Problem Set 3 for Math 250, Fall 2006.

Due on Wednesday, October 11.

1. Let F be a field of characteristic 0. Show that $F(x^2) \cap F(x^2 - x) = F$ as subfields of $F(x)$.

2. Let p be a prime and $c \in \mathbb{Q}$ such that $f(x) = x^p - c$ is irreducible. Prove that the Galois group of $f(x)$ over $\mathbb{Q}$ is isomorphic to the group of permutations of $\mathbb{Z}/p\mathbb{Z}$ of the form $x \mapsto ax + b$.

3. Prove that a finite (multiplicative) subgroup of the units $F^\times$ of a field F is cyclic.

4. (a) Prove that for a finite separable extension E/F there are only finitely many intermediate fields $F \subset K \subset E$.

   (b) Prove that for a simple algebraic extension $F[\alpha]/F$, there are only finitely many intermediate fields $F \subset K \subset F[\alpha]$.

   (c) Let F be an algebraically closed field of characteristic p. Find infinitely many (distinct) intermediate fields for the finite field extension $F(x^p, y^p) \subset F(x, y)$.

5. Write the resolvent cubic $g(x) = x^3 + b_2x^2 + b_1x + b_0$ of $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ as a degree 3 polynomial with coefficients which are expressions involving a_0, a_1, a_2, a_3. Compare the discriminant of $f(x)$ with that of $g(x)$. Use the techniques explained in class to calculate the Galois groups of the following polynomials over $\mathbb{Q}$:

   (a) $x^4 + 4x^2 + 2$

   (b) $x^4 - 2$

   (c) $x^4 - 4x + 2$

   Find an irreducible degree 4 polynomial $f(x) \in \mathbb{Q}[x]$ which has a Galois group different from any of the above polynomials.

6. Fix a prime p. Recall that we constructed a finite field $\mathbb{F}_q$ of order $q = p^n$, which is unique up to isomorphism.

   (a) Prove that $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ with cyclic Galois group generated by the Frobenius automorphism $\sigma(a) = a^p$.

   (b) Show that $\mathbb{F}_q$ contains exactly one field isomorphic to $\mathbb{F}_{q'}$ where $q = p^n$, $q' = p^m$ and m divides n.

   (c) Show that every monic irreducible polynomial of degree d dividing n occurs exactly once as a factor in $x^{p^n} - x$.

   (d) Give a construction of an algebraic closure of $\mathbb{F}_p$. An algebraic closure E of a field F is an algebraic field extension such that E is algebraically closed.

   (e) Find a formula for the number $N(n, q)$ of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n. Your formula should involve the Mobius function μ defined by $\mu(1) = 1$, $\mu(n) = (-1)^r$ if n is the product of r distinct primes, and otherwise $\mu(n) = 0$. Recall that the Mobius inversion formula says that if $f(n) = \sum_{d|n} g(d)$ for all $n \in \mathbb{N}$ then $g(n) = \sum_{d|n} \mu(d) f(n/d)$.