $\gcd(bd,p) = 1$ since $\gcd(b,p) = \gcd(d,p) = 1$. Thus $\frac{ad-bc}{bd} \in Z_{(p)}$.

By the Subring Test, we conclude that $Z_{(p)}$ is a subring of $\mathbb{Q}$ and so $Z_{(p)}$ is a ring. □

38) An element x in a ring is called idempotent if $x^2 = x$. Prove that the only idempotent in an integral domain are 0 and 1. Find a ring with an idempotent x not equal to 0 or 1.

Proof: Let R be an integral domain and $x \in R$ be an idempotent element. Then

$$x^2 = x \implies x^2 - x = 0 \implies x(x-1) = 0.$$

Since R is an integral domain, there are no zero divisors. Thus $x = 0$ or $x - 1 = 0$. So the only idempotents are 0 and 1.

To give an example of a ring with an idempotent x not equal to 0 or 1, consider the ring $\mathbb{Z}_{12}$. Continually squaring elements in $\pmod{12}$ we have that $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 4, 5^2 \equiv 1, 6^2 \equiv 0, 7^2 \equiv 1$, $8^2 \equiv 4, 9^2 \equiv 9, 10^2 \equiv 4, 11^2 \equiv 1$. So in $\mathbb{Z}_{12}$ the idempotent elements are $0,1,4$, and 9. So we have found a ring with idempotent elements other than the trivial ones of 0 and 1 so we are done. □