MATH 521A: Abstract Algebra
Homework 4 Solutions

1. Let R be a ring, with additive and multiplicative neutral elements $0_R, 1_R$. Prove that $0_R, 1_R$ are unique.

Suppose there were some other additive neutral element $0'_R$. Consider $X = 0_R + 0'_R$. On one hand, $X = 0'_R$ since 0_R is neutral. On the other hand, $X = 0_R$ since $0'_R$ is neutral. Hence $0_R = 0'_R$.

Suppose there were some other multiplicative neutral element $1'_R$. Consider $Y = 1_R 1'_R$. On one hand, $Y = 1'_R$ since 1_R is neutral. On the other hand, $Y = 1_R$ since $1'_R$ is neutral. Hence $1_R = 1'_R$.

2. For prime p, set $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$. Prove that $\mathbb{Z}[\sqrt{p}]$ is a subring of $\mathbb{R}$.

There are four things to check. First, $0_\mathbb{R} = 0 + 0\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Second, let $a + b\sqrt{p}, a' + b'\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. We have $(a + b\sqrt{p}) + (a' + b'\sqrt{p}) = (a + a') + (b + b')\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Third, let $a + b\sqrt{p}, a' + b'\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. We have $(a + b\sqrt{p})(a' + b'\sqrt{p}) = (aa' + pbb') + (ab' + ba')\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Fourth, let $a + b\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Now, $-(a + b\sqrt{p}) = (-a) + (-b)\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$.

3. For prime p, set $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$. Prove that $\mathbb{Q}[\sqrt{p}]$ is a subfield of $\mathbb{R}$.

There are five things to check, four of which are very similar to problem #2. First, $0_\mathbb{R} = 0 + 0\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Second, let $a + b\sqrt{p}, a' + b'\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. We have $(a + b\sqrt{p}) + (a' + b'\sqrt{p}) = (a + a') + (b + b')\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Third, let $a + b\sqrt{p}, a' + b'\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. We have $(a + b\sqrt{p})(a' + b'\sqrt{p}) = (aa' + pbb') + (ab' + ba')\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Fourth, let $a + b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$. Now, $-(a + b\sqrt{p}) = (-a) + (-b)\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$.

Fifth, let $a+b\sqrt{p} \in \mathbb{Q}[\sqrt{p}]$ be nonzero. We calculate $\frac{1}{a+b\sqrt{p}} = \frac{1}{a+b\sqrt{p}}\frac{a-b\sqrt{p}}{a-b\sqrt{p}} = \frac{a-b\sqrt{p}}{a^2-pb^2} = (\frac{a}{a^2-pb^2}) + (\frac{-b}{a^2-pb^2})\sqrt{p}$. Now, to show the result is in $\mathbb{Q}[\sqrt{p}]$, we need to prove that $a^2 - pb^2 \neq 0$. Fortunately this was done on the first exam, provided a, b are both nonzero. If just one is zero, that contradicts $a^2 - pb^2 = 0$; if both are zero, that contradicts $a + b\sqrt{p}$ being nonzero.

4. For $k \in \mathbb{Z}$, define object R_k, which has ground set $\mathbb{Z}$, and operations $\oplus, \odot$ defined as:

$$a \oplus b = a + b, \quad a \odot b = k$$

Determine for which k, if any, R_k is a ring.

First consider $k \neq 0$ and suppose R_k were a ring. Then for any a, b, c we have $k = a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) = k \oplus k = k + k = 2k$. Hence $k = 2k$, so $0 = k$, a contradiction. Thus R_k is not a ring for $k \neq 0$.

