McGill University
Math 571: Higher Algebra 2
Assignment 2: due February 26, 2007

1. Show that the Galois group of the polynomial $X^8 - 2 \in \mathbb{Q}[X]$ is isomorphic to a semi-direct product of C_8 and C_2. Find the lattice of subfields of its splitting field.

2. If $E = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$, show that E is a normal extension of $\mathbb{Q}$. Find its Galois group and lattice of subfields.

3. Let k be a field of characteristic $\neq 2$ and let $f(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4 \in k[X]$ having distinct roots r_1, r_2, r_3, r_4. Let $E = k(r_1, r_2, r_3, r_4)$, $G = \mathrm{Gal(E/k)}$ and let $G_f \subseteq S_n$ be the corresponding permutation group of the roots. Let

$$t_1 = r_1r_2 + r_3r_4,\ t_1 = r_1r_3 + r_2r_4,\ t_1 = r_1r_4 + r_2r_3$$

and let $g(X) = (X - t_1)(X - t_2)(X - t_3)$ (the resolvant cubic of the quartic $f(X)$). Let

$$V_4 = \{1, (12)(34), (13)(24), (14)(23)\},$$

a normal subgroup of S_4 known as the Klein four group.

   (a) Show that $g(X) = X^3 + b_1X^2 + b_2X + b_3$ where $b_1 = -a_2$, $b_2 = a_1a_3 - 4a_4$, $b_3 = 4a_2a_4 - a_1^2a_4 - a_3^2$. Show also that $f(X)$ and $g(X)$ have the same discriminant.

   (b) Show that $k(t_1, t_2, t_3)$ is the fixed field of $G_f \cap V_4$ and that the Galois group G_g of $g(X)$ is isomorphic to $G_f/(G_f \cap V_4)$.

   (c) Show that the transitive subgroups of S_4 are (i) S_4, (ii) A_4, (iii) V_4, (iv) $C_3 =< (1234) >$, and its conjugates, (v) $D_4 =< (12), (1234) >$ and its conjugates.

   (d) Assume that $f(X)$ is irreducible. Show that (i) if $G_f = S_4$ then $G_g = S_3$, (ii) if $G_f = A_4$ then $C_g = C_3$, (iii) if $G_f = V$ then $G_g = 1$, (iv) if $G_f = C_4$ or one of its conjugates then G_g is of order 2, (v) if $G_f = D_4$ or any of its conjugates then G_g is of order 2. Prove that if G_g is of order 2 then $G_f \cong D_4$ or C_4 according as $f(X)$ is or is not irreducible over $k(\sqrt{d_f})$.

   (e) Determine the Galois group of $X^4 + 3X^3 - 3X - 2$ over $\mathbb{Q}$.

4. (a) If $f(X) \in \mathbb{Z}[X]$ is of degree ≥ 1, show that the set of prime divisors of the integers $f(n)$ $(n \geq 1)$ is infinite.

   (b) Let p be an odd prime not dividing n and let $\Phi_n(X)$ be the n-th cyclotomic polynomial. If $a \in \mathbb{Z}$ with $p \mid \Phi_n(a)$, show that $p \nmid a$ and that the order of a in $(\mathbb{Z}/p\mathbb{Z})^*$ is n.

   (c) Prove that for any integer $n \geq 2$ there are infinitely many primes with $p \equiv 1 \bmod n$.

5. The purpose of this problem is to prove that any solvable subgroup of S_p, p a prime, is isomorphic to a subgroup of the group L of transformations of $\mathbb{Z}/p\mathbb{Z}$ of the form $x \mapsto ax + b$ $(a \neq 0)$ containing all the translations $x \mapsto x + b$.

   (a) Let G be a transitive subgroup of S_n and $H \neq 1$ a normal subgroup of G. Prove that all the H-orbits have the same cardinality. Deduce that H is transitive if n is a prime.

   (b) Show that the translations $\neq 1$ are the only transformations in L without fixed points. Deduce that these are the only transformations in L which are p-cycles.

   (c) Let G be a subgroup of the group of permutations of $\mathbb{Z}/p\mathbb{Z}$ having, as a normal subgroup, a subgroup of L containing the group H of translations. Show that G is a subgroup of L. **Hint:** If $\tau(x) = x + 1$ and $\sigma \in G$, show that $\sigma\tau\sigma^{-1}(x) = x + a$ for some $a \neq 0$ and deduce that $\sigma(x) = ax + b$.

   (d) Using induction, prove that any solvable transitive subgroup of S_p, p prime, is conjugate to a subgroup of L. Note that here we identify S_p with the group of permutations of $\mathbb{Z}/p\mathbb{Z}$.

   (e) Let $f(X) \in k[X]$ be irreducible of prime degree with k of characteristic 0. Let E be a splitting field for $f(X)$ over k. Show that $f(X)$ is solvable by radicals over k if and only if $E = k(r_1, r_2)$ for any two roots r_1, r_2 of $f(X)$.