Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
The Cohomology of Finite Groups I: Abstract Nonsense

Reference. Milne, II.1. See Serre, *Galois Cohomology* for a much more general presentation. (We will generalize ourselves from finite to profinite groups a bit later on.) Warning: some authors (like Milne, and Neukirch for the most part) put group actions on the left and some (like Neukirch in chapter IV, and me) put them on the right. Of course, the theory is the same either way!

Caveat. This stuff may strike some of you as being a bit dry. If so, don't worry; only a small part of the theory will be relevant for class field theory. However, it doesn't make sense to learn that small part without knowing what it is a part of!

Let G be a finite group and A an abelian group (itself not necessarily finite) with a right G-action, also known as a G-module. I'll write the G-action as a superscript, i.e., the image of the action of g on m is m^g. Alternatively, A can be viewed as a right module for the group algebra $\mathbb{Z}[G]$. A *homomorphism* of G-modules $\phi : M \to N$ is a homomorphism of abelian groups that is compatible with the G-actions: i.e., $\phi(m^g) = \phi(m)^g$. (For those keeping score, the category of G-modules is an abelian category.)

We would like to define some invariants of the pair (G, A) that we can use to get information about G and A. We will use the general methodology of homological algebra to do this. Before doing so, though, we need a few lemmas about G-modules.

If H is a subgroup of G and M is an H-module, we can "induce" a G-module from M by extending scalars: put $\operatorname{Ind}_H^G M = M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$. Explicitly, this module consists of functions $\phi : G \to M$ such that $\phi(gh) = \phi(g)^h$ for $h \in H$.

A G-module M is *injective* if for every inclusion $A \subset B$ of G-modules and every G-module homomorphism $\phi : A \to M$, there is a homomorphism $\psi : B \to M$ that extends ϕ.

Lemma 1. *Every G-module can be embedded into some injective G-module. (That is, the category of G-modules has enough injectives.)*

In particular, any G-module M admits an *injective resolution*: a complex

$$0 \to M \to I_0 \xrightarrow{d_0} I_1 \xrightarrow{d_1} I_2 \xrightarrow{d_2} \dots$$

(that is, $d_{i+1} \circ d_i = 0$ for all i) in which each I_i is injective, which is *exact*: $\operatorname{im} d_i = \ker d_{i+1}$. (Embed M into I_0, embed I_0/M into I_1, et cetera.)

Given a G-module M, let M^G be the abelian group of G-invariant elements of M:

$$M^G = \{m \in M : m^g = m \quad \forall g \in G\}.$$

The functor $M \to M^G$ from G-modules to abelian groups is left exact but not right exact: if $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then $0 \to (M')^G \to M^G \to (M'')^G$ is exact, but $M^G \to (M'')^G$ may not be exact. (Example: take the sequence $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to$

$\mathbb{Z}/p\mathbb{Z}$ of G-modules for $G = \mathbb{Z}/p\mathbb{Z}$, which acts on the middle factor by $a^g = a(1+pg)$. Then $M^G \to (M'')^G$ is the zero map but $(M'')^G$ is nonzero.)

This is the general situation addressed by homological algebra: it provides a canonical way to extend the truncated exact sequence $0 \to (M')^G \to M^G \to (M'')^G$. (Or if you prefer, it helps measure the failure of exactness of the G-invariants functor.) To do this, given M and an injective resolution as above, take G-invariants: the result

$$0 \to I_0^G \xrightarrow{d_0} I_1^G \xrightarrow{d_1} I_2^G \xrightarrow{d_2} \dots$$

is still a complex, but no longer exact. We turn this failure into success by defining the i-th cohomology group as the quotient

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

By convention, we let d_{-1} be the map $0 \to I_0^G$, so $H^0(G, M) = M^G$.

Given a homomorphism $f : M \to N$ and a injective resolution $0 \to N \to J_0 \to J_1 \to \cdots$, there exists a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "f"'] & I_0 \arrow[r, "d_0"] \arrow[d, "f_0"'] & I_1 \arrow[r, "d_1"] \arrow[d, "f_1"'] & I_2 \arrow[r, "d_2"] \arrow[d, "f_2"'] & \cdots \\
0 \arrow[r] & N \arrow[r] & J_0 \arrow[r, "d_0"] & J_1 \arrow[r, "d_1"] & J_2 \arrow[r, "d_2"] & \cdots
\end{tikzcd}$$

and likewise after taking G-invariants, so we get maps $H^i(f) : H^i(G, M) \to H^i(G, N)$.

Lemma 2. *The map $H^i(f)$ does not depend on the choice of the f_i (given the choices of injective resolutions).*

Proof. This proof is a bit of "abstract nonsense". It suffices to check that if $f = 0$, then the $H^i(f)$ are all zero regardless of what the f_i are. In that case, it turns out one can construct maps $g_i : I_{i+1} \to J_i$ (and by convention $g_{-1} = 0$) such that $f_i = g_i \circ d_i + d_{i-1} \circ g_{i-1}$. (Such a set of maps is called a *homotopy*.) Details left as an exercise. (Warning: the diagonal arrows in the diagram below don't commute!)

