1. Let $R$ be a ring. Prove the following basics:

   (a) $0 \cdot a = 0$ for all $a \in R$. Consider $0a + 0a = (0+0)a = 0a$. Taking the additive inverse of $0a$ on both sides gives $0a + 0 = 0$ or $0a = 0$.

   (b) If $a, b \in R$, then $a \cdot (-b) = -(a \cdot b)$. (Be careful as this isn't just "moving around a minus sign"; it says that $a$ times the additive inverse of $b$ is suppose to be the additive inverse of $ab$, and that's what you must prove.) $a(-b) + ab = a(-b+b) = a0 = 0$. Hence, $-ab = a(-b)$.

2. Let $n$ be a positive integer. Prove that the set of zero divisors of $\mathbb{Z}/n\mathbb{Z}$ is precisely the set of elements in $\mathbb{Z}/n\mathbb{Z}$ that are not relatively prime to $n$, and that the set of units in $\mathbb{Z}/n\mathbb{Z}$ is the set of elements that *are* relatively prime to $n$. Suppose that $z \in \{1, \ldots, n-1\}$ is an integer with $\gcd(z, n) = d \neq 1$. Then $\operatorname{lcm}(z, n) = \frac{zn}{d} = z\frac{n}{d}$. By definition of $d$, $\frac{n}{d}$ is an integer that is *strictly* less than $n$ since $d \neq 1$. Thus,

$$\begin{aligned}[z][n/d] &= [zn/d] \\ &= [(z/d)n]\end{aligned}$$

   which is equal to zero since $z/d$ is an integer. Hence, if $z$ and $n$ are not coprime, $z$ is a zero divisor. Now suppose that $[z] \in \mathbb{Z}/n\mathbb{Z}$ is a zero divisor. Then there is a non-zero element $[b] \in \mathbb{Z}/n\mathbb{Z}$ such that $[bz] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$. Without loss of generality, we may assume $z, b \in \{1, \ldots, n-1\}$. Hence, $bz$ is a multiple of $n$, so $bz = kn$ for some integer $k$. But since $b < n$, $zb < zn$. Therefore, the least common multiple of $z$ and $n$ is less than $zn$. This implies that $b$ and $n$ are *not* relatively prime. Suppose that $[z] \in \mathbb{Z}/n\mathbb{Z}$ is a unit. Thus, there is an element $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that $[a][z] = [1]$, i.e., $az - 1$ is a multiple of $n$. Hence, $az - 1 = bn$ for some integer $b$. Equivalently, $az + bn = 1$ for some integers $a$ and $b$. This implies that $\gcd(z, n) = 1$ (since the smallest positive integer that can be written as a $\mathbb{Z}$-linear combination of two integers is their greatest common divisor). The other direction is similar.

3. Prove that if $R$ is an integral domain and the cardinality of $R$ is finite, then $R$ is a field. Suppose that $R$ is an integral domain of finite cardinality. Suppose that $y \in R \setminus \{0\}$, and enumerate the elements of $R$ as $\{x_1, \ldots, x_n\}$. Consider the set of elements $yR = \{yx_1, yx_2, \ldots, yx_n\}$. Note that $|yR| \leq |R|$ since $yR$ has at most $n$ distinct elements. Define a function $f : R \to yR$ via $f(x) = yx$. It is clear that $|yR| \leq |R|$ I claim first that $f$ is injective. Indeed, suppose that $f(x_i) = f(x_j)$ for some $i, j$. Then $yx_i = yx_j$. By the cancellation in integral domains proven in class, $x_i = x_j$. Therefore, $f$ is injective. This implies that $|R| \leq |yR|$. Hence, combined with the other inequality from above, we have $|yR| = |R|$. But $yR \subset R$ since $R$ is closed under multiplication. Since they are of equal and finite cardinality, $yR = R$. Therefore, $1 \in yR$, so $1 = yx_i$ for some $i$.

