Problem 10.1. This is a lemma that will be useful in the future: Let \( k \) be an infinite field.

1. Let \( f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \) and suppose that \( f(\theta_1, \ldots, \theta_n) = 0 \) for all \((\theta_1, \ldots, \theta_n) \in k^n\). Show that \( f \) is the zero polynomial. (Hint: Induct on \( n \).)
2. Let \( H_1, H_2, \ldots, H_N \) be a list of finitely many proper \( k \)-vector subspaces \( H_j \subseteq k^n \). Show that \( \bigcup H_j \neq k^n \).

Problem 10.2. Let \( p \) be prime. Let \( f(x) \in \mathbb{Q}[x] \) be an irreducible polynomial of degree \( p \) that has 2 complex roots and \( p - 2 \) real roots. Let \( L \) be the splitting field of \( f \) over \( \mathbb{Q} \). Show that \( \text{Gal}(L/\mathbb{Q}) = S_p \). (Hint: Look at Problem 9.1.)

Problem 10.3. Let \( L = \mathbb{Q}(\sqrt[44]{3}) \).

1. Show that \( L/\mathbb{Q} \) is Galois. (Hint: recall that the primitive sixth roots of unity are \( \frac{1 \pm \sqrt{-3}}{2} \).)
2. Compute \( \text{Gal}(L/\mathbb{Q}) \).

Problem 10.4. Consider the polynomial \( f(x) = x^{44} - 1 \) in \( \mathbb{F}_3[x] \).

1. Show that \( f(x) \) splits in \( \mathbb{F}_{3^{10}} \).
2. How many roots does \( f(x) \) have in each of the fields \( \mathbb{F}_3, \mathbb{F}_{3^2} \) and \( \mathbb{F}_{3^5} \)?
3. If we factor \( f(x) \) into irreducible factors over \( \mathbb{F}_3 \), how many factors of degree 10 will there be?

Problem 10.5. Let \( \zeta \) be a primitive \( n \)-th root of unity and let \( \Phi_n(x) = \prod_{m \in (\mathbb{Z}/m\mathbb{Z})^\times} (x - \zeta^m) \), which is known as the \( n \)-th cyclotomic polynomial. Let \( L = \mathbb{Q}(\zeta) \).

1. Show that the coefficients of \( f \) are fixed by \( \text{Gal}(L/\mathbb{Q}) \) and deduce\(^1\) that \( \Phi_n(x) \in \mathbb{Q}[x] \).
2. Look at Problem 6.7 and deduce that \( \Phi_n(x) \in \mathbb{Z}[x] \).

Problem 10.6. Let \( p \) be a prime number and let \( \zeta_p \) be a primitive \( p \)-th root of unity. Let
\[
\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.
\]

1. Show that \( \Phi_p(x) \) is the minimal polynomial of \( \zeta_p \) over \( \mathbb{Q} \). Hint: You’ll want to show that \( \Phi_p(x) \) is irreducible; the usual trick is to put \( x = y + 1 \) and use Eisenstein’s irreducibility criterion.
2. Show that \( \text{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \).

Problem 10.7. Let \( R \) be a commutative ring and \( M \) an \( A \)-module. A \textit{derivation from} \( R \to M \) is a map \( D : R \to M \) obeying \( D(f + g) = D(f) + D(g) \) and \( D(fg) = fD(g) + gD(f) \). So \( f(x) \mapsto f'(x) \) is a derivation \( k[x] \to k[x] \).
Let \( k \) be a field and let \( d : k \to k \) be a derivation. Let \( a \in k[y] \). Show that there is a unique derivation \( D : k[y] \to k[y] \) which restricts to \( d \) on \( k \) and has \( D(y) = a \).

Problem 10.8. Let \( K \) be a field of characteristic \( p \) and let \( L/K \) be a Galois extension with Galois group the cyclic group of order \( p \). We write \( g \) for a generator of \( \text{Gal}(L/K) \). In this problem, we consider \( g \) as a \( K \)-linear map from \( L \to L \).

1. Show that the characteristic polynomial of \( g \) is \((T - 1)^p\).
2. Show that the Jordan form of \( g \) consists of a single \( p \times p \) Jordan block, with 1’s on the diagonal.
3. Show that there is an element \( \alpha \) of \( L \) with \( g(\alpha) = \alpha + 1 \).
4. Putting \( \beta = \alpha^p - \alpha \), show that \( \beta \in K \) and show that \( L \cong K[x]/(x^p - x - \beta) \).

You have now proved that any extension \( L/K \) as in the hypotheses of this problem is of the form \( K[x]/(x^p - x - \beta) \) for some \( \beta \in K \). This is the \textit{Artin-Schreier theorem}.

\(^1\)There are other ways to show this, but I’d like you to work through this route because it is an important method that applies to many other examples.