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.

Group Theory Problem

1. Let G be a finite group. For each $n \geq 0$, consider the abelian group E_n defined by

   $$E_n = \overbrace{\mathbb{Z}G \times \mathbb{Z}G \times \ldots \times \mathbb{Z}G}^{n+1}.$$

   A function $f\colon E_n \to A$ from E_n to an abelian group A is called multilinear if f is linear in each component, meaning that

   $$f(x_0, \ldots, x_i + x_i', \ldots, x_n) = f(x_0, \ldots, x_i, \ldots, x_n) + f(x_0, \ldots, x_i', \ldots, x_n)$$

   for each i. We will define an abelian group F_n in terms of a universal property in the category of abelian groups. There exists a multilinear function $\otimes\colon E_n \to F_n$ such that for every multilinear function $f\colon E_n \to A$, there exists a unique homomorphism of abelian groups $g\colon F_n \to A$ with $g \circ \otimes = f$.

   We define a simple tensor in F_n to be an element of the form $\otimes(g_0, g_1, \ldots, g_n)$ for $g_0, g_1, \ldots, g_n \in G$, which we denote by $g_0 \otimes g_1 \otimes \ldots \otimes g_n$.

(a) Show that F_n is generated by the simple tensors.

(b) Show that there is a G-module structure on F_n defined by

$$g \cdot (g_0 \otimes g_1 \otimes \ldots \otimes g_n) = (gg_0) \otimes g_1 \otimes \ldots \otimes g_n.$$

(c) Show that F_n is a free G-module of rank $|G|^n$ with basis given by simple tensors of the form $1 \otimes g_1 \otimes \ldots \otimes g_n$.

Let $\mathrm{aug}\colon F_0 \to \mathbb{Z}$ be defined by $\mathrm{aug}(1) = 1$. Let $d_1\colon F_1 \to F_0$ be defined by $d_1(1 \otimes g_1) = g_1 - 1$. For each $n \geq 2$, let $d_n\colon F_n \to F_{n-1}$ be defined by

$$d_n(1 \otimes g_1 \otimes \ldots \otimes g_n) = g_1 \cdot (1 \otimes g_2 \otimes \ldots \otimes g_n) + \sum_{i=1}^{n-1} (-1)^i (1 \otimes g_1 \otimes \ldots \otimes g_{i-1} \otimes g_i g_{i+1} \otimes g_{i+2} \otimes \ldots \otimes g_n) + (-1)^n (1 \otimes g_1 \otimes \ldots \otimes g_{n-1}).$$

(d) Show that $\cdots \to F_2 \to F_1 \to F_0 \to \mathbb{Z} \to 0$ is a projective resolution of $\mathbb{Z}$.

(e) Let A be a G-module. Show that $\mathrm{Hom}_{\mathbb{Z}G}(F_n, A) \cong C^n(G, A)$ where $C^n(G, A) = \mathrm{Hom}_{\mathbf{Set}}(G^n, A)$.

(f) Let A be a G-module and let $n \geq 0$. The homomorphism $\mathrm{Hom}_{\mathbb{Z}G}(F_n, A) \to \mathrm{Hom}_{\mathbb{Z}G}(F_{n+1}, A)$ induces a homomorphism $d_n\colon C^n(G, A) \to C^{n+1}(G, A)$. Show that d_n is given by

$$d_n(f)(g_1, \ldots, g_{n+1}) = g_1 \cdot f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n).$$

Let A be a G-module. For each $n \geq 0$, we define $Z^n(G, A) = \ker d_n$. For each $n \geq 1$, we define $B^n(G, A) = \mathrm{im}\, d_{n-1}$. We define $B^0(G, A) = 1$.

(g) Show that $H^n(G, A) \cong Z^n(G, A)/B^n(G, A)$.

Tricky Problems

1. 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.

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