Math 250a: Higher Algebra

Problem Set #5 (12 October 2001):

More about trace, norm, and cyclic extensions, and a taste of group cohomology

Cyclic extensions and norms therein:

1. [Construction of cyclic extensions of prime degree.] Let us use Galois' solvability theory to produce a cyclic extension of degree 5 of $\mathbf{Q}$. We know that once we adjoin a fifth root of unity, call it z, the extension can be obtained by extracting a fifth root of some $a \in F = \mathbf{Q}(z)$. But not every a will do... For instance, find integers $c_2, c_3, c_4 \in \{0, 1, 2, 3, 4\}$ such that if we set
$$a = (2+z)(2+z^2)^{c_2}(2+z^3)^{c_3}(2+z^4)^{c_4}$$
and adjoin to $\mathbf{Q}(z)$ a root of $X^5 - a$, the resulting field K is normal over $\mathbf{Q}$ (not just over F), with cyclic Galois group, and thus contains the desired cyclic extension of degree 5. (You may assume that $a \notin F^{*5}$.)

How might you go about proving that $a \notin F^{*5}$, or obtaining an explicit quintic polynomial that gives our cyclic extension of degree 5? Can you generalize the construction to cyclic extensions of arbitrary degree, prime or not? What if the ground field need not be $\mathbf{Q}$ (but still does not have characteristic dividing n)?

2. [Jacobson 4.15, Exercise 1] Let E be a finite field and F a subfield of E. Prove that the norm homomorphism from E^* to F^* is surjective. [Hint: give an upper bound on the size of its kernel.]

3. [Jacobson 4.15, Exercise 2] Let F be a field containing n distinct n-th roots of unity, and E/F a normal extension with $\mathrm{Gal}(E/F)$ cyclic of order n. We have seen (Thm. 4.32) that there exists $u \in E$ with $u^n \in F$ such that $E = F(u)$. Prove that any other $v \in E$ with $v^n \in F$ is of the form bu^k for some $b \in F$ and $k \in \mathbf{Z}$.

Let E/F be any field extension with $[E : F] = n$. We defined the trace and norm in Problem 1 of the first set, in terms of the F-linear operator M_a on E. We next show that these definitions agree with the notions of trace and norm from Jacobson 4.15 when E/F is normal, and indeed generalize to any separable extension.

4. Suppose E/F is a separable field extension with $[E : F] = n$, and K/F is a normal extension containing E. Then by Thm. 4.4 there are n homomorphisms from E to K; call these η_i $(i = 1, \ldots, n)$. Show that for any $a \in E$ the characteristic polynomial of M_a is $\prod_{i=1}^n (X - \eta_i(a))$. Conclude that the trace and norm of a relative to the extension E/F are respectively $\sum_{i=1}^n \eta_i(a)$ and $\prod_{i=1}^n \eta_i(a)$. [It may help to do first the extreme cases $a \in F$ and $E = F(a)$, using part (iii) of PS1 #1 for the latter case.]

The next exercises connect multiplicative and additive Kummer theory with (usually) infinite Galois groups. Don't do them by chasing arrows in exact sequences of Galois cohomology (as in §3 of the Tate handout); we'll get to that later.

For the multiplicative case, let F be a field containing n distinct n-th roots of unity for some $n > 1$. Let L be a separable closure of F, and $K \subseteq L$ the compositum of all $(\mathbf{Z}/n\mathbf{Z})$ extensions of F, that is, the subfield of L generated by all E such that E/F is normal with Galois group $\mathbf{Z}/n\mathbf{Z}$. By Thm. 4.32, E is generated by elements $\sqrt[n]{a}$ with $a \in F^*$; since multiplying a by an n-th power yields the same E, we may regard a as an element of F^*/F^{*n}.

5. For $g \in \mathrm{Gal}(L/F)$ and $a \in F^*$ define $\langle g, a\rangle \in \boldsymbol{\mu}_n$ as follows: find $u \in K$ such that $u^n = a$, and set $\langle g, a\rangle = g(u)/u$. Prove that this is well-defined (does not depend on the choice of root of $u^n = a$) and contained in $\boldsymbol{\mu}_n$ for all g, a. Show that $\langle \cdot, \cdot \rangle$ is continuous with respect to the discrete topologies on F^*, $\boldsymbol{\mu}_n$ and the profinite topology on $\mathrm{Gal}(L/F)$ introduced in the fourth problem set. Verify that $\langle \cdot, \cdot \rangle$ is a pairing, i.e., that $\langle g, a\rangle\langle g', a\rangle = \langle gg', a\rangle$ and $\langle g, a\rangle\langle g, a'\rangle = \langle g, aa'\rangle$ for all $g, g' \in \mathrm{Gal}(L/F)$ and $a, a' \in F^*$. Prove that $g \in \mathrm{Gal}(L/K)$ if and only if $\langle g, a\rangle = 1$ for all $a \in F^*$, and $a \in F^{*n}$ if and only if $\langle g, a\rangle = 1$ for all $g \in \mathrm{Gal}(L/F)$.

Thus $\langle g, a\rangle$ descends to a "perfect pairing" between the quotient groups F^*/F^{*n} and $\mathrm{Gal}(K/F) = \mathrm{Gal}(L/F)/\mathrm{Gal}(L/K)$, taking values in $\boldsymbol{\mu}_n$. This identifies $\mathrm{Gal}(K/F)$ with the "Pontrjagin dual" of F^*/F^{*n}.

6. Now suppose F is a field of characteristic p, and K is the compositum of all Artin-Schreier extensions of F. Mimic Problem 5 to construct a perfect pairing between $\mathrm{Gal}(K/F)$ and [what?], taking values in $\mathbf{Z}/p\mathbf{Z}$.

7. Solve Exercises 2.1 and 2.2 in the Tate handout (identification of $H^2(G, A)$ with extensions of G by A).

Problem set is due in class Friday, October the 19th.