Math 120c
Lloyd Kilford

Coursework 3
Due: 25th April 2003

1. Let L/K be an extension of finite fields. Show that the functions

$$N_{L/K},\ Tr_{L/K} : L \to K$$

are surjective.

Is this still true for an extension of characteristic 0 fields? [Hint: consider an extension over $\mathbf{Q}$.]

2. (a) Let G be a finite abelian group. Show that there is an abelian extension of $\mathbf{Q}$ with Galois group G. [This is the easy case of the Inverse Galois Problem, which is still unproved.]

   (b) Hence show that if K is a finite extension of $\mathbf{Q}$ then there are infinitely many abelian extensions of K with Galois group G.

   (c) Show that there are infinitely many nonzero integers a and b such that $-4a^3 - 27b^2$ is a square in $\mathbf{Z}$.

3. (a) Let K be a field of characteristic p, and let L/K be a cyclic extension of degree p^{m-1} with $m \geq 2$. Let $G = G(L/K) = \langle \sigma \rangle$, and let $\beta \in L$ be such that $Tr_{L/K}(\beta) = 1$. Show that there exists $\alpha \in L$ such that

$$\sigma(\alpha) - \alpha = \beta^p - \beta.$$

   (b) Show that $f := x^p - x - \alpha$ is irreducible over $L[x]$.

   (c) If θ is a root of f, show that $L(\theta)/K$ is Galois and cyclic of degree p^m. Also, show that the Galois group of $L(\theta)/K$ is generated by an element τ satisfying

$$\tau|_L = \sigma,\ \tau(\theta) = \theta + \beta.$$

4. Recall that $\Phi_n(x) \in \mathbf{Z}[x]$ is the minimal polynomial of a primitive n^{th} root of unity over $\mathbf{Q}$. Let p be a prime integer, and let n be a positive integer with $p \nmid n$.

   (a) Let a be a nonzero integer. Prove that $p \mid \Phi_n(x)$ if and only if a has exact order n as an element of $(\mathbf{Z}/p\mathbf{Z})^\times$.

   (b) Show that there exists an integer a with $p \mid \Phi_n(a)$ if and only if we have $p \equiv 1 \mod n$. Hence deduce that there are infinitely many primes $p \equiv 1 \mod n$. [This is a special case of Dirichlet's Theorem, which is proved in Ma160b].