4. Let $R$ be an integral domain, and $a, b \in R$ be elements with $a \neq 0$. Prove that the equation $ax^2 = b$ has at most two solutions in $R$. Then find an example

of an integral domain $R$ and an equation $ax^2 = b$ that has no solutions, one that has exactly one solution, and one that has exactly two solutions. Suppose that $a, b \in R$ with $a \neq 0$, and suppose that $x \neq y \in R$ are two elements with $ax^2 = b$ and $ay^2 = b$. Then $ax^2 = ay^2$, so by cancellation in integral domains, $x^2 = y^2$. Subtracting $y^2$ from both sides and factoring yields

$$x^2 - y^2 = 0$$
$$(x - y)(x + y) = 0.$$

Since $R$ is an integral domain, this implies $x - y = 0$ or $x + y = 0$. Therefore, either $x = y$ (which contradicts the assumption) or $-x = y$. If $z$ is a third solution, then by the same reasoning $-x = z$ as well. But this implies $y = z$, so the only two possible solutions are $x$ and $-x$. $\star$ Note: This does not imply that there *are* two solutions. There could be none, and there could be one. Can you construct examples where this is the case? In $\mathbb{Z}/4\mathbb{Z}$, $x^2 = 1$ has exactly two solutions, $x^2 = 2$ has no solutions, in $\mathbb{Z}/2\mathbb{Z}$, $x^2 = 1$ has only one solution.

5. Let $\varphi : R \to R'$ be a ring homomorphism. Prove that $\ker \varphi$ is a subring with the additional *absorbtion* property. That is, if $x \in \ker \varphi$ and $r \in R$, then $rx \in \ker \varphi$ and $xr \in \ker \varphi$. Such a subring is called a *two-sided ideal* in $R$. Find all two-sided ideals in $\mathbb{Z}/60\mathbb{Z}$. Suppose that $x \in \ker \varphi$ and $r \in R$. Then $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0 = 0$, and similarly with the other order.

6. Consider the ring $\mathbb{Z}$ and a two-sided ideal $I \subset \mathbb{Z}$. Prove that $x, y \in I$ if and only if $\gcd(x, y) \in I$. Suppose that $x, y \in I$. Since $I$ is an ideal, by absorption, $ax, by$ are in $I$ for any $a, b \in \mathbb{Z}$. By closure under addition, $ax + by \in I$ for all $a, b \in \mathbb{Z}$ as well. In particular, $\gcd(x, y)$ is the smallest positive integer that can be written in the form $ax + by$, so $\gcd(x, y) \in I$. Now suppose that $d = \gcd(x, y) \in I$. Then $x = kd$ and $y = ld$ for some $k, l \in \mathbb{Z}$. Hence, by absorption, $x, y \in I$.

7. Let $F$ be a field and $a \in F$ be an arbitrary element. Define the function $\mathrm{ev}_a : F[x] \to F$ via $\mathrm{ev}_a(f) = f(a)$ (i.e., just replace $x$ with $a$ and evaluate).

   (a) Prove that $\mathrm{ev}_a$ is a ring homomorphism. First, $\mathrm{ev}_a(0) = 0$ since the evaluation at any point of the zero polynomial is zero. Now suppose that $f(x), g(x) \in F[x]$. Then $\mathrm{ev}_a(f + g) = (f + g)(a) = f(a) + g(a) = \mathrm{ev}_a(f) + \mathrm{ev}_a(g)$. Finally, $\mathrm{ev}_a(fg) = (fg)(a) = f(a)g(a) = \mathrm{ev}_a(f)\,\mathrm{ev}_a(g)$.

   (b) Compute the kernel of $\mathrm{ev}_a$ and prove your result. Suppose that $f \in \ker \mathrm{ev}_a$. Then $f(a) = 0$. We can apply the division algorithm, dividing $f(x)$ by $(x - a)$, which yields

   $$f(x) = (x - a)g(x) + r(x)$$

   where the degree of $r(x)$ is at most 1. Hence, $f(x) = (x - a)g(x) + c$.

From the above remarks,

$$\begin{aligned} f(a) &= (a-a)g(a) + c \\ 0 &= 0 + c \\ 0 &= c. \end{aligned}$$

Hence, $f(x) = (x-a)g(x)$. Therefore, $f(x) \in \ker \mathrm{ev}_a$ if and only if $f(x) = (x-a)g(x)$ for some polynomial $g(x)$.