If $k = 0$ we will prove that R_k is a ring.
1: $a + b, 0$ are each in $\mathbb{Z}$, so $\oplus, \odot$ are closed.
2: $a \oplus (b \oplus c) = a \oplus (b + c) = a + (b + c) = (a + b) + c = (a + b) \oplus c = (a \oplus b) \oplus c$, so $\oplus$ is associative.
3: $a \oplus b = a + b = b + a = b \oplus a$, so $\oplus$ is commutative.
4: $0 \oplus a = 0 + a = a = a + 0 = a \oplus 0$, so $0_{R_0} = 0$ is neutral under $\oplus$.
5: Let $a \in \mathbb{Z}$. Then $a \oplus (-a) = a + (-a) = 0$, so inverses exist under $\oplus$.
6: $a \odot (b \odot c) = a \odot 0 = 0 = 0 \odot c = (a \odot b) \odot c$, so $\odot$ is associative.
8: $a \odot b = 0 = b \odot a$, so $\odot$ is commutative. This is optional, but makes 7 easier.
7: $a \odot (b \oplus c) = a \odot (b + c) = 0 = 0 + 0 = (a \odot b) + (a \odot c) = (a \odot b) \oplus (a \odot c)$. This proves the distributive property from the left; the distributive property from the right follows by 8, i.e. commutativity of $\odot$.

5. Prove or disprove: If R, S are fields, then $R \times S$ is an integral domain.

We saw a counterexample in HW3. $\mathbb{Z}_2$ and $\mathbb{Z}_5$ are both fields, since $2, 5$ are prime (and, by Thm 2.8, all nonzero elements of these rings are units). But $\mathbb{Z}_2 \times \mathbb{Z}_5$ has zero divisors, e.g. $([1], [0]) \odot ([0], [1]) = ([0], [0]) = 0_R$.

6. Define R, an object with ground set $\mathbb{Z}$, and operations $\oplus, \odot$ defined as:

$$a \oplus b = a + b - 1, \quad a \odot b = a + b - ab$$

Prove that R is an integral domain.

1. $a + b - 1, a + b - ab$ are both integers, so $\oplus, \odot$ are closed.
2. $a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + (b + c - 1) - 1 = (a + b - 1) + c - 1 = (a \oplus b) + c - 1 = (a \oplus b) \oplus c$, so $\oplus$

is associative.
3. $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$, so $\oplus$ is commutative.
4. $a \oplus 1 = a + 1 - 1 = a = 1 + a - 1 = 1 \oplus a$, so $0_R = 1$ is neutral under $\oplus$.
5. Let $a \in \mathbb{Z}$. Then $a \oplus (2-a) = a + (2-a) - 1 = 1 = 0_R$, so inverses exist under $\oplus$.
6. $a \odot (b \odot c) = a \odot (b + c - bc) = a + (b + c - bc) - a(b + c - bc) = (a + b + c) - (bc + ab + ac) + abc = (a + b - ab) + c - (a + b - ab)c = (a + b - ab) \odot c = (a \odot b) \odot c$, so $\odot$ is associative.
8. $a \odot b = a + b - ab = b + a - ba = b \odot a$, so $\odot$ is commutative.
7. $a \odot (b \oplus c) = a \odot (b + c - 1) = a + (b + c - 1) - a(b + c - 1) = (a + b - ab) + (a + c - ac) - 1 = (a \odot b) + (a \odot c) - 1 = (a \odot b) \oplus (a \odot c)$. This proves the distributive property from the left; the distributive property from the right follows by 8, i.e. commutativity of $\odot$.
9. $a \odot 0 = a + 0 - a0 = a = 0 + a - 0a = 0 \cdot a$, so $1_R = 0$ is neutral under $\odot$.
10. $1_R = 0 \neq 1 = 0_R$. Suppose now that $a \odot b = 0_R = 1$. Then $a + b - ab = 1$, which rearranges to $ab - a - b + 1 = 0$ or $(a-1)(b-1) = 0$. Hence either $a = 1 = 0_R$ or $b = 1 = 0_R$. Thus R has no zero divisors.

7. Define R, an object with ground set $\mathbb{Z}$, and operations $\oplus, \odot$ defined as:

$$a \oplus b = a + b - 1, \quad a \odot b = ab - a - b + 2$$

Prove that R is an integral domain.

