LECTURE 7

Chain Complexes and Herbrand Quotients

Last time, we defined the Tate cohomology groups $\hat{H}^0(G, M)$ and $\hat{H}^1(G, M)$ for cyclic groups. Recall that if $G = \mathbb{Z}/n\mathbb{Z}$ with generator σ, then a G-module is an abelian group M with an automorphism $\sigma\colon M \xrightarrow{\sim} M$ such that $\sigma^n = \mathrm{id}_M$. Our main example is when L/K is an extension of fields with $\mathrm{Gal}(L/K) = G$, so that both L and $L^\times$ are G-modules. Then

$$\hat{H}^0(G, M) := M^G/\mathrm{N}(M) = \mathrm{Ker}(1-\sigma)\Big/\Big\{\sum_{i=0}^{n-1}\sigma^i m : m \in M\Big\}$$

$$\hat{H}^1(G, M) := \mathrm{Ker}(\mathrm{N})/(1-\sigma),$$

since an element of $\mathrm{Ker}(1-\sigma)$ is fixed under the action of σ, hence under the action of G. Our goal was to compute, in the example given above, that $\#\hat{H}^0 = n$, using long exact sequences.

We saw that if

$$0 \to M \to E \to N \to 0$$

was a short exact sequence of G-modules (that is, M, E, and N are abelian groups equipped with an order-n automorphism compatible with these maps, and $N = E/M$, so that M is fixed under the automorphism of N), then we had a long exact sequence

$$\hat{H}^0(G, M) \to \hat{H}^0(G, E) \to \hat{H}^0(G, N) \xrightarrow{\delta} \hat{H}^1(G, M) \to \hat{H}^1(G, E) \to \hat{H}^1(G, N),$$

where the boundary map δ lifts $x \in \hat{H}^0(N) = N^G/\mathrm{N}(N)$ to $\tilde{x} \in E$, so that $(1-\sigma)\tilde{x} \in \mathrm{Ker}(\mathrm{N}) \subseteq M$, giving a class in $\hat{H}^1(G, M)$.

Now, define a second boundary map

(7.1)

$$\hat{H}^1(G, M) \to \hat{H}^1(G, E) \to \hat{H}^1(G, N) \xrightarrow{\partial} \hat{H}^0(G, M) \to \hat{H}^0(G, E) \to \hat{H}^0(G, N),$$

which lifts $x \in \hat{H}^1(G, N)$ to an element $\tilde{x} \in E$. Then $\mathrm{N}(\tilde{x}) = \sum_{i=0}^{n-1}\sigma^i\tilde{x} \in M^G$, since it is killed by $1-\sigma$, and so it defines a class in $\hat{H}^0(G, M)$. We check the following:

Claim 7.1. *The boundary map ∂ is well-defined.*

Proof. If $\tilde{\tilde{x}}$ is another lift of x, then $\tilde{x} - \tilde{\tilde{x}} \in M$ since $N = E/M$, and therefore $\sum_{i=0}^{n-1}\sigma^i(\tilde{x} - \tilde{\tilde{x}}) \in \mathrm{N}(M)$ is killed in $\hat{H}^0(G, M)$. □

Claim 7.2. *The sequence in (7.1) is exact.*

Proof. If $x \in \hat{H}^1(G, E)$, then $\mathrm{N}(x) = 0$, so $\partial(x) = 0$ in $\hat{H}^0(G, M)$. If $x \in \mathrm{Ker}(\partial)$, then $N(\tilde{x}) = 0$ for some lift $\tilde{x} \in E$ of x, and x is the image of $\tilde{x}$.

