Modern Algebra 1 Section 1 · Assignment 7

JOHN PERRY

Exercise 1. *(pg. 84 Warm Up d) Give examples of rings satisfying the following:*
(a) A ring with finitely many elements.
(b) A non-commutative ring.

Solution:
(a) $\mathbb{Z}_m$, where $m \in \mathbb{Z}$.
(b) A ring of matrices of fixed dimension. (Recall that matrix multiplication is not commutative.) ◊

Exercise 2. *(pg. 84 Warm Up e) Are the following rings?*
(a) $3\mathbb{Z}$, the set of all integers divisible by 3, together with ordinary addition and multiplication.
(b) The set of all irreducible integers, together with ordinary addition and multiplication.
(c) $\mathbb{R}$, with the operations of addition and division.
(d) The set $\mathbb{R}^*$ of non-zero real numbers, with the operations of multiplication, and the operation $a \circ b = 1$. Note: *We are trying to use ordinary multiplication as the 'addition' in this set!*
(e) The set of polynomials in $\mathbb{Q}[x]$, where the constant term is an integer, with the usual addition and multiplication of polynomials.
(f) The set of all matrices in $M_2(\mathbb{Z})$, whose lower left-hand entry is zero, with the usual matrix addition and multiplication.

Solution:
(a) Yes. Most properties carry easily from $\mathbb{Z}$. For the additive inverse, if $x \in 3\mathbb{Z}$, then $x = 3y$ for some $y \in \mathbb{Z}$, and $-3y \in 3\mathbb{Z}$, so $-x \in 3\mathbb{Z}$.
(b) No. The set is not closed under multiplication, since the product of two irreducible integers is not irreducible.
(c) No. The set is not closed under division, since division by zero is undefined.
(d) Yes. The 'additive' identity is 1, and the 'additive' inverse of $x \in \mathbb{R}$ is $1/x$. It is easy to see that 'multiplication' is associative, since

$$(a \circ b) \circ c = 1 \circ c = 1 \quad \text{and} \quad a \circ (b \circ c) = a \circ 1 = 1.$$

To show that the distributive property is satisfied, we observe that

$$a \circ (b \cdot c) = 1 \quad \text{and} a \circ b \cdot a \circ c = 1 \cdot 1 = 1.$$

(Neat, eh?)
(e) Yes. All properties carry easily from $\mathbb{Q}[x]$. It is easy to see that adding and multiplying any two elements of the set gives a new polynomial in $\mathbb{Q}[x]$, *and* that its constant term is an integer.
(f) Yes. All properties carry easily from $M_2(\mathbb{Z})$, except that multiplication is closed. This is easy to show. For any two 2×2 matrices over $\mathbb{Z}$, we have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix}.$$

◊

Exercise 3. *(pg. 85 Exercise 1) Show that in a ring,* $0a = a0 = 0$.

Solution:

Let R be an arbitary ring. Let $a \in R$ be arbitary, but fixed. Certainly $0 + 0 = 0$. Multiply on the right to both sides and distribute:

$$0a = (0+0)a$$
$$0a = 0a + 0a.$$

Since $0a = 0a + 0$,

$$0a + 0 = 0a + 0a$$

and by Theorem 6.1(a)

$$0 = 0a.$$

A similar argument shows that $a0 = 0$. ◊

Exercise 4. *(pg. 85 Exercise 3) Show that in a ring,* $(-a)b = a(-b) = -(ab)$.

Solution:

Let R be an arbitrary ring. Let $a, b \in R$ be arbitrary, but fixed. First we show that $(-a)b = -(ab)$. Apply the distributive property, the additive inverse property, and the result of Exercise 3 to obtain

$$ab + (-a)b = (a + (-a))b = 0b = 0.$$

Thus $(-a)b$ is the additive inverse of ab; that is, $(-a)b = -(ab)$.

A similar argument shows that $a(-b) = -(ab)$. ◊

Exercise 5. *(pg. 85 Exercise 4) Show that in a ring,* $(-a)(-b) = ab$.

Solution:

Let R be an arbitrary ring. Let $a, b \in R$ be arbitrary, but fixed. Apply the result of Exercise 4 to obtain

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$$

(The last equality follows from Theorem 6.1(c). That is, the inverse of $-(ab)$ is ab, which is how they are inverse in the first place!) ◊

Exercise 6. *(pg. 85 Exercise 5) Prove the following facts about subtraction in a ring* R*, where* $a, b, c \in R$*:*

(a) $a - a = 0$.
(b) $a(b - c) = ab - ac$.
(c) $(b - c)a = (ba - ca)$.

