Lectures on Class Field Theory

Alexander Beilinson

Lecture 5: 10/26/2007

§5.1. Let K be a complete discrete valued field with perfect residue field k, such that $\mathrm{char}(k) = p > 0$. We have $k = \mathcal{O}_K / m_K$, where $\mathcal{O}_K$ is the ring of integers of K and m_K is its unique maximal ideal.

§5.2. Recall that knowing finite unramified extensions of K is the same as knowing finite extensions of k. Finite tamely ramified extensions of K are also not hard to describe.

Let $\lambda_K = m_K / m_K^2$ and consider the category of tuples (k', λ', e, ν), where

k' is a finite extension of k

λ' is a 1-dimensional vector space over k'

e is a positive integer not divisible by p

$\nu : \lambda_K \otimes_k k' \xrightarrow{\simeq} (\lambda_{K'})^{\otimes e}$ is an isomorphism of k'-lines.

Claim: The category of such data is equivalent to the category of finite tamely ramified extensions of K.

§5.3. Let us describe the functor in one direction:

K'/K finite tamely unramified

e = ramification index; $p \nmid e$

By definition, $m_K \mathcal{O}_{K'} = m_{K'}^e$

Then

$$\lambda_K \otimes_k k' \xrightarrow{\simeq} m_{K'}^e / m_{K'}^{e+1} \xleftarrow{\simeq} \lambda_{K'}^{\otimes e}$$

Exercise. Show that this defines an equivalence of categories.

§5.4. Reference for the material that follows:

"Les corps locaux de caracteristique p, limites de corps locaux de car. 0,"

Deligne's article in the book

"Representations des groupes réductifs sur un corps local"

§5.5. We are interested in the question of whether all finite extensions of K can be described in similar terms (maybe by looking at $\mathcal{O}_K / m_K^n$ for larger $n \in \mathbb{N}$).

§5.6. Fix $n \in \mathbb{R}$, $n > 0$. Consider the category $\mathrm{Ext}(K)^n$ of finite separable extensions L of K such that if G is

the Galois group of the normal closure of $L \supset K$, then $G^n = \{1\}$.

We claim that if $n \in \mathbb{N}$, then the category $\mathrm{Ext}(K)^n$ can be described in terms of $\mathcal{O}_K / \mathfrak{m}_K^n$. Consider triples of the form

$$(R, M, \varepsilon),$$

where:
- R is a truncated DVR = a local Artinian ring whose maximal ideal, $\mathfrak{m}_R$, is principal
- M is a free R-module of rank 1
- $\varepsilon : M \longrightarrow \mathfrak{m}_R$ is a surjective homomorphism of R-modules

Example of such a triple:

$\mathcal{O}$ = an actual DVR, $n \in \mathbb{N}$

$\rightsquigarrow R = \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$, $M = \mathfrak{m}_{\mathcal{O}}/\mathfrak{m}_{\mathcal{O}}^{n+1}$

Let us call this the n-truncated triple associated to the DVR $\mathcal{O}$.

§5.7. Claim. If K is as before, the category $\mathrm{Ext}(K)^n$ can be canonically recovered from the n-truncated triple associated to the ring of integers $\mathcal{O}_K$.

(This claim only makes sense for $n \in \mathbb{N}$, though the category $\mathrm{Ext}(K)^n$ is defined for all $n \in \mathbb{R}_{>0}$.)

§5.8. Note that triples of the form introduced in §5.6 form a category. Namely, a morphism

$$\varphi : (R, M, \varepsilon) \longrightarrow (R', M', \varepsilon')$$

consists of the following data:

$$\varphi = (e, \varphi_R, \varphi_M),$$

where $e \in \mathbb{Z}_{>0}$, $\varphi_R : R \longrightarrow R'$ is a (local) ring homomorphism such that $\varphi_R(m_R) \subseteq m_{R'}^e$ (actually, we then have $R'\varphi_R(m_R) = m_{R'}^e$, from the next condition); and $\varphi_M : M \underset{R}{\otimes} R' \xrightarrow{\simeq} (M')^{\oplus e}$ is an isomorphism of R'-modules.

§5.9. Example. Suppose $\mathcal{O}, \mathcal{O}'$ are discrete valuation rings, and $\mathcal{O} \longrightarrow \mathcal{O}'$ is a morphism of ramification degree e. Consider $n, n' \in \mathbb{N}$. In order to get a morphism of the corresponding triples

$$\mathrm{trunc}_n(\mathcal{O}) \longrightarrow \mathrm{trunc}_{n'}(\mathcal{O}'),$$

we need to have $n \cdot e \geq n'$.

