Math 250a: Higher Algebra
Problem Set #4 (22 October 2004):
Pontrjagin duality for finite abelian groups; Galois extras

First, the promised analogue of the Kummer pairing for Artin-Schreier extensions:

1. Let $k_0 = \mathbf{Z}/p\mathbf{Z}$, let F be a field containing k_0 (equivalently: of characteristic p), and let K/F be a finite normal extension with Galois group $G \cong k_0^n$ for some n. Define $\rho : K \to K$ by $\rho(x) = x^p - x$ (so ρ is a homomorphism of additive groups with kernel k_0), and let $M_1 = \rho(K) \cap F$ and $M = M_1/\rho(F)$. For $g \in G$ and $a \in M$ define $(g, a) = g(b) - b$ where $b \in K$ satisfies $b^p - b = a$. Prove that:
   i) $(g, a) \in k_0$;
   ii) (g, a) does not depend on the choice of representative of a in M and of b such that $b^p - b = a$;
   iii) $(\cdot, \cdot)$ is a perfect pairing.

Next, an introduction to representation theory of finite groups via the abelian case (a.k.a. discrete Fourier analysis). Let G be a finite abelian group, N its exponent (the least positive integer such that $g^N = 1$ for all $g \in G$), and K a field in which $X^N - 1$ is separable and split (typically $\mathbf{C}$ or $\mathbf{Q}(e^{2\pi i/N})$, but we'll also use the splitting field of $X^N - 1$ over a finite field of characteristic $p \nmid N$). The *Pontrjagin dual* $\widehat{G}$ is the group of homomorphisms $\chi : G \to K^*$, a.k.a. one-dimensional representations $G \to \mathrm{GL}_1(K)$.

2. Let (V, ρ) be any representation of G (that is, a K-vector space V together with a homomorphism $\rho : G \to \mathrm{GL}(V)$). For $\chi \in \widehat{G}$ define

$$\pi_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g)^{-1} \rho(g) \in \mathrm{Hom}(V).$$

   Prove that $\pi_\chi \in \mathrm{Hom}_G(V)$ (that is, π_χ commutes with $\rho(G)$), that π_χ is a projection (that is, $\pi_\chi \circ \pi_\chi = \pi_\chi$), and that $\pi_\chi(V) = V_\chi$, the "χ-isotypic subspace" or "χ-eigenspace" of V defined by

$$V_\chi := \{v \in V \mid \forall g \in G, \rho(g)(v) = \chi(g)v\}.$$

3. Prove that $\widehat{G} \cong G$, and that the map: $G \times \widehat{G} \to K^*$, $(g, \chi) \mapsto \chi(g)$ is a perfect pairing. (You may use that fact that $G \equiv \prod_{i=1}^r \mathbf{Z}/n_i\mathbf{Z}$ for some positive integers r and $n_i | N$. NB: in general there is no canonical identification of $\widehat{G}$ with G.) Show that $\sum_{\chi \in \widehat{G}} \pi_\chi$ is the identity map, and thus that $V = \oplus_{\chi \in \widehat{G}} V_\chi$.

Next, the cyclotomic proof of Quadratic Reciprocity:

4. Now let $G = k^*$ where k is a finite field of characteristic p, and suppose that $X^p - 1$ is also separable and split in K. Fix a character $\psi \neq 1$ from the additive group of k to K. For $\chi \in \widehat{G}$ with $\chi \neq 1$, the *Gauss sum* τ_χ is defined by

$$\tau_\chi := \sum_{a \in k^*} \chi(a)\psi(a) \in K.$$

   Prove that

$$\tau_\chi \tau_{\chi^{-1}} = \chi(-1)q,$$

   where $q = \#(k)$. In particular, if p is odd, $q = p$, and $\chi^2 = 1$ (so χ is the "quadratic character mod p" or "Dirichlet symbol mod p") then $\tau_\chi^2 = p^*$, where $p^* = p$ or $-p$ according as $p \equiv 1 \bmod 4$ or $p \equiv -1 \bmod 4$.

5. i) Now let l be another odd prime, let K be a splitting field of $X^p - 1$ over $\mathbf{Z}/l\mathbf{Z}$, and deduce the Law of Quadratic Reciprocity: p^* has a square root in $\mathbf{Z}/l\mathbf{Z}$ if and only if l is a square mod p.
   ii) The "auxiliary laws" of quadratic reciprocity characterize the odd primes l such that -1 or 2 is a square mod l. For -1, deduce the auxiliary law from the fact that a fourth root of unity is a square root of -1. Find a cyclotomic proof of the auxiliary law for the quadratic character of 2 mod l.

6. i) Let $f(X) \in \mathbf{Z}[X]$ be an irreducible monic polynomial of degree 3. Let Δ be its discriminant. Prove that if Δ is a square then for every prime $p \nmid \Delta$ the polynomial either remains irreducible mod p or splits into three linear factors mod p. Must the converse hold?
   ii) Exhibit such a polynomial f that splits mod p if and only if $p \equiv 1$ or $-1 \bmod 7$.

Problem set is due in class Friday, October the 29th.