Solution:

(a) By definition, $a - a = a + (-a) = 0$.

(b) Use distribution and the result of Exercise 4 to obtain

$$a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac.$$

(c) An argument similar to that of (b) works. ◊

Exercise 7. *(pg. 86, Exercise 12) Let*

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}.$$

Show that $\mathbb{Z}[i]$ is a commutative ring (see Exercise 11). This is called the ring of ***Gaussian integers****.*

Solution:

Addition and multiplication, defined as in Exercise 11, give Gaussian integers: Let $x, y \in \mathbb{Z}[i]$. Then $x = a + bi$ and $y = c + di$ for some $a, b, c, d \in \mathbb{Z}$. We see that

$$\begin{aligned} x + y &= (a + bi) + (c + di) \\ &= (a + c) + (b + d)i \end{aligned}$$

and

$$\begin{aligned} xy &= (a + bi)(c + di) \\ &= ac + adi + bci - bd \\ &= (ac - bd) + (ad + bc)i. \end{aligned}$$

Since the integers are closed under addition and multiplication, $x + y, xy \in \mathbb{Z}[i]$. Since x, y were arbitrary in $\mathbb{Z}[i]$, it follows that $\mathbb{Z}[i]$ is closed under addition and multiplication.

Now we show that $\mathbb{Z}[i]$ satisfies the six properties of a ring. Let $x, y, z \in \mathbb{Z}[i]$ be arbitrary, but fixed. Let $a, b, c, d, e, f \in \mathbb{Z}$ such that $x = a + bi$, $y = c + di$, and $z = e + fi$.

(Rule 1) By definition,

$$x + y = (a + bi) + (c + di) = (a + c) + (b + d)i.$$

Since the integers are commutative under addition,

$$x + y = (c + a) + (d + b)i = (c + di) + (a + bi) = y + x.$$

(Rule 2) By definition,

$$(x + y) + z = ((a + c) + (b + d)i) + (e + fi) = ((a + c) + e) + ((b + d) + f)i.$$

Since the integers are associative under addition,

$$\begin{aligned} (x + y) + z &= (a + (c + e)) + (b + (d + f))i \\ &= (a + bi) + ((c + e) + (d + f)i) \\ &= (a + bi) + ((c + di) + (e + fi)) \\ &= x + (y + z). \end{aligned}$$

(Rule 3) The zero element of $\mathbb{Z}[i]$ is $0 + 0i$, since

$$x + (0 + 0i) = (a + bi) + (0 + 0i) = (a + 0) + (b + 0)i = a + bi.$$

(Rule 4) The inverse of x is $-a + (-b)i$, since

$$x + (-a + (-b)i) = (a + bi) + (-a + (-b)i) = (a + (-a)) + (b + (-b))i = 0 + 0i.$$

(Rule 5) By definition,

$$\begin{aligned}(xy)z &= ((a+bi)(c+di))(e+fi)\\ &= ((ac-bd)+(ad+bc)i)(e+fi)\\ &= ((ac-bd)e-(ad+bc)f)+((ac-bd)f+(ad+bc)e)i\\ &= (a(ce-df)-b(de+cf))+(a(cf+de)+b(-df+ce))i\\ &= (a+bi)((ce-df)+(cf+de)i)\\ &= (a+bi)((c+di)(e+fi))\\ &= x(yz).\end{aligned}$$

(It might be easier to simplify $(xy)z$ and $x(yz)$ and show that they are equal.)

(Rule 6) By definition,

$$\begin{aligned}x(y+z) &= (a+bi)((c+di)+(e+fi))\\ &= (a+bi)((c+e)+(d+f)i)\\ &= (a(c+e)-b(d+f))+(a(d+f)+b(c+e))i\\ &= (ac+ae-bd-bf)+(ad+af+bc+be)i\\ &= (ac-bd)+(ae-bf)+(ad+bc)i+(bc+be)i\\ &= ((ac-bd)+(ad+bc)i)+((ae-bf)+(bc+be)i)\\ &= xy+xz.\end{aligned}$$

(As with Rule 5, it might be easier to simplify $x(y+z)$ and $xy+xz$ and show that they are equal.) ◊

Exercise 8. *(pg. 87, Exercise 15) Verify that Example 6.10 is a ring. Namely, let R and S be arbitrary rings. Define addition and multiplication appropriately to make $R\times S$ a ring, where $R\times S$ is the set of ordered pairs with first entry from R and second entry from S. Now generalize this to the set $R_1\times R_2\times\cdots\times R_n$ of n-tuples with entries from the rings R_i. This new ring is called the* ***direct product*** *of the rings R_i.*

