LECTURE 3

Norm Groups with Tame Ramification

Let K be a field with $\mathrm{char}(K) \neq 2$. Then

$$\begin{aligned} K^\times/(K^\times)^2 &\simeq \{\text{continuous homomorphisms } \mathrm{Gal}(K) \to \mathbb{Z}/2\mathbb{Z}\} \\ &\simeq \{\text{degree 2 étale algebras over } K\} \end{aligned}$$

which is dual to our original statement in Claim 1.8 (this result is a baby instance of Kummer theory). Note that an étale algebra over K is either $K \times K$ or a quadratic extension $K(\sqrt{d})/K$; the former corresponds to the trivial coset of squares in $K^\times/(K^\times)^2$, and the latter to the coset defined by $d \in K^\times$.

If K is local, then LCFT says that $\mathrm{Gal}^{\mathrm{ab}}(K) \simeq \widehat{K^\times}$ canonically. Combined (as such homomorphisms certainly factor through $\mathrm{Gal}^{\mathrm{ab}}(K)$), we obtain that $K^\times/(K^\times)^2$ is finite and canonically self-dual. This is equivalent to asserting that there exists a "sufficiently nice" pairing

$$(\cdot,\cdot)\colon K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \{1,-1\},$$

that is, one which is *bimultiplicative*, satisfying

$$(a,bc) = (a,b)(a,c), \quad (ab,c) = (a,c)(b,c),$$

and *non-degenerate*, satisfying the condition

$$\text{if } (a,b) = 1 \text{ for all } b, \text{ then } a \in (K^\times)^2.$$

We were able to give an easy definition of this pairing, namely,

$$(a,b) = 1 \iff ax^2 + by^2 = 1 \text{ has a solution in } K.$$

Note that it is clear from this definition that $(a,b) = (b,a)$, but unfortunately neither bimultiplicativity nor non-degeneracy is obvious, though we will prove that they hold in this lecture in many cases. We have shown in Claim 2.11 that a less symmetric definition of the Hilbert symbol holds, namely that for all a,

$$(a,b) = 1 \iff b \text{ is a norm in } K(\sqrt{a})/K = K[t]/(t^2 - a),$$

which if a is a square, is simply isomorphic to $K \times K$ and everything is a norm. At the end of Lecture 2, we made the following claim, and remarked that it was important that this subgroup of norms was "not too big" (not everything) and "not too small," and that K be local.

Claim 3.1. *These "good properties," i.e., bimultiplicativity and non-degeneracy, hold for the Hilbert symbol if and only if, for all quadratic extensions L/K, $\mathrm{N}(L^\times) \subseteq K^\times$ is a subgroup of index 2, that is, $K^\times/\mathrm{N}(L^\times) = \mathbb{Z}/2\mathbb{Z}$.*

Proof. Assume that for all degree two extensions L/K, we have $\mathrm{N}L^\times \subseteq K^\times$ a subgroup of index 2. Let $a \in K^\times$. We'd like to show that

$$(a,\cdot)\colon K^\times \to \{1,-1\} \tag{3.1}$$

is a homomorphism, which is equivalent to the first equation of bimultiplicativity (the other follows by symmetry). If a is a square, then this is clear because its image is identically 1 (we may let $(x, y) = (1/\sqrt{a}, 0)$). If a is not a square, then let $L := K(\sqrt{a})$; by Claim 2.11, we know that $(a, b) = 1$ if and only if $b \in \mathrm{N}(L^\times)$. Now, the Hilbert symbol with a factors as

$$K^\times \twoheadrightarrow K^\times/\mathrm{N}L^\times \simeq \{1, -1\},$$

where the isomorphism is canonical because both groups have order 2; we are using the fact that the group of norms has index 2 to construct the final bijection of order-2 groups preserving the identity, since otherwise the quotient would be too big. The projection is trivially a homomorphism.

Now, to show non-degeneracy, let $a \notin (K^\times)^2$. Then there exists some $b \in K^\times$ which is not a norm from $L := K(\sqrt{a})$, which is true if and only if $(a, b) = -1$, so non-degeneracy holds by contrapositive.

To show the converse, observe that if $a \notin (K^\times)^2$, then the map in (3.1) is surjective by non-degeneracy, and a homomorphism by bimultiplicativity. Hence its kernel, which is $\mathrm{N}(K(\sqrt{a})^\times) \subseteq K^\times$, must have index $\#\{1, -1\} = 2$. □

Example 3.2. Again, the basic case is $\mathbb{C}/\mathbb{R}$, where the group of norms is just $\mathbb{R}$, which has index 2.

Now it remains to show the following:

Theorem 3.3. *If L/K is a quadratic extension of local fields with $\mathrm{char}(K) \neq 2$, then $\mathrm{N}L^\times \subseteq K^\times$ is a subgroup of index 2.*

Note that the following proof does not cover the ramified case in residual characteristic 2.

