



Homework 1: Sections 18 & 19

Seminar in Algebra

Author

Paul Beggs

BeggsPA@Hendrix.edu

Instructor

Dr. Carol Ann Downes, Ph.D.

Due

FEBRUARY 12, 2025



Cover Sheet

This is my first cover sheet that I've written, so I'm not sure how well it will be, but here goes. I thought that for the first couple of Exercises in Section 18 were fairly straightforward. Specifically, I found that doing Exercise 5 in Section 18 really helped with Exercise 32, because I could check unity to make sure that it acted properly (i.e., $e \cdot a = a$). For Exercise 43, I knew that I needed to show that $v = w$ because we had done similar proofs when we had to prove that identities were unique. It helped to just state what resources that I had, then go from there. Exercise 44 followed this same Exercise. For Exercise 46, I actually did the wrong Exercise first, and only realized it when Noah asked me for a hint on how to start. We both knew that we needed to incorporate all information from the Exercise (e.g., use $n, m \in \mathbb{Z}^+$ to show that $(a + b)^{n+m} = 0$), but we initially didn't know how to incorporate the commutativity part of the Exercise. Then, he realized that we could use the binomial theorem, and then I just had two cases to work through. Exercise 50 was straightforward because I had a checklist that I could work toward. For example, on (3), I knew that I needed to show that $bc \in I_a$, so I needed to show that $a(bc) \in I_a$, which was done with associativity and relying on definitions.

The first two Exercises in Section 19 were straightforward: for 4, just iteratively run through all possibilities, and return the only ones that work. For 18, the chart that we had in the notes also helped a ton. It practically did that problem for me (we only didn't have integer domains in the notes, but I knew \mathbb{Z}_p (where p is prime) had no zero divisors, so that helped). For Exercise 23, I was messing around with possible elements on my scratch paper that could be candidates for the two idempotent elements, and I landed on 0 and 1 by just trying a few possible ones. I could easily prove 0, but 1 was a bit more difficult because of when $a = 0$, it doesn't have an inverse. That was until I realized I could just restrict a to be nonzero, and that was the key. Finally, for Exercise 26, I knew for part (a) that I just needed to use the uniqueness identity of b , and rely on definitions. So, I found an element $(b + c)$ that had to equal b (bc uniqueness), and the only way for that equation to be true, would be if $c = 0$. This showed that $ac = 0$, and a was nonzero, so no zero divisors. I was extremely stuck on (b) because I couldn't figure out how to cancel out a with an inverse because I didn't know what that inverse was, or what it would equal after the computation was finished. So, I searched my notes and found the theorem that said cancellation laws held when there were no zero divisors, which was definitely the ah-ha moment of the problem.

Overall, this homework took me about ≈ 9 hours to complete, with trying again and again, but I think I did a good job trying to square off any loose ends or ambiguities.



Section 18

In Exercise 5, compute the product in the given ring.

5. $(2, 3)(3, 5)$ in $\mathbb{Z}_5 \times \mathbb{Z}_9$

Solution.

$$(2, 3)(3, 5) = (6, 15) = (6 \bmod 5, 15 \bmod 9) = (1, 6).$$

In Exercises 16, 18, and 19, describe all units in the given ring.

16. \mathbb{Z}_5

Solution. Every element in \mathbb{Z}_5 is a unit (except 0), as each of them are relatively prime to 5.

18. $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$

Solution. The units in \mathbb{Z} are $\{1, -1\}$, the units in \mathbb{Q} are $\mathbb{Q} \setminus \{0\}$, and the units in the second \mathbb{Z} are also $\{1, -1\}$. Thus, the units in $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ are of the form $(\pm 1, q, \pm 1)$ where $q \in \mathbb{Q} \setminus \{0\}$.

19. \mathbb{Z}_4

Solution. The only relatively prime elements to 4 in \mathbb{Z}_4 are 1 and 3, so they are the units.

Concepts

32. Given an example of a ring with unity $1 \neq 0$ that has a subring with nonzero unity $1' \neq 1$. [Hint: Consider a direct product or a subring of \mathbb{Z}_6]

Solution. Consider the ring \mathbb{Z}_6 . The element 1 is the unity of \mathbb{Z}_6 . However, the subset $\{0, 3\}$ forms a subring of \mathbb{Z}_6 with unity $1' = 3$ because $3 \cdot 3 \equiv 3$ and $3 \cdot 0 \equiv 0$.



