MATH 511B, HOMEWORK 9

1. Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$ and let $F_1 = \mathbb{Q}(i)$, $F_2 = \mathbb{Q}(\sqrt{2})$, $F_3 = \mathbb{Q}(\sqrt{-2})$. Prove that $\mathrm{Gal}(K/F_1) \cong \mathbb{Z}/8\mathbb{Z}$, $\mathrm{Gal}(K/F_2) \cong D_8$, and $\mathrm{Gal}(K/F_3) \cong Q_8$.

2. Determine the Galois group of the splitting field over $\mathbb{Q}$ of $x^4 - 14x^2 + 9$.

3. Let F be a field of characteristic $\neq 2$.

(a) If $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2, or D_1D_2 is a square in F, prove that K/F is a Galois extension whose Galois group is isomorphic to the Klein 4-group.

(b) Conversely, suppose K/F is a Galois extension with $\mathrm{Gal}(K/F)$ isomorphic to the Klein 4-group. Prove that $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ and none of D_1, D_2, or D_1D_2 is a square in F.

4. Let K/F be any finite extension and let $\alpha \in K$. Let L be a Galois extension of F containing K and let $H \leq \mathrm{Gal}(L/F)$ be the subgroup corresponding to K. Define the *norm* of α from K to F to be

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha)\,,$$

where the product is taken over all the embeddings of K into an algebraic closure of F (so over a set of coset representatives for H in $\mathrm{Gal}(L/F)$, by the fundamental theorem of Galois theory). This is a product of conjugates of α. In particular if K/F is Galois this is $\prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$.

(a) Prove that $N_{K/F}(\alpha) \in F$.

(b) Prove that $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$, so that the norm is a multiplicative function from K to F.

(c) Let $K = F(\sqrt{D})$ be a quadratic extension of F. Show that $N_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$.

(d) Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$ over F. Let $n = [K : F]$. Prove that d divides n, that there are d distinct conjugates of α which are all repeated n/d times in the product, and conclude that $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.

5. With notation as in the previous problem, define the *trace* of α from K to F to be

$$Tr_{K/F}(\alpha) = \sum_{\sigma} \sigma(\alpha)\,.$$

(a) Prove that $Tr_{K/F}(\alpha) \in F$.

(b) Use the linear independence of characters to show that for any Galois extension K of F there is an element $\alpha \in K$ with $Tr_{K/F}(\alpha) \neq 0$.

6. Let $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ (for concreteness, use positive real square roots) and consider the extension $E = \mathbb{Q}(\alpha)$.

(a) Show that $a = (2+\sqrt{2})(3+\sqrt{3})$ is not a square in $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, as follows. If $a = c^2$ with $c \in F$, then $a\phi(a) = 6(2+\sqrt{2})^2 = (c\phi(c))^2$ for the automorphism $\phi \in \mathrm{Gal}(F/\mathbb{Q})$ fixing $\mathbb{Q}(\sqrt{2})$. Since $c\phi(c) = N_{F/Q(\sqrt{2})}(c) \in \mathbb{Q}(\sqrt{2})$, conclude that this implies $\sqrt{6} \in \mathbb{Q}(\sqrt{2})$, a contradiction.

(b) Conclude from (a) that $[E : \mathbb{Q}] = 8$, and prove that the roots of the minimal polynomial over $\mathbb{Q}$ of α are the eight elements $\pm\sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})}$.

(c) Let $\beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$. Show that $\alpha\beta = \sqrt{2}(3+\sqrt{3}) \in F$ so that $\beta \in E$. Similarly show that the other roots are alse elements of E, so that $E/\mathbb{Q}$ is a Galois extension. Show that the elements of the Galois group are precisely the maps determined by mapping α to one of the eight elements in (b).

(d) Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ be the automorphism which maps α to β. Show that since $\sigma(\alpha^2) = \beta^2$ that $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$. From $\alpha\beta = \sqrt{2}(3+\sqrt{3})$ conclude that $\sigma(\alpha\beta) = -\alpha\beta$ and hence $\sigma(\beta) = -\alpha$. Show that σ is an element of order 4 in $\mathrm{Gal}(E/\mathbb{Q})$.

(e) Show similarly that the map τ defined by $\tau(\alpha) = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$ is an element of order 4 in $\mathrm{Gal}(E/\mathbb{Q})$. Prove that σ and τ generate the Galois group, $\sigma^4 = \tau^4 = 1$, $\sigma^2 = \tau^2$, and that $\sigma\tau = \tau\sigma^3$.

(f) Conclude that $\mathrm{Gal}(E/\mathbb{Q}) \cong Q_8$, the quaternion group of order 8.

7. We say that K/F is a *p-extension* if K/F is Galois and $[K : F]$ is a power of p. If L/K and K/F are p-extensions, prove that the Galois closure of L over F is also a p-extension. Give a counterexample if we merely assume that $[K : F]$ is a power of p (i.e., if we drop the hypothesis that K/F is Galois).

8. Let p be a prime and $q = p^r$. Determine the characteristic polynomial of Frob_p acting on $\mathbb{F}_q$ (regarded as an $\mathbb{F}_p$-vector space of dimension r).

9. Let $K_n = \mathbb{Q}(\zeta_{2^{n+2}})$ be the cyclotomic field of 2^{n+2}th roots of unity. Set $\alpha_n = \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}$ and $K_n^+ = \mathbb{Q}(\alpha_n)$. Show that $\alpha_{n+1}^2 = 2 + \alpha_n$. Using this, along with the quadratic equation satisfied by $\zeta_{2^{n+2}}$ over K_n^+, give an explicit formula for the 2^{n+2}th roots of unity.

10. Determine the Galois group of $x^6 - 4x^3 + 1$.