Ring Theory Exercises

Jason Sass

April 24, 2023

Exercise 1. Is the algebraic structure$(7\mathbb{Z}, +, \cdot)$ a ring?

Solution. The set $7\mathbb{Z} = \{7k : k \in \mathbb{Z}\}$ is the set of all multiples of 7.
The structure $(7\mathbb{Z}, +)$ is a cyclic group, so $7\mathbb{Z}$ is abelian.
We also can determine that multiplication is associative.
However, there is no multiplicative identity, so $(7\mathbb{Z}, + \cdot)$ is not a ring. □

Exercise 2. Let $(R, +, \cdot)$ be a ring.
Then $(a + b)(c + d) = ac + ad + bc + bd$ for all $a, b, c, d \in R$.

Proof. Let $a, b, c, d \in R$.
Then

$$\begin{aligned}(a+b)(c+d) &= (a+b)c + (a+b)d \\ &= ac + bc + ad + bd \\ &= ac + ad + bc + bd.\end{aligned}$$

□

Exercise 3. Let $(R, +, \cdot)$ be a commutative ring with unity $1 \neq 0$.
Then $(x + 1)^2 = x^2 + 2x + 1$ for all $x \in R$.

Proof. Let $x \in R$.
Let 1 be the unity of R.
Define $2 = 1 + 1$ and $2x = (1 + 1) \cdot x$ and $x^2 = x \cdot x$ for all $x \in R$.
Since $x \in R$ and $1 \in R$, then $x + 1 \in R$.
Hence,

$$\begin{aligned}(x+1)^2 &= (x+1)\cdot(x+1) \\ &= (x+1)\cdot x + (x+1)\cdot 1 \\ &= (x\cdot x + 1\cdot x) + (x\cdot 1 + 1\cdot 1) \\ &= x\cdot x + (1\cdot x + x\cdot 1) + 1\cdot 1 \\ &= x\cdot x + (1\cdot x + 1\cdot x) + 1\cdot 1 \\ &= x\cdot x + (1+1)\cdot x + 1\cdot 1 \\ &= x^2 + 2x + 1.\end{aligned}$$

□

Exercise 4. In any ring R, $(a+b)^2 = a^2 + 2ab + b^2$ iff R is commutative.

Proof. Let R be an arbitrary ring.
Let $a, b \in R$.
We prove if $(a+b)^2 = a^2 + 2ab + b^2$, then R is commutative.
Suppose $(a+b)^2 = a^2 + 2ab + b^2$.
Observe that

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

Observe that

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

Thus, $((a^2 + ab) + b^2) + ba = (a+b)^2 = a^2 + 2ab + b^2 = ((a^2 + ab) + b^2) + ab$.
Hence, $((a^2 + ab) + b^2) + ba = ((a^2 + ab) + b^2) + ab$.
By the cancellation law for addition we obtain $ba = ab$.
Therefore, $ab = ba$ for all $a, b \in R$, so R is commutative.
We prove if R is commutative, then $(a+b)^2 = a^2 + 2ab + b^2$.
Suppose R is commutative.
Then $ab = ba$.
Observe that

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

□

Exercise 5. Let R be a ring such that $a^2 = a$ for all $a \in R$.
Then R is commutative and $a + a = 0$ for all $a \in R$.
We note that R is a **boolean ring**.

Proof. We prove $(\forall a \in R)(a + a = 0)$.
Let $a \in R$.

Then

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

Thus, $a+a=(a+a)+(a+a)$, so $(a+a)+0=(a+a)+(a+a)$.
By the cancellation law for addition we obtain $0=a+a$.
We prove R is commutative.
Let $a,b \in R$.
Then

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

Thus, $a+b=(a+b)+(ab+ba)$, so $(a+b)+0=(a+b)+(ab+ba)$.
By the cancellation law for addition we obtain $0=ab+ba$.
Since $x+x=0$ for all $x \in R$, then in particular, $ab+ab=0$.
Thus, $ab+ab=0=ab+ba$.
By the cancellation law for addition we obtain $ab=ba$.
Therefore, $ab=ba$ for all $a,b \in R$, so $*$ is commutative. □

Exercise 6. Let R be a commutative ring.
For each $a \in R$ let $H_a = \{x \in R : ax = 0\}$.
Then for every $x,y \in H_a$, $xy \in H_a$.

Proof. Let $x,y \in H_a$.
Then $x,y \in R$ and $ax=0$ and $ay=0$.
Observe that

$$\begin{aligned} 0 &= 0y \\ &= (ax)y \\ &= a(xy). \end{aligned}$$

Since R is closed under multiplication, then $xy \in R$.
Thus, $xy \in R$ and $a(xy)=0$, so $xy \in H_a$. □

Exercise 7. Let $n \in \mathbb{N}, n > 1$ and $x^n = x$ for all x in a ring R.
If $a, b \in R$ such that $ab = 0$, then $ba = 0$.

Proof. Let $a, b \in R$ such that $ab = 0$.
Then $ab \in R$ and

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

Hence, $ba = 0$. □

Exercise 8. Let $(R, +, \cdot)$ be a division ring.
Let $a \in R$.
If $a \neq 0$, then $-\frac{1}{a} = \frac{1}{-a}$.

