LECTURE 9

Hilbert's Theorem 90 and Cochain Complexes

As always, $G = \mathbb{Z}/n\mathbb{Z}$ and L/K is a Galois extension of local fields with $\mathrm{Gal}(L/K) = G$ and generator $\sigma \in G$. In the last lecture, we showed:

THEOREM 9.1. *$\chi(L^\times) = n$, where χ denotes the Herbrand quotient.*

Note that our methods actually generalize easily to the non-archimedean case. In this lecture, we will show:

THEOREM 9.2 (Hilbert's Theorem 90). $\hat{H}^1(G, K^\times) = 0$.

Together, these imply that $\hat{H}^0(G, L^\times) = K^\times/\mathrm{N}(L^\times)$ has cardinality n. Another corollary of Hilbert's Theorem 90 is that if L and K are finite fields, then $\hat{H}^i(G, L^\times) = 0$ for all i, because $\chi(L^\times) = 1$ as L is finite (so all cohomologies vanish by periodicity). This is similar to the first result in [**Wei74**]. Explicitly, we have

$$\hat{H}^1(G, L^\times) = \mathrm{Ker}(\mathrm{N}\colon L^\times \to K^\times)/\{y/\sigma y : y \in L^\times\},$$

where each element $y/\sigma y$ has norm 1 as $y/\sigma y \cdot \sigma y/\sigma^2 y \cdots \sigma^{n-1} y/\sigma^n y = 1$. Then Hilbert's Theorem 90 implies the following:

COROLLARY 9.3. *If L/K is a cyclic extension, and $x \in L^\times$ with $\mathrm{N}(x) = 1$, then $x = y/\sigma y$ for some $y \in L^\times$.*

EXAMPLE 9.4. Let $L := \mathbb{Q}(i)$ and $K := \mathbb{Q}$. Choose $x \in \mathbb{Q}(i)$ with $\mathrm{N}(x) = 1$. Then $x = a/c + (b/c)i$ for some $a, b, c \in \mathbb{Z}$ satisfying $a^2 + b^2 = c^2$. Then Hilbert's Theorem 90 yields the usual parametrization of Pythagorean triples, $(r - s)^2 + (2rs)^2 = (r + s)^2$.

For $n = 2$, the proof is simple. We have $\mathrm{N}(x) = x \cdot \sigma x = 1$, so if we let $y := x + 1$ when $x \neq -1$, then $x \cdot \sigma y = x(\sigma x + 1) = \mathrm{N}(x) + x = 1 + x = y$, hence $x = y/\sigma y$ as desired. If $x = -1$, then let $y := \sqrt{d}$, where $L = K(\sqrt{d})$, then again we have $y/\sigma y = \sqrt{d}/(-\sqrt{d}) = -1 = x$. Note that this completes the proof that $\#(K^\times/\mathrm{N}L^\times) = 2$ for a quadratic extension L/K of local fields, and thus of the good properties of Hilbert symbols! Indeed, recall that, for a field $L := K(\sqrt{a})$ with $a \in K^\times$ but not a square, then $(a, b) = 1$ if and only if $b \in \mathrm{N}(L^\times)$.

We now move on to the general case of Hilbert's Theorem 90. Here's the main lemma:

LEMMA 9.5. *For each $x \in L$, let*

$$H_x\colon L \to L, \quad y \mapsto x \cdot \sigma(y),$$

which is a linear map of K-vector spaces. Then the characteristic polynomial of H_x is $t^n - \mathrm{N}(x) \in K[t]$, where we have normalized the definition of the characteristic polynomial to be monic.

Note that this characteristic polynomial is simpler than that of $y \mapsto xy$, which will have a nonzero multiple of t^{n-1} as long as the $\mathrm{T}(x) \neq 0$, which will occur when the trace is nondegenerate (which is true of any separable extension).

