1. ★ Let $R$ be a commutative ring with unity. Prove the following statements.

   (a) An element $u \in R$ is a unit if and only if $(u) = R$.
   (b) Elements $a$ and $b$ are associates if and only if $(a) = (b)$.
   (c) If $a$ and $b$ are elements of $R$, then $a|b$ if and only if $(a) \supset (b)$ with strict containment if and only if $a$ properly divides $b$.

2. ★ Let $r$ be an element of a PID $R$. Prove that $r$ is irreducible if and only if $r$ is prime.

3. Prove that if $R$ is a PID with nonzero element $p$, then $R/(p)$ is a field if and only if $p$ is irreducible in $R$.

4. ★ Let $F$ be a field, $a \in F$, and $f(x) \in F[x]$. Prove that $a$ is a root of $f(x)$ if and only if $x - a$ is a factor of $f(x)$. (Hint: Use Euclidian Division Algorithm.)

5. Prove that the following rings are not unique factorization domains. In each case, give at least two distinct factorizations of some nonzero nonunit.

   (a) $\mathbb{Q}[x^2, x^3]$
   (b) $\mathbb{Z}[\sqrt{-n}]$ where $n$ is a squarefree integer greater than 3.
      (Hint: First show that 2, $\sqrt{-n}$ and $1 + \sqrt{-n}$ are irreducible in $R$.)

6. ★ Prove that the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$, of Gaussian integers is a Euclidian domain and hence a UFD. Explain why the identities $5 = (2 + 1)(2 - i)$ and $2 \cdot 3 = 6 = (1 + i)(1 - i) \cdot 3$ do not violate unique factorization. (Hint: Consider the ‘usual’ complex norm $N(a + bi) = a^2 + b^2$ on $\mathbb{Z}[i]$ and the fact that it is multiplicative; i.e., $N(\alpha \beta) = N(\alpha)N(\beta)$. Given $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, write $\frac{\alpha}{\beta} = r + si$ in $\mathbb{Q}(i)$ (the quotient field of $\mathbb{Z}[i]$, cf. 9) and find integers $p$ and $q$ sufficiently close to $r$ and $s$ respectively so that you can apply the division algorithm in $\mathbb{Z}$.)

7. Generalize the statements and proofs of Lemma 17 through Theorem 22 to $R$ a UFD and $F$ its quotient field. Prove Theorem 24.

8. (Mod $p$ Irreducibility Test) Let $f \in \mathbb{Z}[x]$ such that a prime $p$ does not divide the leading coefficient of $f$. Prove that if $\overline{f}$, the polynomial $f$ with coefficients reduced modulo $p$, is irreducible in $\mathbb{Z}_p[x]$, then $f$ is irreducible in $\mathbb{Z}[x]$. (Hint: reduce to primitive polynomials.) Use this fact to prove that $x^4 - 6x^3 + 12x^2 - 3x + 9$ is irreducible in $\mathbb{Z}[x]$.
9. ★ In this sequence of exercises, you will develop the quotient field of an integral domain, analogous to the field of rational numbers which contains the ring of integers.

(a) Let $R$ be an integral domain and define a fraction to be a symbol $a/b$ with $a, b \in R$ and $b \neq 0$. Let $S$ denote the set of all fractions of elements in $R$. We define a relation $\approx$ on the set $S$ of symbols as follows: $a/b \approx c/d$ if and only if $ad = bc$ in $R$. Prove that $\approx$ is an equivalence relation on $S$.

(b) Define $F = S/\approx$ to be the set of equivalence classes of fractions. That is, we consider two fractions to be equal in $F$ if they are equivalent in $S$. Define multiplication and addition of fractions in the obvious ways: $(a/b)(c/d) = (ac)/(bd)$, $a/b + c/d = (ad + bc)/(bd)$. Prove that these are well-defined operations on $F$; i.e., verify that these rules lead to equivalent answers if the fractions $a/b$ and $c/d$ are each replaced by equivalent fractions.

(c) Prove that $F$ is a field (that contains $R$) by proving the following items.
   - Prove that $F$ is an abelian group with respect to addition.
   - Prove that multiplication in $F$ is commutative and associative and that it distributes across addition.
   - Prove that $F$ has a multiplicative identity and that every nonzero element has a multiplicative inverse.

(d) Finally, prove that $F$ is unique up to isomorphism. In other words, prove that if $\phi : R \to K$ is an injective ring homomorphism such that $K$ is a field, then the function $\Phi(a/b) = \phi(a)/\phi(b)^{-1}$ defines a unique extension of $\phi$ to a ring homomorphism $\Phi : F \to K$.

10. ★ Let $D$ be an integral domain with quotient field $K$. Let $f, g \in K[x]$, and $a \in D$. If $fD[x] \subseteq gD[x]$, then $f(a)D \subseteq g(a)D$.

Supplemental Reading and Exercises

- Read Chapter 3 (pages 36–38 and pages 41 (the last third)–43 of M. F. Atiyah and I. G. MacDonald Introduction to Commutative Algebra.
- Work exercises # 3 and # 9.