Proof. Suppose $a \neq 0$.
Since $a = 0$ implies $-a = 0$ for all a in a ring, then $-a = 0$ implies $-(-a) = 0$.
Hence, $-a = 0$ implies $a = 0$, so $a \neq 0$ implies $-a \neq 0$.
Since $a \neq 0$, then $-a \neq 0$.
Thus, $(-a)^{-1} \in R$, so $(-a)^{-1} = \frac{1}{-a}$.
Consequently, $(-a)(\frac{1}{-a}) = 1$.
Since $a \neq 0$, then $\frac{1}{a} \in R$, so $-\frac{1}{a} \in R$.
Observe that

$$\begin{aligned} -\frac{1}{a} &= -\frac{1}{a} \cdot 1 \\ &= (-\frac{1}{a})[(-a)(\frac{1}{-a})] \\ &= [(-\frac{1}{a})(-a)](\frac{1}{-a}) \\ &= [(\frac{1}{a})(a)](\frac{1}{-a}) \\ &= 1 \cdot \frac{1}{-a} \\ &= \frac{1}{-a}. \end{aligned}$$

Therefore, $-\frac{1}{a} = \frac{1}{-a}$. □

Exercise 9. Let $(R, +, \cdot)$ be a division ring.
Let $a, b \in R$.
If $b \neq 0$, then $-\frac{a}{b} = \frac{-a}{b}$.

Proof. Suppose $b \neq 0$.
Then $b^{-1} \in R$ and $\frac{a}{b} \in R$, so $-\frac{a}{b} \in R$.
Observe that

$$\begin{aligned} -\frac{a}{b} &= (-1) \cdot \frac{a}{b} \\ &= (-1) \cdot (a \cdot b^{-1}) \\ &= [(-1)(a)](b^{-1}) \\ &= (-a)(b^{-1}) \\ &= \frac{-a}{b}. \end{aligned}$$

Therefore, $-\frac{a}{b} = \frac{-a}{b}$. ☐

Integral domains

Exercise 10. Let D be an integral domain.
Let $x \in D$ such that $x^2 = x$.
Then either $x = 0$ or $x = 1$.

Proof. Since $x^2 = x$, then $0 = x^2 - x = x(x-1)$.
Hence, either $x = 0$ or $x - 1 = 0$.
Therefore, either $x = 0$ or $x = 1$. ☐

Exercise 11. Let D be an integral domain.
If $a^2 = 1$, then $a = \pm 1$.

Proof. Let $a \in D$ such that $a^2 = 1$.
Observe that $1^2 = 1 \cdot 1 = 1 = a^2$.
Thus, $a^2 - 1^2 = 0$, so $(a+1)(a-1) = 0$.
Since D is an integral domain, then either $a + 1 = 0$ or $a - 1 = 0$.
Hence, either $a = -1$ or $a = 1$, so $a = \pm 1$. ☐

Exercise 12. Let D be an integral domain.
Let $a, b \in D$.
Then $a^2 = b^2$ iff $a = b$ or $a = -b$.

Proof. We prove if $a^2 = b^2$ then $a = b$ or $a = -b$.
Suppose $a^2 = b^2$.
Then $0 = a^2 - b^2 = (a-b)(a+b)$.
Since D is an integral domain, then either $a - b = 0$ or $a + b = 0$.
Therefore, either $a = b$ or $a = -b$.
Conversely, we prove if $a = b$ or $a = -b$, then $a^2 = b^2$.
Suppose $a = b$ or $a = -b$.
If $a = b$, then $a^2 = aa = bb = b^2$.
If $a = -b$, then $a^2 = aa = (-b)(-b) = bb = b^2$. ☐

Ideals

Exercise 13. The set $\{[0],[2],[4]\}$ is an ideal of $\mathbb{Z}_6$.

Solution. Let $R = \mathbb{Z}_6$ and $I = \{[0],[2],[4]\}$.

Observe that I is a cyclic subgroup of $(\mathbb{Z}_6, +)$ and $I = \{k[2]_6 : k \in \mathbb{Z}\} = [2k]_6 : k \in \mathbb{Z}\}$.

Let $x \in I$.

Then $x = [2k]$ for some $k \in \mathbb{Z}$.

Let $a \in Rx$.

Then $a = [r]_6 x$ for some $r \in \mathbb{Z}$.

Thus, $a = [r]([2k]) = [(2k)r] = [2(kr)]$.

Since $\mathbb{Z}$ is closed under multiplication and $k, r \in \mathbb{Z}$, then $kr \in \mathbb{Z}$.

Hence, $a \in I$, by definition of I.

Thus, $a \in Rx$ implies $a \in I$, so $Rx \subset I$.

Let $b \in xR$.

Then $b = x[r]_6$ for some $r \in \mathbb{Z}$.

Thus, $b = [2k][r] = [(2k)r] = [2(kr)]$.

Since $\mathbb{Z}$ is closed under multiplication and $k, r \in \mathbb{Z}$, then $kr \in \mathbb{Z}$.

Hence, $a \in I$, by definition of I.

Thus, $a \in xR$ implies $a \in I$, so $xR \subset I$.

Therefore, $RI \subset I$ and $IR \subset I$.

Since $(I, +)$ is an abelian subgroup of $(R, +)$ and $RI \subset I$ and $IR \subset I$, then I is an ideal of R.

Thus, the set $\{[0],[2],[4]\}$ is an ideal of $\mathbb{Z}_6$. □

Proposition 14. *$\langle \mathbb{Z}, +, \cdot \rangle$ is a ring.*

Proof. We know $\langle \mathbb{Z}, + \rangle$ is an abelian group.

We know $\mathbb{Z}$ is closed under multiplication and $ab \in \mathbb{Z}$ is unique for all $a, b \in \mathbb{Z}$.

Therefore, multiplication is a binary operation on $\mathbb{Z}$.

Also, multiplication of integers is associative so $a(bc) = (ab)c$ for all $a, b, c \in \mathbb{Z}$.

We know multiplication is distributive over addition.

Thus, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in \mathbb{Z}$. □