1. Let $R$ be a ring with operations $\oplus, \odot$. Define its annihilation ring $R^{\text{ann}}$ as follows. $R^{\text{ann}}$ has the same ground set as $R$. We define addition in $R^{\text{ann}}$ to be the same as in $R$, i.e. $\forall a, b \in R^{\text{ann}}, a \oplus^{\text{ann}} b = a \oplus b$. We define multiplication in $R^{\text{ann}}$ as $\forall a, b \in R^{\text{ann}}, a \odot^{\text{ann}} b = 0_R$. Prove that $R^{\text{ann}}$ is a ring.

Most of the ring axioms don’t involve multiplication, so $R^{\text{ann}}$ inherits them from $R$, since it has the same addition. Let $a, b, c \in R^{\text{ann}}$ be arbitrary. We have $a \odot^{\text{ann}} (b \odot^{\text{ann}} c) = a \odot^{\text{ann}} 0_R = 0_R = 0_R \odot^{\text{ann}} c = (a \odot^{\text{ann}} b) \odot^{\text{ann}} c$. We also have $a \odot^{\text{ann}} (b \odot^{\text{ann}} c) = 0_R = 0_R \odot^{\text{ann}} 0_R = 0_R \odot^{\text{ann}} 0_R = (a \odot^{\text{ann}} b) \odot^{\text{ann}} (a \odot^{\text{ann}} c)$. Lastly, we have $(b \odot^{\text{ann}} c) \odot^{\text{ann}} a = 0_R = 0_R \odot^{\text{ann}} 0_R = (b \odot^{\text{ann}} a) \odot^{\text{ann}} (c \odot^{\text{ann}} a)$.

2. Let $R$ be a ring with just two elements: $\{0, a\}$. How many such rings are there? Be sure to prove your answer.

The addition table must be $0 + 0 = 0 = a + a$, and $0 + a = a + 0 = a$, because 0 is neutral and $a$ must have an inverse. The multiplication table must have $0 \cdot 0 = 0 \cdot a = a \cdot 0 = 0$, by theorem 3.5. However we don’t know if $a \cdot a = a$ or $a \cdot a = 0$. It turns out both are possible; the former is isomorphic to $\mathbb{Z}_2$, while the latter is isomorphic to $\mathbb{Z}_2^{\text{ann}}$.

3. Let $R$ be a ring with identity with just three elements: $\{0, 1, a\}$. How many such rings are there? Be sure to prove your answer.

Consider first $1 + a$. It can’t equal 1, else $a = 0$. It can’t equal $a$, else $1 = 0$. Hence $1 + a = 0$. Now consider $1 + a$. It can’t equal 1, else $1 = 0$. It can’t equal 0, else $1 + 1 = 0 = 1 + a$, so $a = 1$. Hence $1 + 1 = a$. Lastly, $a + a$ can’t be 0, else $a + a = 0 = 1 + a$ so $a = 1$, and $a + a$ can’t be $a$, else $a = 0$. Hence $a + a = 1$. Putting this all together gives the same addition table as $\mathbb{Z}_3$.

For the multiplication, we know that $0 \cdot 0 = 0 \cdot 0 = 0 \cdot 1 = 0 \cdot a = 1 \cdot 0 = a \cdot 0$. We also know that $1 \cdot 1 = 1$ and $1 \cdot a = a \cdot 1 = a$. The only mystery is $a \cdot a$. However we know that $a = 1 + 1$, so we have $a \cdot a = (1 + 1) \cdot (1 + 1) = 1 + 1 + 1 + 1 = a + a = 1$. Hence the multiplication agrees with $\mathbb{Z}_3$; so any such ring must be isomorphic to $\mathbb{Z}_3$.

4. Let $R$ be a ring with identity. Suppose that $a, b \in R$ such that $a, ab$ are both units. Prove that $b$ is a unit. Do not assume that $R$ is commutative.

Since $a$ is a unit, there is some $c \in R$ with $ca = ac = 1_R$. Similarly, since $ab$ is a unit, there is some $d \in R$ with $d(ab) = (ab)d = 1_R$. We will prove that $u = da$ is the reciprocal of $b$. First, multiply $1_R = abd$ on the left by $c$, to get $c = c1_R = (ca)bd = 1_Rbd = bd$. Multiply this by $a$ on the right to get $1_R = ca = b(da) = bu$. The other direction is easier; $ub = (da)b = d(ab) = 1_R$. Hence $b$ is a unit.

5. Let $R = \{(a/b, c/d) : a, b, c, d \in \mathbb{Q}\}$, the ring of $2 \times 2$ matrices over $\mathbb{Q}$, with operations of the usual matrix addition and matrix multiplication. Prove that every nonzero element of $R$ is either a unit or a zero divisor.

