Week 7: The fundamental theorem of Galois theory (14.1, 14.2)

On this homework, you may assume without proof that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois with $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, with the isomorphism given by $a \mapsto (\zeta_n \mapsto \zeta_n^a)$. We will prove this result next week.

Practice Problems

1. Let $\tau\colon \mathbb{C} \to \mathbb{C}$ be given by complex conjugation. Show directly that τ is a field automorphism of $\mathbb{C}$. What is the fixed field of τ?
2. Determine the lattice of subfields of $\mathbb{Q}(\zeta_5)$. *Hint*: $\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$.
3. Determine the lattice of subfields of $\mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(\zeta_{12})$.

Presentation Problems

1. Let $\alpha = \sqrt{2+\sqrt{2}}$. Compute $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.
2. Let $\tau\colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ be given by complex conjugation. What is a primitive element for the fixed field of τ? *Hint*: For the hard direction, use the fact that ζ_n satisfies the quadratic $x^2 - (\zeta_n + \zeta_n^{-1})x + 1 = 0$.
3. Determine the lattice of subfields of $\mathbb{Q}(\zeta_{20})$.
4. Let $L/K/F$ be a tower of field extension with L/F Galois. Let $G = \mathrm{Gal}(L/F)$, let $H = \mathrm{Gal}(L/K)$, and let G/H denote the collection of left cosets of H in G.
   (a) Show that for each left coset $C \in G/H$ and each $\alpha \in K$, the value of $C(\alpha)$ does not depend on the choice of an element of C.

   For $\alpha \in K$, the trace and norm of α from K to F are defined by

   $$\mathrm{Tr}_{K/F}(\alpha) = \sum_{C \in G/H} C(\alpha), \qquad \mathrm{N}_{K/F}(\alpha) = \prod_{C \in G/H} C(\alpha).$$

   (b) Let $\alpha \in K$. Show that $\mathrm{Tr}_{K/F}(\alpha) \in F$ and $\mathrm{N}_{K/F}(\alpha) \in F$.
   (c) Show that $\mathrm{Tr}_{K/F}$ is additive and $\mathrm{N}_{K/F}$ is multiplicative.

Tricky Problems

1. Existence of abelian Galois groups.
2. Let $n \geq 1$, let $K = \mathbb{Q}(\sqrt[n]{2})$, let $L = \mathbb{Q}(\zeta_n)$, and let $M = KL = \mathbb{Q}(\sqrt[n]{2}, \zeta_n)$.
   (a) Show that $f(x) = x^n - 2$ is irreducible and that $[K : \mathbb{Q}] = n$.
   (b) Show that M is a splitting field of $f(x)$ over $\mathbb{Q}$.
   (c) Show that if F is a subfield of K then $F = \mathbb{Q}(\sqrt[d]{2})$ for some $d \mid n$. *Hint*: Let $d = [F : \mathbb{Q}]$ and show that $N_{K/F}(\sqrt[n]{2}) = \sqrt[d]{2}$.
   (d) Show that if F is a subfield of L then F is Galois over $\mathbb{Q}$.
   (e) Show that

   $$K \cap L = \begin{cases} \mathbb{Q} & 8 \nmid n, \\ \mathbb{Q}(\sqrt{2}) & 8 \mid n. \end{cases}$$

(f) Use the isomorphism $\mathrm{Gal}(KL/K) \cong \mathrm{Gal}(L/(K \cap L))$ to show that

$$[M : \mathbb{Q}] = \begin{cases} n\varphi(n) & 8 \nmid n, \\ n\varphi(n)/2 & 8 \mid n. \end{cases}$$

(g) Show that if $8 \nmid n$ then $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi (\mathbb{Z}/n\mathbb{Z})^\times$ where $\varphi\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is the multiplication isomorphism. *Hint*: Produce an injective group homomorphism from $\mathrm{Gal}(M/\mathbb{Q})$ to $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi (\mathbb{Z}/n\mathbb{Z})^\times$ by considering the action on $\sqrt[n]{2}$ and ζ_n.

3. Let $\alpha = \sqrt{\left(2+\sqrt{2}\right)\left(3+\sqrt{3}\right)}$. Compute $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.