PROOF ($9.5 \Longrightarrow 9.2$). Let $x \in L$, and assume $\mathrm{N}(x) = 1$. Then the characteristic polynomial of $\hat{H}_x$ is $t^n - 1$, implying 1 is a root and hence an eigenvalue of H_x. Thus, $\mathrm{Ker}((H_x - 1) \otimes_K \overline{K}) \neq 0$, so since for fields tensor products commute with taking kernels, we have $\mathrm{Ker}(H_x - 1) \neq 0$. Thus, there exists some $y \in L^\times$ such that $H_x(y) = x \cdot \sigma(y) = y$, that is, $x = y/\sigma y$, as desired. $\square$

PROOF (OF LEMMA). First observe that H_x^n corresponds to multiplication by $\mathrm{N}(x)$, since

$$H_x^n(y) = x \cdot \sigma(x \cdot \sigma(x \cdots \sigma(y))) = x \cdot \sigma(x) \cdot \sigma^2(x) \cdots \sigma^{n-1}(x) \cdot \sigma^n(y) = \mathrm{N}(x)y$$

for any $y \in L$. It follows that the minimal polynomial of H_x divides $t^n - \mathrm{N}(x)$. Now, recall that the minimal polynomial of a linear operator T always divides its characteristic polynomial, which has degree n, so showing that they are equal suffices. Thus is true if and only if there are no blocks with shared eigenvalues in the Jordan decomposition of T, which is true if and only if $\dim_K(\mathrm{Ker}(T - \lambda I)) \leq 1$, for all $\lambda \in \overline{K}$.

Here's a proof that doesn't quite work. Suppose that $H_x(y_1) = \lambda y_1$, $H_x(y_2) = \lambda y_2$, and $y_1, y_2 \neq 0$ (so that the two are "honest eigenvalues"). We'd like to show that y_2 is a multiple of y_1, that is, $y_2/y_1 \in K$, i.e., is fixed by $\mathrm{Gal}(L/K)$. Indeed, we have

$$\frac{\sigma y_2}{\sigma y_1} = \frac{\frac{1}{x}\lambda y_2}{\frac{1}{x}\lambda y_1} = \frac{y_2}{y_1},$$

since $\sigma y_2 = H_x(y_2)/x$, and similarly for y_1. However, the issue is that this proof occurred in L, and not $\overline{K}$, which is where our eigenvalues actually live! Thus, we need to work in $L \otimes_K \overline{K} \simeq \prod_{g \in G} \overline{K}$, which is not necessarily a field.

We can compute the characteristic polynomial after extension of scalars. Recall that

$$L \otimes_K \overline{K} \xrightarrow{\sim} \prod_{i=0}^{n-1} \overline{K}, \quad a \otimes b \mapsto ((\sigma^i a) \cdot b)_{i=0}^{n-1}.$$

This extends non-canonically to an automorphism of $\overline{K}$, but otherwise everything is canonical, with the group acting on the set of coordinates by left multiplication. The map

$$\sigma \otimes \mathrm{id} \colon L \otimes_K \overline{K} \to L \otimes_K \overline{K}$$

corresponds to permuting the coordinates, and we have a map

$$\mu_x \otimes \mathrm{id} \colon L \otimes_K \overline{K} \to L \otimes_K \overline{K}, \quad (y_0, \ldots, y_{n-1}) \mapsto (xy_0, (\sigma x)y_1, \ldots, (\sigma^{n-1}x)y_{n-1}),$$

where μ_x denotes multiplication by x. Now, say $\lambda \in \overline{K}$ is an eigenvalue of H_x with corresponding eigenvector $(y_0, \ldots, y_{n-1})$. Then

$$H_x(y) = (xy_1, (\sigma x)y_2, (\sigma^2 x)y_3, \ldots, (\sigma^{n-1}x)y_0) = (\lambda y_0, \lambda y_1, \lambda y_2, \ldots, \lambda y_{n-1}),$$

and so $xy_1 = \lambda y_0$, implying $y_1 = (\lambda/x)y_0$, and similarly $y_2 = (\lambda/\sigma x)y_1 = (\lambda^2/(x \cdot \sigma x))y_0$. In general, we have

$$y_i = \frac{\lambda^i}{x \cdots \sigma^{i-1}x} y_0,$$

so all coordinates are uniquely determined by y_0, i.e.,

$$(y_0, \ldots, y_{n-1}) = y_0 \left(1, \frac{\lambda}{x}, \frac{\lambda^2}{x \cdot \sigma x}, \ldots, \frac{\lambda^{n-1}}{\prod_{i=0}^{n-2} \sigma^i x}\right).$$

So indeed, our eigenspaces each only have dimension one, as desired. Note that this only defines an eigenvector if

$$\frac{\lambda^n}{x \cdots \sigma^{n-1} x} = \frac{\lambda^n}{\mathrm{N}(x)} = 1,$$

that is, if $\lambda^n = \mathrm{N}(x)$, which is consistent with what we expected (and all nth roots appear with multiplicity one). $\square$

Now, we recall that our goal was to show that for an abelian extension L/K of local fields,

$$K^\times / \mathrm{N}L^\times \simeq \mathrm{Gal}(L/K)$$

canonically (in a strong sense). We've shown that $K^\times/\mathrm{N}L^\times$ has the right order, but we'll prove this generally for non-cyclic groups using cohomology. We now introduce the language of homological algebra, which will be central to our approach.

