Problem 1. Quadratic extensions of \( \mathbb{Q} \).

(1) Show that \( \mathbb{Q}(\sqrt{2}) \) is not isomorphic to \( \mathbb{Q}(\sqrt{3}) \) as abstract fields.

(2) Find the Galois group of \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) over \( \mathbb{Q} \).

Problem 2. Let \( E \) be the splitting field of \( x^5 - 2 \) over \( \mathbb{Q} \).

(1) Find the degree of \( E \) over \( \mathbb{Q} \). (Hint: \( E = \mathbb{Q}(\sqrt[5]{2}, \zeta) \).)

(2) Find the Galois Group of \( E \) over \( \mathbb{Q} \). Denote elements of the Galois group \( \sigma_{i,j} \), where \( i,j \) indicate where the generators are mapped. Explain how to multiply these elements. Find \( C_4 \) as a normal subgroup of the Galois group so that the quotient is also cyclic.

Problem 3. The following steps prove that the cyclotomic polynomial \( \Phi_n(x) \) is irreducible in \( \mathbb{Z}[x] \) (and hence also irreducible in \( \mathbb{Q}[x] \)). This proof is due to Landau. Recall that we defined \( \Phi_n(x) \) as the monic polynomial with roots all primitive \( n \)-th roots of 1. Let us fix one primitive root \( \zeta \).

\[
\Phi_n(x) = \prod_{i=1}^{n-1} (x - \zeta^i),
\]

where \( i \) runs over integers \( 1, \ldots, n-1 \) such that \( \gcd(i,n) = 1 \). Let \( f(x) \in \mathbb{Z}[x] \) be monic the irreducible polynomial of degree \( d \) that has \( \zeta \) as a root. It is a factor of \( \Phi_n(x) \), which itself is a factor of \( x^n - 1 \).

(1) Apply division algorithm to \( f(x^j) \) and \( f(x) \),

\[
f(x^j) = q_j(x)f(x) + r_j(x)
\]

to deduce that there are integer polynomials \( r_1(x), \ldots, r_n(x) \) of degree \( < d \) such that for any \( i \geq 0 \),

\[
f(\zeta^i) = r_j(x)
\]

for some \( j \). Moreover, if \( f(\zeta^i) = s(\zeta) \) for any polynomial \( s(x) \) of degree \( < d \) then \( s = r_j \). (Hint consider \( s(\zeta) - r(\zeta) \).)

(2) When \( p \) is a prime number, show that \( f(x^p) = (f(x))^p \mod p \) (this is true for any integer polynomial, not just \( f(x) \)). Applying the division algorithm to \( f(x^p) \) we get

\[
f(x^p) = f(x)q(x) + ps(x).
\]

for some integer polynomial \( s(x) \) of degree \( < d \). Deduce that \( p \) must divide \( r_j(x) \) for some \( j = 1, \ldots, n \).

(3) Show that if \( p \) is large enough then some \( r_j(x) = 0 \) and \( f(\zeta^p) = 0 \).

(4) Show that \( f(\zeta^i) = 0 \) for all \( i \) such that \( \gcd(i,n) = 1 \) and hence \( f(x) = \Phi_n(x) \). (Hint: we may run the same argument as above with \( \zeta \) replaced by another root of \( f(x) \), for example \( \zeta^p \), and the prime \( p \) replaced by a prime \( q \). This will produce more and more roots of \( f(x) \).)