LECTURES ON CLASS FIELD THEORY

ALEXANDER BEILINSON

Lecture 3: 10/12/2007

§3.1. Last time we explained the idea of the Tate-Nakayama construction of the main isomorphism of local CFT. It was based on a certain key vanishing result, and we explained that this vanishing result can be proved using Tate's theorem in two different ways: either by showing that a certain Brauer group vanishes, or by showing that a certain norm map is surjective.

§3.2. Some complements to the last lecture.

Let \( L \supset K \) be a Galois extension of local fields of degree \( n \), and \( G = \text{Gal}(L/K) \). Then

\[
H^2(G, L^\times) \xrightarrow{\sim} \left( \frac{\mathbb{Z}}{n\mathbb{Z}} \right) / \mathbb{Z},
\]

and we get an isomorphism

\[
\check{H}^0(G, \mathbb{Z}) \xrightarrow{\sim} \check{H}^0(G, L^\times).
\]

In particular, this produces the local reciprocity isomorphism

\[
\text{Gal}(L) \xrightarrow{\sim} K^\times / N_{L/K}(L^\times).
\]

We would like to obtain a more explicit formula for this isomorphism.
Let us denote the inverse of this isomorphism by \( \varphi : \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z} \). Given a homomorphism \( \alpha : G \rightarrow \mathbb{Q}/\mathbb{Z} \), we wish to compute \( \alpha(\varphi(x)) \) for a given \( x \in K^*/N_GK(L^x) \).

**Exercise.** Viewing \( \alpha \) as an element of \( H^1(G, \mathbb{Q}/\mathbb{Z}) \), we have

\[
\alpha(\varphi(x)) = \text{inv}(\bar{x} \cup S(\alpha))
\]

where \( \bar{x} : H^1(G, \mathbb{Q}/\mathbb{Z}) \rightarrow H^2(G, \mathbb{Z}) \) is the connecting homomorphism for the exact sequence \( 0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0 \), and \( \bar{x} \) is a lift of \( x \) to an element of \( K^x = H^0(G, L^x) \). Also, \( \text{inv} \) is the cup product and

\[
\text{inv} : H^2(G, L^x) \rightarrow \mathbb{Q}/\mathbb{Z}
\]

is the standard embedding.

**Exercise.** Consider a tower of local fields \( K \rightarrow L \rightarrow L' \), where \( L' \) and \( L \) are both Galois over \( K \). Show that the induced diagram (see below) commutes using the explicit formula from the previous exercise.
Thus we obtain an isomorphism
\[ G_K^{ab} \cong \text{completion of } K^x \text{ } \]
\[ \text{w.r.t. the "norm topology"} \]

§3.4. Now consider the case where \( L \supseteq K \) is a totally ramified Galois extension of local fields:

\[
\begin{array}{ccc}
L & \overset{\sim}{\longrightarrow} & L_{nr} \\
\downarrow & & \downarrow \cong \\
\mathbb{Z} & \overset{\cong}{\longrightarrow} & K_{nr} \\
\downarrow & & \downarrow \\
G & \overset{\cong}{\longrightarrow} & \mathbb{Z} \\
\end{array}
\]

Look at \[ 1 \rightarrow \mathcal{O}_{L_{nr}}^x \rightarrow (L_{nr})^x \rightarrow \mathbb{Z} \rightarrow 0 \]

We also have another exact sequence:
\[ 1 \rightarrow \mathcal{O}_L^x \rightarrow \mathcal{O}_{L_{nr}}^x \xrightarrow{\text{Fr}^{-1}} \mathcal{O}_{L_{nr}}^x \rightarrow 1 \]

\[ \text{where } \text{Fr} \in \text{Gal}(L_{nr}/L) \text{ corresponds to } 1 \in \mathbb{Z} \]

Exercise. Check that \( \text{Fr}^{-1} \) is surjective using the standard filtration on \( \mathcal{O}_{L_{nr}}^x \).
Consider the induced composition

\[ \mathbb{Z} \rightarrow O^x_{L_{nr}} \rightarrow O^x_L \rightarrow L^x \]

\[ \text{induced by} \quad \text{the first exact sequence} \]
\[ \text{induced by} \quad \text{the second exact sequence} \]
\[ \text{induced by} \quad \mathbb{Q}^x_{L} \rightarrow L^x \]

**Exercise.** This composition is the canonical generator of \( H^2(G, L^x) \).

(A solution of this exercise may be explained at the beginning of the next lecture.)