Also require compatibility with ε

§5.10. **Definition.** A morphism

$$\varphi : (R, M, \varepsilon) \longrightarrow (R', M', \varepsilon')$$

of triples as above is *flat* if

$$\text{length}(R') = e \cdot \text{length}(R).$$

Exercise. If R is *not* a field, this condition is equivalent to R' being flat as an R-algebra in the usual sense.

[The *length* of an artinian ring is defined as its length as a module over itself.]

§5.11. Fix $n \in \mathbb{N}$. We have a functor

$$\begin{array}{ccc} \text{Ext}(K) & \longrightarrow & \text{Ext}(\mathcal{O}_K/\mathfrak{M}_K^n, \ldots) \\ \uparrow & & \uparrow \\ \text{all finite separable extensions of } K & & \text{flat morphisms with source} = \text{the given triple} \end{array}$$

defined by

$$(L > K) \longmapsto (\mathcal{O}_L/\mathfrak{M}_L^{e \cdot n}, \ldots)$$

Lemma. This functor is essentially surjective

Proof. Any morphism of triples decomposes as a composition of an unramified one and a totally ramified one.

The theory of unramified ones is the same as for extensions of local fields, and this case is completely trivial.

Now we consider the totally ramified case. First let us recall what happens for the (more familiar) totally ramified extensions of local fields.

§5.12. Let $L \supset K$ be a finite separable totally ramified extension. Then $L = K[\pi_L]$. Let $f(t)$ be the minimal monic polynomial of π_L over K. Write $f(t) = t^n + a_1 t^{n-1} + \dots + a_n$. Then $a_1, a_2, \dots, a_n \in \mathfrak{m}_K$, and $a_n \notin \mathfrak{m}_K^2$.

(Proof: Use the facts that $\pi^n \in \mathfrak{m}_L^n = \mathcal{O}_L \mathfrak{m}_K$ and $1, \pi_L, \dots, \pi_L^{n-1}$ form an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.) This shows immediately that $a_j \in \pi_K$ for all j. To prove that $a_n \notin \mathfrak{m}_K^2$, reduce mod. $\mathfrak{m}_L^{n+1}$.

In other words, f is an Eisenstein polynomial over $\mathcal{O}_K$.

Conversely, given any Eisenstein polynomial over $\mathcal{O}_K$, it is automatically irreducible, and by adjoining a root of this polynomial, we obtain a totally ramified extension.

§5.13. In fact, the same thing goes through for triples.

Def. A uniformizer (or uniformizing parameter) for (R, M, ε) is a (free) generator of M as an R-module.

Claim. For a fixed (R, M, ε), we have a natural bijection between flat totally ramified extensions $(R, M, \varepsilon) \longrightarrow (R', M', \varepsilon')$ equipped with a choice of a uniformizer for (R', M', ε'), and Eisenstein polynomials (truncated) over (R, M, ε).

(Totally ramified means that the induced homomorphism $R/M_R \longrightarrow R'/M_{R'}$ is an isomorphism.)

Exercise. Formulate the definition of an Eisenstein polynomial in this context and prove the claim stated above.

§5.14. Now it is trivial to finish the proof of Lemma 5.11 by lifting truncated Eisenstein polynomials for $(\mathcal{O}_K/M_K^n, \dots)$ to Eisenstein polynomials over $\mathcal{O}_K$.

§5.15. Fix $n \in \mathbb{N}$. We now want to describe the category $Ext(K)^n$.

Lemma. Let L be a finite Galois totally ramified extension of K, choose a uniformizer $\pi_L \in L$, and let $f(t)$ be the corresponding Eisenstein polynomial.

Then the property $L \in Ext(K)^n$ can be checked by looking at the n-truncated Eisenstein polynomial corresponding to $f(t)$.

Exercise. Prove this lemma.

§5.16. The next problem is that extensions of triples have too many automorphisms, in general. To get rid of this problem, we will impose a certain equivalence relation on morphisms in the category of triples.

Consider two morphisms of triples,

$$(R, M, \varepsilon) \underset{\varphi_2}{\overset{\varphi_1}{\rightrightarrows}} (R', M', \varepsilon').$$

In fact, we assume here that φ_1, φ_2 are morphisms of flat extensions of a given truncated triple

$$(\mathcal{O}_K/m_K^n, \dots).$$

Thus φ_1, φ_2 are automatically flat.

Moreover, φ_1 and φ_2 have the same ramification index, $e_{R'/R}$.

