1. Find all irreducible polynomials of degree at most 3 in \( \mathbb{Z}_2[x] \).

All linear polynomials are irreducible, which in this case are \( x, x+1 \). We have \( x \cdot x = x^2, (x+1)(x+1) = x^2 + 1, x(x+1) = x^2 + x; \) these are reducible. Hence the only irreducible degree-2 polynomial is \( x^2 + x + 1 \). We have \( x^3 = x \cdot x^2, x^3 + 1 = (x^2 + x + 1)(x + 1), x^3 + x = x(x + 1)^2, x^3 + x^2 = x^2(x + 1), x^3 + x^2 + x = x(x^2 + x + 1), x^3 + x^2 + x + 1 = (x + 1)^3 \). This leaves two irreducible degree-3 polynomials: \( x^3 + x^2 + 1, x^3 + x + 1 \).

2. Express \( x^4 - 4 \) as a product of irreducibles in \( \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}_3[x] \).

\( \mathbb{Q}[x] \): \( (x^2 - 2)(x^2 + 2) \), where each is irreducible because each is degree 2 and neither has a root in \( \mathbb{Q} \).

\( \mathbb{R}[x] \): \( (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2) \), where \( x^2 + 2 \) is irreducible since it has no root in \( \mathbb{R} \).

\( \mathbb{C}[x] \): \( (x - \sqrt{2}i)(x + \sqrt{2}i)(x + \sqrt{2}i)(x - \sqrt{2}i) \). Finally the polynomial splits.

\( \mathbb{Z}_3[x] \): Write \( x^4 - 4 = x^4 - 1 = (x + 1)(x - 1)(x^2 + 1) \), where \( x^2 + 1 \) is irreducible since it is degree 2 and has no root in \( \mathbb{Z}_3 \).

3. Prove that \( x^3 - 2 \) is irreducible in \( \mathbb{Z}_7[x] \).

Note that, in \( \mathbb{Z}_7 \), \( 0^3 = 0, 1^3 = 1, 2^3 = 1, 3^3 = 6, 4^3 = 1, 5^3 = 6, 6^3 = 6 \). Since none of these are 2, \( x^3 - 2 \) has no root; since it is of degree 3 it is therefore irreducible in \( \mathbb{Z}_7[x] \).

4. Find all roots of \( x^2 + 11 \) in \( \mathbb{Z}_{12}[x] \).

Note that, in \( \mathbb{Z}_{12} \), \( 0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 4, 5^2 = 1, 6^2 = 0, 7^2 = 1, 8^2 = 4, 9^2 = 9, 10^2 = 4, 11^2 = 1 \). Hence this degree-2 polynomial has FOUR roots: 1, 5, 7, 11. This can happen when your coefficients are drawn from a ring (not a field).

5. Express \( x^{11} - x \) as a product of irreducibles in \( \mathbb{Z}_{11}[x] \). Hint: FLT.

By Fermat’s Little Theorem, since 11 is prime, for all \( x \): \( x^{11} \equiv x \pmod{11} \). Hence this polynomial splits, i.e. has all linear factors. We have \( x^{11} - x = x(x - 1)(x - 2)(x - 3)(x - 4)(x - 5)(x - 6)(x - 7)(x - 8)(x - 9)(x - 10) \).

Note: this same method can be used to prove Wilson’s theorem. Look at the coefficient of \( x \) on both sides; on the left it is \( -1 \), while on the right it is \( ( -1)( -2) \cdots ( -10) = ( -1)^{10}10! = 10! \). Hence \( 10! \equiv -1 \pmod{11} \).

6. Suppose \( F \subseteq K \) are both fields. Let \( f \in F[x] \subseteq K[x] \). Suppose that \( f \) is irreducible in \( K[x] \). Prove that \( f \) is also irreducible in \( F[x] \).

Suppose, by way of contradiction, that \( f \) is reducible in \( F[x] \). Then we may write \( f = gh \), where \( g, h \in F[x] \) are nonconstant polynomials. Since \( F \subseteq K \), also \( F[x] \subseteq K[x] \) so \( g, h \in K[x] \) and now \( f \) is reducible in \( K[x] \), a contradiction.

7. Suppose \( p(x) \) is irreducible in \( F[x] \), and \( a \in F \) is nonzero. Prove that \( ap(x) \) is also irreducible.