**§3.5.** We also have

\[ G^{ab} = \hat{H}^{-2}(G, \mathbb{Z}) \rightarrow \hat{H}^{-1}(G, O^x_{L_{nr}}) \]

\[ \text{Ker} (O^x_{L_{nr}} \rightarrow O^x_{K_{nr}}) \]

this homomorphism is surjective (this is the first time that we use the assumption that \( L \) is totally unramified over \( K \)).

So we get a short exact sequence

\[ 1 \rightarrow G^{ab} \rightarrow (O^x_{L_{nr}}) \rightarrow O^x_{K_{nr}} \rightarrow 1 \]

It carries an obvious action of \( \mathbb{Z} \), i.e., it is a short exact sequence of \( \mathbb{Z} \)-modules.
Look at the associated long exact cohomology sequence:

$$
0 \xrightarrow{\mathcal{L}} H^0(\hat{\mathbb{Z}}, \mathcal{O}^*_{\text{Kn}}) \xrightarrow{\delta} H^1(\hat{\mathbb{Z}}, \mathcal{G}_{\text{ab}}) \xrightarrow{\text{Hom}(\hat{\mathbb{Z}}, \mathcal{G}_{\text{ab}})} \mathcal{O}^*_{\text{K}} \xrightarrow{\text{norm}} \mathcal{G}_{\text{ab}}
$$

**Exercise.** The map $\mathcal{O}^*_{\text{K}} \to \mathcal{G}_{\text{ab}}$ we obtain corresponds to the inverse of the local reciprocity isomorphism for $L/K$.

---

**Ramification theory**

§3.6. Today we will begin a discussion of the higher ramification theory and use it to show that for any Galois extension of $\text{Kn}$ where $K$ is a local field, the norm homomorphism is surjective.

§3.7. Most of the story will go through for an arbitrary complete discretely normed field with perfect residue field. (Let us agree that local fields have finite residue field.)
Consider a finite Galois extension $L/K$ with $G = \text{Gal}(L/K)$. Given $g \in G$, we define the \underline{Lefschetz number} of $g$, written $i_g(L) \in \mathbb{Z}$, as follows:

$$i_g(L) := \inf_{y \in \mathcal{O}_L} \text{val}_L(g(y) - y)$$

In fact, $i_g(L) = \text{val}_L(g(c) - c)$, where $c \in \mathcal{O}_L$ is a generator of $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra (it is known that such a $c$ always exists).

Remark: $\mathcal{O}_L/m^L_iL(g)$ is the maximal quotient ring of $\mathcal{O}_L$ on which $g$ acts trivially.

\subsection{3.9. Geometric Interpretation}

$$\text{Spec } \mathcal{O}_L \xrightarrow{\Delta} (\text{Spec } \mathcal{O}_L) \times_{\text{Spec } \mathcal{O}_K} (\text{Spec } \mathcal{O}_L)$$

Then $\text{Spec } (\mathcal{O}_L/m^L_iL(g))$ is precisely the fiber product of the two morphisms $\Delta$ and $(g, \text{id}) \circ \Delta$ (which is a closed subscheme of $\text{Spec } \mathcal{O}_L$, as it should be).
This explains the term “Lefschetz number,” because we see that \( i_\mathfrak{L}(g) \) is the length of the intersection of the diagonal for \( \text{Spec} \mathcal{O}_L \) with the graph of \( g \).

\[ \text{(3.10)} \quad \text{Note that if the characteristic of the residue field of } K \text{ is zero, then } i_\mathfrak{L}(g) \text{ can only be equal to either } 0 \text{ or } 1. \]

(This is an easy exercise.)

