1. Throughout this problem, \( \mathbb{F}_2 \) denotes the finite field with 2 elements.

   (i) Let \( \mathbb{F}_2(\alpha) \) be a simple extension of \( \mathbb{F}_2 \), generated by an element \( \alpha \) such that \( \alpha^2 + \alpha + 1 = 0 \), i.e. \( \alpha \) is a root of the polynomial \( x^2 + x + 1 \). What is \( \mathbb{F}_2(\alpha) : \mathbb{F}_2 \)? Show that \( \alpha^2 = \alpha + 1 \) is also a root of \( x^2 + x + 1 \), and hence \( x^2 + x + 1 \) factors into linear factors in \( \mathbb{F}_2(\alpha)[x] \).

   (ii) Let \( \mathbb{F}_2(\beta) \) be a simple extension of \( \mathbb{F}_2 \), generated by an element \( \beta \) such that \( \beta^3 + \beta + 1 = 0 \), i.e. \( \beta \) is a root of the polynomial \( x^3 + x + 1 \). What is \( \mathbb{F}_2(\beta) : \mathbb{F}_2 \)? How many elements does \( \mathbb{F}_2(\beta) \) have? Show (without any computation) that \( \beta^2 \) and \( \beta^4 \) are also roots of \( x^3 + x + 1 \). (Hint: apply the Frobenius homomorphism to the relation \( \beta^3 + \beta + 1 = 0 \).) Express \( \beta^4 \) as an element of the form \( a_0 + a_1 \beta + a_2 \beta^2 \), with \( a_i = 0 \) or 1, and verify directly that \( x^3 + x + 1 \) factors into linear factors in \( \mathbb{F}_2(\beta)[x] \).

   (iii) Let \( \beta \) be as in (ii). Since \( x^3 + x^2 + 1 \) is irreducible over \( \mathbb{F}_2 \), argue that there is a root of \( x^3 + x^2 + 1 \) in \( \mathbb{F}_2(\beta) \). In fact, simply by counting, every element of \( \mathbb{F}_2(\beta) \) either lies in \( \mathbb{F}_2 \) or is a root of \( x^3 + x + 1 \) or of \( x^3 + x^2 + 1 \), in other words its irreducible polynomial is of degree one or three. How do you know this without any computation, in particular how do you know that there is no element of \( \mathbb{F}_2(\beta) \) which satisfies an irreducible quadratic polynomial over \( \mathbb{F}_2 \)? Conclude that, in \( \mathbb{F}_2[x] \),

\[
x^8 - x = x^8 + x = x(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).
\]

2. Let \( \mathbb{F}_3 \) denote the finite field with 3 elements.

   (i) Show that \( x^2 + 1 \), \( x^2 + x + 2 \), and \( x^2 + 2x + 2 \) are exactly the three monic irreducible polynomials of degree two in \( \mathbb{F}_3[x] \). (Note that this agrees with the formula \( \sum_{d \mid n} dN_p(d) = p^n \), where \( N_p(d) \) is the number of monic irreducible polynomials of degree \( d \) in \( \mathbb{F}_p[x] \), for the case \( p = 3 \), \( n = 2 \).)

   (ii) If \( \alpha \) is a root of \( x^2 + 1 \), show that \( x^2 + x + 2 \) and \( x^2 + 2x + 2 \) also factor into products of two linear polynomials in \( \mathbb{F}_3(\alpha)[x] \).

   (iii) Explain why, without directly computing the product, we know that, in \( \mathbb{F}_3[x] \),

\[
x^9 - x = x(x - 1)(x - 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2).
\]
3. Let \( R \) be a ring. Show that the relation \( \sim \) on \( R \) defined by \( r \sim s \iff \text{there exists a unit } u \in R^* \text{ such that } r = us \) is an equivalence relation.

4. Let \( R \) be a PID. Assume that \( R \) is not a field (in other words, the ideal \((0)\) is not a maximal ideal). Let \( I \) be an ideal in \( R \). Arguing as we did for the polynomial ring \( F[x] \), show that the following are equivalent:
   (i) \( I \) is a maximal ideal.
   (ii) \( I \) is a prime ideal and \( I \neq (0) \).
   (iii) \( I = (r) \), where \( r \) is irreducible.

5. Factor the following into irreducibles in \( \mathbb{Z}[i] \): (a) \( 3 + 4i \); (b) \( 3 + 5i \). In your factorizations, identify which factors are associates.

6. Let \( R = \mathbb{Z}[\sqrt{-2}] \) and let \( N(\alpha) = \overline{\alpha} \alpha = |\alpha|^2 \), where \( \overline{\alpha} \) denotes complex conjugation. Thus \( n + m\sqrt{-2} = n - m\sqrt{-2} \) and \( N(n + m\sqrt{-2}) = n^2 + 2m^2 \). By adapting the argument given in class for \( \mathbb{Z}[i] \), show that \( N \) is a Euclidean norm on \( R - \{0\} \) and hence that \( R \) is a Euclidean domain, a PID, and a UFD.

7. In the ring \( \mathbb{Z}[^{\sqrt{-3}}] \), let \( N: \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z} \) be the multiplicative function \( N(\alpha) = \overline{\alpha} \alpha = |\alpha|^2 \), so that \( N(a + b\sqrt{-3}) = a^2 + 3b^2 \). You may use the facts (proved in the same way as for \( \mathbb{Z}[i] \)) that \( N \) is multiplicative (\( N(\alpha \beta) = N(\alpha)N(\beta) \) for all \( \alpha, \beta \in \mathbb{Z}[\sqrt{-3}] \)) and that \( \alpha \) is a unit in \( \mathbb{Z}[\sqrt{-3}] \iff N(\alpha) = 1 \iff \alpha = \pm 1 \).
   (i) Show that there is no \( \alpha \in \mathbb{Z}[\sqrt{-3}] \) with \( N(\alpha) = 2 \).
   (ii) Show that the elements \( 2 \) and \( 1 \pm \sqrt{-3} \) are irreducible. (If say \( 2 = \alpha \beta \), then \( 4 = N(2) = N(\alpha)N(\beta) \), and thus one of \( N(\alpha), N(\beta) \) is equal to 1.)
   (iii) Show that \( 4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}) \) are two essentially different factorizations of the element \( 4 \) in \( \mathbb{Z}[\sqrt{-3}] \) into irreducibles. Thus \( \mathbb{Z}[\sqrt{-3}] \) is not a UFD or a PID.

Arguing similarly, show that \( \mathbb{Z}[\sqrt{-5}] \) is not a UFD and hence not a PID, by showing that \( 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \) gives two essentially different factorizations of the element \( 6 \) in \( \mathbb{Z}[\sqrt{-5}] \).