Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
Homology of Finite Groups

Reference. Milne, II.2; for cyclic groups, also Neukirch, IV.7 and Lang, IX.1.

Caveat. The Galois cohomology groups used in Neukirch are not the ones we defined earlier. They are the Tate cohomology groups we are going to define below.

Leftover reinterpretation from last time (or, fun with H^1).

I should have mentioned when we were discussing H^1 that it can be interpreted in terms of "principal homogeneous spaces", an interpretation that naturally comes up in practice fairly often. Namely, let G be a finite group and M a G-module. Then the elements of $H^1(G, M)$ correspond to sets A with both a G-action and an M-action, subject to the following restrictions:

(a) for any a, the map $M \to M$ given by $m \mapsto m(a)$ is a bijection;

(b) for $a \in A$, $g \in G$ and $m \in M$, $m(a)^g = m^g(a)$ (i.e., the G-action and M-action commute).

(The trivial example is $A = M$ with the same G-action, and M acting by translation: $m(a) = m + a$.) In particular, there is a well-defined "subtraction" map $A \times A \to M$ sending (a, b) to the element m of M such that $m(a) = b$. The correspondence is as follows: given such a set A, pick $a \in A$, take the map $\rho : G \to M$ given by $\rho(g) = a^g - a$, and let ϕ be the 1-cocycle with $\phi(e, g) = \rho(g)$. Details left to the reader.

This comes up, for example, in the theory of elliptic curves. If L is a finite extension of K and E is an elliptic curve over E, then $H^1(\mathrm{Gal}(L/K), E(\overline{K}))$ is the set of K-isomorphism classes of curves whose Jacobians are K-isomorphic to E (but which might not themselves be isomorphic to E by virtue of not having a K-rational point).

Another example from elliptic curves: $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(E))$ parametrizes twists of E, elliptic curves defined over K which are L-isomorphic to E. (E.g., $y^2 = x^3 + x + 1$ versus $2y^2 = x^3 + x + 1$, with $L = \mathbb{Q}(\sqrt{2})$.) See Silverman, *The Arithmetic of Elliptic Curves*, especially Chapter X, for all this and more fun with H^1, including the infamous "Selmer group" and "Tate-Shafarevich group".

Homology.

You may not be surprised to learn that there is a "dual" theory to the theory of group cohomology, namely group homology. What you may be surprised to learn is that one can actually fit the two together, so that in a sense the homology groups become cohomology groups with negative indices. (Since the arguments are similar to those for cohomology, I'm going to skip details.)

Let M_G denote the maximal quotient of M on which G acts trivially. In other words, M_G is the quotient of M by the submodule spanned by $m^g - m$ for all $m \in M$ and $g \in G$. In yet other words, $M_G = M/MI_G$, where I_G is the *augmentation ideal* of the group algebra

$\mathbb{Z}[G]$:

$$I_G = \{\sum_{g \in G} z_g[g] : \sum_g z_g = 0\}.$$

Or if you like, $M_G = M \otimes_{\mathbb{Z}[G]} \mathbb{Z}$. Since M^G is the group of G-invariants, we call M_G the group of G-coinvariants.

The functor $M \to M^G$ is right exact but not left exact: if $0 \to M' \to M \to M'' \to 0$, then $M'_G \to M_G \to M''_G \to 0$ is exact but the map on the left is not injective. Again, we can fill in the exact sequence by defining homology groups.

A G-module M is *projective* if for any surjection $N \to N'$ of G-modules and any map $\phi : M \to N'$, there exists a map $\psi : M \to N$ lifting ϕ. This is the reverse notion to injective; but it's much easier to find projectives than injectives. For example, any G-module which is a free module over the ring $\mathbb{Z}[G]$ is projective, e.g., $\mathbb{Z}[G]$ itself!