However, if the residue field characteristic is \( p > 0 \), the Lefschetz number could be as large as we like.

\[ \text{(3.11)} \quad \text{Let us declare that } i_\mathfrak{L}(1) = +\infty. \]

Then we obtain a filtration on \( G \) defined as follows: \( a > -1 \Rightarrow \)

\[ G_a := \{ g \in G \mid i_\mathfrak{L}(g) \geq a + 1 \} \]

\[ = \{ g \in G \mid g \text{ acts trivially on } \mathcal{O}_L / \mathfrak{m}_L^{a+1} \} \]

This shows immediately that each \( G_a \) is a subgroup of \( G \). We get:

\[ G = G_{-1} \supset G_0 = 1 \supset G_1 \supset G_2 \supset \cdots \]

...the inertia subgroup of \( \text{Gal}(L/K) \)
Also, \( G/G_1 \) is the maximal tamely ramified quotient of \( G \) (this is either a tautology or an easy exercise depending on which definition of “tamely ramified” one decides to use).

\[ 3.12 \] Consider the filtration
\[ L^x = \mathcal{O}_L^x = U_0 \supset U_1 \supset U_2 \supset \ldots, \]
where \( U_i = 1 + m_L^i \). We would like to compare it with the filtration of \( G = \text{Gal}(L/K) \) introduced in \( 3.11 \).

**Observation.** Fix \( g \in G_0 \) and \( a \geq 0 \). Then
\[ g \in G_a \setminus G_{a+1} \iff \text{val}_L(g(\pi_L) - \pi_L) = a + 1 \]
where \( \pi_L \in \mathfrak{m}_L \) is a uniformizer.

Moreover, an element \( g \) with this property acts trivially on \( U_0 / U_{a+1} \).

**Corollary.** The map
\[ G_a \rightarrow U_a / U_{a+1}, \quad g \mapsto g(\pi_L) / \pi_L \]
is a well-defined homomorphism, independent of \( \pi_L \), with kernel equal to \( G_{a+1} \).
Thus we obtain canonical embeddings \( \frac{G_a}{G_{a+1}} \rightarrow \frac{U_a}{U_{a+1}} \)
for all \( a \geq 0 \).

**Corollary 1.** \( \frac{G_0}{G_1} \) is a cyclic group of order prime to \( p \), and for every \( a \geq 1 \), \( \frac{G_a}{G_{a+1}} \) is an elementary abelian \( p \)-group (i.e., an \( \mathbb{F}_p \)-vector space).

**Corollary 2.** The group \( G_0 \) is solvable.

Thus, if the residue field of \( K \) is finite, then \( G \) is solvable as well.

**§3.14. Different.** Let \( L/K \) be as before. We know that \( \mathcal{O}_L \) is generated by one element as an \( \mathcal{O}_K \)-algebra. Consider the module of relative Kähler differentials, \( \omega_{\mathcal{O}_L/\mathcal{O}_K} \).

It is a cyclic torsion (because \( L/K \) is separable) \( \mathcal{O}_L \)-module (generated by \( d(c) \) if \( \mathcal{O}_L = \mathcal{O}_K(c) \)).

Hence \( \mathcal{O}_L/\mathcal{O}_K \cong \mathcal{O}_L/\mathcal{D}_{L/K} \) for a nonzero ideal \( \mathcal{D}_{L/K} \subset \mathcal{O}_L \). This ideal is called the different of the extension \( L/K \).

How to compute the different explicitly?
Write \( O_L = O_K[t]/(f(t)) \) for a monic polynomial \( f(t) \in O_K[t] \). Then, by definition, \( \mathfrak{D}_{L/K} \) is the ideal generated by \( f'(c) \). Let us write \( f(t) = \prod_{t \in G} (t - g(t)) \).

Then \( f'(c) = \prod_{g \neq 1} (c - g(c)) \).

Next, observe that the ideal \( (f'(c)) \) is determined by \( \text{val}_{\mathfrak{p}}(f'(c)) \). Also, as we have seen earlier, \( \text{val}_{\mathfrak{p}}(c - g(c)) = i_{\mathfrak{p}}(g) \).

Thus we obtain the formula

\[
\nu_{\mathfrak{p}}(\mathfrak{D}_{L/K}) = \sum_{a = 0}^{\infty} (|G_a| - 1)
\]

\[\text{§3.15.}\] We will soon see that the collection of integers \( \{i_{\mathfrak{p}}(g)\}_{g \in G} \) can be recovered from the Newton polygon of the translated polynomial \( \bar{f}(t) = f(t + c) \).

