1. Let $R \neq 0$ be a commutative ring with 1 and let $S \subseteq R$ be the subset of nonzero elements which are not zero divisors.

   (a) Show that $S$ is multiplicatively closed.

   (b) By definition, the total ring of fractions of $R$ is the ring $\text{Frac}(R) := S^{-1}R$; it is a ring equipped with a canonical ring homomorphism $R \to S^{-1}R$. If $T$ is any multiplicatively closed subset of $R$ that is contained in $S$, show that there is a canonical injective ring homomorphism $T^{-1}R \to \text{Frac}(R)$, and conclude that $T^{-1}R$ is isomorphic to a subring of $\text{Frac}(R)$.

   (c) If $R$ is a domain, prove that $\text{Frac}(R)$ is a field and hence that $T^{-1}R$ is a domain for any $T$ as above.

2. Let $R$ be a commutative ring with 1.

   (a) Let $S \subseteq R$ be a multiplicatively closed subset. Prove that the prime ideals of $S^{-1}R$ are in bijective correspondence with the prime ideals of $R$ whose intersection with $S$ is empty.

   (b) If $p$ is an ideal of $R$, show that $S := R \setminus p$ is a multiplicatively closed subset if and only if $p$ is a prime ideal. Writing $R_p$ for the ring of fractions $S^{-1}R$, show that $R_p$ has a unique maximal ideal, and that this ideal is the image of $p$ under the canonical ring homomorphism $R \to R_p$. (In other words, the localization of $R$ at $p$ is a local ring).

   (c) Let $r \in R$ be arbitrary. Show that the following are equivalent:

      i. $r = 0$

      ii. The image of $r$ in $R_p$ is zero for all prime ideals $p$ of $R$.

      iii. The image of $r$ in $R_p$ is zero for all maximal ideals $p$ of $R$.

3. Do exercises 8–11 in §7.6 of Dummit and Foote (inductive and projective limits).

4. A Bézout domain is an integral domain in which every finitely generated ideal is principal.

   (a) Show that a Bézout domain is a PID if and only if it is noetherian.

   (b) Let $R$ be an integral domain. Prove that $R$ is a Bézout domain if and only if every pair of elements $a, b \in R$ has a GCD $d \in R$ that can be written as an $R$-linear combination of $a$ and $b$, i.e. such that there exist $x, y \in R$ with $d = ax + by$.

   (c) Prove that a ring $R$ is a PID if and only if it is a Bézout domain that is also a UFD.
(d) Let \( R \) be the quotient ring of the polynomial ring \( \mathbb{Q}[x_0, x_1, \ldots] \) over \( \mathbb{Q} \) in countably many variables by the ideal \( I \) generated by the set \( \{x_i - x_{i+1}^2\}_{i \geq 0} \). Show that \( R \) is a Bézout domain which is not a PID (Hint: have a look at Dummit and Foote, §9.2 #12).

Remark: The above example of a Bézout domain which is not a PID is somewhat artificial. More natural examples include the “ring of algebraic integers” (i.e. the set of all roots of monic irreducible polynomials in one variable over \( \mathbb{Z} \)) and the ring of holomorphic functions on the complex plane. The proofs that these are Bézout domains is, as far as I know, difficult. For example, in the case of the algebraic integers, one needs the theory of class groups).

5. Let \( R = \mathbb{Z}[i] := \mathbb{Z}[X]/(X^2 + 1) \) be the ring of Gaussian integers.

(a) Let \( N : R \to \mathbb{Z}_{\geq 0} \) be the field norm, that is

\[
N(a + bi) := (a + bi)(a - bi) = a^2 + b^2.
\]

Prove that \( R \) is a Euclidean domain with this norm. Hint: there is a proof in the book on pg. 272, but you should try to find a different proof by thinking geometrically.

(b) Show that \( N \) is multiplicative, i.e. \( N(xy) = N(x)N(y) \) and deduce that \( u \in R \) is a unit if and only if \( N(u) = 1 \). Conclude that \( R^\times \) is a cyclic group of order 4, with generator \( \pm i \).

(c) Let \( p \in \mathbb{Z} \) be a (positive) prime number. If \( p \equiv 3 \mod 4 \), show that \( p \) is prime in \( \mathbb{Z}[i] \) and that \( \mathbb{Z}[i]/(p) \) is a finite field of characteristic \( p \) which, as a vector space over \( \mathbb{F}_p \), has dimension 2.

If \( p = 2 \) or \( p \equiv 1 \mod 4 \), prove that \( p \) is not prime in \( \mathbb{Z}[i] \), but is the norm of a prime \( p \in \mathbb{Z}[i] \) with \( \mathbb{Z}[i]/(p) \) isomorphic to the finite field \( \mathbb{F}_p \). Conclude that \( p \in \mathbb{Z} \) can be written as the sum of two integer squares if and only if \( p = 2 \) or \( p \equiv 1 \mod 4 \).