The trick is to find a test that classifies elements, namely the determinant $ad - bc$. Claim 1: If $ad - bc \neq 0$, then $(a/b, c/d)$ is a unit. Proof: Set $f = ad - bc$ and just compute $(a/b, c/d) \begin{pmatrix} d/f & -b/f \\ -c/f & a/f \end{pmatrix}$ =
Let \( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 1_R. \)

Claim 2: If \( ab - bc = 0 \), then \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) is a (two-sided) zero divisor. Compute \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) \( \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_R. \)

6. Let \( R \) be a ring. Consider the diagonal map \( f : R \to R \times R \) given by \( f : r \mapsto (r, r) \). Prove that \( f \) is a (ring) homomorphism.

Let \( a, b \in R \). We have \( f(a + b) = (a + b, a + b) = (a, a) + (b, b) = f(a) + f(b) \), and \( f(ab) = (ab, ab) = (a, a)(b, b) = f(a)f(b) \).

7. Let \( R, S, T \) be rings. Prove that the ring \( (R \times S) \times T \) is isomorphic to the ring \( R \times (S \times T) \).

We need to find a candidate isomorphism, and the natural choice is \( f : ((x, y), z) \mapsto (x, (y, z)) \). First, let’s prove it’s a homomorphism. Let \( x, x' \in R, y, y' \in S, z, z' \in T \), and we have \( f(((x, y), z) + ((x', y'), z')) = f(((x + x', y + y'), z + z')) = ((x, y) + (x', y'), z + z') = (x, (y, z)) + ((x', y', z'), z') \). Similarly, we have \( f(((x, y), z)((x', y'), z')) = f(((x', y'), z')) = (x, (y, z))(x', (y', z')) = f((x, (y, z))f((x', (y', z'))) \).

Now, to prove bijection, we need to prove surjectivity and injectivity. Suppose that \( f(((x, y), z))) = f(((x', y'), z')) \). Then \( (x, (y, z)) = (x', (y', z')) \) and hence \( x = x', y = y', z = z' \), so \( ((x, y), z) = ((x', y'), z') \). This proves one-to-one. Lastly, let \( (a, (b, c)) \in R \times (S \times T) \). We see that \( ((a, b), c) \in (R \times S) \times T \) and \( f(((a, b), c)) = (a, (b, c)) \). This proves onto.

8. Prove that \( \mathbb{Z}_9 \) is not isomorphic to \( \mathbb{Z}_3 \times \mathbb{Z}_3 \), despite having the same number of elements.

Suppose there were some isomorphism \( f : \mathbb{Z}_9 \to \mathbb{Z}_3 \times \mathbb{Z}_3 \). Note that if \( a, b \in \mathbb{Z}_9 \) with \( ab = 1_9 \), then \( f(a)f(b) = f(ab) = f(1_9) = 1_{3 \times 3} \), so every unit in \( \mathbb{Z}_9 \) must map to a unit in \( \mathbb{Z}_3 \times \mathbb{Z}_3 \). However we found six units in \( \mathbb{Z}_9 \) and only four in \( \mathbb{Z}_3 \times \mathbb{Z}_3 \). Thus no such isomorphism can exist. One could consider zero divisors instead.

9. Consider the function \( f : \mathbb{Z}_7 \to \mathbb{Z}_{56} \) given by \( f : [x]_7 \mapsto [8x]_{56} \). Prove that \( f \) is an injective homomorphism, but not an isomorphism.

Let \([x], [y] \in \mathbb{Z}_7\). We have \( f([x] + [y]) = f([x + y]) = [8(x + y)]_{56} = [8x]_{56} + [8y]_{56} = f([x]) + f([y]), \) and \( f([x][y]) = f([xy]) = [8(xy)]_{56} = [8(x)]_{56} [8(y)]_{56} = [64(xy)]_{56} = [8x]_{56}[8y]_{56} = f([x])f([y]). \) Hence \( f \) is a homomorphism. Proving injectivity is as simple as noting the image of \( f \) is \( \{[0]_{56}, [8]_{56}, [16]_{56}, [24]_{56}, [32]_{56}, [40]_{56}, [48]_{56} \} \), which has just seven elements. Since \( 7 < 56 \), \( f \) is not surjective.

10. Consider the ring \( R \), on ground set \( \mathbb{Z} \), with operations \( \oplus, \odot \) defined as \( a \oplus b = a + b + 1, \) \( a \odot b = ab + a + b \). Prove that \( R \) is isomorphic to \( \mathbb{Z} \). (you may assume that \( R \) is a ring)

The hard part is finding the right isomorphism, which is \( f : R \to \mathbb{Z} \) given by \( f(x) = x + 1 \). First, let’s prove homomorphism. Let \( a, b \in \mathbb{Z} \). We have \( f(a \oplus b) = f(a + b + 1) = a + b + 2 = (a + 1) + (b + 1) = f(a) + f(b) \). We also have \( f(a \odot b) = f(ab + a + b) = ab + a + b + 1 = (a + 1)(b + 1) = f(a)f(b) \). Lastly we prove isomorphism. Suppose that \( f(a) = f(b) \). Then \( a + 1 = b + 1 \), so \( a = b \). Hence \( f \) is injective. Let \( a \in \mathbb{Z} \); we have \( f(a - 1) = (a - 1) + 1 = a \), so \( f \) is surjective.