ALGEBRAIC STRUCTURES - PRACTICAL 6 (SOLUTIONS)

This week's Exercises

Solve **all** the exercises of this section (i.e. Exercises 6.1 to 6.4) before Week 21.

6.1. Which elements of $\mathbb{Z}/4\mathbb{Z}$ are zero divisors? Which of $\mathbb{Z}/12\mathbb{Z}$?

Solution: We see that $\overline{2}$ is a zero divisors of $\mathbb{Z}/4\mathbb{Z}$ because $\overline{2}\cdot\overline{2}=\overline{0}$. Let us check whether this is the only zero divisor:

- We see that $\overline{1}$ is not a zero divisor because $\overline{1}\cdot a=a$, so if $a\neq\overline{0}$ then $\overline{1}\cdot a\neq\overline{0}$.
- $\overline{3}$ is not a zero divisor because $\overline{3}\cdot\overline{2}=\overline{2}$ and $\overline{3}\cdot\overline{3}=\overline{1}$. (We do not need to check $\overline{3}\cdot\overline{1}$ because we already know $\overline{1}$ is not a zero divisor.

It follows that the only zero divisor of $\mathbb{Z}/4\mathbb{Z}$ is $\overline{2}$.

The elements $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{6}$, $\overline{8}$, $\overline{9}$, and $\overline{10}$ are zero divisors of $\mathbb{Z}/12\mathbb{Z}$ because

$$\overline{2}\cdot\overline{6}=\overline{0},\quad \overline{3}\cdot\overline{8}=\overline{0},\quad \overline{4}\cdot\overline{9}=\overline{0},\quad \text{and } \overline{6}\cdot\overline{10}=\overline{0}.$$

Let us check whether those are the only zero divisors:

- As above, $\overline{1}$ is not a zero divisor.
- $\overline{5}$ is not a zero divisor because $\overline{5}\cdot\overline{2}=\overline{10}$, $\overline{5}\cdot\overline{3}=\overline{3}$, $\overline{5}\cdot\overline{4}=\overline{8}$, and $\overline{5}\cdot\overline{5}=\overline{1}$. (We do not need to check the next multiplications because we reached $\overline{1}$, so the values start to repeat.)
- Similarly, $\overline{7}$ and $\overline{11}$ are not a zero divisors. (It is a good exercise to check this!)

6.2. Consider the rings $\mathbb{Z}$ and $\mathbb{Z}\times\mathbb{Z}$.

(*1*) Which ones have unity? Write down the unities (if any).
(*2*) Which of them have zero divisors? Write down all zero divisors (if any).
(*3*) Which ones are integral domains? Justify.
(*4*) Which ones are fields? Justify.

Solution: **(1)** They all have unity. The unities are 1 and $(1,1)$ respectively.

(2) $\mathbb{Z}$ has no zero divisor. We know that if a and b are non-zero integers, then $a\cdot b\neq 0$.

Now, let us check whether $\mathbb{Z}\times\mathbb{Z}$ has zero divisors. The product of two arbitrary elements of $\mathbb{Z}\times\mathbb{Z}$ is $(a,b)\cdot(c,d)=(ac,bd)$.

Suppose the pair (a,b) is a zero divisor. Then $(a,b)\neq(0,0)$ and there is some pair $(c,d)\neq(0,0)$ with $(a,b)\cdot(c,d)=(0,0)$, which means $ac=0$ and $bd=0$. Because $(c,d)\neq(0,0)$, either $c\neq0$ or $d\neq0$ (or both). In the former case $ac=0$ shows $a=0$, and in the latter case $bd=0$ shows $b=0$. Hence any zero divisor (a,b) must have either $a=0$ or $b=0$, but nor both because $(a,b)\neq(0,0)$.

Conversely, we see that any such pair is a zero divisor: for any pair $(a,0)$ we have $(a,0)\cdot(0,1)=(0,0)$, and similarly in the other case.