Proof. Let $L := K(\sqrt{d})$ (where d is as a was before), so that L only depends on d up to multiplication by squares. Then we have two cases: where $v(d) = 0$, which is true if and only if $\mathcal{O}_K^\times$, and where $v(d) = 1$, which is true if and only if d is a uniformizer (as we can repeatedly cancel factors of π^2; note here v is the valuation as usual).

Case 1. Here d is a square, and $\sqrt{d} \in \mathcal{O}_K^\times$. This extension is not necessarily unramified, but we'll only do the unramified case and leave the ramified case for next week. An example of ramification is $\mathbb{Q}_2(\sqrt{3})/\mathbb{Q}_2$ (or $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{-1})$, etc.); the extension $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is unramified. We need the following:

Claim 3.4. *$\mathrm{N}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$, and more generally, $x \in K^\times$ is a norm if and only if $v(x)$ is even (so uniformizers in K are not norms).*

Proof. We make use of the "filtration trick." We have the following filtrations, which are preserved by the norm homomorphism:

$$\begin{array}{ccccccc} \mathcal{O}_L^\times & \supseteq & 1 + \mathfrak{p}_L & \supseteq & 1 + \mathfrak{p}_L^\times & \supseteq & \cdots \\ \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \\ \mathcal{O}_K^\times & \supseteq & 1 + \mathfrak{p}_K & \supseteq & 1 + \mathfrak{p}_K^\times & \supseteq & \cdots. \end{array}$$

On the associated graded terms, we first have

$$\begin{array}{ccc} \mathcal{O}_L^\times/(1+\mathfrak{p}_L) & \xrightarrow{\mathrm{N}} & \mathcal{O}_K^\times/(1+\mathfrak{p}_K) \\ \| & & \| \\ k_L^\times & \xrightarrow{\mathrm{N}} & k_K^\times. \end{array}$$

Since we are in the unramified case, k_L/k_K is a degree-two extension like L/K. To show that the norm map is surjective on the associated graded terms, we can show that it is surjective on the residue fields, that is:

Claim 3.5. *The norm map*

$$\mathrm{N}\colon \mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times, \quad x \mapsto x^{q+1} = \mathrm{Frob}(x)\cdot x,$$

is surjective (note that since $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q) \simeq \mathbb{Z}/2\mathbb{Z}$*,* $x \mapsto x^q$ *is an automorphism fixing* $\mathbb{F}_q$*; in a Galois extension, the field norm is defined as the product of all Galois conjugates of an element).*

Proof 1. The unit group of a finite field must be cyclic, so the map corresponds to

$$\mathbb{Z}/(q^2-1)\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z} \subseteq (q^2-1)\mathbb{Z}, \quad n \mapsto (q+1)n.$$

□

Proof 2 (for $p \neq 2$). If $x \in \mathbb{F}_q^\times$, then $x = \mathrm{N}(\sqrt{-x})$, and $\sqrt{-x} \in \mathbb{F}_{q^2}^\times$ since $\mathbb{F}_{q^2}$ is the unique degree two extension of $\mathbb{F}_q$. □

Proof 3. We have $\#\mathbb{F}_{q^2}^\times = q^2-1$, $\#\mathbb{F}_q^\times = q-1$, and $\#\mathrm{Ker}(\mathrm{N}) \leq (q^2-1)/(q-1) = q+1$, but the polynomial $x^{q+1}-1$ has exactly $q+1$ roots in $\overline{\mathbb{F}}_q$ since $\mathbb{F}_{q^2}/\mathbb{F}_q$ is a separable extension (finite fields are perfect). □

Thus, the map on the first associated graded term Gr_0 is surjective. On subsequent terms, we have

$$\begin{array}{ccc} (1+\mathfrak{p}_L^n)/(1+\mathfrak{p}_L^{n+1}) & \xrightarrow{\mathrm{N}} & (1+\mathfrak{p}_K^n)/(1+\mathfrak{p}_K^{n+1}) \\ \| & & \| \\ k_L & \xrightarrow{\mathrm{T}} & k_K. \end{array}$$

To check that this diagram commutes, note that because we have assumed that L/K is unramified, π is also a uniformizer of L (for instance $\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p$ is a ramified extension, and p is no longer a uniformizer of $\mathbb{Q}_p(\sqrt{p})$). Thus, under the norm map, we have

$$1+a\pi^n \xmapsto{\mathrm{N}} (1+a\pi^n)(1+\sigma a\pi^n) = 1+(a+\sigma a)\pi^n + a\sigma a\pi^{2n} \equiv 1+\mathrm{T}a\pi^n \bmod \pi^{n+1}.$$

Again, we make the following claim:

Claim 3.6. *The trace map*

$$\mathrm{T}\colon \mathbb{F}_{q^2} \to \mathbb{F}_q, \quad x \mapsto x + x^q = x + \mathrm{Frob}(x)$$

is surjective.

