Math 581 Assignment 11
due Friday 7 December

Instructions. In the problems about cyclotomic extensions of \( \mathbb{Q} \), feel free to use the fact that if \( K \) is the splitting field over \( \mathbb{Q} \) of \( x^n - 1 \), then \( \text{Gal}(K/\mathbb{Q}) \) is isomorphic to \( (\mathbb{Z}_n)^* \), the group of units of the ring \( \mathbb{Z}_n \). We will write \( \mathbb{Q}_n \) for the field \( K \) below.

We also write \( \mathbb{F}_q \) for the unique, up to isomorphism field with \( q \) elements (when \( q \) is a power of a prime).

1. Let \( q \) be a power of a prime \( p \) and let \( n \) be a positive integer with \( \gcd(n,q) = 1 \). If \( K \) is the splitting field of \( x^n - 1 \) over \( \mathbb{F}_q \), prove that \( |K| = q^r \), where \( r \) is the order of \( q \) in \( (\mathbb{Z}_n)^* \).
   (Hint: when does \( \mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \)?)

2. Let \( p \) be an odd prime. If \( F \) is a field with \( |F| = p^2 \), prove that \( x^2 - a \) splits over \( F \) for each \( a \in \mathbb{Z}_p \).

3. Determine all the subfields of \( \mathbb{Q}_{12} \).

4. Let \( n, m \) be positive integers with \( d = \gcd(n, m) \) and \( l = \text{lcm}(n, m) \).
   (a) If \( n \) divides \( m \), prove that \( \mathbb{Q}_n \subseteq \mathbb{Q}_m \).
   (b) Prove that \( \mathbb{Q}_n \mathbb{Q}_m = \mathbb{Q}_l \).
   (c) Prove that \( \mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}_d \).
      (Hint for (c): prove or lookup the result that \( \phi(n)\phi(m) = \phi(l)\phi(d) \).)

5. Let \( V \) be the subgroup of \( S_4 \) consisting of the identity and the three elements which are products of two disjoint 2-cycles. For each adjacent pair \( H \subseteq K \) in the sequence \( \{e\} \subseteq V \subseteq A_4 \subseteq S_4 \), show that \( H \) is normal in \( K \) and \( K/H \) is Abelian. Furthermore, if \( G \) is a subgroup of \( S_4 \), prove that \( \{e\} \subseteq V \cap G \subseteq A_4 \cap G \subseteq G \) satisfies the same property as the original sequence of subgroups of \( S_4 \).

6. Let \( G \) be a finite group. Prove that there is a Galois extension \( K/F \) with \( \text{Gal}(K/F) \cong G \).

Optional Problems

1. Let \( F \) be a finite field, and let \( K \) and \( L \) be extensions of \( F \) of degree \( n \) and \( m \), respectively. Prove that \( KL \) has degree \( \text{lcm}(n, m) \) over \( F \) and \( K \cap L \) has degree \( \gcd(n, m) \) over \( F \).

2. If \( n \) is odd, prove that \( \mathbb{Q}_{2n} = \mathbb{Q}_n \).
3. Let \( c \in \mathbb{R} \). Prove that \( c \) is constructible by ruler and compass if and only if \( c \) is contained in a Galois extension \( K \) of \( \mathbb{Q} \) with \( [K : \mathbb{Q}] \) a power of 2.

4. A Fermat number is an integer of the form \( 2^{2^r} + 1 \) for some \( r \). Suppose that \( p \) is an odd prime such that a regular \( p \)-gon is constructible. Show that \( p \) is a Fermat number.

5. Solvability by real radicals. Suppose that \( f(x) \in \mathbb{Q}[x] \) has all real roots. If \( f \) is solvable by radicals, is \( f \) solvable by “real radicals”? That is, does there exist a chain of fields \( \mathbb{Q} = Q_0 \subseteq Q_1 \subseteq \cdots \subseteq Q_n \subseteq \mathbb{R} \) such that \( Q_n \) contains all the roots of \( f \), and \( Q_{i+1} = Q_i(\sqrt[n]{a_i}) \)? The answer is no, in general, and this problem gives a criterion for when \( f \) is solvable by real radicals. Use the following steps to prove the following statement: If \( f(x) \in \mathbb{Q}[x] \) is an irreducible polynomial with all real roots, and if \( N \) is the splitting field of \( f \) over \( \mathbb{Q} \), then \( [N : \mathbb{Q}] \) is a power of 2 if and only if \( f \) is solvable by real radicals. You may assume the following nontrivial fact: If \( F \subseteq K \) are subfields of \( \mathbb{R} \) with \( K = F(a) \) such that \( a^n \in F \), and if \( L \) is an intermediate field of \( K/F \) Galois over \( F \), then \( [L : F] \leq 2 \).

(a) If \( [N : \mathbb{Q}] \) is not a power of 2, let \( p \) be an odd prime divisor of \( [N : \mathbb{Q}] \). Let \( P \) be the subgroup of \( G = \text{Gal}(N/\mathbb{Q}) \) generated by all elements of order \( p \). Show that \( P \) is a normal subgroup of \( G \) and that \( P \neq \{\text{id}\} \).

(b) Let \( \alpha \) be a root of \( f \), and let \( T = \mathbb{Q}(\alpha) \). If \( H = \text{Gal}(N/T) \), show that \( P \) is not contained in \( H \). Conclude that there is an element \( \sigma \in G \) of order \( p \) not contained in \( H \).

(c) Let \( F = \mathcal{F}(\langle \sigma \rangle) \). Show that \( \alpha \notin F \). Let \( Q_i \) be in the chain above, and set \( F_i = FQ_i \). Show that there is an integer \( r > 0 \) with \( \alpha \notin F_{r-1} \) but \( \alpha \in F_r \). Show that \( F = F_{r-1} \cap N \) and \( N \subseteq F_r \).

(d) Let \( E = NF_{r-1} \). Then \( F_{r-1} \subseteq E \subseteq F_r \). Conclude from the assumption above and the theorem of natural irrationalities that \( p = [E : F_{r-1}] \leq 2 \), a contradiction.