In conclusion, the zero divisors in $\mathbb{Z} \times \mathbb{Z}$ are all pairs of the form $(a, 0)$ with $a \neq 0$, and those of the form $(0, b)$ with $b \neq 0$.

(3) $\mathbb{Z}$ is an integral domains because it is commutative, has unity 1 and it has no zero divisors.

$\mathbb{Z} \times \mathbb{Z}$ is not an integral domain because (although it is commutative and has unity) it has zero divisors.

(4) Neither are fields: $\mathbb{Z}$ does not have inverses and $\mathbb{Z} \times \mathbb{Z}$ is not even an integral domain.

6.3. Prove that $a^2 - b^2 = (a+b)(a-b)$ for all a, b in a ring R if and only if R is commutative.

Solution:

First, suppose $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$. We must show that the ring R is commutative. That is, given $x, y \in R$, we must show $xy = yx$ using the fact that $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$.

In fact,

$$(x + y)(x - y) = x^2 + yx - xy - y^2,$$

so if $x^2 - y^2 = (x + y)(x - y)$, then

$$yx - xy = 0$$

i.e. $yx = xy$.

Now, we need to show the other direction. That is, we assume that R is commutative and show that $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$. We have

$$(a + b)(a - b) = a^2 + ba - ab - b^2 = a^2 - b^2,$$

as required.

6.4.

(*1*) Prove that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.
(*2*) Prove that if p is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is an integral domain.

Solution: **(1)** By definition, if n is non-prime, then there are two integers a and b such that $a \neq \pm 1$, $b \neq \pm 1$ and $n = ab$.

This means in particular that $a < n$ and $b < n$, so that $\overline{a} \neq \overline{0}$ and $\overline{b} \neq \overline{0}$ and $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{n} = \overline{0}$.

This means that $\overline{a}$ and $\overline{b}$ are zero divisors.

(2) To show that $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, we must show that it has no zero divisors. That is, given elements $\overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$, we must show that either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.

Suppose $\overline{a} \neq \overline{0}$. Let us show that $\overline{b} = \overline{0}$. Since $\overline{ab} = \overline{a} \cdot \overline{b} = \overline{0}$, we know that p divides ab.

Since $\overline{a} \neq \overline{0}$, $p \nmid a$. Because p is a prime, we must have $p \mid b$. In other words, $\overline{b} = \overline{0}$.

Practice Exercises

The next exercises are meant to give you some extra practice to better prepare for assessments.

6.5. Let D be an integral domain.
(1) Show that if $a \in D$ satisfies $a^2 = 1$, then a is either 1 or -1.
[*Hint:* Show that $a^2 - 1 = 0$ and factorise the left-hand side.]
(2) Show that if $a \in D$ satisfies $a^2 = a$, then a is either 0 or 1.
(3) Show that if $a \in D$ satisfies $a^n = 0$ for some positive integer n, then $a = 0$.

Solution: (1) Subtracting 1 from both sides of $a^2 = 1$ we find $a^2 - 1 = 0$, which can be written as $(a-1)(a+1) = 0$. This is because the identity $a^2 - b^2 = (a-b)(a+b)$ holds in any commutative ring. (We need the ring to be commutative in order to cancel ab with ba in $(a-b)(a+b) = a^2 + ab - ba - b^2$). Since D is an integral domain, so it has no zero divisors, this implies either $a - 1 = 0$ or $a + 1 = 0$. In the former case we get $a = 1$, and in the latter case we get $a = -1$.

(2) Subtracting a from both sides of $a^2 = a$ we find $a^2 - a = 0$, which can be written as $a(a-1) = 0$ after collecting a. Like in part (1) we conclude that either $a = 0$, or $a - 1 = 0$, which in turn means $a = 1$.

(3) We can show this by induction on n. Clearly true when $n = 1$, so let $n > 1$ and assume the statement to be true when n is replaced with any smaller integer. If $a^n = 0$ then we may rewrite this condition as $a \cdot a^{n-1} = 0$, Because D is an integral domain, either $a = 0$, which is the desired conclusion, or $a^{n-1} = 0$. In the latter case $a = 0$ follows by the inductive hypothesis, so this completes our induction step.

