LECTURE 2

Hilbert Symbols

Let K be a local field over $\mathbb{Q}_p$ (though any local field suffices) with $\mathrm{char}(K) \neq 2$. Note that this includes fields over $\mathbb{Q}_2$, since it is the characteristic of the field, and not the residue field, with which we are concerned. Recall from the previous lecture the duality

$$\mathrm{Gal}_2(K) := \mathrm{Gal}^{\mathrm{ab}}(K)/\{g^2 : g \in \mathrm{Gal}^{\mathrm{ab}}(K)\} \simeq \mathrm{Hom}\left(K^\times/(K^\times)^2, \mathbb{Z}/2\mathbb{Z}\right), \tag{2.1}$$

where $\mathrm{Gal}_2(K)$ and $\mathrm{Gal}^{\mathrm{ab}}(K)$ are profinite groups, the latter being the Galois group of the maximal abelian extension of K, and $K^\times/(K^\times)^2$ is a vector space of finite or infinite dimension over the two-element field $\mathbb{Z}/2\mathbb{Z}$ (in dualizing, the direct sum of copies of $\mathbb{Z}/2\mathbb{Z}$ comprising $K^\times/(K^\times)^2$ is changed to a product, reflecting the profinite nature of the left-hand side).

Also recall that LCFT states that $K^\times \to \mathrm{Gal}^{\mathrm{ab}}(K)$ is a profinite completion, and therefore that $\mathrm{Gal}_2(K) \simeq K^\times/(K^\times)^2$ in contrast to (2.1). Thus, LCFT predicts that there exists a canonical pairing of the following form:

DEFINITION 2.1. Let the *Hilbert symbol*

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

be defined by

$$(a,b) := \begin{cases} 1 & \text{if there exist } x,y \in K \text{ such that } ax^2+by^2=1, \\ -1 & \text{otherwise,} \end{cases}$$

for $a, b \in K^\times$.

REMARK 2.2. This definition is only well-behaved for local fields. Also note that (a,b) really is defined modulo multiplication by squares in a and b, as these can be absorbed in x and y.

PROPOSITION 2.3. *The Hilbert symbol satisfies the following properties:*

(1) Bimultiplicativity. *For all $a,b,c \in K^\times$,*

$$(a,bc) = (a,b)\cdot(a,c).$$

(2) Non-degeneracy. *For all $a \in K^\times$, if $(a,b) = 1$ for all $b \in K^\times$, then $a \in (K^\times)^2$.*

Note that $(a,b) = (b,a)$ trivially. Bimultiplicativity says that we can solve $ax^2+by^2=1$ if and only if either we can solve both $ax^2+by^2=1$ and $ax^2+cy^2=1$ separately, or we can't solve either equation. This is a bit strange, and turns out to only hold in general for local fields.

EXAMPLE 2.4. Let $K := \mathbb{R}$. Then we can solve $ax^2 + by^2 = 1$ as long as a and b are not both negative. As such, we have $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \{1, -1\}$, since $(\mathbb{R}^\times)^2 = \mathbb{R}_{>0}$, and so the pairing $\{1, -1\} \times \{1, -1\} \to \{1, -1\}$ is indeed non-degenerate.

We now ask: when is $x \in K^\times$ a square? When $K = \mathbb{R}, \mathbb{C}$, the answer is clear. When, for instance, $x \in \mathbb{Q}_2^\times$, then we may write $x = 2^{v(x)}y$ where $y \in \mathbb{Z}_2^\times$, and x is a square if and only if $v_2(x)$ is even and y is a square (which, as will be shown in Problem 1(c) of Problem Set 1, is true if and only if $y \equiv 1 \bmod 8$).

Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be the unique maximal ideal, $k := \mathcal{O}_K/\mathfrak{p}$ be the residue field with $\mathrm{char}(k) = p$, an odd prime, and $\pi \in \mathfrak{p}$ a uniformizer, that is, $\pi \notin \mathfrak{p}^2$.

CLAIM 2.5. *Let $x \in K^\times$, and write $x = \pi^{v(x)}y$, where $y \in \mathcal{O}_K^\times$. Then the following are equivalent:*

(1) x is a square;
(2) $v(x)$ is even and y is a square;
(3) $y \bmod \mathfrak{p}$ is a square in $K^\times$.

