1. Prove that, for an integral domain $R$, the ring of polynomials $R[x]$ is an integral domain, and that the units in $R[x]$ are exactly the units in $R$.

Proof. Suppose contrariwise that $R[x]$ has nonzero zero divisors; let $f(x), g(x) \in R[x]$ thus be nonzero polynomials of degree $n$ and $m$ respectively such that $f(x)g(x) = 0$. Thus $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $g(x) = b_mx^m + \cdots + b_0$, where each $a_i, b_j \in R$. Then the coefficient of $x^{n+m}$ in $f(x)g(x)$ is $a_nb_m$; since $f(x)g(x) = 0$ as polynomials, each coefficient of $f(x)g(x)$ is zero, and specifically $a_nb_m = 0$. Since $R$ is an integral domain, either $a_n = 0$ or $b_m = 0$, contradicting the degree criteria for $f(x)$ or $g(x)$.

In addition, let us show that no nonconstant element of $R[x]$ can be a unit. Because $R$ is an integral domain, with $f(x)$ and $g(x)$ defined as above, $f(x)g(x)$ will have a nonzero coefficient for $x^{m+n}$, so the degree of a product is the sum of the degrees of the factors. Since 1 is a polynomial of degree zero, $f(x)g(x) = 1$ only if $f(x)$ and $g(x)$ are themselves polynomials of degree zero; i.e., constant polynomials. So in order for them to be inverses, $f(x)$ and $g(x)$ must be equal to some $a$ and $b$ respectively with $a, b \in R$, and $ab = 1$; which is to say, $f(x)$ is a unit if and only if it is equal to a degree-zero polynomial whose constant term is a unit. \hfill \Box

2. Prove that the ring $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ is a field, but that $\mathbb{Z}_3[x]/\langle x^3 + x + 1 \rangle$ is not a field.

Proof. The easiest way to prove this is to show that $\langle x^3 + x + 1 \rangle$ is a maximal ideal in $\mathbb{Z}_2[x]$ but not in $\mathbb{Z}_3$, and appeal to the known result that $R/I$ is a field iff $I$ is maximal in $R$.

For our former assertion, suppose $\langle x^3 + x + 1 \rangle \subseteq I \subseteq \mathbb{Z}_2[x]$. Thus, there must be at least one element of $I$ which is not in $\langle x^3 + x + 1 \rangle$, but $1 \notin I$, since any ideal containing 1 would contain all of $\mathbb{Z}_2[x]$. We shall show that no such $I$ can exist, and thus that $\langle x^3 + x + 1 \rangle$ is in fact maximal. Let $f(x)$ be an element of $I$ which is not a multiple of $\langle x^3 + x + 1 \rangle$ and which is of the least degree possible under that condition. We shall see by process of elimination below that $f(x)$ could only be a linear polynomial, an that neither of the linear polynomials are in fact possible additions to the ideal:

Case I: $f(x)$ has degree 0. Since $f(x)$ is a nonzero constant, then $f(x) = 1$ and then $I = \mathbb{Z}_2[x]$, contradicting its propriety as an ideal.

Case II: $f(x)$ has degree of 3 or more. Then $f(x)$ and $x^{\deg f-3}(x^3 + x + 1)$ are polynomials with the same leading term, so $f(x) - x^{\deg f-3}(x^3 + x + 1)$ will be an element of $I$ of lower degree, and since $f(x)$ was not a multiple of $x^3 + x + 1$, neither is $x^{\deg f-3}(x^3 + x + 1)$, contradicting our claim that $f(x)$ had the lowest degree possible.

Case III: $f(x)$ has degree 2. $f(x)$ will have leading term $x^2$, so that $x^3 + x + 1 - xf(x)$ is an element of $I$ of degree less than 3, and it will be nonzero, since its constant term is nonzero. If $x^3 + x + 1 - xf(x)$ has degree less than 2, that contradicts our assertion that $f(x)$ is the nonzero element of $I$ of least degree. If the degree of $x^3 + x + 1 - xf(x)$ is exactly 2, on the other hand, then $x^3 + x + 1 - xf(x) - x^2f(x) = x^3 + x + 1 - (x + 1)f(x)$ will itself be an element of $I$ of degree less than 2, since the leading terms of $x^2$ will cancel. Note that since $x^3 + x + 1 - (x + 1)f(x)$ evaluated at $x = 1$ is nonzero, it is a nonzero polynomial, and since it is of degree less than 3, it is not a multiple of $x^3 + x + 1$; thus, as a result of the $I$ of degree 1, it contradicts our assertion that $f(x)$ has the lowest degree possible.