Definition. We say that $\varphi_1 \sim \varphi_2$ if φ_1 and φ_2 coincide on the residue field $k_R = R/\mathfrak{m}_R$, and for all $x \in M$, we have

$$\frac{\mathrm{val}_{R'}}{e_{R'/R}}\left(\varphi_{M1}(x) - \varphi_{M2}(x)\right) \geq \psi_{R/(\mathcal{O}_K/\mathfrak{m}_K^n)}(n) + 1.$$

Here we assume that the triple (R, M, ε) comes from an object L of $\mathrm{Ext}(K)^n$, in which case it is an exercise to show that the Herbrand function $\psi_{L/K}(R, M, \varepsilon)$ is completely determined by (R, M, ε), so that we can write $\psi_{L/K} = \psi_{R/(\mathcal{O}_K/\mathfrak{m}_K^n)}$.

§5.16. Key proposition (Krasner).

Let $L \supset K$ be a finite Galois extension with $G = \mathrm{Gal}(L/K)$, such that $G^n = \{1\}$. Let $c \in \mathcal{O}_L$ be any element with $\mathcal{O}_L = \mathcal{O}_K[c]$, and let $f(t) \in \mathcal{O}_K[t]$ be the minimal monic polynomial of c.

Suppose $y \in \overline{K}$ is such that

$$\mathrm{val}_K(f(y)) \geq n+1$$

(i.e., y is an "approximate root" of f in $\overline{K}$).

Then there is a unique root of f in $\overline{K}$ which is closest to y.

§5.17. Exercise. Show that the proposition above implies that the functor

$$\mathrm{Ext}(K)^n \longrightarrow \mathrm{Ext}(\mathcal{O}_K/\mathfrak{m}_K^n, \ldots)$$

induces an equivalence between $\mathrm{Ext}(K)^n$ and the quotient of the essential image of this functor by the equivalence relation on morphisms introduced in §5.15.

§5.18. Proof of Proposition 5.16. We begin with a

Lemma. $G^n = \{1\} \iff \sum_{\substack{g \in G \\ g \neq 1}} \frac{i_G(g)}{|G_0|} + \max_{\substack{g' \in G \\ g' \neq 1}} \frac{i_G(g')}{|G_0|} < n+1.$

The proof of the lemma is rather formal.

Proof of $\Rightarrow$: $\sum_{\substack{g \in G \\ g \neq 1}} \frac{i_G(g)}{|G_0|} = \sum_{i \geq 0} \frac{|G_i|-1}{|G_0|} =$

(assuming $G_m \neq \{1\}$, $G_{m+1} = \{1\}$)

$$= -\frac{m+1}{|G_0|} + \sum_{i=0}^{m} \frac{|G_i|}{|G_0|}.$$

This (hopefully) implies that

$$\varphi_{L/K}(m) = \sum_{\substack{g \in G \\ g \neq 1}} \frac{i_G(g)}{|G_0|} + \frac{m}{|G_0|} - 1.$$

Check that this is equivalent to the inequality stated in the lemma.

The proof of the reverse implication is similar.

§5.19. Now we finish the proof of Prop. 5.16. Let $z \in \overline{K}$ be some root of $f(t)$ which is closest to y. This implies (in view of the nonarchimedean triangle inequality) that $v_K(y-z') = \min\{v_K(y-z), v_K(z-z')\}$ for every root z' of $f(t)$ in $\overline{K}$.

We have

$$v_K(f(y)) = v_K\left(\prod_{\substack{z'' = \text{root} \\ \text{of } f \text{ in } \overline{K}}} (y-z'')\right)$$

$$= v_K(y-z) + \sum_{\substack{z' \neq z \\ f(z')=0}} \min\{v_K(y-z), v_K(z-z')\}$$

By assumption, $v_K(f(y)) \geq n+1$.

Now suppose that for some root z' of $f(t)$ in $\overline{K}$, where $z' \neq z$, we have $v_K(y-z') = v_K(y-z)$.

This means that

$$v_K(y-z) = v_K(y-z') \leq v_K(z-z'),$$

which implies that

$$v_K(f(y)) \leq v_K(z-z') + \sum_{z'' \neq z} v_K(z-z'') \quad (*)$$

Now the second sum is the first sum in the inequality of Lemma 5.18, and the first term on the RHS of (*) is the second term on the LHS of the inequality of Lemma 5.18. We get $n+1 < n+1$, which is a contradiction.

Next subject: Introduction to p-adic Galois representations

§5.20. Let K be a local field such that the residue field has characteristic p. The absolute Galois group G_K has a huge pro-p part, P, which acts semisimply on torsion G_K-modules whose torsion is relatively prime to p. However, if we look at p-adic representations, the situation changes completely.