1. Prove that the following polynomials are irreducible:

(a) \( x^n - 12 \in \mathbb{Q}[x] \) if \( n \geq 2 \).

   It suffices to show \( x^n - 12 \) is irreducible in \( \mathbb{Z}[x] \) by Gauss’s lemma. \( 3 \mid 12 \) and \( 3^2 = 9 \nmid 12 \) so the conclusion follows by Eisenstein Criterion applied for the prime 3.

(b) \( x^3 - 3x^2 + 3x + 4 \in \mathbb{Q}[x] \).

   Since a polynomial of degree two or three over a field \( F \) is reducible iff it has a root in \( F \), it is enough to show the above polynomial \( f(x) \) has no roots in \( \mathbb{Q} \). By rational root theorem, if it has a root \( r/s \), then \( s \mid 1 \) and \( r \mid 4 \). Since \( f(r) \neq 0 \) for \( r = \pm 1, \pm 2, \pm 4 \), it has no rational roots.

(c) \( x^5 - 10x^3 + 25x^2 - 51x + 2017 \in \mathbb{Q}[x] \).

   It suffices to show the above polynomial is irreducible in \( \mathbb{Z}[x] \) by Gauss’s lemma. Reduce modulo 5, \( x^5 - x^2 \in \mathbb{Z}/5\mathbb{Z}[x] \) is irreducible. Hence the original polynomial is irreducible in \( \mathbb{Z}[x] \).

(d) \( x^4 + 3x^2 + 27x - 12 \in \mathbb{Q}[x] \).

   It suffices to show the above polynomial is irreducible in \( \mathbb{Z}[x] \) by Gauss’s lemma. 3 divides all the coefficients except the leading coefficient and \( 3^2 = 9 \nmid 12 \), so the conclusion follows by Eisenstein Criterion applied for the prime 3.

(e) \( x^5 - x + 1 \in \mathbb{Z}/3\mathbb{Z}[x] \).

   \( 0^5 - 0 + 1 = 1 \), \( 1^5 - 1 + 1 = 1 \), and \( 2^5 - 2 + 1 = 1 \) so \( x^5 - x + 1 \) has no roots in \( \mathbb{Z}/3\mathbb{Z} \). If it were reducible, it must have a factor of a monic polynomial of degree 2 because it can not have linear factors, which give rise to roots. Since the only monic polynomial of degree 2 in \( \mathbb{Z}/3\mathbb{Z}[x] \) that do not have a root in \( \mathbb{Z}/3\mathbb{Z} \) are \( x^2 + 1 \), \( x^2 + x - 1 \), and \( x^2 - x - 1 \) and by long division none of these divide \( x^5 - x + 1 \), \( x^5 - x + 1 \) is irreducible in \( \mathbb{Z}/3\mathbb{Z}[x] \).

(f) \( x^5 + 2x + 4 \in \mathbb{Q}[x] \).

   It suffices to show the above polynomial is irreducible in \( \mathbb{Z}[x] \) by Gauss’s lemma. Reduce modulo 3, \( x^5 + 2x + 1 = x^5 - x + 1 \) is irreducible in \( \mathbb{Z}/3\mathbb{Z}[x] \) by part (e). Hence the conclusion follows.
2. Prove that \( \mathbb{Z}/3\mathbb{Z}[x]/\langle x^5 - x + 1 \rangle \) is a field of order 3^5.

*Proof.* By part (e), \( x^5 - x + 1 \) is irreducible in \( \mathbb{Z}/3\mathbb{Z}[x] \). Since \( \mathbb{Z}/3\mathbb{Z} \) is a field, \( \mathbb{Z}/3\mathbb{Z}[x] \) is a Euclidean domain and hence a P.I.D. So the ideal generated by the irreducible element \( x^5 - x + 1 \) is maximal. Hence \( \mathbb{Z}/3\mathbb{Z}[x]/\langle x^5 - x + 1 \rangle \) is a field. By the division algorithm in \( \mathbb{Z}/3\mathbb{Z}[x] \), for every \( f(x) \in \mathbb{Z}/3\mathbb{Z}[x] \), \( \exists q(x), r(x) \in \mathbb{Z}/3\mathbb{Z}[x] \) such that \( f(x) = q(x)(x^5 - x + 1) + r(x) \), where \( r(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \), and \( a_i \in \mathbb{Z}/3\mathbb{Z} \). Hence

\[
\overline{f(x)} = f(x) + \langle x^5 - x + 1 \rangle = r(x) + \langle x^5 - x + 1 \rangle.
\]

Let \( \phi \) be the map from \( \mathbb{Z}/3\mathbb{Z}[x]/\langle x^5 - x + 1 \rangle \) to \( (\mathbb{Z}/3\mathbb{Z})^5 \) given by

\[
\overline{f(x)} = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \langle x^5 - x + 1 \rangle \mapsto (a_0, a_1, \ldots, a_4).
\]

\( \phi \) is obviously surjective. Suppose \( \phi(f(x)) = \phi(g(x)) \). Then \( \overline{f(x)} - \overline{g(x)} = 0 \). So \( \phi \) is injective. Since \( \phi \) is a bijective, \(|\mathbb{Z}/3\mathbb{Z}[x]/\langle x^5 - x + 1 \rangle| = |(\mathbb{Z}/3\mathbb{Z})^5| = 3^5 \). ■

**Remark** (Construction of field of order \( p^n \)). *To construct a field of order \( p^n \), take a monic irreducible polynomial \( f(x) \) of degree \( n \) in \( \mathbb{Z}/p\mathbb{Z}[x] \), which always exist, and the field \( \mathbb{Z}/p\mathbb{Z}[x]/\langle f(x) \rangle \) is a field of order \( p^n \) by the same reasoning as the above problem.*