Suppose, by way of contradiction, that \( ap(x) \) is reducible in \( F[x] \). Then we may write \( ap(x) = g(x)h(x) \), where \( g, h \in F[x] \) are nonconstant polynomials. Since \( F \) is a field and
a is nonzero, there is some \( b \in F \) with \( ab = 1 \). Hence \( bap(x) = bg(x)h(x) \), and thus \( p(x) = (bg(x))h(x) \). Now, the leading coefficient of \( bg(x) \) has the same degree as the leading coefficient of \( g(x) \), since \( b \) is nonzero and \( F \) is an integral domain. Thus \( bg(x) \) and \( h(x) \) are both nonconstant polynomials whose product is \( p(x) \). Thus \( p(x) \) is reducible, a contradiction.

8. Let \( f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in F[x] \). Define \( \bar{f}(x) = a_n + a_{n-1}x + \cdots + a_1x^{n-1} + a_0x^n \in F[x] \). Suppose that \( c \neq 0 \) is a zero of \( f(x) \). Prove that \( c^{-1} \) is a zero of \( \bar{f}(x) \).

Since \( c \) is a zero of \( f(x) \), we have \( 0 = f(c) = a_0 + a_1c + \cdots + a_{n-1}c^{n-1} + a_nc^n \). Multiply both sides by \((c^{-1})^n\) to get \( 0 = a_0(c^{-1})^n + a_1c(c^{-1})^n + \cdots + a_{n-1}c^{n-1}(c^{-1})^n + a_nc^n(c^{-1})^n = a_0(c^{-1})^n + a_1(c^{-1})^{n-1} + \cdots + a_{n-1}(c^{-1}) + a_n = \bar{f}(c^{-1}) \).

9. Let \( a \in F \) and define \( \phi_a : F[x] \to F \) via \( \phi_a : f(x) \mapsto f(a) \). Prove that \( \phi_a \) is a surjective (ring) homomorphism.

We first prove \( \phi_a \) is a homomorphism. \( \phi_a(f + g) = (f + g)(a) = f(a) + g(a) = \phi_a(f) + \phi_a(g) \), and \( \phi_a(fg) = (fg)(a) = f(a)g(a) = \phi_a(f)\phi_a(g) \). To prove \( \phi_a \) surjective, let \( c \in F \). Take \( f(x) = c \), the constant polynomial. We have \( \phi_a(f) = c \).

10. Define \( \mathbb{Q}[^2] = \{ r_0 + r_1\sqrt{2} + r_2(\sqrt{2})^2 + \cdots + r_n(\sqrt{2})^n : n \geq 0, r_i \in \mathbb{Q} \} \). Note that this definition differs from our previous one for \( \mathbb{Q}[^2] \) (although they can be proved equivalent). Consider the function \( \phi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}] \) via \( \phi : f(x) \mapsto f(\sqrt{2}) \). Prove that \( \phi \) is a (ring) homomorphism, is surjective, and is not injective.

Let \( f(x) = \sum_{n \geq 0} a_nx^n, g(x) = \sum_{n \geq 0} b_nx^n \) be arbitrary polynomials in \( \mathbb{Q}[x] \), both finite sums. We have \( \phi(f + g) = \phi(\sum_{n \geq 0}(a_n + b_n)x^n) = \sum_{n \geq 0}(a_n + b_n)\sqrt{2}^n = \sum_{n \geq 0}a_n\sqrt{2}^n + \sum_{n \geq 0}b_n\sqrt{2}^n = \phi(f) + \phi(g) \). Setting \( \epsilon_n = \sum_{i=0}^n a_ib_{n-i} \), we have \( \phi(fg) = \phi(\sum_{n \geq 0} \epsilon_nx^n) = \sum_{n \geq 0} \epsilon_n\sqrt{2}^n = \left( \sum_{n \geq 0} a_n\sqrt{2}^n \right) \left( \sum_{n \geq 0} b_n\sqrt{2}^n \right) = \phi(f)\phi(g) \). Hence \( \phi \) is a homomorphism.

Given an arbitrary \( r = \sum_{n \geq 0} r_n\sqrt{2}^n \in \mathbb{Q}[^2] \), we set \( f(x) = \sum_{n \geq 0} r_nx^n \) (taking \( r_i = 0 \) for \( i > n \)), and have \( \phi(f) = r \). Hence \( \phi \) is surjective.

Lastly, we note that \( \phi(2) = \phi(x^2) = 2 \), so \( \phi \) is not injective.