Solution:

We will prove that $R_1\times R_2\times\cdots\times R_n$ is a ring under the operations

$$\begin{aligned}(r_{11},r_{12},\ldots,r_{1n})+(r_{21},r_{22},\ldots,r_{2n}) &= (r_{11}+r_{21},r_{12}+r_{22},\ldots,r_{1n}+r_{2n})\\ (r_{11},r_{12},\ldots,r_{1n})\,(r_{21},r_{22},\ldots,r_{2n}) &= (r_{11}r_{21},r_{12}r_{22},\ldots,r_{1n}r_{2n}).\end{aligned}$$

Since R_i is closed uner addition and multiplication for each $i:1\leq i\leq n$, $R_1\times R_2\times\cdots\times R_n$ are closed under addition and multiplication.

We now show that the six properties of a ring are satisfied. Let $r_1,r_2,r_3\in R_1\times R_2\times\cdots\times R_n$ be arbitrary, but fixed.

(Rule 1) That addition is commutative,

$$
\begin{aligned}
r_1 + r_2 &= (r_{11}, r_{12}, \ldots, r_{1n}) + (r_{21}, r_{22}, \ldots, r_{2n}) \\
&= (r_{11} + r_{21}, r_{12} + r_{22}, \ldots, r_{1n} + r_{2n}) \qquad (1) \\
&= (r_{21} + r_{11}, r_{22} + r_{12}, \ldots, r_{2n} + r_{1n}) \qquad (2) \\
&= (r_{21}, r_{22}, \ldots, r_{2n}) + (r_{11}, r_{12}, \ldots, r_{1n}) \\
&= r_1 + r_2.
\end{aligned}
$$

Notice that we used the commutative property of R_1, R_2, ..., R_n when moving from line (1) to line (2).

(Rule 2) That addition is associative,

$$
\begin{aligned}
r_1 + (r_2 + r_3) &= (r_{11}, r_{12}, \ldots, r_{1n}) + ((r_{21}, r_{22}, \ldots, r_{2n}) + (r_{31}, r_{32}, \ldots, r_{3n})) \\
&= (r_{11}, r_{12}, \ldots, r_{1n}) + (r_{21} + r_{31}, r_{22} + r_{32}, \ldots, r_{2n} + r_{3n}) \\
&= (r_{11} + (r_{21} + r_{31}), r_{12} + (r_{22} + r_{32}), \ldots, r_{1n} + (r_{2n} + r_{3n})) \qquad (3) \\
&= ((r_{11} + r_{21}) + r_{31}, (r_{12} + r_{22}) + r_{32}, \ldots, (r_{1n} + r_{2n}) + r_{3n}) \qquad (4) \\
&= (r_{11} + r_{21}, r_{12} + r_{22}, \ldots, r_{1n} + r_{2n}) + (r_{31}, r_{32}, \ldots, r_{3n}) \\
&= ((r_{11}, r_{12}, \ldots, r_{1n}) + (r_{21}, r_{22}, \ldots, r_{2n})) + (r_{31}, r_{32}, \ldots, r_{3n}) \\
&= (r_1 + r_2) + r_3.
\end{aligned}
$$

Notice that we used the associative property of R_1, R_2, ..., R_n when moving from line (3) to line (4).

(Rule 3) Let $z = (0, 0, \ldots, 0)$. Notice that $z \in R_1 \times R_2 \times \cdots \times R_n$ since each of R_1, R_2, ..., R_n has a zero element. Then

$$
\begin{aligned}
r_1 + z &= (r_{11}, r_{12}, \ldots, r_{1n}) + (0, 0, \ldots, 0) \\
&= (r_{11} + 0, r_{12} + 0, \ldots, r_{1n} + 0) \\
&= (r_{11}, r_{12}, \ldots, r_{1n}) \\
&= r_1.
\end{aligned}
$$

Hence z is a zero element of $R_1 \times R_2 \times \cdots \times R_n$.

(Rule 4) Let $n = (-r_{11}, -r_{12}, \ldots, -r_{1n})$. Notice that $n \in R_1 \times R_2 \times \cdots \times R_n$ since r_{11} has an additive inverse in R_1, r_{12} has an additive inverse in R_2, $\ldots$, r_{1n} has an additive inverse in R_n. Then

$$
\begin{aligned}
r_1 + n &= (r_{11}, r_{12}, \ldots, r_{1n}) + (-r_{11}, -r_{12}, \ldots, -r_{1n}) \\
&= (r_{11} + (-r_{11}), r_{12} + (-r_{12}), \ldots, r_{1n} + (-r_{1n})) \\
&= (0, 0, \ldots, 0).
\end{aligned}
$$

Hence $n = -r_1$.