Given a projective resolution $\cdots \to P_1 \to P_0 \to M \to 0$ of a G-module M (an exact sequence in which the P_i are injective), take coinvariants to get a no longer exact complex

$$\cdots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \to 0,$$

then put $H_i(G, M) = \ker(d_{i-1})/\operatorname{im}(d_i)$. Again, this is canonically independent of the resolution and functorial, and there is a long exact sequence which starts out

$$\cdots \to H_1(G, M'') \to\xrightarrow{\delta} H_0(G, M') \to H_0(G, M) \to H_0(G, M'') \to 0.$$

Also, you can replace the projective resolution by an acyclic resolution (where here M being acyclic means $H_i(G, M) = 0$ for $i > 0$) and get the same homology groups. But since free modules are projective, this is rarely useful.

One can give a concrete description of homology as well, but we won't need it for our purposes. Even without one, though, we can calculate $H_1(G, \mathbb{Z})$, using the exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

By the long exact sequence in homology,

$$0 = H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G])$$

is exact, i.e. $0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G$ is exact. The last map is induced by $I_G \hookrightarrow \mathbb{Z}[G]$ and so is the zero map. Thus $H_1(G, \mathbb{Z}) \cong I_G/I_G^2$, which on a previous homework we showed was isomorphic to G^{ab}.

The Tate groups.

We now "fit together" the long exact sequences of cohomology and homology to get a doubly infinite exact sequence. Define the map $\mathrm{Norm}_G : M \to M$ by

$$\mathrm{Norm}_G(m) = \sum_{g \in G} m^g.$$

(It looks like it should be called "trace", but in practice our modules M will be groups which are most naturally written multiplicatively, i.e., the nonzero elements of a field.) Then Norm_G induces a homomorphism

$$\mathrm{Norm}_G : H_0(M, G) = M_G \to M^G = H^0(M, G).$$

Now define

$$H_T^i = \begin{cases} H^i(G, M) & i > 0 \\ M^G / \mathrm{Norm}_G(M) & i = 0 \\ \ker(\mathrm{Norm}_G)/MI_G & i = -1 \\ H_{-i-1}(G, M) & i < -1; \end{cases}$$

then for any short exact sequence $0 \to M' \to M \to M'' \to 0$, we get an exact sequence

$$\cdots \to H_T^{i-1}(G, M'') \to H_T^i(G, M') \to H_T^i(G, M) \to H_T^i(G, M'') \to H_T^{i+1}(G, M') \to \cdots$$

which extends infinitely in both directions. (The T stands for Tate, who had a major part in introducing Galois cohomology into algebraic number theory.)

Finite cyclic groups.

In general, for any given G and M, it is at worst a tedious exercise to compute $H_T^i(G, M)$ for any single value of i, but try to compute all of these at once and you discover that they exhibit very little obvious structure. Thankfully, there is an exception to that dreary rule when G is cyclic.

Theorem 1. *Let G be a finite cyclic group and M a G-module. Then there is a canonical, functorial isomorphism $H_T^i(G, M) \to H_T^{i+2}(G, M)$ for all $i \in \mathbb{Z}$.*

Proof. Choose a generator g of G. We start with the four-term exact sequence of G-modules

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

in which the first map is $1 \mapsto [1]$, the second map is $[h] \mapsto [hg] - [h]$, and the third map is $[h] \mapsto 1$. Since everything in sight is a free abelian group, we can tensor over $\mathbb{Z}$ with M and get another exact sequence:

$$0 \to M \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to M \to 0.$$

The terms in the middle are just $\mathrm{Ind}_{\{e\}}^G(M)$, where we first restrict M to a module for the trivial group and then induce back up. Thus their Tate groups are all zero. The desired result now follows from the following general fact: if

