1. Recall that in order to prove that given a chain of ideals $J \subset I \subset R$, there is an isomorphism $(R/I)/(J/I) \cong R/J$, we wanted to study the function

$$\varphi : R/I \to R/J$$
$$\varphi : r + I \mapsto r + J.$$

Prove that φ is a well-defined ring homomorphism with $\ker(\varphi) = J/I = \{j+I \mid j \in J\}$. [Well-defined] Suppose that $r_1 + I = r_2 + I$. Equivalently, $r_1 - r_2 \in I$. Then

$$\varphi(r_1 + I) = r_1 + J$$
$$\varphi(r_2 + I) = r_2 + J.$$

But $r_1 - r_2 \in I \subset J$, so $r_1 + J = r_2 + J$. Hence, $\varphi(r_1 + I) = \varphi(r_2 + I)$. [Homomorphism] Suppose that $r, s \in R$. Then

$$\begin{aligned} \varphi((r+I)+(s+I)) &= \varphi((r+s)+I) \qquad\qquad = r + s + J \\ &= (r+J)+(s+J) \\ &= \varphi(r+I)+\varphi(s+I). \end{aligned}$$

The multiplication is similar. [Kernel] We have $x + I \in \ker(\varphi)$ if and only if $\varphi(x + I) = x + J = 0 + J$, which holds if and only if $x \in J$. Thus, $\ker(\varphi) = \{x + I \mid x \in J\}$, which we denote J/I.

2. Describe all ideals in $\mathbb{Z}/n\mathbb{Z}$ for any positive integer n. Recall that in any ring R and for any ideal I, there is a bijection between ideals J containing I and ideals in R/I. Thus, the ideals in $\mathbb{Z}/n\mathbb{Z}$ are all associated with ideals $m\mathbb{Z}$ in $\mathbb{Z}$ that contain $n\mathbb{Z}$. But these are precisely the ideals $m\mathbb{Z}$ with $m \mid n$. Hence, for each $m \mid n$, there is an ideal $m\mathbb{Z}/n\mathbb{Z}$ consisting of all multiples of $[m]$ in $\mathbb{Z}/n\mathbb{Z}$.

3. Suppose that R is an ring. Prove that $R[x]$ is an integral domain if and only if R is an integral domain. First, R can be viewed as a subset of $R[x]$ by inclusion as the constant polynomials. Thus, if R is not an integral domain, $R[x]$ cannot be either. On the other hand, suppose that R is an integral domain. Define the function $\deg : R[x] \to \mathbb{Z}$ by taking the degree of a polynomial to be the largest power of x that occurs in a polynomial with non-zero coefficient. Note that the degree is multiplicative, since the highest power of x possibly occuring in $f(x)g(x)$ is $x^{\deg f + \deg g}$ and it occurs with non-zero coefficient since its coefficient is the product of the coefficients of $x^{\deg f}$ and $x^{\deg g}$ in f and g and R is an integral domain.

4. Suppose that F is a field. Prove the following:

   (a) If $f(x), g(x) \in F[x]$, then there exists polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$ where $\deg(r(x)) < deg(g(x))$. If $\deg f(x) < \deg g(x)$, then $q(x) = 0$ and $r(x) = f(x)$ work. Otherwise, suppose that $f(x) = \sum_{i=0}^{N} a_i x^i$ and $g(x) = \sum_{i=0}^{M} b_i x^i$ so that $a_N \neq 0$ and $b_M \neq 0$. Then

$$f(x) - \left(\frac{a_N}{b_M} x^{N-M}\right) g(x)$$

is a polynomial of degree $N-1$. If $N = M$, then take this resulting polynomial to be $r(x)$. So $f(x) = \left(\frac{a_N}{b_M} x^{N-M}\right) g(x) + r(x)$ and $\deg r(x) < M$. If $N > M$, then by induction $f(x) - \left(\frac{a_N}{b_M} x^{N-M}\right) g(x) = g(x)q(x) + r(x)$ for some polynomial $r(x)$ of degree less than M. Hence, $f(x) = g(x)\left[q(x) + \left(\frac{a_N}{b_M} x^{N-M}\right) x^{N-M}\right] + r(x)$ and $\deg r(x) < M$.

(b) Suppose that $f(x), g(x) \in F[x]$. Prove that if $f(x) = g(x)q(x) + r(x)$ where $q(x), r(x)$ are the polynomials guaranteed from above, then $\gcd(f(x), g(x)) = \gcd(g(x), r(x))$. [1] Suppose that $d(x) \mid f(x)$ and $d(x) \mid g(x)$. But $r(x) = f(x) - g(x)q(x)$, so $d(x)$ divides $r(x)$. Now suppose that $h(x)$ divides $g(x), r(x)$. Then clearly $h(x)$ dividies $f(x)$. Hence, the set of divisors of $f(x)$ and $g(x)$ is the set as the set of divisors of $g(x), r(x)$. Thus, their maximal elements are equal.

5. Suppose that R is a commutative local ring. I.e., a commutative ring with $1 \neq 0$ which has a unique maximal ideal, which we'll call $\mathfrak{m}$. Prove that $R^* = R \setminus \mathfrak{m}$. Suppose that $x \in R \setminus \mathfrak{m}$, and take (x) the ideal generated by x. Since $x \notin \mathfrak{m}$, $(x) \not\subset \mathfrak{m}$. But $\mathfrak{m}$ contains all proper ideals, so $(x) = R$. Thus, there is an element $y \in R$ such that $yx = 1$. Hence x is invertible. Now suppose that x is invertible. Then $x \notin \mathfrak{m}$ since otherwise $1 = x^{-1}x \in \mathfrak{m}$, implying $\mathfrak{m} = R$, but this is not the case.

6. Suppose that $\mathfrak{p}$ is an ideal in a commutative ring with identity $1 \neq 0$. Prove that $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is an integral domain. Suppose that p is a prime ideal, and let $x, y \in R$ such that $(x+p)(y+p) = 0 + p$ in R/p. Then $xy \in p$. By definition, then, either $x \in p$ or $y \in p$. Hence, $x + p = 0$ or $y + p = 0$. Now suppose that R/p is an integral domain, and $x, y \in R$ such that $xy \in p$. Then $(x+p)(y+p) = 0 + p$, and by assumption, one of the two must be zero. Hence, for example, $x + p = 0$ implies $x \in p$.

7. Suppose that $n, m \in \mathbb{Z}$, and consider the function

$$\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
$$\varphi : x \mapsto ([x]_n, [x]_m)$$

where $[x]_n$ indicates the equivalence class of x modulo n.

(a) Prove that φ is a ring homomorphism. Projection maps are homomorphisms and products of homomorphisms are homomorphisms.

[1] This can be iterated to prove that $\gcd(f(x), g(x))$ can be written as a linear combination of $f(x)$ and $g(x)$.

(b) Compute the kernel of φ and determine the cardinality of its image. Suppose $x \in \ker \varphi$. Then $[x]_n = 0$ and $[x]_m = 0$. Hence, x is a multiple of both n and m. Thus, $\ker \varphi = (\operatorname{lcm}(n, m))\mathbb{Z}$. Note that the cardinality of the image is, therefore, equal to the cardinality of $\mathbb{Z}/\operatorname{lcm}(n, m)\mathbb{Z}$, which is precisely $\operatorname{lcm}(n, m)$.

(c) What does this tell you in the case that $\gcd(n, m) = 1$. In this case, the cardinality of the image is nm, which is precisely the cardinality of the codomain. Hence, φ is onto, so $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as rings.