Solutions to Assignment 9

1. Which of the following sets are rings with respect to the usual operations of addition and multiplication? If the set is a ring, is it also a field?

(a) \(4\mathbb{Z}\)

4\(\mathbb{Z}\) is an abelian group (it is a subgroup of \(\mathbb{Z}\)). Furthermore, if \(4a, 4b \in 4\mathbb{Z}\), then \((4a)(4b) = 16ab \in 4\mathbb{Z}\), so it is closed under multiplication. Multiplication is associative and distributive because it is the usual notion of addition of reals. This is not a field because 4 is not invertible.

(b) \(\mathbb{Z}^{\geq 0} = \{ z \in \mathbb{Z} \mid z \geq 0 \}\)

\(\mathbb{Z}^{\geq 0}\) is not an abelian group because 1 doesn’t have an additive inverse, so this is not a ring.

(c) \(\mathbb{Z}_{20}\)

\(\mathbb{Z}_{20}\) is an abelian group, is closed under multiplication, and multiplication is associative and distributive. This is not a field because it is not an integral domain — \(4 \cdot 5 = 20 \equiv 0 \pmod{20}\).

(d) \(\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}\)

If \(a, b, c, d \in \mathbb{Q}\), then
\[
(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}
\]
\[
(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + bd(\sqrt{2})^2
\]
\[
= (ac + 2bd) + (ad + bc)\sqrt{2}
\]
so \(\mathbb{Q}(\sqrt{2})\) is closed under addition, additive inverses, and multiplication. Therefore, \(\mathbb{Q}(\sqrt{2})\) is an additive subgroup of \(\mathbb{R}\). Furthermore, multiplication is associative and distributive, so \(\mathbb{Q}(\sqrt{2})\) is a ring. This is also a field:
\[
\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{-b}{a^2 - 2b^2} \sqrt{2}
\]
so as long as \(a^2 \neq 2b^2\), we know that \(a + \sqrt{2}b\) has a multiplicative inverse. If \(a^2 = 2b^2\), then either \(a = b = 0\) or \(\frac{a}{b} = \pm \sqrt{2}\), but \(\sqrt{2}\) is irrational, so this can only happen when \(a = b = 0\), i.e., \(a + \sqrt{2}b = 0\).

(e) \(R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}\)

This is not a ring because it is not closed under multiplication. We have \(\sqrt{2} \in R\), but \((\sqrt{2})^2 = 2^{2/3}\) is not an element of \(R\).

2. Let

\[R = \{ f : [0, 1] \to \mathbb{R} \mid f \text{ is continuous} \}\]

be the set of continuous real-valued functions on the interval \([0, 1]\). Show that \(R\) is a ring with respect to the operations \((f + g)(x) = f(x) + g(x)\) and \((fg)(x) = f(x)g(x)\). Show that \(R\) is a unital ring (i.e., has a multiplicative identity). What elements of \(R\) have multiplicative inverses? Is \(R\) an integral domain?

We have:

- \((R, +)\) is an abelian group: If \(f, g \in R\), then \(f + g\) is continuous, so it is an element of \(R\). If \(f, g, h \in R\), then
\[
((f + g) + h)(x) = f(x) + g(x) + h(x) = (f + (g + h))(x)
\]
for all \(x \in [0, 1]\), so \((f + g) + h = f + (g + h)\). If \(z(x) = 0\) for all \(x\), then \((f + z)(x) = f(x)\), so there is an identity element. Finally, if \((-f)(x) = -f(x)\), then \((f + (-f))(x) = 0\) for all \(x\), so every element has an additive inverse.
• **R is closed under multiplication:** If \( f \) and \( g \) are continuous, then \( fg \) is continuous.

• **Multiplication is associative:** If \( f, g, h \in R \), then

\[
((fg)h)(x) = f(x)g(x)h(x) = (f(h))g(x)
\]

• **Distributivity:** If \( f, g, h \in R \), then

\[
((f + g)h)(x) = f(x)h(x) + g(x)h(x) = (fh + gh)(x)
\]

and

\[
(h(f + g))(x) = h(x)f(x) + h(x)g(x) = (hf + hg)(x)
\]

for all \( x \).

Therefore, \( R \) is a ring.

It is unital because the constant function 1 is a multiplicative identity. Whenever \( f(x) \) is a function such that \( f(x) \neq 0 \) for all \( x \), then \( (1/f)(x) = 1/f(x) \) is continuous and \( f \cdot (1/f) = 1 \), so \( f \) has a multiplicative inverse. On the other hand, if \( f \cdot g = 1 \), then \( f(x) \neq 0 \) for all \( x \in [0,1] \), so the invertible functions are exactly those functions that are never zero.

\( R \) is not an integral domain because it has zero-divisors. Let

\[
f(x) = \begin{cases} 
0 & x < 1/2 \\
x - 1/2 & x \geq 1/2
\end{cases}
\]

and

\[
g(x) = \begin{cases} 
1/2 - x & x < 1/2 \\
0 & x \geq 1/2.
\end{cases}
\]

Then

\[
(fg)(x) = \begin{cases} 
0 \cdot (1/2 - x) & x < 1/2 \\
(x - 1/2) \cdot 0 & x \geq 1/2
\end{cases} = 0,
\]

but \( f \) and \( g \) are nonzero.

3. If \( R \) is a ring, \( n \in \mathbb{N} \), and \( a \in R \), let

\[
a_n = a + \cdots + a.
\]

Show that if \( a, b \in R \) and \( m, n \in \mathbb{N} \), then

\[
(na)(mb) = (nm)(ab).
\]

\[
(na)(mb) = (a + \cdots + a)(mb)
\]

\[
\underbrace{a(mb) + \cdots + a(mb)}_{n \text{ times}}
\]

\[
= n(a(mb))
\]

\[
= n(a(b + \cdots + b))
\]

\[
= n(ab + \cdots + ab)
\]

\[
= ab + \cdots + ab
\]

\[
= (nm)(ab)
\]
4. Herstein, p. 130: #3

For each natural number \( n \), the product \((a + b)^n\) is the sum of the \( 2^n \) products of the form \( r_1 \ldots r_n \), where \( r_i = a \) or \( r_i = b \) for all \( i \). That is,

\[
(a + b)^n = \sum_{r_1, \ldots, r_n \in \{a, b\}} r_1 \ldots r_n.
\]

We prove this by induction. When \( n = 1 \), this is true: \((a + b)^1 = a + b\). Suppose that \((a + b)^n = \sum_{r_1, \ldots, r_n \in \{a, b\}} r_1 \ldots r_n\) is true for \( n \).

Then

\[
(a + b)^{n+1} = (a + b)^n (a + b) \]
\[
= \left[ \sum_{r_1, \ldots, r_n \in \{a, b\}} r_1 \ldots r_n \right] (a + b) \\
= \sum_{r_1, \ldots, r_n \in \{a, b\}} r_1 \ldots r_n a + \sum_{r_1, \ldots, r_n \in \{a, b\}} r_1 \ldots r_n b \\
= \sum_{r_1, \ldots, r_{n+1} \in \{a, b\}} r_1 \ldots r_{n+1}
\]

as desired.

Herstein, p. 130: #4

First, note that for all \( x \in R \), we have

\[
x = x^2 = (-x)^2 = -x,
\]

so \( x = -x \).

Furthermore, if \( x, y \in R \), then

\[
x + y = (x + y)^2 \\
x + y = x^2 + xy + yx + y^2 \\
x + y = x + xy + yx + y0 = xy + yx.
\]

Therefore, \( xy = -yx = yx \), so \( R \) is commutative.