**Math 254B, UC Berkeley, Spring 2002 (Kedlaya)**
**The Cohomology of Finite Groups II: Concrete Nonsense**

**Reference**. Milne, II.1.

Last time, we associated to a finite group $G$ and a (right) $G$-module $M$ a sequence of abelian groups $H^i(G, M)$, called the cohomology groups of $M$. (Also called the *Galois cohomology* groups because in number theory, $G$ will invariably be the Galois group of some extension of number fields, and $A$ will be some object manufactured from this extension.) What we didn't do is make the construction at all usable in practice! This time we will remedy this.

Recall the last point from last time: if

$$0 \to M \to M_0 \to M_1 \to \cdots$$

is an acyclic resolution of $M$ (i.e., the sequence is exact, and $H^i(G, M_j) = 0$ for $i > 0$ and all $j$), then

$$H^i(G, M) = \ker(M_i^G \to M_{i+1}^G)/\operatorname{im}(M_{i-1}^G \to M_i^G).$$

Thus to compute cohomology, we are going to need an ample supply of acyclic $G$-modules. As we did for injectives, we'll get these by inducing up from the trivial group. Note that if $G$ is the trivial group, *every* $G$-module is acyclic: if $0 \to M \to I_0 \to I_1 \cdots$ is an injective resolution, taking $G$-invariants has no effect, so $0 \to I_0 \to I_1 \to \cdots$ is still exact except at $I_0$ (where we omitted $M$).

We say $M$ is an *induced* $G$-module if it has the form $\operatorname{Ind}_{\{e\}}^G N$ for some abelian group (i.e., module for the trivial group) $N$, i.e., can be written as $N \otimes_{\mathbb{Z}} \mathbb{Z}[G]$.

**Lemma 1 (Shapiro's Lemma).** *If $H$ is a subgroup of $G$ and $N$ is an $H$-module, then there is a canonical isomorphism $H^i(G, \operatorname{Ind}_H^G(N)) \to H^i(H, N)$. In particular, $N$ is an acyclic $H$-module if and only if $\operatorname{Ind}_H^G(N)$ is an acyclic $G$-module.*

*Proof.* The key points are:

(a) $\operatorname{Ind}_H^G(N)^G = N^H$, so there is an isomorphism for $i = 0$;

(b) the functor $\operatorname{Ind}_H^G$ from $H$-modules to $G$-modules is exact (that is, $\mathbb{Z}[G]$ is flat over $\mathbb{Z}[H]$, which is easy to see because it in fact is free over $\mathbb{Z}[H]$);

(c) if $I$ is an injective $H$-module, then $\operatorname{Ind}_H^G(I)$ is an injective $G$-module. (This is similar to the proof from the previous homework that there are enough injectives; or you can use the canonical isomorphism $\operatorname{Hom}_G(M, \operatorname{Ind}_H^G(I)) = \operatorname{Hom}_H(M, I)$.)

Now take an injective resolution of $N$, apply $\operatorname{Ind}_H^G$ to it, and the result is an injective resolution of $\operatorname{Ind}_H^G(N)$. $\square$

**Corollary 2.** *If $M$ is an induced $G$-module, then $M$ is acyclic.*

It is much easier to embed $M$ into an acyclic $G$-module than into an injective $G$-module. For example, let $M_0$ be the underlying abelian group of $M$, regarded as a module for the trivial group, and put $N = \mathrm{Ind}^G(M_0) = M_0 \otimes_{\mathbb{Z}} \mathbb{Z}[G]$. Then $M$ has a natural map into $N$:

$$m \mapsto \sum_{g \in G} m^g \otimes [g^{-1}].$$

The point is that

$$m^h \mapsto \sum_{g \in G} m^{hg} \otimes [g^{-1}] = \sum_{g \in G} m^g \otimes [(h^{-1}g)^{-1}] = \left( \sum_{g \in G} m^g \otimes [g^{-1}] \right) [h],$$

so the map is compatible with the $G$-actions.

Immediate consequence: if $M$ is finite, it can be embedded into a finite acyclic $G$-module. Thus $H^i(G, M)$ is finite for all $i$. (But contrary to what you might expect, for fixed $M$, the groups $H^i(G, M)$ do not necessarily become zero for $i$ large, even if $M$ is finite! We'll see explicit examples next time.)

Another consequence is the following result. (The case $i = 1$ was a homework problem.)

**Theorem 3.** *Let $L/K$ be a finite Galois extension of fields. Then $H^i(\mathrm{Gal}(L/K), L) = 0$ for $i > 0$.*

*Proof.* Put $G = \mathrm{Gal}(L/K)$. The normal basis theorem (see Lang, *Algebra* or Milne, Lemma II.1.24) states that there exists $\alpha \in L$ whose conjugates form a basis of $L$ as a $K$-vector space. This implies that $L \cong \mathrm{Ind}^G_{\{e\}} K$, so $L$ is an induced $G$-module and so is acyclic. $\square$

Now let's see an explicit way to compute group cohomology. Given a group $G$ and a $G$-module $M$, define the $G$-modules $N_i$ for $i \geq 0$ as functions $\phi : G^i \to M$, with the $G$-action

$$(\phi^g)(g_0, \dots, g_i) = \phi(g_0 g^{-1}, \dots, g_i g^{-1})^g.$$

Notice that this module is induced: any such function is determined by its values with $g_0 = e$.

