1876

HENDRIX

COLLEGE

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

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

44. 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. □

45. An element of 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. □

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. (Linear algebra) Recall that for an $m \times n$ matrix A, the *transpose* A^T of A is the matrix whose jth column is the jth row of A. Show that if A is an $m \times n$ matrix such that A^TA is invertible, then the *projection matrix* $P = A(A^TA)^{-1}A^T$ is an idempotent in the ring of $n \times n$ matrices.

Proof. We will show that P is an idempotent by computing P^2:

$$\begin{aligned}
P^2 &= [A(A^TA)^{-1}A^T][A(A^TA)^{-1}A^T] && \\
&= A[(A^TA)^{-1}(A^TA)][(A^TA)^{-1}A^T] && \text{matrix associativity,}\\
&= A(I_A)[(A^TA)^{-1}A^T] && \text{matrix inverses,}\\
&= A[(A^TA)^{-1}A^T] && \text{matrix identity,}\\
&= A(A^TA)^{-1}A^T && \text{matrix associativity,}\\
&= P && \text{definition of } P.
\end{aligned}$$

Thus, we have shown that $P^2 = P$. Therefore, P is an idempotent. □

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:

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

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

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 $c = 0$.

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.