6.6. Finish the proof of the properties of rings: show that, if $(R, +, \cdot)$ is a ring and $a, b, c \in R$, then

(*1*) Each equation $a + x = b$ (or $x + a = b$) has a unique solution.

(*2*) $-(-a) = a$ and $-(a+b) = (-a) + (-b)$.

(*3*) If m and n are integers, then $(m+n) \cdot a = ma + na$, $m \cdot (a+b) = ma + mb$, and $m(na) = (mn)a$.

In **(3)**, given a positive integer m, what we mean by ma is

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ times}} \quad \text{and } (-m)a = \underbrace{-a - a - \cdots - a}_{m \text{ times}}.$$

Solution: **(1)** First, we show that a solution exists. Notice that $b - a \in R$ because $a, b \in R$ and R is a ring. Hence, $x = b - a$ satisfies $a + x = b$.

Now, we show that the solution is unique. Suppose $r, s \in R$ are solutions of the equation $a + x = b$. Let us show that $r = s$. In fact, $a + r = b = a + s$. Subtracting a from both sides of $a + r = a + s$ gives $r = s$.

Similar arguments show that $x + a = b$ has a unique solution.

(2) We have that $a + (-a) = 0$. In particular, this means that a is the additive inverse of $-a$. In symbols: $-(-a) = a$.

(3) Let us show these equalities for m and n positive. The other cases follow from similar arguments.

Notice that everything follows from definition:

$$(m+n)a = \underbrace{a+a+\cdots+a}_{m+n \text{ times}} = \underbrace{a+a+\cdots+a}_{m \text{ times}} + \underbrace{a+a+\cdots+a}_{n \text{ times}} = ma+na.$$

Also,

$$m(a+b) = \underbrace{(a+b)+(a+b)+\cdots+(a+b)}_{m+n \text{ times}} = \underbrace{a+a+\cdots+a}_{m \text{ times}} + \underbrace{b+b+\cdots+b}_{n \text{ times}} = ma+mb,$$

where we are using the fact that $(R,+)$ is an abelian group (i.e. $a+b=b+a$). Moreover, $(m(na)) = \underbrace{na+na+\cdots+na}_{m \text{ times}}$ and $na = \underbrace{a+a+\cdots+a}_{n \text{ times}}$, so that

$$(m(na)) = \underbrace{a+a+\cdots+a}_{mn \text{ times}} = (mn)a.$$

6.7. The centre of a ring R is defined to be $\{c \in R \mid cr = rc \text{ for every } r \in R\}$. Show that the centre of a ring **with unity** is a subring.

Solution: Let us apply the QST. Denote by $Z = \{c \in R \mid cr = rc \text{ for every } r \in R\}$.

Non-empty: Since R is a ring with unity e, and the unity satisfies $er = re$ for all $r \in R$, we see that $e \in Z$.

Closed under addition: For $c, d \in Z$, we must show $c+d \in Z$. Now, what does it mean for $c+d$ to be an element of Z? (Think a bit before checking the solution!)

$c+d$ only belongs to Z if $(c+d)r = r(c+d)$ for all $r \in R$. Now, to show this, we can use the fact that $c, d \in Z$, i.e. $cr = rc$ and $dr = rd$ for all $r \in R$. So that

$$\begin{aligned} r(c+d) &= rc + rd && (R \text{ is a ring–hence distributive–and } r,c,d \in R) \\ &= cr + dr && (cr = rc \text{ and } dr = rd \text{ for all } r \in R) \\ &= (c+d)r && (\text{Distributivity of } R \text{ again}) \end{aligned}$$

as required.