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "f"'] & I_0 \arrow[r, "d_0"] \arrow[d, "f_0"'] & I_1 \arrow[r, "d_1"] \arrow[d, "f_1"'] \arrow[dl, "g_0"'] & I_2 \arrow[r, "d_2"] \arrow[d, "f_2"'] \arrow[dl, "g_1"'] & \cdots \\
0 \arrow[r] & N \arrow[r] & J_0 \arrow[r, "d_0"] & J_1 \arrow[r, "d_1"] & J_2 \arrow[r, "d_2"] & \cdots
\end{tikzcd}$$

$\square$

In particular, if $M = N$ and f is the identity, we get a canonical map between $H^i(G, M)$ and $H^i(G, N)$ for each i. That is, the groups $H^i(G, M)$ are well-defined independent of the choice of the injective resolution. Likewise, the map $H^i(f)$ is also independent of the choice of resolutions.

If you know any homological algebra, you'll recognize what comes next: given a short exact sequence $0 \to M' \to M \to M'' \to 0$ of G-modules, there is a canonical long exact sequence

$$0 \to H^0(G, M') \to \cdots \to H^i(G, M'') \xrightarrow{\delta_i} H^{i+1}(G, M') \to H^{i+1}(G, M) \to H^{i+1}(G, M'') \cdots ,$$

where the δ_i are certain "connecting homomorphisms" (or "snake maps"). I won't punish you with the proof of this; if you've never seen it before, deduce it yourself from the Snake Lemma. (For the proof of the latter, engage in "diagram chasing", or see the movie *It's My Turn.* To define δ: given $x \in \ker(f_2) \subseteq M_2$, lift x to M_1, push it into N_1 by f_1, then check that the image has a preimage in N_0. Then verify that the result is well-defined, et cetera.)

Lemma 3 (Snake Lemma). *Given a commuting diagram*

$$\begin{tikzcd} 0 \arrow[r] & M_0 \arrow[r] \arrow[d, "f_0"] & M_1 \arrow[r] \arrow[d, "f_1"] & M_2 \arrow[r] \arrow[d, "f_2"] & 0 \\ 0 \arrow[r] & N_0 \arrow[r] & N_1 \arrow[r] & N_2 \arrow[r] & 0 \end{tikzcd}$$

in which the rows are exact, there is a canonical map $\delta : \ker(f_2) \to \operatorname{coker}(f_0)$ *such that the sequence*

$$0 \to \ker(f_0) \to \ker(f_1) \to \ker(f_2) \xrightarrow{\delta} \operatorname{coker}(f_0) \to \operatorname{coker}(f_1) \to \operatorname{coker}(f_2) \to 0$$

is exact.

One important consequence of the long exact sequence is that if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of G-modules and $H^1(G, M'') = 0$, then $0 \to (M')^G \to M^G \to (M'')^G \to 0$ is also exact.

More abstract nonsense:

- If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of G-modules and $H^i(G, M) = 0$ for all $i > 0$, then the connecting homomorphisms in the long exact sequence induce isomorphisms $H^i(G, M'') \to H^{i+1}(G, M')$ for all $i \geq 0$. This sometimes allows one to prove general facts by proving them first for H^0, where they have a direct interpretation, then "dimension shifting".

- If M is an injective G-module, then $H^i(G, M) = 0$ for all $i > 0$. (Use $0 \to M \to M \to 0 \to \cdots$ as an injective resolution.) This fact has a sort of converse: see next bullet.

- We say M is *acyclic* if $H^i(G, M) = 0$ for all $i > 0$; so in particular, injective G-modules are acyclic. If $0 \to M \to M_0 \to M_1 \cdots$ is an exact sequence of G-modules, and each M_i is acyclic, then the cohomology groups of the complex $0 \to M_0^G \to M_1^G \to \cdots$ coincide with $H^i(G, M)$. That is, we can replace the injective resolution in the definition by an acyclic resolution for the purposes of doing a computation. Proof: see exercises.

Of course, the abstract nature of the proofs so far gives us almost no insight into what the objects are that we've just constructed. We'll remedy that next time by giving more concrete descriptions that one can actually compute with.

Exercises.

1. Let G be the one-element group. Show that a G-module (i.e., abelian group) is injective if and only if it is divisible, i.e., the map $x \mapsto nx$ is surjective for any nonzero integer n. (Hint: you'll need Zorn's lemma or equivalent in one direction.)

2. Let A be an abelian group, regarded as a G-module for G the trivial group. Prove that A can be embedded in an injective G-module. (Hint: embed each cyclic subgroup of A in an injective, then take the product.)

3. Prove Lemma 1. (Hint: let H be the one-element group. Show that if M is any G-module and N is an injective H-module containing M, then $\operatorname{Ind}_H^G N$ is an injective G-module containing N.)

4. Prove Lemma 3, following the sketch given. (Hint: construct g_i given f_{i-1} and g_{i-1}, using that the J's are injective G-modules.)

5. Prove the last bullet above. (Hint: construct the canonical long exact sequence from the exact sequence $0 \to M \to M_0 \to \ker(M_1 \to M_2) \to 0$; use it to do dimension shifting.)