Math 422/501: Problem set 9 (due 13/11/09)

Galois theory

1. Let L/K be a finite Galois extension. Let $K \subset M_1, M_2 \subset L$ be two intermediate fields. Show that the following are equivalent:
   (1) M_1/K and M_2/K are isomorphic extensions.
   (2) There exists $\sigma \in \mathrm{Gal}(L : K)$ such that $\sigma(M_1) = M_2$.
   (3) $\mathrm{Gal}(L : M_i)$ are conjugate subgroups of $\mathrm{Gal}(L : K)$.

2. (V-extensions) Let K have characteristic different from 2.
   (a) Suppose L/K is normal, separable, with Galois group $C_2 \times C_2$. Show that $L = K(\alpha, \beta)$ with $\alpha^2, \beta^2 \in K$.
   (b) Suppose $a, b \in K$ are such that none of a, b, ab is a square in K. Show that $\mathrm{Gal}(K(\sqrt{a}, \sqrt{b}) : K) \simeq C_2 \times C_2$.

The fundamental theorem of algebra

3. (Preliminaries)
   (a) Show that every simple extension of $\mathbb{R}$ has even order.
   (b) Show that every quadratic extension of $\mathbb{R}$ is isomorphic to $\mathbb{C}$.

4. (Punch-line)
   (a) Let $F : \mathbb{R}$ be a finite extension. Show that $[F : \mathbb{R}]$ is a power of 2.
   Hint: Consider the 2-Sylow subgroup of the Galois group of the normal closure.
   (b) Show that every proper algebraic extension of $\mathbb{R}$ contains $\mathbb{C}$.
   (c) Show that every proper extension of $\mathbb{C}$ contains a quadratic extension of $\mathbb{C}$.
   (d) Show that $\mathbb{C} : \mathbb{R}$ is an algebraic closure.

Example: Cyclotomic fields

$\mu_n \subset \mathbb{C}^\times$ will denote the group of nth roots of unity, $S_n \subset \mu_n$ the primitive nth roots of unity.

5. (prime order) Let p be an odd prime, and recall the proof from class that $\Phi_p(x) = \frac{x^p - 1}{x - 1}$ is irreducible in $\mathbb{Q}[x]$.
   (a) Let ζ_p be a root of Φ_p. Show that $\mathbb{Q}(\zeta_p)$ is a splitting field for Φ_p. What is its degree?
   (b) Show that $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ is cyclic.
   (c) Show that $\mathbb{Q}(\zeta_p)$ has a unique subfield K so that $[K : \mathbb{Q}] = 2$.
   (d) Show that there is a unique non-trivial homomorphism $\chi \colon G \to \{\pm 1\}$.
   (e) Let $g = \sum_{\sigma \in G} \chi(\sigma)\sigma(\zeta)$ ("Gauss sum"). Show that $g \in K$ and that $g^2 \in \mathbb{Q}$.
   OPT Show that $g^2 = (-1)^{\frac{p-1}{2}} p$, hence that $K = \mathbb{Q}(g)$.

6. Let $\zeta_n \in \mathbb{C}$ be a primitive nth root of unity.
   (a) Show that $\mathbb{Q}(\zeta_n)$ is normal over $\mathbb{Q}$.
   Hint: Show that every embedding of $\mathbb{Q}(\zeta_n)$ in $\mathbb{C}$ is an automorphism.
   (b) Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$. Show for every $\sigma \in G$ there is $j \in (\mathbb{Z}/n\mathbb{Z})^\times$ so that $\sigma(\zeta_n) = \zeta_n^{j(\sigma)}$ and that $j \colon G \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an injective homomorphism.
   (c) Let $\Phi_n(x) = \prod_{\zeta \in S_n}(x - \zeta)$. Show that $\Phi_n(x) \in \mathbb{Q}[x]$ (in fact, $\Phi_n(x) \in \mathbb{Z}[x]$). Show that the degree of Φ_n is exactly $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.
   (d) Show that the definitions of $\Phi_p(x)$ in problems 5 and 6(c) agree.

7. (prime power order) Let p be prime, $r \geq 1$ and let $n = p^r$.
   (a) Show that $\Phi_n(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1}$.
   (b) Show that Φ_n is irreducible.
   Hint: Change variables to $\Phi_n(1+y)$ and reduce mod p.
   (c) Conclude that $\mathrm{Gal}(\Phi_{p^r}) \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times$.

8. (general order) Let $n = \prod_{i=1}^s p_i^{r_i}$ with p_i distinct primes. Let G, j be as in 6(b).
   (a) Show that $\mathbb{Q}(\zeta_n) = \mathbb{Q}\left(\zeta_{p_1^{r_1}}, \ldots, \zeta_{p_s^{r_s}}\right)$.
   (b) For each i let $\pi_i \colon (\mathbb{Z}/n\mathbb{Z})^\times \to \left(\mathbb{Z}/p_i^{r_i}\mathbb{Z}\right)^\times$ be the natural quotient map. Show that the maps $\pi_i \circ j \colon G \to \left(\mathbb{Z}/p_i^{r_i}\mathbb{Z}\right)^\times$ are surjective.
   (c) [deferred]

Example: Cubic extensions

9. Let K be a field, $f \in K[x]$ of degree n, and let $\{\alpha_i\}_{i=1}^n \subset \Sigma$ be the roots of f in a splitting field Σ, counted with multiplicity.
   (a) Let $\{s_r\}_{r=1}^n$ be the elementary symmetric polynomials in n variables, thought of as elements of $K[y_1, \ldots, y_n]$. Show that $s_r(\alpha_1, \ldots, \alpha_n) \in K$.
   Hint: Consider the factorization of f in Σ.
   (b) Let $t \in K[\underline{y}]^{S_n}$ be any symmetric polynomial. Show that $t(\alpha_1, \ldots, \alpha_n) \in K$.

10. Let K be a field of characteristic zero, and let $f \in K[x]$ be an irreducible cubic. Let Σ be a splitting field for f, and let $\{\alpha_i\}_{i=1}^3$ be the roots.
   (a) Show that $[\Sigma : K] \in \{3, 6\}$ and that $\mathrm{Gal}(\Sigma : K)$ is isomorphic to C_3 or S_3.
   Hint: The Galois group acts transitively on the roots.
   (b) Let $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$, and let $\Delta = \delta^2$. Show that $\Delta \in K^\times$.
   (c) Let $M = K(\delta)$. Show that $[\Sigma : M] = 3$ and hence that $[\Sigma : K] = 3$ iff $\delta \in K$. Conclude that f is still irreducible in $M[x]$.
   (d) Assume that $K \subset \mathbb{R}$ and that $\Sigma \subset \mathbb{C}$. Show that $\Sigma \subset \mathbb{R}$ iff $M \subset \mathbb{R}$ iff $\delta \in \mathbb{R}$ iff $\Delta > 0$.
   — We now adjoin ω so that $\omega^3 = 1$.
   (e) Show that $[\Sigma(\omega) : M(\omega)] \in \{1, 3\}$, and in the first case that Σ is contained in a radical extension.
   (f) Assuming $[\Sigma(\omega) : M(\omega)] = 3$ show that this extension is still normal.
   (g) Let $y = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \in \Sigma(\omega)$. Show that for any $\sigma \in \mathrm{Gal}(\Sigma(\omega) : M(\omega))$ there is j so that $\sigma y = \omega^j y$. Conclude that $y^3 \in M(\omega)$.