Modern Algebra 1 Section 1 · Assignment 9

JOHN PERRY

Exercise 1. *(pg. 114 Warm Up a) Determine the units and the zero divisors in the following rings:*

$$\mathbb{Z}\times\mathbb{Z}, \quad \mathbb{Z}_{20}, \quad \mathbb{Z}_4\times\mathbb{Z}_2, \quad \mathbb{Z}_{11}, \quad \mathbb{Z}[x].$$

Solution:

For $\mathbb{Z}\times\mathbb{Z}$, the only units are $(1,1),(1,-1),(-1,1),(-1,-1)$. The zero divisors are all elements (a,b) such that $a=0$ or $b=0$, but not both. (For example, $(0,b)\cdot(1,0)=(0,0)$.)

For $\mathbb{Z}_{20}$, Theorem 8.6 tells us that the units are $[1],[3],[7],[9],[11],[13],[17],[19]$. The zero divisors are the remaining non-zero units.

For $\mathbb{Z}_4\times\mathbb{Z}_2$, the units are $(1,1),(3,1)$. The zero divisors are $(1,0),(2,0),(3,0),(0,1),(2,1)$.

For $\mathbb{Z}_{11}$, Theorem 8.5 tells us that every non-zero element is a unit.

For $\mathbb{Z}[x]$, there are no units except 1, and no zero divisors. ◊

Exercise 2. *(pg. 114 Warm Up b) Suppose that a is a unit in a ring. Is $-a$ a unit? Why or why not?*

Solution:

If a is a unit in a ring R, then $1/a\in R$. Certainly the additive inverse $-1/a\in R$ also, and by a previous homework problem we can rewrite

$$(-a)\left(-\frac{1}{a}\right)=a\cdot\frac{1}{a}=1.$$

◊

Exercise 3. *(pg. 115 Warm Up d) Find a non-zero matrix A in $M_2(\mathbb{Z})$ so that $A^2=0$. Then A is a zero divisor. (A ring element a so that $a^n=0$, for some positive integer n is called* nilpotent. *See Exercise 7.15.)*

Solution:

Let

$$A=\begin{pmatrix}1 & -1\\ 1 & -1\end{pmatrix}.$$

Then $A^2=0$ even though $A\neq 0$.

Another one that works is

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

◊

Exercise 4. *(pg. 115 Warm Up e) Suppose that D is a domain. Show that the direct product $D\times D$ is not a domain.*

Solution:

Since D is a domain, we know that $0,1\in D$. Then $(1,0),(0,1)\in D\times D$ are non-zero and $(1,0)\cdot(0,1)=(0,0)$. Since $(1,0)$ and $(0,1)$ are zero divisors, $D\times D$ is not a domain. ◊

Exercise 5. *(pg. 115 Warm Up l) Give examples of the following, or explain why they don't exist:*
(a) A finite field.
(b) A finite field that isn't a domain.
(c) A finite domain that isn't a field.
(d) An infinite field.
(e) An infinite domain that isn't a field.

Solution:

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

(b) This is impossible. A field is a special kind of domain (a domain with the property that non-zero elements are units), so every field is a domain, including every finite field.

(c) This is impossible. Theorem 8.8 tells us that every finite domain is a field.

(d) $\mathbb{R}$.

(e) $\mathbb{Z}$. ◊

Exercise 6. *(pg. 116 Warm Up m) Does there exist an integer m for which $\mathbb{Z}_m$ is a domain, but not a field? Explain.*

Solution:

No. Let $m \in \mathbb{Z}$ be arbitrary, but fixed. Assume $m \geq 2$ (otherwise we can't talk about $\mathbb{Z}_m$.) If m is prime, then $\mathbb{Z}_m$ is a field (Theorem 8.5). If m is not prime, then there exist $p, q \in \mathbb{Z}$ such that $0 < p \leq q < m$ and $pq = m$. Then $[p][q] = [m] = [0]$ in $\mathbb{Z}_m$. Since $\mathbb{Z}_m$ has zero divisors, it is not a domain.

So the only time $\mathbb{Z}_m$ is a domain is when it is a field.

Alternately, one could use Theorem 8.8; since $\mathbb{Z}_m$ is always finite, then any time it is a domain, it is also a field. ◊

Exercise 7. *(pg. 116 Warm Up n) Use Euclid's Algorithm to compute the multiplicative inverse of $[2]$ in $\mathbb{Z}_9$.*

Solution:

Applying Euclid's Algorithm, we see that

$$9 = 4 \times 2 + 1$$
$$2 = 2 \times 1 + 0.$$

So $1 = 9 + (-4) \cdot 2$. Hence the multiplicative inverse of $[2]$ in $\mathbb{Z}_9$ is $[-4] = [5]$. ◊

Exercise 8. *(pg. 116 Warm Up o) Use Fermat's Little Theorem 8.7 to compute the multiplicative inverse of $[2]$ in $\mathbb{Z}_5$.*

Solution:

$[2]^{5-2} = [2]^3 = [8] = [3]$. Indeed, $[2][3] = [6] = [1]$. ◊

Exercise 9. *(pg. 116 Exercise 1) Prove that if R is a commutative ring and $a \in R$ is a zero divisor, then ax is also a zero divisor or 0, for all $x \in R$.*

Solution:

Let R be a commutative ring. Let $a \in R$ be arbitrary, but fixed. Assume that a is a zero divisor. Let $x \in R$ be arbitrary, but fixed.