Closed under multiplication: For $c, d \in Z$, we must show $cd \in Z$. Similarly as before, this means we need to show $(cd)r = r(cd)$ for all $r \in R$. To show this, we can use the fact that $c, d \in Z$, i.e. $cs = sc$ and $ds = sd$ for all $s \in R$. So that

$$\begin{aligned} r(cd) &= (rc)d && (R \text{ is associative and } r,c,d \in R) \\ &= (cr)d && (cr = rc \text{ for all } r \in R) \\ &= d(cr) && (ds = sd \text{ for all } s \in R \text{ and } cr \in R) \\ &= (dc)r && (\text{Associativity of } R \text{ again}) \\ &= (cd)r && (ds = sd \text{ for all } s \in R) \end{aligned}$$

Negatives: For each $c \in Z$, we already know that its additive inverse exists because R is a ring, so $-c \in R$. We are left to show that $-c \in Z$. That is, we must show that $(-c)r = r(-c)$ for all $r \in R$. In fact,

$$(-c)r = -(cr) = -(rc) = r(-c)$$

for all $r \in R$. Hence Z contains the negative of each of its elements.

Therefore Z is a subring of R.

6.8. What is the smallest subring of $\mathbb{Z}$ containing 3? What is the smallest subring of $\mathbb{R}$ containing $1/2$?

[By smallest we mean with respect to inclusion. For instance, we say that R is the smallest subring of $\mathbb{Z}$ containing 3 if every subring S of $\mathbb{Z}$ containing 3 is such that $R \subseteq S$.]

Solution: Let denote by S be the smallest subring of $\mathbb{Z}$ containing 3 so that we can find out what S is.

By definition, S is closed under addition because it is a ring. Since $3 \in S$, we see that every multiple of 3 is also in S. Therefore $3\mathbb{Z} \subseteq S$.

Let us now show that $S \subseteq 3\mathbb{Z}$ so that we can conclude $S = 3\mathbb{Z}$.

We have already shown that $3\mathbb{Z}$ is a subring of $\mathbb{Z}$. We defined S to be the smallest ring containing 3. This means that for every ring R containing 3, we must have $S \subseteq R$. In particular, $S \subseteq 3\mathbb{Z}$ as desired.

Let us now find the smallest subring of $\mathbb{R}$ containing $1/2$. Denote it by T.

Because T is a ring, it is closed under addition so that $n \cdot \frac{1}{2} \in T$ for all $n \in \mathbb{N}$.

Also, since the negative of every element in T is again in T, we get that $n \cdot \frac{1}{2} \in T$ for all $n \in \mathbb{Z}$. In other words, $\frac{1}{2}\mathbb{Z} \subseteq T$.

However $\frac{1}{2}\mathbb{Z}$ is not closed under multiplication, since $1/2 \cdot 1/2 = 1/4 \notin \frac{1}{2}\mathbb{Z}$. But we see that $\frac{1}{4} \in T$ because T is a ring containing $\frac{1}{2}$. We conclude that $\frac{1}{4}\mathbb{Z} \subseteq T$.

Now, because $\frac{1}{2}, \frac{1}{4} \in T$, we must have that $\frac{1}{8} = \frac{1}{2} \cdot \frac{1}{4} \in T$, hence $\frac{1}{8}\mathbb{Z} \subseteq T$. And so on. We then get

$$\frac{1}{2}\mathbb{Z} \cup \frac{1}{4}\mathbb{Z} \cup \frac{1}{8}\mathbb{Z} \cup \ldots = \left\{\frac{1}{2^n} \cdot k \mid k \in \mathbb{Z}, n \in \mathbb{N}\right\} \subseteq T.$$

Applying the QST we see that (you should check!)

$$\frac{1}{2}\mathbb{Z} \cup \frac{1}{4}\mathbb{Z} \cup \frac{1}{8}\mathbb{Z} \cup \ldots = \left\{\frac{1}{2^n} \cdot k \mid k \in \mathbb{Z}, n \in \mathbb{N}\right\}$$

is a subring of $\mathbb{R}$. Since T is the smallest subring of $\mathbb{R}$ containing $1/2$, it follows that $T = \{\frac{1}{2^n} \cdot k \mid k \in \mathbb{Z}, n \in \mathbb{N}\}$.