Theory

43. Show that the multiplicative inverse of a unit in a ring with unity is unique.

Proof. Let u be a unit in a ring R with unity, and suppose v and w are both multiplicative inverses of u . Then we have $uv = vu = 1$ and $uw = wu = 1$. Multiply the equation $uv = 1$ on the left by w :

$$\begin{aligned}
 w(uv) &= w \cdot 1 \\
 (wu)v &= w && \text{associativity \& identity property,} \\
 1 \cdot v &= w && \text{since } wu = 1, \\
 v &= w && \text{identity property.}
 \end{aligned}$$

Thus, the multiplicative inverse of a unit in a ring with unity is unique. \square

44. An element a of a ring R is **idempotent** if $a^2 = a$.

- a. Show that the set of all idempotent elements of a commutative ring is closed under multiplication.

Proof. Let a and b be idempotent elements in a commutative ring R . Then we have $a^2 = a$ and $b^2 = b$. We want to show that the product ab is also idempotent, i.e., $(ab)^2 = ab$.

$$\begin{aligned}
 (ab)^2 &= (ab)(ab) \\
 &= a(b(ab)) && \text{associativity,} \\
 &= a((ab)b) && \text{since } R \text{ is commutative,} \\
 &= (a^2b)b && \text{associativity,} \\
 &= (ab)b && \text{since } a^2 = a, \\
 &= a(b^2) && \text{associativity,} \\
 &= ab && \text{since } b^2 = b.
 \end{aligned}$$

Thus, the set of all idempotent elements of a commutative ring is closed under multiplication. \square

- b. Find all idempotents in the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

Solution. Using a Python script and exhaustively searching \mathbb{Z}_6 and \mathbb{Z}_{12} , we get the individual idempotents of 0, 1, 3, and 4 for \mathbb{Z}_6 and 0, 1, 4, and 9 for \mathbb{Z}_{12} . Taking a combination of each element, we get 16 idempotent sets.



46. An element a for ring R is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{Z}^+$. Show that if a and b are nilpotent elts of a commutative ring, then $a+b$ is also nilpotent.

Proof. Let $a, b \in \mathbb{Z}^+$. This means there exists some $n, m \in \mathbb{Z}^+$ for which $a^n = 0$ and $b^m = 0$. Our goal is to show that $(a+b)^{n+m} = 0$. Since R is a commutative ring, we can use the binomial theorem to help here (thanks to an insight from Noah). Thus, consider the following:

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{(n+m)-k}.$$

Note that every element in each term is a multiple of our nilpotent elements, so our goal is to show that each of these elements are 0 for any value of k . Thus, consider these two cases:

- $k \geq n$: If $k \geq n$, then $a^k = a^n a^{k-n} = 0 a^{k-n} = 0$, so the whole term is 0.
- $k < n$: Since $k < n$, it follows that $-k > -n$. Therefore, $(n+m) - k > n+m-n = m$ (because R is commutative). Since the exponent of b is greater than m , $b^{(n+m)-k} = 0$.

Therefore, we have shown that $(a+b)^{n+m} = 0$. □

50. Let R be a ring, and let a be a fixed element of R . Let $I_a = \{x \in R \mid ax = 0\}$. Show that I_a is a subring of R .

Proof. To prove that I_a is a subring of R , we need to prove the statements given by Exercise 48 (& from theorem in notes):

(1) $0 \in I_a$ because $a \cdot 0 = 0$.

(2) If $b, c \in I_a$ then

$$\begin{aligned} a(b-c) &= ab - ac && \text{left distributive laws from } R, \\ &= 0 - 0 && \text{definition of } I_a, \\ &= 0 && \text{inverse property from } R. \end{aligned}$$

Thus, $b-c \in I_a$.

(3) If $b, c \in I_a$ then

$$\begin{aligned} a(bc) &= (ab)c && \text{associativity from } R, \\ &= 0 \cdot c && \text{definition of } I_a, \\ &= 0 && \text{definition of } I_a. \end{aligned}$$

Thus, $bc \in I_a$.

Therefore, I_a is a subring of R . □



Section 19

4. Find all solutions of $x^2 + 2x + 4 = 0$ in \mathbb{Z}_6 .

Solution. Using a Python script to search through values $x \in [0, 5]$, we find the only solution to the equation is $x = 2$.

