1. *For each of the following rings R and subsets S thereof, determine whether S is a subring of R.*

   (a) *$R = \mathbb{Q}$; S is the set of all rational numbers whose denominators are not divisible by 3.*

   Here S is a subring of R because it is closed under addition, multiplication, and additive inverses. Considering $\frac{a}{b}$ and $\frac{c}{d}$ where b and c are not multiples of 3, we may note that $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, whose denominator is not divisible by 3; likewise $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$, which has the same denominator, and $-\frac{a}{b} = \frac{-a}{b}$, which again is in S since b is not divisible by 3.

   Addendum: note that the fact that 3 is prime is critical here; if we were to use, say, divisibility 6, there would be a real problem in that $\frac{1}{2}$ and $\frac{1}{3}$ would be in the putative ring while their product is not.

   (b) *R is the ring of all real 2×2 matrices; S is the set of all matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ for real numbers a and b.*

   Addition and additive inverses are clearly closed: $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} (a+c) & (b+d) \\ -(b+d) & (a+c) \end{bmatrix}$, and $-\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} -a & (-b) \\ -(-b) & -a \end{bmatrix}$. Multiplicative closure takes a bit more work: $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & ac-bd \end{bmatrix}$, which is of the right form to be an element of S.

2. *Prove the two following facts about ideal intersections.*

   (a) *If I and J are ideals of a commutative ring R, then $I \cap J$ is also an ideal of R.*

   We can show $I \cap J$ is a subring easily: associativity and distributivity are inherited directly from R, and we need only show this set contains 0, is closed under addition, multiplication, and additive inverses. Since $0 \in I$ and $0 \in J$, $0 \in I \cap J$. Likewise, if we consider $a, b \in I \cap J$, then $a, b \in I$ and $a, b \in J$, which respectively requires that $a + b, ab, -a \in I$ and $a + b, ab, -a \in J$. Thus $a + b$, ab, and $-a$ are in $I \cap J$.

   Absorption is proved similarly. Consider an $a \in I \cap J$ and $r \in R$; since $a \in I$, absorption of I tells us $ar \in I$; likewise since $a \in J$, $ar \in J$, so $ar \in I \cap J$, demonstrating absorption of $I \cap J$.

   (b) *If I and J are both* prime *ideals of a ring R, then $I \cap J$ is also a* prime *ideal of R (you may, of course, use the result from the previous part in this question).*

   Humiliatingly, this is false, and easily shown to be false: in $\mathbb{Z}$, $\langle 2 \rangle$ and $\langle 3 \rangle$ are prime, and their intersection $\langle 6 \rangle$ is not. My (very short) proof incorporated a common MATH 311-level flaw: I assumed that if either a or b was in I, and either a or b was in J, then either a or b was in $I \cap J$ — which is not, of course, the case.

3. *Let the homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{R}$ be defined by the mappings $\varphi(1) = 1$ and $\varphi(x) = 1 + \sqrt{2}$. Describe* $\ker \varphi$.

   This homomorphism essentially evaluates a polynomial at $1 + \sqrt{2}$. In order for an integer-valued polynomial to have $1 + \sqrt{2}$ as a root, it will also have $1 - \sqrt{2}$ as a root and be divisible by $(x - (1 + \sqrt{2}))(x - (1 - \sqrt{2})) = x^2 - 2x - 1$. In fact, the kernel is exactly $\langle x^2 - 2x - 1 \rangle$.

4. *For rings R and S, the direct product ring $R \oplus S$ consits of ordered pairs from $R \times S$, with termwise operations: $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ and $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$. Prove that if R and S both have at least 2 elements, then $R \oplus S$ is not an integral domain.*

   There is some nonzero $r \in R$ and $s \in S$; note that $(r, 0)(0, s) = (0, 0)$ so $R \oplus S$ has zero divisors and is thus not an integral domain.

5. *Let φ be a surjective homomorphism from $\mathbb{Z}$ to a field F. Prove that F is isomorphic to $\mathbb{Z}_p$ for some prime p.*

   Using the First Isomorphism Theorem, $F \cong \mathbb{Z}/\ker\varphi$. Since $\mathbb{Z}$ is a principal ideal domain, $\mathbb{Z}/\ker\varphi$ is thus isomorphic to either $\mathbb{Z}$ (if $\ker\varphi = \{0\}$) or $\mathbb{Z}_n$ for some natural number n (if $\ker\varphi = \langle n\rangle$). Since of these choices only $\mathbb{Z}_n$ with prime n is a field, it must be the case that $F \cong \mathbb{Z}_p$ for some prime p.