1. $a + b - 1, ab - (a + b) + 2$ are both integers, so $\oplus, \odot$ are closed.
2-5. $\oplus$ here is identical to problem 6, so the same arguments work.
6. $a \odot (b \odot c) = a \odot (bc - b - c + 2) = a(bc - b - c + 2) - a - (bc - b - c + 2) + 2 = (a + b + c) - (ab + ac + bc) + abc = (ab - a - b + 2)c - (ab - a - b + 2) - c + 2 = (ab - a - b + 2) \odot c = (a \odot b) \odot c$, so $\odot$ is associative.
8. $a \odot b = ab - a - b + 2 = ba - b - a + 2 = b \odot a$, so $\odot$ is commutative.
7. $a \odot (b \oplus c) = a \odot (b + c - 1) = a(b + c - 1) - a - (b + c - 1) + 2 = (ab - a - b + 2) + (ac - a - c + 2) - 1 = (ab - a - b + 2) \oplus (ac - a - c + 2) = (a \odot b) \oplus (a \odot c)$. This proves the distributive property from the left; the distributive property from the right follows by 8, i.e. commutativity of $\odot$.
9. $2 \cdot a = 2a - 2 - a + 2 = a = a2 - a - 2 + 2 = a \cdot 2$, so $1_R = 2$ is neutral under $\odot$.
10. $1_R = 2 \neq 1 = 0_R$. Suppose now that $a \odot b = 0_R = 1$. Then $ab - a - b + 2 = 1$, which rearranges to $ab - a - b + 1 = 0$ or $(a-1)(b-1) = 0$. Hence either $a = 1 = 0_R$ or $b = 1 = 0_R$. Thus R has no zero divisors.

8. Define R, an object with ground set $\mathbb{Z} \cup \{+\infty\}$, and operations $\oplus, \odot$ defined as:

$$a \oplus b = \min(a, b), \quad a \odot b = a + b$$

Prove that R satisfies every field axiom except one, and prove that R fails to satisfy that one.

1. $\min(a, b), a + b$ are both integers, so $\oplus, \odot$ are closed.
2. $a \oplus (b \oplus c) = a \oplus (\min(b, c)) = \min(a, \min(b, c)) = \min(a, b, c) = \min(\min(a, b), c) = \min(a, b) \oplus c = (a \oplus b) \oplus c$, so $\oplus$ is associative.
3. $a \oplus b = \min(a, b) = \min(b, a) = b \oplus a$, so $\oplus$ is commutative.
4. $a \oplus \infty = \min(a, \infty) = a = \min(\infty, a) = \infty \oplus a$, so $0_R = \infty$ is neutral under $\oplus$.
5. Inverses under $\oplus$ need not exist. As proof, consider the counterexample of 7. There is no additive inverse to 7, because there is no $x \in R$ with $7 \oplus x = \min(7, x) = \infty = 0_R$. In fact, only ∞ has an additive inverse.
6. $a \odot (b \odot c) = a \odot (b + c) = a + (b + c) = (a + b) + c = (a + b) \odot c = (a \odot b) \odot c$. Hence $\odot$ is associative.
8. $a \odot b = a + b = b + a = b \odot a$. Hence $\odot$ is commutative.
7. $a \odot (b \oplus c) = a \odot (\min(b, c)) = a + \min(b, c) = \min(a + b, a + c) = (a + b) \oplus (a + c) = (a \odot b) \oplus (a \odot c)$. This proves the distributive property from the left; the distributive property from the right follows by 8, i.e. commutativity of $\odot$.
9. $a \odot 0 = a + 0 = a = 0 + a = 0 \odot a$, so $1_R = 0$ is neutral under $\odot$.
10. $0_R = \infty \neq 0 = 1_R$. Suppose now that $a \odot b = 0_R = \infty$. Then $a + b = \infty$, which can only happen if $a = \infty = 0_R$ or $b = \infty = 0_R$. Thus R has no zero divisors.
11. Let $a \in R$ satisfy $a \neq 0_R$, i.e. $a \neq \infty$. We have $a \odot (-a) = a + (-a) = 0 = 1_R$. Hence every nonzero element of R is a unit.