Definition 9.6. A (cochain) complex X of abelian groups is a sequence

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

such that the *differential* satisfies $d^{i+1}d^i = 0$ for each i.

Notation 9.7. We often refer to the entire complex as $X^\bullet$, where the '$\bullet$' is in the location of the indices. We will also often omit indices, e.g. by writing d for d^i and $d \cdot d = d^2 = 0$. Note that some authors write $H_i := H^{-i}$, and similarly for X_i, so that the differential lowers degree. Our convention, however, is that differentials raise degree.

Definition 9.8. The *ith cohomology group* is $H^i(X) := \mathrm{Ker}(d^i)/\mathrm{Im}(d^{i-1})$.

These are, in fact, the invariants we are after, but X is a "richer" object, so it is better to pass to cohomology at the very end of our processes. We now introduce the important idea of a null-homotopy of a map of chain complexes.

Definition 9.9. A map f such that the diagram

$$\begin{tikzcd}
\cdots \arrow[r] & X^{-1} \arrow[r, "d^{-1}"] \arrow[d, "f^{-1}"] & X^0 \arrow[r, "d^0"] \arrow[d, "f^0"] & X^1 \arrow[r] \arrow[d, "f^1"] & \cdots \\
\cdots \arrow[r] & Y^{-1} \arrow[r, "d^{-1}"] & Y^0 \arrow[r, "d^0"] & Y^1 \arrow[r] & \cdots
\end{tikzcd}$$

commutes is a *map of complexes*. Note that f induces a map of cohomologies because both the kernel and image of the differentials in $X^\bullet$ are preserved in $Y^\bullet$ by commutativity. A map h as in the following diagram

$$\begin{tikzcd}
\cdots \arrow[r] & X^{-1} \arrow[r, "d^{-1}"] \arrow[d, "f^{-1}"] \arrow[dl] & X^0 \arrow[r, "d^0"] \arrow[d, "f^0"] \arrow[dl, "h^0"'] & X^1 \arrow[r] \arrow[d, "f^1"] \arrow[dl, "h^1"'] & \cdots \arrow[dl] \\
\cdots \arrow[r] & Y^{-1} \arrow[r, "d^{-1}"] & Y^0 \arrow[r, "d^0"] & Y^1 \arrow[r] & \cdots
\end{tikzcd}$$

such that $dh + hd = f$, or more precisely, $d^i h^{i+1} + h^i d^{i+1} = f^{i+1}$ for each i, is a *null-homotopy of f*.

LEMMA 9.10. *If f is null-homotopic, then the induced map on cohomology $H^i(X) \xrightarrow{H^i(f)} H^i(Y)$ is zero for all i.*

PROOF. Let $x \in X^i$ such that $dx = 0$. Then $f(x) = (dh + hd)(x) = d(h(x))$, so $f(x) \in \mathrm{Im}(d^{i-1})$, and hence $f(x) = 0$ in $H^i(Y)$. $\square$

Now, our guiding principal here is that for algebra, isomorphism is a much better notion than equality, which refers to sets without structure. Thus, if $f \simeq g$, i.e., f is homotopic to g by which we mean that there exists a null-homotopy of $f - g$, then no test of actual mathematics can distinguish f and g anymore.

We'd like to define some notion of "cokernel" for a map of complexes. A bad idea is, for a map $f\colon X \to Y$ of complexes, to form $\mathrm{Coker}(f)$. A better idea is the following:

DEFINITION 9.11. The *homotopy cokernel* or *cone* $\mathrm{hCoker}(f) = \mathrm{Cone}(f)$ has the universal property that maps of chain complexes $\mathrm{hCoker}(f) \to Z$ are equivalent to maps $Y \to Z$ along with the data of a null-homotopy of $X \to Z$, which we note yields the following commutative diagram:

$$\begin{tikzcd} X \arrow[r] \arrow[d, "f"] & Z \\ Y. \arrow[ur] & \end{tikzcd}$$

Note the similarity with the universal property of an ordinary cokernel.