Define the map $d_i : N_i \to N_{i+1}$ by

$$(d_i \phi)(g_0, \dots, g_{i+1}) = \sum_{j=0}^{i+1} (-1)^j \phi(g_0, \dots, \widehat{g_j}, \dots, g_{i+1}),$$

where the hat over $g_j$ means you omit it from the list. Then one checks that the sequence

$$0 \to M = N_0 \to N_1 \to \dots$$

is exact. Since the $N_i$ are induced, this is an acyclic resolution: thus the cohomology of the complex

$$0 \to N_0^G \to N_1^G \to \cdots$$

coincides with the cohomology groups $H^i(G, M)$. And now we have something we can actually compute! (Terminology: the elements of $N_i^G$ in the kernel of $d_i$ are called (homogeneous) $i$-cochains; the ones in the image of $d_{i-1}$ are called $i$-coboundaries.)

For example, we can give a very simple description of $H^1(G, M)$. Namely, a 1-cochain $\phi : G^2 \to M$ is determined by $\rho(g) = \phi(e, g)$ which by $G$-invariance satisfies the relation

$$\begin{aligned}
0 &= (d_1\phi)(e, h, gh) \\
&= \phi(h, gh) - \phi(e, gh) + \phi(e, h) \\
&= (\phi^h)(h, gh) - \rho(gh) + \rho(h) \\
&= \phi(e, g)^h - \rho(gh) + \rho(h) \\
&= \rho(g)^h + \rho(h) - \rho(gh).
\end{aligned}$$

It is the coboundary of a 0-cochain $\psi : G \to M$ if and only if

$$\rho(g) = \phi(e, g) = \psi(e) - \psi(g) = \psi(e) - \psi(e)^g.$$

That is, $H^1(G, M)$ is equal to crossed homomorphisms modulo principal crossed homomorphisms, consistent with the definition we gave in the section on Kummer theory.

We can also give an explicit interpretation of $H^2(G, M)$ (see Milne, example II.1.19). It classifies short exact sequences

$$1 \to M \to E \to G \to 1$$

of (not necessarily abelian) groups on which $G$ has a fixed action on $M$. (The action is given as follows: given $g \in G$ and $m \in M$, choose $h \in E$ lifting $G$; then $h^{-1}mh$ maps to the identity in $G$, so comes from $M$, and we call it $m^g$ since it depends only on $g$.) Namely, given the sequence, choose a map $s : G \to E$ (not a homomorphism) such that $s(g)$ maps to $g$ under the map $E \to G$. Then the map $\phi : G^3 \to M$ given by

$$\phi(a, b, c) = s(a)^{-1}s(ba^{-1})^{-1}s(cb^{-1})^{-1}s(ca^{-1})s(a)$$

is a 2-cocycle, and any two choices of $s$ give maps that differ by a 2-coboundary. (Truth in advertising disclosure: I may have messed up the formula. Verify before using.)

What "classifies" means precisely is that two sequences give the same element of $H^2(G, M)$ if and only if one can find an arrow $E \to E'$ making the following diagram commute:

$$\begin{tikzcd}
1 \arrow[r] & M \arrow[r] \arrow[d, "\mathrm{id}"] & E \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & M \arrow[r] & E' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

Note that two sequences may not be isomorphic under this definition even if $E$ and $E'$ are abstractly isomorphic as groups. For example, if $G = M = \mathbb{Z}/p\mathbb{Z}$ and the action is trivial, then $H^2(G, M) = \mathbb{Z}/p\mathbb{Z}$ even though there are only two possible groups $E$, namely $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

**Exercises.**

1. The set $H^2(G, M)$ has the structure of an abelian group. Describe the corresponding structure on short exact sequences $0 \to M \to E \to G \to 0$.

2. Let $G = S_3$ (the symmetric group on three letters), let $M = \mathbb{Z}^3$ with the natural $G$-action permuting the factors, and let $N = M^G$. Compute $H^i(G, M/N)$ for $i = 1, 2$ however you want. (You can explicitly compute cochains, use the alternate interpretations given above, or use the exact sequence $0 \to N \to M \to M/N \to 0$.) Optional: use more than one method and make sure that you get the same answer.

3. (Artin-Schreier) Let $L/K$ be a $\mathbb{Z}/p\mathbb{Z}$-extension of fields of characteristic $p > 0$. Prove that $L = K(\alpha)$ for some $\alpha$ such that $\alpha^p - \alpha \in K$. (Hint: consider the short exact sequence $0 \to \mathbb{F}_p \to L \to L/\mathbb{F}_p \to 0$ in which the map $L \to L/\mathbb{F}_p$ is given by $x \mapsto x^p - x$.)