(Rule 5) That multiplication is associative,

$$
\begin{aligned}
r_1(r_2r_3) &= (r_{11}, r_{12}, \ldots, r_{1n})\left((r_{21}, r_{22}, \ldots, r_{2n})(r_{31}, r_{32}, \ldots, r_{3n})\right)\\
&= (r_{11}, r_{12}, \ldots, r_{1n})(r_{21}r_{31}, r_{22}r_{32}, \ldots, r_{2n}r_{3n})\\
&= (r_{11}(r_{21}r_{31}), r_{12}(r_{22}r_{32}), \ldots, r_{1n}(r_{2n}r_{3n})) \qquad (5)\\
&= ((r_{11}r_{21})r_{31}, (r_{12}r_{22})r_{32}, \ldots, (r_{1n}r_{2n})r_{3n}) \qquad (6)\\
&= (r_{11}r_{21}, r_{12}r_{22}, \ldots, r_{1n}r_{2n})(r_{31}, r_{32}, \ldots, r_{3n})\\
&= \left((r_{11}, r_{12}, \ldots, r_{1n})(r_{21}, r_{22}, \ldots, r_{2n})\right)(r_{31}, r_{32}, \ldots, r_{3n})\\
&= (r_1r_2)r_3.
\end{aligned}
$$

Notice that we used the associative property of R_1, R_2, ..., R_n when moving from line (5) to line (6).

(Rule 6) That there is distribution,

$$
\begin{aligned}
r_1(r_2+r_3) &= (r_{11}, r_{12}, \ldots, r_{1n})\left((r_{21}, r_{22}, \ldots, r_{2n}) + (r_{31}, r_{32}, \ldots, r_{3n})\right)\\
&= (r_{11}, r_{12}, \ldots, r_{1n})(r_{21}+r_{31}, r_{22}+r_{32}, \ldots, r_{2n}+r_{3n})\\
&= (r_{11}(r_{21}+r_{31}), r_{12}(r_{22}+r_{32}), \ldots, r_{1n}(r_{2n}+r_{3n})) \qquad (7)\\
&= (r_{11}r_{21}+r_{11}r_{31}, r_{12}r_{22}+r_{12}r_{32}, \ldots, r_{1n}r_{2n}+r_{1n}r_{3n}) \qquad (8)\\
&= (r_{11}r_{21}, r_{12}r_{22}, \ldots, r_{1n}r_{2n}) + (r_{11}r_{31}, r_{12}r_{32}, \ldots, r_{1n}r_{3n})\\
&= (r_{11}, r_{12}, \ldots, r_{1n})(r_{21}, r_{22}, \ldots, r_{2n}) + (r_{11}, r_{12}, \ldots, r_{1n})(r_{31}, r_{32}, \ldots, r_{3n})\\
&= r_1r_2 + r_1r_3.
\end{aligned}
$$

Notice that we used the distributive property of R_1, R_2, ..., R_n when moving from line (7) to line (8).

We have shown that r_1, r_2, r_3 satisfy the six properties of a ring. Since these are arbitrary elements of $R_1 \times R_2 \times \cdots \times R_n$, it is a ring. ◊

Exercise 9. *s(pg. 87 Exercise 18) Suppose that $a \cdot a = a$ for every element a in a ring R. (Elements a in a ring where $a^2 = a$ are called **idempotent**.)*

(a) Show that $a = -a$.

(b) Now show that R is commutative.

Solution:

(a) If $a \cdot a = a$ for every element $a \in R$, then

$$
\begin{aligned}
a + a &= (a+a)^2\\
&= (a+a)(a+b)\\
&= a^2 + a^2 + a^2 + a^2\\
&= a + a + a + a.
\end{aligned}
$$

Apply the definition of zero and Theorem 6.1(a) to obtain

$$
\begin{aligned}
(a+a) + 0 &= (a+a) + (a+a)\\
0 &= a + a.
\end{aligned}
$$

Since $a + a = 0$, it must be that a is its own additive inverse. In symbols, $a = -a$.

(b) Using the same approach,

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

(Notice that we do not assume that $ab = ba$, because we are trying to prove this!) Thus

$$\begin{aligned} (a+b)+0 &= (a+b)+(ab+ba) \\ 0 &= ab+ba. \end{aligned}$$

Hence $ab = -(ba)$. We showed in part (a) that every element of R is its own additive inverse, so $-(ba) = ba$. Hence $ab = ba$. $\Diamond$