Modern Algebra I Section 1 · Assignment 8

JOHN PERRY

Exercise 1. *(pg. 95 Warm Up c) Find all the subrings of these rings:* $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_{12}$.

Solution:

I list only the proper subrings.

$\mathbb{Z}_5$ and $\mathbb{Z}_7$ have no proper subrings. For any non-zero residue class of $\mathbb{Z}_5$ (resp. $\mathbb{Z}_7$), its elements are relatively prime to 5 (resp. 7). Thus, the GCD identity means that there is a way to write 1 as an integer combination of any such element and 5 (resp. 7). Since 5 (resp. 7) is an element of the zero residue class, and zero must be an element of any subring, the residue class of 1 will also be an element of the subring, too. Once 1 is in there, we get everything in the set.

$\mathbb{Z}_6$ has the proper subrings $\{0,2,4\}$ and $\{0,3\}$.

$\mathbb{Z}_{12}$ has the proper subrings $\{0,2,4,6,8,10\}$, $\{0,3,6,9\}$, $\{0,4,8\}$, and $\{0,6\}$. ______ ◊

Exercise 2. *(pg. 95 Warm Up d) Give examples of the following (or explain why they don't exist):*

(a) A commutative subring of a non-commutative ring.

(b) A non-commutative subring of a commutative ring.

(c) A subring without unity, of a ring with unity. (See Exercise 22 for the converse possibility.)

(d) A ring (with more than one element) whose only subrings are itself, and the zero subring. Hint: *Look at an earlier Warm-up Exercise.*

Solution:

(a) The only non-commutative ring we have encountered so far is a ring of $m \times n$ matrices. There are a number of commutative subrings, but the simplest is $\{0, I\}$ (where I is the identity matrix). You could expand this somewhat by going with the subring of diagonal matrices.

(b) This doesn't exist. By way of contradiction, assume that S is a non-commutative subring of the commutative ring R. Then there exist $a, b \in S$ such that $ab \neq ba$. But $S \subseteq R$ implies that $a, b \in R$, which contradicts the assumption that R is commutative.

(c) $2\mathbb{Z} \subset \mathbb{Z}$.

(d) $\mathbb{Z}_p$, where p is a prime number. ______ ◊

Exercise 3. *(pg. 95 Warm Up f) What is the unity of the ring* $\mathbb{Z} \times \mathbb{Z}$*? (See Example 6.9.) What about* $R \times S$*, where* R *and* S *are rings with unity? (See Example 6.10).*

Solution:

$(1,1)$. ______ ◊

Exercise 4. *(pg. 96 Exercise 1) Let* $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$. *Show that* $\mathbb{Z}\left[\sqrt{2}\right]$ *is a commutative ring by showing it is a subring of* $\mathbb{R}$.

Solution:

It is clear that $\mathbb{Z}\left[\sqrt{2}\right] \subset \mathbb{R}$. We apply Theorem 7.1 to show that it is a subring.

Let $x, y \in \mathbb{Z}[2]$. Then there exist, $a, b, c, d \in \mathbb{Z}$ such that $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$.

Observe that

$$x - y = (a + bi) - (c + di) = (a - c) + (b - d)\sqrt{2}.$$

Since $a - c, b - d \in \mathbb{Z}$, $x - y \in \mathbb{Z}[2]$. Since x, y were arbitrary in $\mathbb{Z}\left[\sqrt{2}\right]$, $\mathbb{Z}\left[\sqrt{2}\right]$ is closed under subtraction.

Also,

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

Since $ac + 2bd, ad + bc \in \mathbb{Z}$, $xy \in \mathbb{Z}\left[\sqrt{2}\right]$. Since x, y were arbitrary in $\mathbb{Z}\left[\sqrt{2}\right]$, $\mathbb{Z}\left[\sqrt{2}\right]$ is closed under multiplication.

Since $\mathbb{Z}\left[\sqrt{2}\right]$ is closed under subtraction and multiplication, by Theorem 7.1 it is a subring of $\mathbb{R}$. Since $\mathbb{R}$ is a commutative ring, $\mathbb{Z}\left[\sqrt{2}\right]$ is also a commutative ring. ◊

Exercise 5. *(pg. 96 Exercise 4) Show that $m\mathbb{Z}$ is a subring of $n\mathbb{Z}$ if and only if n divides m. (See Example 7.7.)*

Solution:

Let $m, n \in \mathbb{Z}$ be arbitrary, but fixed.

($\Longrightarrow$) Assume that $m\mathbb{Z}$ is a subring of $n\mathbb{Z}$. Then $m\mathbb{Z} \subseteq n\mathbb{Z}$. Now, $m \in m\mathbb{Z}$ since $m = m \cdot 1$, so by the definition of a subset $m \in n\mathbb{Z}$. By the definition of $n\mathbb{Z}$, there exists some $x \in \mathbb{Z}$ such that $m = nx$. By the definition of divisibility, n divides m.

($\Longleftarrow$) Assume that n divides m. Then there exists $d \in \mathbb{Z}$ such that $m = dn$. Let $x, y \in m\mathbb{Z}$ be arbitrary, but fixed. We must show three things: (a) $x \in n\mathbb{Z}$ (so that $m\mathbb{Z} \subset n\mathbb{Z}$), (b) $x - y \in m\mathbb{Z}$, and (c) $xy \in m\mathbb{Z}$.