If $x \in \hat{H}^1(G,N)$ with lift $\tilde{x} \in E$, then $\partial(x) = \mathrm{N}(\tilde{x})$ is zero in $\hat{H}^0(G,E)$ by definition. If $x \in \hat{H}^0(G,M)$ is 0 in $\hat{H}^0(G,E)$, then $x \in \mathrm{N}(E)$, hence $x \in \mathrm{Im}(\partial)$. ☐

Thus, we obtain a "2-periodic" exact sequence for Tate cohomology of cyclic groups, motivating the following definition:

DEFINITION 7.3. For each $i \in \mathbb{Z}$ (both positive and negative), define

$$\hat{H}^i(G,M) := \begin{cases} \hat{H}^0(G,M) & \text{if } i \equiv 0 \bmod 2, \\ \hat{H}^1(G,M) & \text{if } i \equiv 1 \bmod 2. \end{cases}$$

This nice property does not hold for non-cyclic groups, so we will often attempt to reduce cohomology to the case of cyclic groups.

As a reformulation, write

$$\cdots \xrightarrow{\sum_{i=0}^{n-1}\sigma^i} M \xrightarrow{1-\sigma} M \xrightarrow{\sum_{i=0}^{n-1}\sigma^i} M \xrightarrow{1-\sigma} \cdots, \tag{7.2}$$

and observe that this forms what we will call a chain complex:

DEFINITION 7.4. A *chain complex* $X^\bullet$ is a sequence

$$\cdots \xrightarrow{d^{-2}} X^{-1} \xrightarrow{d^{-1}} X^0 \xrightarrow{d^0} X^1 \xrightarrow{d^1} X^2 \xrightarrow{d^2} \cdots,$$

such that $d^{i+1}d^i = 0$ for all $i \in \mathbb{Z}$ (that is, $\mathrm{Ker}(d^{i+1}) \supset \mathrm{Ker}(d^i)$, but we need not have equality as for an exact sequence). Then define the *ith cohomology* of $X^\bullet$ as

$$H^i(X^\bullet) := \mathrm{Ker}(d^i)/\,\mathrm{Im}(d^{i-1}).$$

Thus, a long exact sequence is a type of chain complex. We note that (7.2) satisfies this definition as

$$(1-\sigma)\sum_{i=0}^{n-1}\sigma^i x = \sum_{i=0}^{n-1}\sigma^i x - \sum_{i=0}^{n-1}\sigma^{i+1}x = \mathrm{N}x - \mathrm{N}x = 0$$

and the two maps clearly commute. The Tate cohomology groups are then the cohomologies of this chain complex, which makes it clear that they are 2-periodic.

DEFINITION 7.5. The *Herbrand quotient* or *Euler characteristic* of a G-module M is

$$\chi(M) := \frac{\#\hat{H}^0(G,M)}{\#\hat{H}^1(G,M)},$$

which is only defined when both are finite.

This definition generalizes our previous discussion of the trivial G-module, as $\hat{H}^0(G,M) = M/n$ and $\hat{H}^1(G,M) = M[n]$, though note that the boundary maps from even to odd cohomologies will be zero.

LEMMA 7.6. *Let*

$$0 \to M \to E \to N \to 0$$

be a short exact sequence of G-modules. If χ is defined for two of the three G-modules, then it is defined for all three, in which case $\chi(M)\cdot\chi(N) = \chi(E)$.

PROOF. Construct a long exact sequence

$$0 \to \mathrm{Ker}(\alpha) \to \hat{H}^0(M) \xrightarrow{\alpha} \hat{H}^0(E) \to \hat{H}^0(N) \to$$
$$\xrightarrow{\delta} \hat{H}^1(M) \to \hat{H}^1(E) \xrightarrow{\beta} \hat{H}^1(N) \to \mathrm{Coker}(\beta) \to 0.$$

Since the second boundary map yields an exact sequence

$$\hat{H}^1(E) \xrightarrow{\beta} \hat{H}^1(N) \xrightarrow{\partial} \hat{H}^0(M) \xrightarrow{\alpha} \hat{H}^0(E),$$

we have

$$\operatorname{Ker}(\alpha) = \operatorname{Im}(\partial) = \hat{H}^1(N)/\operatorname{Ker}(\partial) = \hat{H}^1(N)/\operatorname{Im}(\beta) = \operatorname{Coker}(\beta).$$