Case IV: $f(x)$ has degree 1. There are exactly two possibilities: either $f(x) = x$ or $f(x) = x + 1$. If $f(x) = x$, then $x^3 + x + 1 - (x^2 + 1)f(x) = 1$, contradicting $f(x)$’s minimality. If $f(x) = x + 1$, then $x^3 + x + 1 - (x^2 + x)f(x) = 1$, again contradicting $f(x)$’s minimality.

Thus we see that no ideal can lie strictly in inclusion between $\langle x^3 + x + 1 \rangle$ and the whole ring in $\mathbb{Z}_2[x]$, so $\langle x^3 + x + 1 \rangle$ is maximal.
Given a ring homomorphism $\varphi : R \to R'$ on commutative rings, let $\varphi^{-1}(S) = \{ r \in R : \varphi(r) \in S \}$. Note that $\varphi^{-1}$ will map ideals to ideals.

(a) Prove that if $I'$ is a prime ideal of $R'$, then $\varphi^{-1}(I')$ is a prime ideal of $R$.

Proof. For brevity, let us define $I = \varphi^{-1}(I')$, and prove the contrapositive: that if $I$ is nonprime, then $I'$ is nonprime as well. From nonprimeness of $I$, there exist $a, b \in R - I$ such that $ab \in I$. Since $a, b \notin I$, it follows from the definition of $\varphi^{-1}$ that $\varphi(a)$ and $\varphi(b)$ are not in $I'$. Likewise, from the definition of $\varphi^{-1}$, since $ab \in \varphi^{-1}(I')$, $\varphi(ab) \in I'$. Since $\varphi(ab) = \varphi(a)\varphi(b)$, we can express this element of $I'$ as a product of two demonstrated non-elements of $I'$, so $I'$ is not prime. □

(b) Demonstrate that if $I'$ is a maximal ideal of $R'$, then $\varphi^{-1}(I')$ need not be a maximal ideal of $R$.

One straightforward possibility is that $\varphi^{-1}(I')$ may not be a proper ideal of $R$ at all; for instance, if $R = 7\mathbb{Z}$, $R' = \mathbb{Z}$, and $\varphi$ is the inclusion map, then $I' = \langle 7 \rangle$ is a maximal ideal whose pullback is the entirety of $R$, and thus not maximal because it is not proper. □

4. Prove that for ideals $I$ and $J$ of a commutative ring, and $IJ$ representing the set consisting of every product of terms from $I$ and $J$, it is the case that $IJ \subseteq I \cap J$. Under what circumstances will $IJ = I \cap J$?

Proof. For every $j \in J$, we know $Ij \subseteq I$ by the absorption property of ideals, so $IJ = \bigcup_{j \in J} Ij \subseteq I$. Likewise each $iJ \subseteq J$ so $IJ \subseteq J$. Then since $IJ$ is a subset of both $I$ and $J$, it is a subset of $I \cap J$. □

Clearly, if either $I$ or $J$ is the entire ring or trivial, then $IJ = I \cap J$. In general, however, if neither $I$ nor $J$ is trivial or the entire ring, $IJ$ will not necessarily equal $I \cap J$. Note that in $\mathbb{Z}$, for instance, $\langle a \rangle \langle b \rangle = \langle ab \rangle$, while in general $\langle a \rangle \cap \langle b \rangle = \langle \text{lcm}(a, b) \rangle$, and these expressions are only the same if $a$ and $b$ are relatively prime.

5. For any subset $A$ of a commutative ring $R$, the annihilator $\text{Ann}(A)$ of $A$ is the set of all $r \in R$ such that $ra = 0$ for all $a \in A$. Prove that $\text{Ann}(A)$ is always an ideal in $R$.

Proof. Let us show first $\text{Ann}(A)$ is a subring of $R$. Note that $0a = 0$ is always true, so $0 \in \text{Ann}(A)$. If $xa = 0$ and $ya = 0$ for every $a \in A$, it is also the case that $(x+y)a = xa + ya = 0 + 0 = 0$, $(-x)a = -(xa) = -0 = 0$, and $(xy)a = x(ya) = x0 = 0$, so $x + y$, $-x$, and $xy$ are also in $\text{Ann}(A)$, guaranteeing the closure and additive inverse properties.

Now we need simply show that $\text{Ann}(A)$ is absorbing, and that for any $r \in R$ and $x \in \text{Ann}(A)$, $rx \in \text{Ann}(A)$. This will be true because by definition $xa = 0$ for all $a \in A$, and so $(rx)a = r(xa) = r0 = 0$. □