Math 250a: Higher Algebra
Problem Set #3 (28 September 2001): Galois theory III

1. (Problem 5 of Jacobson 4.5, generalized) Let k be a finite field of q elements, and let E be the field $E = k(t)$ of rational functions in one variable over k. For each $c \in k$, let g_c be the automorphism of E taking each function $f(t)$ to $f(t+c)$. Clearly $g_c g_{c'} = g_{c+c'}$. In particular, the g_c constitute a group G isomorphic with the additive group of k. Determine E^G.
[The next, much harder, problem in Jacobson asks to do the same for the group $\mathrm{PGL}_2(k)$ of "fractional linear transformations" taking t to $(at+b)/(ct+d)$ with $a, b, c, d \in k$ such that $ad - bc \neq 0$. Can you figure out E^G in that case?]

2. (Discriminant of a polynomial) Let $s_1, \ldots, s_n$ be the elementary symmetric functions of indeterminates $x_1, \ldots, x_n$ over a field k. Let
$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$
in $E = k(x_1, \ldots, x_n)$. Then Δ^2 is a symmetric function of the x_i, and can thus be written as $P_n(s_1, \ldots, s_n)$ for some polynomial[1] $P_n \in k[s_1, \ldots, s_n]$. Determine P_1 and P_2. Prove that any monic polynomial $f = X^n + \sum_{j=1}^{n} (-1)^j a_j X^{n-j}$ in $K[X]$ (K some field containing k) is coprime with f' if and only if $P_n(a_1, \ldots, a_n) \neq 0$.
[$P_n(a_1, \ldots, a_n)$ is known as the discrimininant of f. As n grows, the expression for P_n as a polynomial in the a_j gets complicated very quickly; already for $n = 3$ we have $P_3(A, B, C) = -4A^3C + A^2B^2 + 18ABC - 4B^3 - 27C^2$, and you don't want to see P_4. In practice P_n can be computed much more efficiently by writing it as a determinant, or as the "resultant" of f and f'.]

3. (Variant of Problem 11 of Jacobson 4.5) Now assume that k is not of characteristic 2. Prove that $k(s_1, \ldots, s_n, \Delta)$ is a degree-2 extension of $F = k(s_1, \ldots, s_n)$. What is the subgroup of $S_n = \mathrm{Gal}(E/F)$ that corresponds to this subfield of E/F?

4. Let $s_1, \ldots, s_n$ be indeterminates over a field k not of characteristic 2. Determine the Galois group of the polynomial
$$X^{2n} + \sum_{j=1}^{n} (-1)^j s_j X^{2(n-j)} = X^{2n} - s_1 X^{2n-2} + s_2 X^{2n-4} - \cdots + (-1)^n s_n$$
over $k(s_1, \ldots, s_n)$.
[Mimic the proof of Theorem 4.15. Under what conditions on k does this generalize to the polynomial $X^{an} + \sum_{j=1}^{n} (-1)^j s_j X^{a(n-j)}$?]

[1] We are assuming here a result not yet proved in class, though you may have already seen it: $k[s_1, \ldots, s_n]$ is the sub*ring* of $k[x_1, \ldots, x_n]$ fixed under S_n.

5. (Jacobson 4.6, problem 6: lower central series and nilpotency) For subgroups H, K of a group G, define $[H, K]$ to be the subgroup generated by $\{h^{-1}k^{-1}hk : h \in H, k \in K\}$. (The expression $[h, k] = h^{-1}k^{-1}hk$ is called the *commutator* of h, k, since $[h, k] = 1$ if and only if h, k commute). For any group G, the lower central series of G is the sequence $G^1 \supseteq G^2 \supseteq G^3 \supseteq \ldots$ of subgroups of G defined inductively by $G^1 = G$ and, for $i > 1$, $G^i = [G^{i-1}, G]$. The group G is said to be *nilpotent* if some G^k is $\{1\}$.

i) Prove that $[H, K] = [K, H]$ for any subgroups H, K of G, and that this is a normal subgroup of G when both H and K are.

ii) Prove that $G^i \triangleleft G$ for each i. Conclude that any nilpotent group is solvable.

iii) Give an example of a solvable group that is not nilpotent.

6. (Jacobson 4.6, problem 10: upper central series) For any group G, the upper central series of G is the sequence $C_1 \subseteq C_2 \subseteq C_3 \subseteq \ldots$ of subgroups of G defined inductively by $C_1 = C(G)$, the center of G, and C_i for $i > 1$ is the normal subgroup of G such that C_i/C_{i-1} is the center of G/C_{i-1}. Prove that G is nilpotent if and only if $G = C_k$ for some integer k.

7. (Jacobson 4.7, Problem 2; Cf. Problem 5 from the first set) Let p be a prime and $c \in \mathbf{Q}$ a nonzero number such that $x^p - c$ is irreducible. Prove that the Galois group of $x^p - c$ over $\mathbf{Q}$ is isomorphic to the "$ax + b$ group mod p", that is, the group of permutations of $\mathbf{Z}/p\mathbf{Z}$ of the form $x \mapsto ax + b$.

Problem set is due in class Friday, October the 5th.