Applying Lemma 6.4 and canceling $\#\operatorname{Ker}(\alpha)$ and $\#\operatorname{Coker}(\beta)$ then yields the desired result (as for Lemma 6.7). □

A quick digression about finiteness:

Claim 7.7. *The groups $\hat{H}^0(G,M)$ and $\hat{H}^1(G,M)$ are n-torsion.*

Proof. Let $x \in M^G$. Then $\mathrm{N}(x) = \sum_{i=0}^{n-1} \sigma^i x = \sum_{i=0}^{n-1} x = nx$. Thus, $nx \in N(M)$, and $\hat{H}^0(G,M)$ is n-torsion. Now let $x \in \operatorname{Ker}(\mathrm{N})$. Then

$$nx = nx - \mathrm{N}x = \sum_{i=1}^{n} (1-\sigma^i)x = (1-\sigma)\sum_{i=1}^{n}(1+\cdots+\sigma^{i-1})x,$$

hence $nx \in (1-\sigma)M$, and $\hat{H}^1(G,M)$ is n-torsion as well. □

Thus, finite generation of $\hat{H}^0(G,M)$ and $\hat{H}^1(G,M)$ implies finiteness. Now, we recall that our goal was to show that $\#\hat{H}^0(L^\times) = n$ for a cyclic degree-n extension of local fields L/K. We have the following refined claims:

Claim 7.8. *Preserving the setup above,*

(1) $\hat{H}^1(L^\times) = 0$ *(implying* $\chi(L^\times) = \#\hat{H}^0(L^\times)$*);*
(2) $\chi(\mathcal{O}_L^\times) = 1$*;*
(3) $\chi(L^\times) = n$*.*

Proof. We first show that (2) implies (3). We have an exact sequence

$$1 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v} \mathbb{Z} \to 0,$$

where v denotes the valuation. Then by Lemma 7.6, we have

$$\chi(L^\times) = \chi(\mathcal{O}_L^\times)\cdot\chi(\mathbb{Z}) = 1\cdot n = n$$

by (2), where we note that

$$\hat{H}^0(\mathbb{Z}) = \mathbb{Z}^G/\mathrm{N}\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \quad \text{and} \quad \hat{H}^1(\mathbb{Z}) = \operatorname{Ker}(\mathrm{N})/(1-\sigma) = 0.$$

We now show (2).

Lemma 7.9. *If M is a finite G-module, then $\chi(M) = 1$.*

Proof. We have exact sequences

$$0 \to M^G \to M \xrightarrow{1-\sigma} \operatorname{Ker}(\mathrm{N}) \to \hat{H}^1(G,M) \to 0,$$

$$0 \to \operatorname{Ker}(\mathrm{N}) \to M \xrightarrow{\sum_{i=0}^{n-1}\sigma^i} M^G \to \hat{H}^0(G,M) \to 0,$$

hence by Lemma 7.6,

$$\#\operatorname{Ker}(\mathrm{N})\cdot\#M^G = \#M\cdot\#\hat{H}^0(G,M),$$
$$\#M^G\cdot\#\operatorname{Ker}(\mathrm{N}) = \#M\cdot\#\hat{H}^1(G,M),$$

and so $\#\hat{H}^0(G,M) = \#\hat{H}^1(G,M)$ and $\chi(M) = 1$ as desired. □

The analogous statement is $\chi(\mathcal{O}_L) = 1$, where we regard $\mathcal{O}_L$ as an additive group. In fact, an even easier statement to establish is $\chi(L) = 1$. Intuitively, this is because since we are working over the p-adic numbers, everything must be a $\mathbb{Q}$-vector space, hence n is invertible; but our cohomology groups are all n-torsion by Claim 7.7, hence our cohomology groups must both vanish and $\chi(L) = 1$.

By the normal basis theorem, if L/K is a finite Galois extension, we have

$$L \simeq \prod_{g \in G} K = K[G]$$

as a $K[G]$-module, where G acts by permuting coordinates. This is because the action of K (by homothety, as L is a K-vector space) commutes with the action of G (which acts on L as a K-vector space), hence we have a $K[G]$-action on L.

