MATH 121 PROBLEM SET 5

This set is due at noon on Friday March 2 in Jason Lo's mailbox.

1. Suppose m is a factor of n. Find $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$. Show that it is cyclic, and generated by Frob^m.

2. Find (with proof!) $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})/\mathbb{Q})$. (For example, this will involve showing that $\sqrt{11} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$.)

3. (a) Suppose n is prime. Show that if G is a subgroup of S_n that is transitive and contains a two-cycle, then $G = S_n$.
(b) Suppose n is prime. Let K be the splitting field of an irreducible degree n polynomial in $\mathbb{Q}[x]$ with precisely two non-real roots (necessarily conjugate). Show that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_n$. Hint: use (a).

4. Suppose ζ is a primitive fifth root of unity, a root of $f(x) = (x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1 = 0$. Show that $f(x)$ is irreducible over $\mathbb{Q}$. Show that $\mathbb{Q}(\zeta)$ is the splitting field of $f(x)$. Show that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic of order four. Let $\alpha = \zeta + \zeta^{-1}$. Show that $\mathbb{Q}(\alpha)$ is the unique intermediate field in the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Show that α is degree 2 over $\mathbb{Q}$, and then use the quadratic formula to find α. Use the quadratic formula again to solve for ζ in terms of α, and hence to compute ζ.

Date: Friday, February 23, 2007.