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \to 0$$

is exact and B and C have all Tate groups zero, then there is a canonical isomorphism $H_T^{i+2}(G, A) \to H_T^i(G, D)$. To see this, apply the long exact sequence to the short exact sequences

$$0 \to A \to B \to B/\operatorname{im}(f) \to 0$$
$$0 \to B/\ker(g) \to C \to D \to 0$$

to get

$$H^{i+2}(G, A) \cong H^{i+1}(G, B/\operatorname{im}(f)) = H^{i+1}(G, B/\ker(g)) \cong H^i(G, D).$$

□

In particular, the long exact sequence of a short exact sequence $0 \to M' \to M \to M'' \to 0$ of G-modules curls up into an exact hexagon:

$$\begin{tikzcd}
 & H_T^{-1}(G, M) \arrow[r] & H_T^{-1}(G, M'') \arrow[dr] & \\
H_T^{-1}(G, M') \arrow[ur] & & & H_T^0(G, M') \arrow[dl] \\
 & H_T^0(G, M'') \arrow[ul] & H_T^0(G, M) \arrow[l] &
\end{tikzcd}$$

If the groups $H_T^i(G, M)$ are finite, we define the *Herbrand quotient*

$$h(M) = \#H_T^0(G, M)/\#H_T^{-1}(G, M).$$

Then from the exactness of the hexagon, if M', M, M'' all have Herbrand quotients, then

$$h(M) = h(M')h(M'').$$

Moreover, if two of M', M, M'' have Herbrand quotients, so does the third. For example, if M' and M'' have Herbrand quotients, i.e., their Tate groups are finite, then we have an exact sequence

$$H_T^{-1}(G, M') \to H_T^{-1}(G, M) \to H^{-1}(G, M'')$$

and the outer groups are all finite. In particular, the first map is out of a finite group and so has finite image, and modulo that image, $H_T^{-1}(G, M)$ injects into another finite group. So it's also finite, and so on.

In practice, it will often be much easier to compute the Herbrand quotient of a G-module than to compute either of its Tate groups directly. The Herbrand quotient will then do "half the work for free"; once one group is computed directly, at least the order of the other will be automatically known.

One special case is easy to work out: if M is finite, then $h(M) = 1$, because the sequences

$$0 \to M^G \to M \to M \to M_G \to 0$$
$$0 \to H_T^{-1}(G, M) \to M_G \overset{\mathrm{Norm}_G}{\to} M^G \to H_T^0(G, M) \to 0$$

are exact, where $M \to M$ is the map $m \mapsto m^g - m$, so M_G and M^G have the same order, as do H^{-1} and H^0.

Extended functoriality.

We already saw that if we have a homomorphism of G-modules, we get induced homomorphisms on homology and cohomology, and thus also on the Tate groups. But what if we want to relate G-modules for different groups G, as will happen in our study of class field theory? It turns out that in a suitable sense, the Tate groups are also functorial with respect to changing groups.

Let M be a G-module and M' a G'-module. Suppose we are given a homomorphism $\alpha : G' \to G$ of groups and a homomorphism $\beta : M \to M'$ of abelian groups (note that they go in opposite directions!). We say these are *compatible* if $\beta(m^{\alpha(g)}) = \beta(m)^g$ for all $g \in G$ and $m \in M$. In this case, one gets canonical homomorphisms $H^i(G, M) \to H^i(G', M')$, $H_i(G, M) \to H_i(G', M')$ (construct them on pairs of injective/projective resolutions, then show that any two choices are homotopic), and $H^i_T(G, M) \to H^i_T(G, M)$. The principal examples are as follows. (For the rest of this section I write $H(G, M)$ to mean either a cohomology group, a homology group, or a Tate group of some index. If there are more than one such group in a display, they all have the same type and index.)

(a) If H is a subgroup of G, M is an H-module, and $M' = \mathrm{Ind}_H^G(M) = M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$, then we have a map $M' \to M$ in which $m \otimes g \mapsto m^g$. The resulting homomorphisms

$$H(G, \mathrm{Ind}_H^G(M)) \to H(H, M)$$

are all isomorphisms; this was Shapiro's Lemma for cohomology, and it also holds for homology and Tate groups.

