Consider the polynomial $x^n - 1 \in \mathbb{Q}[x]$. Its splitting field $K_n$ is called the $n$-th cyclotomic extension of $\mathbb{Q}$. [CAUTION: the degree of this field extension is NOT $n$.

(1) Show that $x^n - 1$ has exactly $n$-distinct roots, and that they form a cyclic subgroup $\mu_n$ of the multiplicative group $\mathbb{C}^\times$. Any generator for the group $\mu_n$ is called a primitive $n$-th root of unity.

(2) Show that $K_n = \mathbb{Q}(\zeta_n)$ where $\zeta_n$ is a primitive $n$-th root of unity.

(3) Which permutations of the elements of $\mu_n$ induce $\mathbb{Q}$-automorphisms of $K_n$?

(4) Prove that the Galois group of $K_n$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

(5) Show that if $n = p$ is prime, then the Galois group is cyclic of order $p - 1$.

(6) Show that $K_8$ has Galois group isomorphic to the Klein 4-group. So not all cyclotomic extensions have cyclic Galois groups.

(7) Compute the Galois group, the lattice of all subgroups, and the corresponding lattice of all fixed fields of subgroups for the following examples: $K_4/\mathbb{Q}$, $K_5/\mathbb{Q}$, $K_6/\mathbb{Q}$, and $K_8/\mathbb{Q}$.

(8) Notice that if $d|n$, then $K_d \subset K_n$. What is happening in the case where $d = 3$ and $n = 6$?

The cardinality of the group $(\mathbb{Z}/n\mathbb{Z})^\times$, interpreted as a function of $n$, is called the “Euler $\varphi$ function” and denoted $\varphi(n)$. That is, $\varphi(n)$ is the number of positive integers less than $n$ and relatively prime to $n$.

(1) Show that $\mu_d \subset \mu_n$ if and only if $d|n$.

(2) Define the $n$th cyclotomic polynomial $\Phi_n$ to be the polynomial whose roots are the primitive $n$-th roots of unity. Show

$$\Phi_n(x) = \Pi_{\zeta \text{ primitive in } \mu_n} (x - \zeta) = \Pi_a \text{ s.t. } 1 \leq a < n; (a,n) = 1 (x - \zeta_n^a).$$

(This generalizes the cyclotomic polynomial you have studied before).

(3) Show that $x^n - 1 = \Pi_{d|n} \Phi_d(x)$, where the product is taken over all divisors of $n$.

(4) Work out (2) and (3) explicitly for small $n$. (Say $n \leq 8$). There are some cool recursive relationships you might discover. Is $\Phi_n \in \mathbb{Q}[x]$ for all $n$?

(5) Show that $n = \sum_{d|n} \varphi(d)$, where the sum is over all positive divisors of $n$.

(6) Show that the minimal polynomial of $\zeta_n$ over $\mathbb{Q}$ is $\Phi_n$. 