Concepts

18. Each of the six numbered regions in Fig. 19.10 corresponds to a certain type of ring. Give an example of a ring in each of the six cells. For example, a ring in the region numbered 3 must be commutative (it is inside the commutative circle), have unity, but not be an integral domain.

Solution. Starting from 6 and working inward, we have: 6. $M_2(2\mathbb{Z})$; 5. $M_2(\mathbb{R})$; 4. $2\mathbb{Z}$; 3. \mathbb{Z}_6 ; 2. \mathbb{Z}_2 ; 1. \mathbb{R} .

Theory

23. An element a of a ring R is **idempotent** if $a^2 = a$. Show that a division ring contains exactly two idempotent elements.

Proof. Let R be a division ring and let $a \in R$ be an idempotent element, so $a^2 = a$. First, note that $0^2 = 0$, so 0 is an idempotent element. Now, suppose $a \neq 0$. Since R is a division ring, a is a unit, so a^{-1} exists. Rearranging $a^2 = a$ gives $a^2 - a = 0$, which factors as $a(a - 1) = 0$. We can solve for $a - 1$ as follows:

$$\begin{array}{ll}
 a(a - 1) = 0 & \\
 a^{-1}(a(a - 1)) = a^{-1} \cdot 0 & \text{left multiply by } a^{-1}, \\
 (a^{-1}a)(a - 1) = 0 & \text{associativity,} \\
 1(a - 1) = 0 & \text{inverse property,} \\
 a - 1 = 0 & \text{identity property,} \\
 a = 1 & \text{add 1 to both sides.}
 \end{array}$$

Thus, the only nonzero idempotent element is 1. Therefore, there are exactly two idempotent elements. \square



26. Let R be a ring that contains at least two elements. Suppose for each nonzero $a \in R$, there exists a unique $b \in R$ such that $aba = a$.

a. Show that R has no divisors of 0.

Solution. Let $a, c \in R$ with $a \neq 0$ such that $ac = 0$. Additionally, assume there exists a unique $b \in R$ such that $aba = a$. Our goal is to show that $b + c = b$, implying $c = 0$. Hence, consider the following computation:

$$\begin{aligned}
 a(b + c)a &= aba + aca && \text{left and right distribution,} \\
 &= a + aca && aba = a \text{ property,} \\
 &= a + (ac)a && \text{associativity,} \\
 &= a + 0a && ac = 0 \text{ property,} \\
 &= a && \text{Theorem 18.8 (1) \& add. id.}
 \end{aligned}$$

Thus, we have shown that $(b + c)$ behaves exactly like b , meaning $b + c = b$ because b is unique, so $c = 0$. Thus, R has no zero divisors.

b. Show that $bab = b$.

Solution. To show that $bab = b$, we are going to leverage the theorem in the notes that states, “The cancellation laws hold in ring R if, and only if, R has no zero divisors.” This allows us to compute the following:

$$\begin{aligned}
 aba &= a \\
 baba &= ba && \text{left multiplication,} \\
 bab &= b && \text{cancellation laws for } a.
 \end{aligned}$$

c. Show that R has unity.

Solution. Given the results from (b) and R ’s $aba = a$ property, we conjecture that $ab = 1$ (i.e., ab is R ’s unity). To prove this conjecture, we must show that for an element $c \in R$, that $c(ab) = (ab)c = c$. Thus, consider the following computation:

$$\begin{aligned}
 aba &= a \\
 caba &= ca && \text{left multiplication by } c, \\
 c(ab) &= c && \text{cancellation laws \& associativity.}
 \end{aligned}$$

Now, for the other direction:

$$\begin{aligned}
 bab &= b \\
 babc &= bc && \text{right multiplication by } c, \\
 (ab)c &= c && \text{cancellation laws \& associativity.}
 \end{aligned}$$

Thus, we have shown that R ’s unity is ab .



d. Show that R is a division ring.

Solution. From part (c), we know R has a unity, 1, and for any nonzero a , $ab = 1$. From part (b), we have $bab = b$. Multiplying by a on the right gives $baba = ba$. Substituting $aba = a$, we get $ba = 1$. Thus, for every a , there exists $b \in R$ such that $ab = ba = 1$. This means every nonzero element is a unit. Since R is a ring with unity and every nonzero element has an inverse, R is a division ring.