(b) If H is a subgroup of G, M is a G-module, and M' is just M with all but the H-action forgotten, we get the *restriction homomorphisms*

$$\mathrm{Res} : H(G, M) \to H(H, M).$$

Another way to get the same map: use the homomorphism of G-modules $M \to \mathrm{Ind}_H^G(M)$ sending m to $\sum_i m \otimes g_i$, where g_i runs over a set of right coset representatives of H in G, then apply Shapiro's Lemma to get

$$H(G, M) \to H(G, \mathrm{Ind}_H^G(M)) \xrightarrow{\sim} H(H, M).$$

(c) If H is a *normal* subgroup of G, let α be the surjection $G \to G/H$, and let β be the injection $M^H \hookrightarrow M$. Note that G/H acts on M^H; in this case, we get the *inflation homomorphisms*

$$\mathrm{Inf} : H(G/H, M^H) \to H(G, M).$$

(d) I pointed out in class earlier that homology and cohomology groups don't seem to carry a nontrivial G-action, because you compute them by taking invariants and coinvariants.

This can be reinterpreted in terms of extended functoriality: let $\alpha : G \to G$ be the conjugation by some fixed h: $g \mapsto h^{-1}gh$, and let $\beta : M \to M$ be the map $m \mapsto m^h$. Then the induced homomorphisms $H(G, M) \to H(G, M)$ are all the identity map.

(e) If M is a G-module and H is a subgroup of G, then there is a canonical G-module homomorphism $M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G] = \mathrm{Ind}_H^G(M) \to M$ sending $m \otimes g$ to m^g. (Note: we first restrict M to be an H-module, then induce it back up.) This gives maps $H(G, \mathrm{Ind}_H^G(M)) \to H(G, M)$, which together with the isomorphisms of Shapiro's lemma gives what are called the *corestriction homomorphisms*:

$$\mathrm{Cor} : H(H, M) \xrightarrow{\sim} H(G, \mathrm{Ind}_H^G(M)) \to H(G, M).$$

(f) The composition $\mathrm{Cor} \circ \mathrm{Res}$ is induced by the homomorphism of G-modules $M \to \mathrm{Ind}_H^G(M) \to M$ given by

$$m \mapsto \sum_i m \otimes g_i \to \sum_i m = [G : H]m.$$

Thus $\mathrm{Cor} \circ \mathrm{Res}$ acts as multiplication by $[G : H]$ on each (co)homology group. Bonus consequence: taking H to be the trivial group, then the group in the middle is isomorphic to $H(H, M) = 0$. So every (co)homology group for G is killed by $\#G$, and in particular is a torsion group. In fact, if M is finitely generated as an abelian group, this means $H(G, M)$ is always finite, because each of these will be finitely generated and torsion. (Of course, this won't happen in many of our favorite examples, e.g., $H(\mathrm{Gal}(L/K), L^*)$ for L and K fields.)

Exercises.

1. The periodicity of the Tate groups for G cyclic means that there is a canonical isomorphism between $H_T^{-1}(G, M)$ and $H_T^1(G, M)$, i.e., between $\ker(\mathrm{Norm}_G)/MI_G$ and the set of equivalence classes of 1-cocycles. What is this isomorphism explicitly? I.e, given an element of $\ker(\mathrm{Norm}_G)/MI_G$, what is the corresponding 1-cocycle?

2. Put $K = \mathbb{Q}_p(\sqrt{p})$. Compute the Herbrand quotient of K^* as a G-module for $G = \mathrm{Gal}(\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p)$. (Hint: use the exact sequence $1 \to \mathfrak{o}_K^* \to K^* \to \mathbb{Z} \to 1$.)

3. Show that $\mathrm{Res} : H_T^{-2}(G, \mathbb{Z}) \to H_T^{-2}(H, \mathbb{Z})$ corresponds to the transfer (Verlagerung) map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.