Let us recall what this means. Write

\[
f(t) = t^n + q_1 t^{n-1} + q_2 t^{n-2} + \ldots + q_{n-1} t
\]

To produce the Newton polygon of \( \bar{f}(t) \), we plot the points \( \{(i, \text{val}_{\mathfrak{p}}(q_i))\}_{i = 0}^{n-1} \) (where \( q_0 = 1 \)).
and form the "upper convex envelope" of this finite set of points.

Since the elements \( \{ g(c) - c \} \) are roots of \( \bar{E}(t) \), their valuations are precisely the slopes of the Newton polygon of \( \bar{E} \), with multiplicities equal to the lengths of the corresponding horizontal intervals. (It would help if I were less lazy and drew an illustration.)

\[ \textit{Moral.} \quad \text{The Lefschetz numbers } i_L(g), \text{ where } g \in \text{Gal}(L/K), \text{ are easily computable.} \]

\[ \textit{§3.16.} \quad \text{Another interpretation.} \quad \text{Let us view } \]

\[ \text{L as a finite dimensional } K \text{-vector space.} \]

\[ \text{It carries a nondegenerate symmetric bilinear form} \]

\[ (a, b) := \text{tr}_{L/K} (a \cdot b) \]

If \( M \subset L \) is an \( \mathcal{O}_K \)-lattice, we can consider \( M^\perp := \{ y \in L \mid (y, M) \subset \mathcal{O}_K \} \).

This is again an \( \mathcal{O}_K \)-lattice in \( L \), and if \( M \) is an \( \mathcal{O}_L \)-submodule of \( L \), then so is \( M^\perp \) (evidently).
Now the $O_L$-submodules of $L$ that are $O_K$-lattices are precisely the integral powers of $M_L$.

**Lemma.** \[ Q^{-1} = O_L \]

From this lemma, we can determine $M^\perp$ for any $O_L$-submodule $M \subset L$ which is an $O_K$-lattice.

§3.17. Let us sketch a proof of Lemma 3.16.

We use the so-called "Euler identity".

Let $c \in O_L$ and $f(t)$ be as before:

\[ O_L = O_K[c] \leq O_K[t]/(f(t)). \]

**Exercise** (Euler identity).

\[
\text{tr}_{L/K} \left( \frac{c^k}{f'(c)} \right) = \begin{cases} 
0, & k = 0, 1, \ldots, n-2 \\
1, & k = n-1.
\end{cases}
\]

Now $1, c, \ldots, c^{n-1}$ is a basis of $O_L$ as an $O_K$-module. The Euler identity immediately implies that $O_L^\perp \subset L$ is generated, as an $O_L$-module, by $\frac{1}{f'(c)}$, which is what was to be shown.
§3.18. Consider the standard filtration on the additive group of $\mathbb{Q}_2$, by powers of $m_L$, and look at the trace of this filtration from $L$ to $K$. It compares to the standard filtration on $\mathbb{Q}_K$ as follows.

Corollary. $\text{tr} \frac{L/K}{e} \left( \mathcal{O}_L^{-1}, m_L^s \right) = m_K \left[ s/e \right]$

where $e = e(L/K)$ is the ramification index of the extension $L/K$, and $\left[ s/e \right]$ denotes the largest integer $\leq s/e$.

This is easy to deduce from the Euler identity.

§3.19. Theorem. Let $K$ be a complete discretely normed field with algebraically closed residue field, and let $L$ be any finite Galois extension of $K$. Then

$$N_{L/K} : L^* \longrightarrow K^*$$

is surjective.

[Let us recall that if $G = \text{Gal}(L/K)$, then $K^*/N_{L/K}(L^*) = \hat{H}^0(G, L^*)$, and showing the vanishing of this was one of the ways to prove that $L^*$ is a cohomologically trivial $G$-module.]


§3.20. Note first that since $G$ is solvable, we are immediately reduced to the case where $G$ is cyclic of prime order (using induction on $[L:K]$).

It is enough to show that

$$N_{L/K} : \mathcal{O}_L^\times \longrightarrow \mathcal{O}_K^\times$$

is surjective, because of the commutative diagram

$$\begin{array}{ccc}
L^\times & \xrightarrow{N_{L/K}} & K^\times \\
\downarrow \text{val}_L & & \downarrow \text{val}_K \\
\mathbb{Z} & \longrightarrow & \mathbb{Z}
\end{array}$$

multiplication by the degree of the residue field extension, which equals 1 in view of our assumption.