CLAIM 7.10. *Let A be any abelian group, and $A[G] := \prod_{g \in G} A$ be a G-module where G acts by permuting coordinates. If G is cyclic, then*

$$\hat{H}^0(G, A[G]) = \hat{H}^1(G, A[G]) = 0.$$

PROOF. We reformulate the claim as follows: let R be a commutative ring, so that $R[G]$ is an (possibly non-commutative) R-algebra via the multiplicative operation

$$\left(\sum_{g \in G} x_g[g]\right)\left(\sum_{h \in G} y_h[h]\right) := \sum_{g,h \in G} x_g y_h [gh],$$

where we have let $[h] \in \prod_{g \in G} R$ denote the element that is 1 in the h-coordinate, and 0 otherwise. Thus, $R[G]$-modules are equivalent to R-modules equipped with a homomorphism $G \to \mathrm{Aut}_R(M)$. In particular, $\mathbb{Z}[G]$-modules are equivalent to G-modules.

Now, we have $\hat{H}^0(G, A[G]) = A[G]^G/\mathrm{N}$, where $A[G]^G$ is equivalent to a diagonally embedded $A \subset \prod_{g \in G} A$, and $\mathrm{N}((a, 0, \dots, 0)) = \sum_{g \in G} a[g]$ which is equal to the diagonal embedding of A, hence $\hat{H}^0(G, A[G]) = 0$.

Similarly, $\hat{H}^1(G, A[G]) = \mathrm{Ker}(\mathrm{N})/(1 = \sigma)$, and

$$A[G] \supseteq \mathrm{Ker}(\mathrm{N}) = \left\{ \sum_{g \in G} a_g[g] \in A[G] : \sum_{g \in G} a_g = 0 \right\}.$$

Now, we may write a general element as $\sum_{i=0}^{n-1} a_i[\sigma^i]$, and choose b_i such that $(1 - \sigma^{n-i})a_i = (1 - \sigma)b_i$ for each i. Then

$$(1-\sigma)\sum_{i=0}^{n-1} b_i[\sigma^i] = \sum_{i=0}^{n-1}(1-\sigma^{n-i})a_i[\sigma^i] = \sum_{i=0}^{n-1} a_i[\sigma^i] - \sum_{i=0}^{n-1} a_i[1] = \sum_{i=0}^{n-1} a_i[\sigma^i],$$

hence $\mathrm{Ker}(\mathrm{N}) \subset (1 - \sigma)A[G]$, and therefore $\hat{H}^1(G, A[G]) = 0$ as desired. □

Thus, we see that we cannot obtain interesting Tate cohomology in this manner. Now we return to showing $\chi(\mathcal{O}_L) = 1$. The problem is that the normal basis theorem does not apply as for L, that is, whereas $L = K[G]$, we do not necessarily have $\mathcal{O}_L \simeq \mathcal{O}_K[G]$.

However, there does exist an open subgroup of $\mathcal{O}_L$ with a normal basis. Choose a normal basis $\{e_1, \dots, e_n\}$ of L/K. For large enough N, we have $\pi^N e_1, \dots, \pi^N e_n \in$

$\mathcal{O}_L$, where π is a uniformizer of L, hence they freely span some open subgroup of $\mathcal{O}_L$. Because this subgroup, call it Γ, is finite index, we have

$$\chi(\mathcal{O}_K) = \chi(\Gamma) = \chi(\mathcal{O}_K[G]) = 1$$

by (6.2).

To show that $\chi(\mathcal{O}_L^\times) = 1$ (a more complete proof will be provided in the following lecture), observe that $\mathcal{O}_L^\times \supseteq \Gamma \simeq \mathcal{O}_L^+$ via G-equivalence, where Γ is an open subgroup (the proof of this fact uses the p-adic exponential). Then $\chi(\mathcal{O}_L^\times) = \chi(\Gamma) = 1$, as desired. □

REMARK 7.11. In this course, all rings and modules are assumed to be unital.

18.786 Number Theory II: Class Field Theory
Spring 2016