Problem Set 4 for Math 250, Fall 2006.

Due on Friday, October 20.

1. Let $f(x) \in F[x]$ be irreducible of prime degree over F of characteristic 0, and let E be a splitting field of $f(x)$ over F. Show that $f(x)$ is solvable by radicals if and only if $E = F(r_i, r_j)$ for any two roots r_i, r_j of $f(x)$.

2. Let E/F be an extension of finite fields. Show that the norm homomorphism from $E^\times$ to $F^\times$ is surjective.

In the rest of this pset you will do a bit of group cohomology. Recall that a G-module M is an abelian group equipped with an action of G compatible with the group structure of M. The group structure on M will in general be written additively in these exercises.

1. Let G be a group. For any G-module M, define the *homogeneous* r-cochains $\tilde{C}^r(G, M)$ of G with values in M to be the set of functions $\phi : G^{r+1} \to M$ satisfying $\phi(gg_0, \ldots, gg_r) = g \cdot \phi(g_0, \ldots, g_r)$, for all $g, g_i \in G$. The set $\tilde{C}^r(G, M)$ is an abelian group (why?).

   Define $\tilde{d}^r : \tilde{C}^r(G, M) \to \tilde{C}^{r+1}(G, M)$ by

   $$(\tilde{d}^r\phi)(g_0, \ldots, g_{r+1}) = \sum_{i=0}^{r+1} (-1)^i \phi(g_0, \ldots, \hat{g}_i, \ldots, g_{r+1})$$

   where $\hat{g}_i$ denotes omission. Show that $\tilde{d}^r \circ \tilde{d}^{r-1} = 0$. We may thus (why?) define the r-th cohomology group of G with values in M to be the abelian group $H^r(G, M) = \mathrm{Ker}(\tilde{d}^r)/\mathrm{Im}(\tilde{d}^{r-1})$.

2. Define the set of *inhomogeneous* r-cochains $C^r(G, M)$ of G with values in M to be the group of all maps $\psi : G^r \to M$ (for $r = 0$, take $G^r = \{1\}$). Given $\tilde{\phi} \in \tilde{C}^r(G, M)$, define $\phi \in C^r(G, M)$ by

   $$\phi(g_1, g_2, \ldots, g_r) = \tilde{\phi}(1, g_1, g_1g_2, \ldots, g_1 \cdots g_r).$$

   Show that $\tilde{\phi} \mapsto \phi$ is a bijection transforming $\tilde{d}^r$ into the map $d^r : C^r(G, M) \to C^{r+1}(G, M)$ given by $(d^r\phi)(g_1, \ldots, g_{r+1}) =$

   $$g_1\phi(g_2, \ldots, g_{r+1}) + \sum (-1)^j \phi(g_1, \ldots, g_jg_{j+1}, \ldots, g_{r+1}) + (-1)^{r+1}\phi(g_1, \ldots, g_r).$$

   Thus $H^r(G, M) = \mathrm{Ker}(d^r)/\mathrm{Im}(d^{r-1})$. The set $B^r(G, M) = \mathrm{Im}(d^{r-1})$ is called the r-coboundaries and the set $Z^r(G, M) = \mathrm{Ker}(d^r)$ is called the r-cocycles. Check that actually $B^r(G, M)$ and $Z^r(G, M)$ are abelian groups.

3. Let $r = 1$ in this problem.

   (a) Write down the conditions for a function $\phi : G \to M$ to lie in $Z^1(G, M)$ or to lie in $B^1(G, M)$. These maps are known as *crossed homomorphisms* and *principal crossed homomorphisms* respectively.

   (b) Suppose that the action of G on M is trivial (that is, every $g \in G$ acts as the identity on M). What is $H^1(G, M)$ in this case?

   (c) Let $G = \langle \sigma \rangle$ be a cyclic group of order n.. Check that the map $\phi \mapsto \phi(\sigma)$ induces a bijection between $\phi \in Z^1(G, M)$ and $m \in M$ satisfying $m + \sigma m + \cdots + \sigma^{n-1} m = 0$.

   (d) Let E/F be any Galois extension. Check we have proved in class that the cohomology groups $H^1(\mathrm{Gal}(E/F), E^\times)$ and $H^1(\mathrm{Gal}(E/F), E^+)$ are trivial. Here E^+ denotes E treated as an abelian group with its additive structure.

4. In this problem we will interpret $H^2(G, M)$. Let M be an abelian group and G a finite group. We will write all group operations multiplicatively. An extension of G by M is an exact sequence

$$1 \longrightarrow M \longrightarrow H \longrightarrow G \longrightarrow 1$$

   of finite groups. Thus M is a (normal) subgroup of H which is the kernel of a surjective homomorphism $\pi : H \to G$.

   (a) First we give M an action of G. Let $g \in G$ and $h \in H$ satisfy $\pi(h) = g$. We define $g \cdot m$ by hmh^{-1}. Check that this does not depend on the choice of h, and defines an action of G on M.

   (b) Let $\tau : G \to H$ be any section of π. In other words, $\pi \circ \tau$ is the identity. Check that the formula $\tau(g_1)\tau(g_2) = \phi(g_1, g_2)\tau(g_1 g_2)$ defines a map $\phi : G^2 \to M$ and that $\phi \in Z^2(G, M)$.

   (c) Show that every $\phi \in Z^2(G, M)$ arises (in this way) from an extension of G by M (with the same action of G on M).

   (d) Show that two $\phi, \phi' \in Z^2(G, M)$ arising from the same extension (by making a different choice of τ) differs by an element of $B^2(G, M)$. Hence explain why $H^2(G, M)$ "classifies" the extensions of G by M (when an action of G on M is fixed).