Exercise 1. A subset \( S \subset R \) of a commutative ring is **multiplicatively closed** if \( 1 \in S \) and \( s, t \in S \) implies \( st \in S \). Define a relation on the set of pairs \((a, s) \in R \times S\) by
\[
(a, s) \sim (a', s') \iff \exists t \in S. t(s'a - sa') = 0.
\]
(i) Prove that this is an equivalence relation.
(ii) Write \( \frac{a}{s} \) for the equivalence class of \((a, s)\). Define addition and multiplication of “fractions” and verify that these operations are well-defined.
Essentially you’ve verified that the set \( S^{-1}R \) of fractions is a ring under these operations with a canonical ring homomorphism \( \ell : R \to S^{-1}R \) defined by \( a \mapsto \frac{a}{1} \).

Note that \( S^{-1}R = 0 \) iff \( 0 \in S \).
(iii) Prove that \( \ell(s) \) is invertible for every \( s \in S \).
(iv) Prove that \( R \to S^{-1}R \) is initial among ring homomorphisms \( R \to T \) that send every element of \( S \) to a unit in \( T \).
(v) Prove that \( S^{-1}R \) is an integral domain if \( R \) is an integral domain.

Exercise 2. Let \( S \subset R \) as in Exercise 1. For every \( R \)-module \( M \) define a relation \( \sim \) on pairs \((m, s) \in M \times S\) by
\[
(m, s) \sim (m', s') \iff \exists t \in S. t(s'm - sm') = 0.
\]
(i) Prove that the set \( S^{-1}M \) of equivalence classes is an \( S^{-1}R \) module in a way compatible with the action of \( R \) on \( M \): explicitly, the \( S^{-1}R \)-action on \( S^{-1}M \) restricts along \( \ell : R \to S^{-1}R \) to define an \( R \)-module structure on \( S^{-1}M \) and \( M \) should be a submodule of this represented by those fractions of the form \( \frac{m}{1} \).
(ii) Verify the following universal property of \( S^{-1}M \): for any \( S^{-1}R \)-module \( N \) there is a bijection
\[
\hom_{\text{Mod}_{S^{-1}R}}(S^{-1}M, N) \cong \hom_{\text{Mod}_R}(M, N)
\]
where the \( N \) on the right is the \( R \)-module obtained by restriction of scalars along \( \ell : R \to S^{-1}R \).

Exercise 3. Let \( R \) be commutative and let \( p \subset R \) be a prime ideal.
(i) Prove that \( S = R \setminus p \) is multiplicatively closed. The localizations \( S^{-1}R \) and \( S^{-1}M \), for \( M \) an \( R \)-module, are then denoted by \( R_p \) and \( M_p \).
(ii) Prove that there is an inclusion preserving bijection between prime ideals of \( R_p \) and prime ideas of \( R \) contained in \( p \). Deduce that \( R_p \) is a **local ring**, i.e., has a single maximal ideal.

Exercise 4. Let \( R \) be a commutative ring and let \( M \) be an \( R \)-module. Prove the following are equivalent:
(i) \( M = 0 \)

---

1Problems labelled \( n^* \) are optional (fun!) challenge exercises that will not be graded.
2This \( S^{-1}R \) module was denoted by \( S^{-1}R \otimes_R M \) in class.
(ii) $M_p = 0$ for every prime ideal $p$
(iii) $M_m = 0$ for every maximal ideal $m$

[Hint: the annihilator of a non-zero element $m$ defines a proper ideal $\{ r \mid rm = 0 \}$, which is therefore contained in some maximal ideal.]

**Exercise 5.** Let $n \in \mathbb{Z}$ be a positive integer with prime factorization $n = p_1^{a_1} \cdots p_r^{a_r}$.

(i) Define a canonical isomorphism of abelian groups
$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{a_1} \times \cdots \times \mathbb{Z}/p_r^{a_r}. $$

(ii) Use Sunzi’s remainder theorem to prove that in fact this is a ring isomorphism.

(iii) Prove that
$$(\mathbb{Z}/n)\times \cong (\mathbb{Z}/p_1^{a_1})\times \times \cdots \times (\mathbb{Z}/p_r^{a_r})\times.$$

(iv) **Euler’s $\phi$-function** $\phi(n)$ counts the number of positive integers less than or equal to $n$ that are relatively prime to $n$. Prove that
$$\phi(n) = p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1). $$

**Exercise 6*.** Prove Fermat’s last theorem for polynomials: the equation
$$f^n + g^n = h^n$$
has no solutions in $\mathbb{C}[t]$ for $n > 2$ and $f, g, h$ not all constant.\(^3\)

---

\(^3\)Hints can be found in Aluffi V.4.25, who also notes that similar arguments work in any UFD. In particular, if $\mathbb{Z}[\xi_n]$, where $\xi_n$ is an $n$th root of unity were a UFD, then the full-fledged Fermat’s last theorem could be proven along these lines, as mistakenly claimed by G. Lamé.