§3.21. From now on we can forget the assumption that the residue field of $K$ is algebraically closed. Let us try to analyze the relationship between $N_{L/K} : \mathcal{O}_L^\times \longrightarrow \mathcal{O}_K^\times$ and the standard filtrations on $\mathcal{O}_L^\times$ and $\mathcal{O}_K^\times$.

**Unramified case.** If $L$ is unramified over $K$, then $N_{L/K}$ is compatible with the filtrations, and the associated graded maps are as follows:

$$\text{gr}_0(N_{L/K}) = N_{L/K} : L^\times \longrightarrow K^\times$$

$$\text{gr}_j(N_{L/K}) = T_{L/K} : L \longrightarrow K \quad (\text{the trace})$$

for all $j \geq 1$. 
Here, \( l \) and \( k \) are the residue fields of \( L \) and \( K \), respectively.

### 33.22. Tame case.

Let us now assume that \( L \) is totally and tamely ramified over \( K \). In this case the situation is also quite simple.

\[
\mathcal{O}_L^\times \supset U_{L,1} \supset U_{L,2} \supset \cdots \supset U_{L,j} \supset U_{L,j+1} \supset \cdots \\

\mathcal{O}_K^\times \supset U_{K,1} \supset U_{K,2} \supset \cdots
\]

In general: \( N_{L/K}(U_{L,j}, e) \subseteq U_{K,j} \) for all \( j \geq 0 \).

Now let us look at the associated graded homomorphisms. First,

\[
\text{gro}(N_{L/K}) : \mathbb{K}^\times \rightarrow \mathbb{K}^\times \\
\text{is given by } x \mapsto x^e \quad (e = e_{L/K}, \text{ as usual})
\]

Next, the induced homomorphism

\[
U_L / U_{L,e+1} \rightarrow U_1 / U_2 \\
1 \rightarrow M_{K} / M_{K}^e \supseteq \mathbb{K}
\]

\( k \equiv M_{L}^e / M_{L}^{e+1} \)

equals the multiplication by \( e \), and similarly for \( U_{j,e} / U_{j,e+1} \rightarrow U_j / U_{j+1} \).
33.23. **Wild case.** Finally, let us consider the most interesting case, where \( L \supset K \) is totally ramified, and \([L:K] \) is a power of \( p = \text{char}(k) \).

In fact, we assume that \([L:K] = p\) (in particular, \(L\) is a cyclic extension of \(K\)). We have \( G \cong \mathbb{Z}/p\mathbb{Z} \). In particular, there exists \( s \geq 1 \) such that \( G = G_s \) and \( G_{s+1} = \{1\} \).

We would like to describe the picture of the norm map \( N_{L/K} \) in terms of \( s \).

**Proposition.**

1. \( N_{L/K} (U_{L,i}) \subseteq U_{K,i} \) for all \( 0 \leq i \leq s+1 \).

2. We have: \( gr_0 (N_{L/K}) = \text{Frob}_L : a \mapsto a^p \) and if we choose uniformizers \( \pi_L \in L \) and \( \pi_K \in K \) so that \( \pi_K = N_{L/K} (\pi_L) \), then

\[
    gr_i (N_{L/K}) (1 + \Theta \pi_L^i) = 1 + \Theta^{p^i} \pi_K 
\]

mod \( U_{K,i+1} \) (so that we again get the Frobenius), for all \( 1 \leq i \leq s-1 \). (The formula changes when \( i = s \).)
(3) The associated graded map
\[ \text{gr}_s(N_{L/K}) : U_{L,s}/U_{L,s+1} \longrightarrow U_{K,s}/U_{K,s+1} \]
is given by the formula
\[ 1 + \Theta \pi_L^s \longmapsto 1 + (\Theta^p - \eta \Theta) \pi_K^s \pmod{U_{K,s+1}} \]
where \( \eta \) is defined as follows:
\[ \sigma(\pi_L)/\pi_L = 1 + \eta \pi_L^s, \]
where \( \sigma \) is a generator of \( G \).

**Remark.** The map \( \Theta \mapsto \Theta^p - \eta \Theta \) on the residue field \( k \) is an Artin–Schreier covering.

