1. **Prime vs Irreducible Elements.** Let \( R \) be a domain, and let \( f \in R \) be a non-zero, non-unit.

1. Prove that if \( f \) is prime, then \( f \) is irreducible.
2. Prove that \( f \) is prime if and only if the ideal generated by \( f \) is a prime ideal.
3. Show that in any ring, every maximal ideal is prime. [Hint: Use ideas from Homework Set 3.]
4. Show that in a principal ideal domain, every prime ideal is maximal.
5. Show that in a principal ideal domain, every irreducible element is prime.
6. Prove Proposition 2.8 in Chapter 11. [Note: this completes the proof that every PID is a UFD; run over the outline of the argument to make sure you understand; I won’t make you write it down since it is in the text and we did it in class.]

2. **A non-UFD.** Let \( \mathbb{Z}[\sqrt{D}] \) be the subring of the quadratic field \( \mathbb{Q}[\sqrt{D}] \) (defined on Homework Set 1) consisting of elements of the form \( a + b\sqrt{D} \) where \( a, b \in \mathbb{Z} \).

1. Show that \( a + b\sqrt{D} \) is a unit in \( \mathbb{Z}[\sqrt{D}] \) if and only if its quadratic norm \( a^2 - Db^2 \) is a unit in \( \mathbb{Z} \).
2. Prove that in \( \mathbb{Z}[\sqrt{-5}] \), the element 3 is irreducible but not prime. [Hint: Use the quadratic norm.]
3. Find two essentially different factorizations of 9 into irreducibles.

3. **Another non-UFD.** Let \( R \) be the quotient ring of \( \mathbb{R}[X, Y, Z] \) by the principal ideal \( (Z^2 - XY) \). Let \( x, y, z \) denote the classes of \( X, Y, Z \) respectively, in the quotient ring.

1. Show that the units of \( R \) are the (classes of) non-zero constant polynomials. [Hint: Reinterpret in the polynomial ring, and think about the degrees of polynomials in \( \mathbb{R}[X, Y, Z] \).]
2. Show that the elements \( x, y \) and \( z \) are all irreducible elements of \( R \). [Hint: same as (1).]
3. Show that \( R \) is not a UFD.

4. **Noetherian Rings.** A ring \( R \) is Noetherian if every properly ascending chain of ideals

\[
I_1 \subset I_2 \subset I_3 \subset \ldots
\]

eventually terminates. Prove that \( R \) is Noetherian if and only if every ideal is finitely generated.

5. **Gaussian Integers.**

1. Show that the ring \( \mathbb{Z}[i] \) of Gaussian integers is a Euclidean domain, where the “size function” is the square of the usual absolute value in \( \mathbb{C} \). Conclude that \( \mathbb{Z}[i] \) is a UFD.
2. Let \( p \in \mathbb{Z} \) be a prime integer. Show that \( p \) is irreducible as an element of \( \mathbb{Z}[i] \) if and only if the polynomial \( x^2 + 1 \) is irreducible in \( \mathbb{F}_p[x] \). [Hint: If you fully understand the Third Isomorphism Theorem, this is not hard. Alternatively, you can read Artin, Chapter 11 Section 5, for more helpful discussion of the third isomorphism theorem in the context of the Gaussian Integers.]
3. Factor 30 uniquely into irreducible (=prime) elements of \( \mathbb{Z}[i] \).

\(^1\)and make use of previously proven facts from this and other homework sets
6. Fermat’s Theorem on the Sum of squares.

(1) Prove that the equation $x^2 + 1$ has a solution in $\mathbb{Z}_p$ (where $p$ is prime) if and only if $p = 2$ or $p$ is congruent to 1 mod 4. [Hint: For odd $p$, show that $\bar{n}$ is a solution if and only if $n$ has order 4 in the group of units $\mathbb{Z}_p^\times$; invoke a (hard) theorem from 512 about the structure of this group.]

(2) (Fermat) Prove that a prime number $p$ can be written in the form $p = a^2 + b^2$ for integers $a$ and $b$ if and only if $p = 2$ or $p$ is congruent to 1 mod 4. Prove also that in this case, the integers $a$ and $b$ are unique, up to sign. [Hint: Use the Gaussian integers.]

From Artin: Chapter 11: 1.5, 1.9, 2.7, 2.10