Proof 1. The kernel of the trace map corresponds to the roots of the Artin–Schreier polynomial $x^q + x$, which is separable, and therefore has q roots, implying $\#\mathrm{Ker}(\mathrm{T}) = q$ and $\#\mathrm{Coker}(\mathrm{T}) = q^2/q = q = \#\mathbb{F}_q$. □

PROOF 2. If q is prime to 2, then for any $x \in \mathbb{F}_q$, we have $x = \mathrm{T}(x/2)$ (proceed as above). Otherwise, if $q = 2^r$, then over $\mathbb{F}_2$, $x^2 + x + 1$ is the only monic irreducible polynomial, and $\mathbb{F}_4$ is the splitting field of this polynomial. In general, for the extension $\mathbb{F}_{2^{n+1}}/\mathbb{F}_{2^n}$, the splitting polynomial is $x^2+x+\alpha$, where we choose some α for which it's irreducible. This works for precisely half of the choices for α because the additive homomorphism

$$\mathbb{F}_{2^n} \xrightarrow{x \mapsto x^2+x} \mathbb{F}_{2^n}$$

has kernel $\mathbb{F}_2$, and therefore its image is of index 2. Any root of these polynomials will have trace 1, since they are monic, and to get an element of any other trace, simply multiply by any element of $\mathbb{F}_{2^n}$ (as the trace map is $\mathbb{F}_{2^n}$-linear). □

PROOF 3. The trace map on an extension L/K is surjective if and only if the extension is separable, which is true in this case because finite fields are perfect. □

Thus, since both the trace and norm maps are surjective for finite fields, the norm map is surjective on all associated graded terms, which by Proposition 2.9, implies that the norm map is surjective on $\mathcal{O}_L^\times$, which proves the claim. □

Now, to complete the proof of Case 1, we'd like to show that $x \in K^\times$ is a norm if and only if its valuation is even. To this end, observe that for any $y \in L^\times$, we have $N(y) = y \cdot \sigma y$, and $v(y\sigma(y)) = 2v(y)$, since $\mathrm{Gal}(L/K)$ preserves valuations. For the converse direction, simply note that π^2 is a norm. Hence if $v(d) = 0$, then $\mathrm{N}L^\times \subseteq K^\times$ is a subgroup of index 2, as desired.

Case 2. Here $v(d) = 1$, and again, $\mathrm{char}(K) \neq 2$. This ensures tame ramification, since we are working with a quadratic extension (the ramification index is not divisible by p; we will handle the wildly ramified case (where it is divisible by p) in the next lecture. We claim that $\mathrm{N}(\mathcal{O}_L^\times) \subseteq \mathcal{O}_K^\times$ has index 2 (explicitly, that $\mathrm{N}(\mathcal{O}_L^\times) = (\mathcal{O}_K^\times)^2$), and there exists some $\pi \in \mathcal{O}_K$ that is both a uniformizer and a norm. Clearly, this suffices to show that the group of norms of $L^\times$ has index 2 in $K^\times$.

Let $L := K(\sqrt{d})$, where $v(d) = 1$ and thus d is not a square. Then $N(\alpha + \beta\sqrt{d}) = \alpha^2 - d\beta^2$, and if $x \in (\mathcal{O}_K^\times)^2$, then $x \in N(\sqrt{x})$, so x is a norm. Conversely,

$$v(\alpha^2 - d\beta^2) = 0 = \min\{v(\alpha^2), v(\beta^2 + 1)\} = v(\alpha^2),$$

since the former is even and the latter odd, hence the two are unequal. It follows that $\alpha, \beta \in \mathcal{O}_K^\times$, so $x = \alpha^2 - d\beta^2$ is a square mod $\mathfrak{p}$, and this is true if and only if x is a square in $\mathcal{O}_K^\times$. Finally, since $-d = N(\sqrt{d})$, it follows that there exists a uniformizer of K that is a norm.

So the upshot is that $x \in K^\times$ is a norm for $K(\sqrt{d})$ if and only if $(-d)^{-v(x)}x$, an integral unit, is a square mod $\mathfrak{p}$, so the theorem holds in this case. □

We conclude that we can treat the case of tame ramification (which, for our purposes, includes the unramified case) by guessing explicitly what $\mathrm{N}L^\times \subseteq K^\times$ is. Wild ramification is much trickier. All of this amounts to explicit formulae for the Hilbert symbol, as we saw on Problem 2 of Problem Set 1. There is also such a formula for $\mathbb{Q}_2$, and with elbow grease, we can prove that all "good" properties of the Hilbert symbol hold in this case (see for instance **[Ser73]**).

18.786 Number Theory II: Class Field Theory

Spring 2016