It is surjective if \( k \) is algebraically closed.

(4) We also have:
\[ N_{L/K} : U_{s+jp+1}, U_{s+jp+2}, \ldots, U_{s+(j+1)p} \longrightarrow U_{s+jp}, \]
The associated graded map at the lowest level equals multiplication by \( \eta^{p-1} \).

**3.24.** Putting all of the above results together, we see that \( N_{L/K} : \mathcal{O}_L^x \longrightarrow \mathcal{O}_K^x \) is surjective whenever \( K \) has algebraically closed residue field. This proves Theorem 3.19.

**3.25.** Next we explain how to perform the computations whose results were stated in 
\[ \S\S 3.21 - 3.23. \]
Observation. Let \( L \supset K \) be cyclic of prime degree (without any assumptions about the ramification).

If \( y \in m_L \), then

\[
N_{L/K}(1+y) = 1 + N_{L/K}(y) + T_{L/K}(y) + \text{Tr}_{L/K}(y)
\]

\[
\text{where } \text{val}_L(y) \geq 2 \cdot \text{val}_L(y).
\]

Proof: We have

\[
N_{L/K}(1+y) = \prod_{g \in \text{Gal}(L/K)} (1 + g(y))
\]

\[
= 1 + N_{L/K}(y) + T_{L/K}(y) + \sum_{A \subseteq G} \left( \prod_{g \in A} g(y) \right)
\]

\[\text{such that } 1 < |A| < |G|\]

Now \( G \) acts on itself by translations, and this induces a free action of \( G \) on the collection of subsets \( A \subseteq G \) with \( 1 < |A| < |G| \), because \( G \) has prime order.

Choosing a representative in each \( G \)-orbit acting on this collection of subsets \( A \), and using \( |A| \geq 2 \), we immediately get our result.
§3.26. Now we perform the calculations from §3.23. We have \( \mathcal{V}_L(\mathcal{D}_L/K) = (p-1)(s+1) \), because every nontrivial element of \( G \) has Lefschetz number \( s+1 \). 

Now \( \mathcal{V}_L(\pi_L^i \mathcal{O}_L) = \pi_K^i \mathcal{O}_K \), where \( j(i) = s+1 + \left[ \frac{i-1-s}{p} \right] \).

Consider an element \( 1 + \Theta \pi_L^i \in \mathcal{U}_i \setminus \mathcal{U}_{i+1} \). We would like to compute \( N_{L/K}(1 + \Theta \pi_L^i) \).

Remark: We may assume that \( \Theta \in \mathcal{O}_K \), because we only care about \( \Theta \mod \mathfrak{m}_K \), and the residue fields of \( K \) and \( L \) are the same.

Now \( N_{L/K}(1 + \Theta \pi_L^i) = 1 + \Theta \pi_K^i + (\text{other terms}) \).

(Remember again that \( \pi_K = N_{L/K}(\pi_L) \).)

If \( i < s \), then we claim that these other terms can be ignored. However, it is obvious that \( j(i) \geq i \), which proves the claim.

§3.27. Next, consider the case \( i = s \). We get

\[
N_{L/K}(1 + \Theta \pi_L^s) = 1 + \Theta \pi_K^s + T_{L/K}(\Theta \pi_L^s) + (\text{irrelevant terms})
\]

What can we do with this formula?
Observe that if we replace $\Theta$ with $\eta$, then the whole thing becomes 1, because

$$N_{L/K}(1 + \eta \pi_L^s) = N_{L/K}(\sigma(\pi_L)/\pi_L) = 1.$$ 

On the other hand,

$$\eta^p \pi_K^s + Tr_{L/K}(\eta \pi_L^s) = 0.$$ 

Now replace $\Theta$ with $\eta \Theta$. Then both sides become 1 when $\Theta = 1$, which leads to the formula

$$N_{L/K}(1 + \Theta \pi_L^s) = 1 + (\Theta^p - \eta \Theta) \pi_K^s + \text{(irrelevant terms)},$$

which is what we claimed.

§3.28. Finally, we need to deal with $i > s$. This is left as an exercise using the identity

$$\eta^p \pi_K^s + Tr_{L/K}(\eta \pi_L^s) = 0.$$