If $ax = 0$, then we are done. So assume $ax \neq 0$. Recall that a is a zero divisor. Thus $a \neq 0$ and there exists $b \in R$ such that $b \neq 0$ and $ab = 0$. Using the fact that R is a commutative ring, along with Exercise 6.1,

$$(ax)b = a(xb) = a(bx) = (ab)x = 0x = 0.$$

Since $ax \neq 0$ and $b \neq 0$, ax is a zero divisor. ◊

Exercise 10. *(pg. 116 Exercise 3) Find two non-commuting units A, B in $M_2(\mathbb{R})$, and check that $(AB)^{-1} = B^{-1}A^{-1}$ and $(AB)^{-1} \neq A^{-1}B^{-1}$.*

Solution:

Two non-commuting units are

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};$$

note that

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \quad \text{and} \quad BA = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$$

so $A \neq B$. Their inverses are

$$A^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \quad \text{and} \quad B^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

So

$$(AB)(B^{-1}A^{-1}) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}\left(\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}\right) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} = I$$

and

$$\begin{aligned}(AB)(A^{-1}B^{-1}) &= \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}\left(\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\right) \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix} \\ &= \begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & 1 \end{pmatrix} \\ &\neq I.\end{aligned}$$

◊

Exercise 11. *(pg. 117 Exercise 9) Suppose that $b \in R$, a non-commutative ring with unity. Suppose that $ab = bc = 1$; that is, b has a* ***right inverse*** *c and a* ***left inverse*** *a. Prove that $a = c$ and that b is a unit.*

Solution:

Let R be a non-commutative ring with unity. Let $a, b \in R$. Assume that $ab = bc = 1$. Begin with

$$ab = 1.$$

Multiply both sides by c on the right hand side to obtain

$$\begin{aligned}(ab)c &= 1 \cdot c \\ a(bc) &= c \\ a(1) &= c \\ a &= c\end{aligned}$$

where each step is justified by the associate and multiplicative identity properties, the multiplicative inverse property, and the multiplicative identity property. Hence $ba = bc = 1$, so $ab = ba = 1$. Thus b has a multiplicative inverse a. By definition of a unit, b is a unit. ______ ◊

Exercise 12. *(pg. 118 Exercise 11) Let R be a commutative ring with unity. Suppose that n is the least positive integer for which we get 0 when we add 1 to itself n times; we the say R has* ***characteristic*** *n. If there exists no such n, we say that R has* ***characteristic*** *0. For example, the characteristic of* $\mathbb{Z}_5$ *is 5 because* $1+1+1+1+1=0$, *whereas* $1+1+1+1 \neq 0$. *(Note that here we have suppressed '[' and ']'.)*

(a) Show that, if the characteristic of a commutative ring with unity R is n and a is any *element of R, then* $na = 0$.

(b) What are the characteristics of $\mathbb{Q}, \mathbb{R}, \mathbb{Z}_{17}$*?*

(c) Prove that if a field F has characteristic n, where $n > 0$, *then n is a prime integer.*

Solution:

(a) Let $a \in R$, where R is any commutative ring. Apply the distributive property of R and Exercise 6.1 to see that $na = a + a + \cdots + a = a \cdot 1 + a \cdot 1 + \cdots + a \cdot 1 = a(1 + 1 + \cdots + 1) = a \cdot 0 = 0$.

(b) The characteristics of $\mathbb{Q}$ and $\mathbb{R}$ are both 0. The characteristic of $\mathbb{Z}_{17}$ is 17, since (a) $17[1] = [17] = [0]$ and (b) $0 < n \cdot 1 < 17$ for all $n : 0 < n < 17$, so $n \cdot [1] \neq [17]$..

(c) Assume that F has characteristic $n > 0$. Then $n \cdot 1 = 0$. Let p be the smallest prime number that divides n; say $n = pd$. Then $(pd)1 = 0$, so $p(d \cdot 1) = 0$. Now, $d \cdot 1 \in F$ by closure of addition.[1] Since F is a field, $d \cdot 1$ has an inverse; write e for the inverse. Apply Exercise 6.1, the associative property, and the property of the multiplicative inverse to obtain[2]

$$0 = 0e = (p(d \cdot 1))e = p((d \cdot 1)e) = p \cdot 1.$$

Recall that n is the characteristic of 1, so it is the *least* positive integer such that $n \cdot 1 = 0$. So $n \leq p$. On the other hand, p divides n, so $p \leq n$. Since $n \leq p$ and $n \geq p$, it follows that $p = n$. ◊

Exercise 13. *(pg. 118 Exercise 13) Suppose that R is a commutative ring and a is a non-zero nilpotent element. (See Exercise 7.15; this means that* $a^n = 0$ *for some positive integer n.) Prove that* $1 - a$ *is a unit.* Hint: *You can actually obtain a formula for the inverse.*

Solution:

Let $b = 1 + a + a^2 + \cdots + a^{n-1}$. Then

$$\begin{aligned}(1-a)b &= (1-a)\left(1 + a + a^2 + \cdots + a^{n-1}\right)\\ &= \left(1 + a + a^2 + \cdots + a^{n-1}\right) - \left(a + a^2 + a^3 + \cdots + a^n\right)\\ &= 1 - a^n\\ &= 1 - 0\\ &= 1.\end{aligned}$$

______ ◊

[1] Notice that I do not write $d \in F$. I cannot write $d \cdot 1 = d$, because $d \in \mathbb{Z}$ and $1 \in F$ and $\mathbb{Z} \neq F$, so they are elements of different sets, which may be different objects. As a matter of fact, $\mathbb{Z}$ is not even a field!

[2] Again, $p \cdot 1 \neq p$ because $p \in \mathbb{Z}$ and $1 \in F$.