Note that we may reduce to $x \in \mathcal{O}_K^\times$. We offer two proofs:

PROOF (VIA HENSEL'S LEMMA). All explanations aside from that from the final condition are clear. So suppose $x \bmod \mathfrak{p}$ is a square in $\mathcal{O}_K^\times$. By Hensel's Lemma, the polynomial $p(t) = t^2 - x \in \mathcal{O}_K[t]$ has a root $r \in \mathcal{O}_K$ if it has a root $\bar{r}$ modulo $\mathfrak{p}$ such that $\bar{p}'(\bar{r}) \neq 0$, i.e., the derivative is nonzero. But the first condition holds by assumption, and in this case $p'(t) = 2t$ which is surely nonzero as $x = 0$, and therefore $\sqrt{x} = 0$, hence the second condition holds as well. □

PROOF (EXPLICIT). Consider the map $x \overset{\sigma}{\mapsto} x^2$, by which

$$\mathcal{O}_K^\times \xrightarrow{\sigma} S \subseteq \mathcal{O}_K^\times, \quad S := \{x \in \mathcal{O}_K^\times : x \text{ is a square mod } \mathfrak{p}\}.$$

We'd like to show that σ is surjective, that is, every element of $\mathcal{O}_K$ that is a square mod $\mathfrak{p}$ is a square in $\mathcal{O}_K^\times$. Now, observe that $\mathcal{O}_K^\times$ is a filtered abelian group with complete filtration (see Definition 2.7 below)

$$\mathcal{O}_K^\times \supseteq 1 + \mathfrak{p} \supseteq 1 + \mathfrak{p}^2 \supseteq 1 + \mathfrak{p}^2 \supseteq \cdots,$$

where the $1 + \mathfrak{p}^n$ are all open subgroups of $\mathcal{O}_K^\times$. Clearly $\mathcal{O}_K^\times/(1 + \mathfrak{p}) = k^\times$, and similarly $(1 + \mathfrak{p})/(1 + \mathfrak{p}^2) \simeq k$ as for any $1 + a\pi, 1 + b\pi \in 1 + \mathfrak{p}$, where $a, b \in \mathcal{O}_K/\mathfrak{p}$, we have $(1 + a\pi)(1 + b\pi) = 1 + (a + b)\pi + ab\pi^2$, and since $ab\pi^2 \in \mathfrak{p}^2$, we are left with $1 + (a + b)\pi$ in the associated graded term, hence multiplication simply corresponds to addition in k. Similarly, for each $n \geq 1$, we have $(1 + \mathfrak{p}^n)/(1 + \mathfrak{p}^{n+1}) \simeq k$ by a similar argument, since $n + 1 \leq 2n$. Now, σ acts on the filtration as

$$\begin{array}{ccccccc} \mathcal{O}_K^\times & \supseteq & 1 + \mathfrak{p} & \supseteq & 1 + \mathfrak{p}^2 & \supseteq & \cdots \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} & & \\ \mathcal{O}_K^\times & \supseteq & S & \supseteq 1 + \mathfrak{p} & \supseteq 1 + \mathfrak{p}^2 & \supseteq & \cdots, \end{array}$$

where the inclusion $1 + \mathfrak{p} \subseteq S$ holds since 1 is trivially a square. Now, the map

$$\mathcal{O}_K^\times/(1 + \mathfrak{p}) = k^\times \xrightarrow{\sigma} (k^\times)^2 = S/(1 + \mathfrak{p})$$

on Gr_0 is trivially surjective (and has a small kernel). Moreover, for each $n \geq 1$, the map on Gr_n is

$$(1 + \mathfrak{p}^n)/(1 + \mathfrak{p}^{n+1}) \xrightarrow{\sigma} (1 + \mathfrak{p}^n)/(1 + \mathfrak{p}^{n+1}),$$

which, since for any $x \in k$ we have

$$(1+\pi^2 x)^2 = 1 + 2x\pi^n + x^2\pi^{2n} \equiv 1 + 2x\pi^n \bmod \mathfrak{p}^{n+1}$$

as $2n \geq n+1$, is equivalent to the map $k \xrightarrow{x \mapsto 2x} k$, which is an isomorphism because $\#k = p$ is an odd prime. Thus, σ is surjective on each graded term, so by Proposition 2.9, the map $\mathcal{O}_K^\times \xrightarrow{\sigma} S$ is surjective, as desired. □

REMARK 2.6. In general, the tools we have to deal with $\mathcal{O}_K^\times$ are the $\mathfrak{p}$-adic exponential map, and this filtration, which, though an abstract formalism, has the advantage of being simpler than $\mathcal{O}_K^\times$, as the quotients are all isomorphic to finite fields. As a general principle, we can understand many things about A via its associated graded $\mathrm{Gr}_* A$.

DEFINITION 2.7. Let A be an abelian group. A *filtration* on A is a descending sequence of subgroups

$$A =: F_0 A \supseteq F_1 A \supseteq F_2 A \supseteq \cdots,$$

and it is said to be *complete* if $A \xrightarrow{\sim} \varprojlim_n A/F_n A$. The groups $\mathrm{Gr}_n A := F_n A / F_{n+1} A$ are the *associated graded terms* of the filtration.

EXAMPLE 2.8. The groups

$$\mathcal{O}_K \simeq \varprojlim_n \mathcal{O}_K/\mathfrak{p}^n \quad \text{and} \quad \mathcal{O}_K^\times \simeq \varprojlim_n \mathcal{O}_K^\times/(1+\mathfrak{p}^n)$$

are complete filtrations.