Since $x \in m\mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $x = bm$. Recall that $m = dn$; then $x = b(dn) = (bd)n$. So $x \in n\mathbb{Z}$. Since x was arbitrary, $m\mathbb{Z} \subseteq n\mathbb{Z}$.

Since $y \in m\mathbb{Z}$, there exists $c \in \mathbb{Z}$ such that $y = cm$. Then $x - y = bm - cm = (b - c)m \in m\mathbb{Z}$. So $m\mathbb{Z}$ is closed under subtraction. Moreover, $xy = (bm)(cm) = (bcm)m \in m\mathbb{Z}$. So $m\mathbb{Z}$ is closed under multiplication. By Theorem 7.1, $m\mathbb{Z}$ is a subring of $n\mathbb{Z}$. ◊

Exercise 6. *(pg. 97 Exercise 9) Show that the intersection of any two rings is a subring.*

Solution:

Let R_1, R_2 be rings. Write $S = R_1 \cap R_2$. By definition, $S \subseteq R_1$ and $S \subseteq R_2$.

Let $x, y \in S$ be arbitrary, but fixed. Then $x, y \in R_1$ and $x, y \in R_2$. Since R_1 and R_2 are both rings, $x - y, xy \in R_1$ and $x - y, xy \in R_2$. By definition of intersection, $x - y, xy \in R_1 \cap R_2 = S$. Since x and y are arbitrary in S, S is closed under subtraction and multiplication. Since S is closed under subtraction and multiplication, Theorem 7.1 tells us that S is a subring. ◊

Exercise 7. *(pg. 97 Exercise 10) Show by example that the union of any two subrings of a ring need* not *be a subring.* Hint: *You can certainly find such an example by working in $\mathbb{Z}$.*

Solution:

Recall that $2\mathbb{Z}$ and $3\mathbb{Z}$ are subrings of $\mathbb{Z}$. Consider $S = 2\mathbb{Z} \cup 3\mathbb{Z}$. Certainly $2 \in 2\mathbb{Z}$, $3 \in 3\mathbb{Z}$, and 3-2=1, but $1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Since S is not closed under subtraction, Theorem 7.1 tells us that it is not a subring of $\mathbb{Z}$. ◊

Exercise 8. *(pg. 98 Exercise 15)*

(a) An element a of a ring is ***nilpotent*** *if $a^n = 0$ for some positive integer n. Given a ring R, denote by $N(R)$ the set of all nilpotent elements of R. (This subring is called the* ***nilradical*** *of the ring.) If R is any commutative ring, show that $N(R)$ is a subring.*

(b) Determine $N(\mathbb{Z}_{10})$, the nilradical of $\mathbb{Z}_{10}$.
(c) Determine $N(\mathbb{Z}_8)$, the nilradical of $\mathbb{Z}_8$.

Solution:

(a) Certainly $N(R)$ is a subset of R. We can use Theorem 7.1 to show that it is a subring.

Let $x, y \in N(R)$. By definition, there exist $m, n \in \mathbb{N}$ such that $x^m = y^n = 0$.

We need to show that $x - y, xy \in N(R)$. That means we need positive integers i, j such that $(x-y)^i = (xy)^j = 0$. What values should we choose for i, j?

The problem is easier for multiplication. Since R is commutative, $(xy)^j = x^j y^j$. We need j to be large enough that either x^j or y^j will be zero (a previous exercise tells us that $a0 = 0a = 0$ for all $a \in R$). Let $j = \min(m, n)$. Without loss of generality, $j = m$. Then $(xy)^j = x^j y^j = 0y^j = 0$.

For subtraction, consider that by the binomial theorem,

$$(x-y)^i = \sum_{k=0}^{i} \binom{i}{k} x^k y^{i-k}.$$

Set $i = m + n$. Then

$$\begin{aligned}
(x-y)^{m+n} &= \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} \\
&= \sum_{k=0}^{m-1} \binom{m+n}{k} x^k y^{m+n-k} + \sum_{k=m}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} \\
&= \sum_{k=0}^{m-1} \binom{m+n}{k} x^k \cdot 0 + \sum_{k=m}^{m+n} \binom{m+n}{k} 0 \cdot y^{m+n-k} \\
&= 0.
\end{aligned}$$

Since $N(R)$ is closed under subtraction and multiplication, Theorem 7.1 tells us that it is a subring of R.

(How on earth did I decide on a value for i? Each term of the sum will be zero so long as $k \geq m$ or $i - k \geq n$. Since k increases from 0 to i, as long as $i \geq m$, k will eventually be greater than m, too.

What do we do if $k < m$? Since $x^k \neq 0$ in this case, we need $i - k \geq n$. Since $k < m$, it follows that $i - k \geq i - m$. So we will be okay as long as we keep $i - m \geq n$. Thus $i - k \geq n$ if we set $i = m + n$.)

(b) $N(\mathbb{Z}_{10}) = \{0\}$. No other element, when powered up, gives a multiple of 10.

(c) $N(\mathbb{Z}_8) = \{0, 2, 4\}$ since $2^3 = 8$ and $4^2 = 2 \times 8$. ◊

Exercise 9. *(pg. 98 Exercise 17) Show that if a ring has unity, it is unique.*

Solution:

Let R be an arbitrary ring. Suppose R has unity. Let $e, u \in R$ be two unities. Because e is a unity, then $eu = u$. Because u is a unity, $eu = e$. Thus $e = eu = u$. So unity, if it exists, is unique. ◊