PROPOSITION 2.9. *Let $f\colon A \to B$ be a homomorphism of completely filtered abelian groups, i.e., $f(F_n A) \subset F_n B$ for each $n \geq 0$. If the induced map*

$$F_n A / F_{n+1} A \to F_n B / F_{n+1} B$$

is surjective (resp. injective), then f is surjective (resp. injective).

PROOF. Assume that the associated graded maps are surjective and that both filtrations are complete, as in the explicit proof of Claim 2.5. Suppose we have some $x \in B$, and we'd like to solve the equation $f(y) = x$ for $y \in A$. We can solve the equation $f(y_0) \equiv x \bmod F_1 B$, so that $x - f(y_0) \in F_1 B$. Then, since the associated graded map is surjective by assumption, we can solve the equation $f(\epsilon_1) \equiv x - f(y_0) \bmod F_2 B$, where $\epsilon_1 \in F_1 A$ describes an "error term" lifted from $\mathrm{Gr}_1 A$. Observe that, since f is a homomorphism, we have

$$f(y_1) = f(y_0 + \epsilon_1) = f(y_0) + f(\epsilon_1) \equiv x \bmod F_2 B,$$

where we have defined $y_1 := y_0 + \epsilon_1$. This is an equation of the same form as before, and we may iterate to find a "compatible" system of y_n such that $f(y_n) = x \bmod F_{n+1} B$ for each $n \geq 0$, where by "compatible" we mean that for each n we have $y_n \equiv y_{n+1} \bmod F_{n+1} A$. But then there is an induced element $y \in \varprojlim A/F_n A = A$ corresponding to $(y_0, y_1, \ldots)$ under the inverse limit (note that the y_n stabilize modulo $F_n A$ for large enough n), which satisfies the initial equation $f(y) = x$ since both filtrations are complete by assumption. □

REMARK 2.10. Though simple and abstract, many things (such as the previous claim) can be proved easily with the preceding proposition. The advantage of the approach via Hensel's Lemma is that here we needed to use the fact that the squaring map σ is a homomorphism, which is not true in general. Still, this

approach was able to tell us which elements of $\mathcal{O}_K^\times$ are squares in local fields of odd residual characteristic.

The upshot is that when K is a local field of odd residual characteristic, we have $[K^\times : (K^\times)^2] = 4$ since $[\mathcal{O}_K^\times : (\mathcal{O}_K^\times)^2] = 2$, and similarly for $2\mathbb{Z} \subseteq \mathbb{Z}$, so $K^\times/(K^\times)^2$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as it has a basis $\{\pi, r\} \subset \mathcal{O}_K^\times$, where π is a uniformizer and r is not a square modulo $\mathfrak{p}$ (so certainly π and r don't differ by a square).

We now reformulate the Hilbert symbol in terms of norms over extension fields; in contrast to the original definition, here we will view it asymmetrically. Suppose a is not a square, so that $K(\sqrt{a})$ is a degree 2 extension of K (note that if a is a nonzero square, then we need only understand $K(\sqrt{a})$ to be the corresponding étale extension of K, isomorphic to $K \times K$).

Claim 2.11. *We have $(a, b) = 1$ if and only if b is a norm for the extension $K(\sqrt{a})/K$, i.e., there is some element of $K(\sqrt{a})$ whose norm is b.*

Proof. Assume b is a norm, that is, there exist $\alpha, \beta \in K$ such that

$$\alpha^2 - \beta^2 a = \mathrm{N}(\alpha + \beta\sqrt{a}) = b,$$

hence $\alpha^2 = a\beta^2 + b$. Then if $\alpha \neq 0$, we have

$$a\left(\frac{\beta}{\alpha}\right)^2 + b\left(\frac{1}{\alpha}\right)^2 = 1,$$

so $(a, b) = 1$. If $\alpha = 0$, then $b + \beta^2 a = 0$. Letting

$$x := \frac{1}{2}\left(1 + \frac{1}{a}\right) \quad \text{and} \quad y := \frac{1}{2\beta}\left(1 - \frac{1}{a}\right),$$

we have

$$ax^2 + by^2 = a \cdot \frac{1}{4} \cdot \frac{(a+1)^2}{a^2} + (-\beta^2 a) \cdot \frac{1}{4\beta^2} \cdot \frac{(a-1)^2}{a^2} = \frac{(a+1)^2 - (a-1)^2}{4a} = 1,$$

so again $(a, b) = 1$.

The forward implication is a trivial reversal of the argument for nonzero α. □

We state, without proof, the main result about Hilbert Symbols. It's important that that the image of $L^\times$ under the norm is not too big (not everything), and not too small. We will see that this theorem is equivalent to the non-degeneracy of Hilbert Symbols.

Theorem 2.12. *If L/K is a quadratic extension of local fields, then the norm $\mathrm{N}\colon L^\times \to K^\times$ is a homomorphism, and $\mathrm{N}(L^\times) \subseteq K^\times$ is a subgroup of index 2.*

Example 2.13. Consider $\mathbb{C}/\mathbb{R}$.

18.786 Number Theory II: Class Field Theory

Spring 2016