EXERCISES AND SUPPLEMENTAL TOPICS FOR LECTURE 6

1. The Hilbert symbol

Let E be a local field of characteristic $\neq 2$. For $a, b \in E^\times$, the *Hilbert symbol* is defined as

$$(a,b)_E = \begin{cases} 1 & \text{if } z^2 = ax^2 + by^2 \text{ admits a nontrivial solution} \\ -1 & \text{otherwise} \end{cases}.$$

The Hilbert symbol defines a map

$$(\cdot,\cdot)_E : E^\times \times E^\times \to \mathbb{Z}/2 = \{\pm 1\}.$$

Verify the following features of the Hilbert symbol:

(1) $(\cdot,\cdot)_E$ depends only on the class modulo squares and hence defines a function $E^\times/E^{\times 2} \times E^\times/E^{\times 2} \to \{\pm 1\}$.
(2) $(a,-a)_E = 1$ for any $a \in E^\times$.
(3) $(a, 1-a)_E = 1$ for any $a \in E \setminus \{0,1\}$.
(4) $(a,1)_E = 1$ for any $a \in E^\times$.

So far, the condition that E should be a local field was not used. However, this is only a good definition in this case. The key feature is that for E a local field (of characteristic $\neq 2$), the Hilbert symbol defines a *nondegenerate bilinear pairing* (of finite-dimensional $\mathbb{F}_2$-vector spaces)

$$E^\times/E^{\times 2} \times E^\times/E^{\times 2} \to \mathbb{Z}/2.$$

We don't have the machinery to prove this in general. However, we can check it in some special cases and work out some examples.

(1) For $p > 2$, recall that $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \simeq \mathbb{F}_2^2$ where basis elements can be taken to be the classes of $\{p, \epsilon\}$ where $\epsilon \in \mathbb{Z}_p^\times$ is not a square modulo p. Work out the Hilbert symbol explicitly and check that it is bilinear.
(2) Work out the Hilbert symbol for $E = \mathbb{R}$ (and check it is bilinear).
(3) Show that if $x, y \in \mathbb{Z}_2^\times$, then the Hilbert symbol $(x,y)_2$ is given by $(-1)^{\epsilon_x \epsilon_y}$ where $\epsilon_x = \frac{x-1}{2} \bmod 2, \epsilon_y = \frac{y-1}{2} \bmod 2$. In particular, if both $x, y \equiv 1 \bmod 4$, then $(x,y)_2 = 1$. (If you are feeling ambitious, work out the Hilbert symbol on $\mathbb{Q}_2$ in general and check the bilinearity.)

The Hilbert symbol (and its bilinearity) is closely related to the structure of the Witt ring $W(E)$. The Witt ring $W(E)$ has the *fundamental ideal* $I \subset W(E)$ of even-dimensional forms, and we always have

$$W(E)/I \simeq \mathbb{Z}/2, \quad I/I^2 \simeq E^\times/E^{\times 2}.$$

(This is true without the assumption that E is a local field.) The second map $E^\times/E^{\times 2} \to I/I^2$ is given by $a \mapsto \langle 1, -a \rangle$ and its inverse is given by the *signed determinant*.

When E is a nonarchimedean local field of characteristic $\neq 2$, we have in addition

$$I^2/I^3 = \mathbb{Z}/2, \quad I^3 = 0.$$

Date: July 19, 2021.

The multiplication map

$$E^\times/E^\times \times E^\times/E^{\times 2} = I/I^2 \times I/I^2 \to I^2/I^3 = \mathbb{Z}/2$$

is exactly the Hilbert symbol.

We can work this out pretty explicitly in the case of $\mathbb{Q}_p, p > 2$ (and for $\mathbb{Q}_2$ with some more calculation).

(1) Consider the ternary quadratic form $\langle 1, -a, -b\rangle$ over the field F. Then the following are equivalent:
   - $\langle 1, -a, -b\rangle$ is isotropic over F.
   - $\langle 1, -a, -b, ab\rangle$ is hyperbolic (isomorphic to the direct sum of two hyperbolic planes).
   - b is a norm from the extension $F(\sqrt{a})$.
   - a is a norm from the extension $F(\sqrt{a})$.

(2) Check that for $\mathbb{Q}_p$ with $p > 2$, we have $I^3 = 0$ and $I/I^2 = \mathbb{Z}/2$. (Use the classification of anisotropic quadratic forms over $\mathbb{Q}_p, p > 2$.)

(3) Check that the multiplication map in the Witt ring gives the Hilbert symbol.

2. General exercises

(1) Let $p > 2$, and let $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots \in \mathbb{F}_p[[t]]$ be such that $a_0 \in \mathbb{F}_p^\times$ is a square. Then $f(t)$ is a square in $\mathbb{F}_p[[t]]$. In particular, determine the structure of squares in $\mathbb{F}_p((t))$. (This is the t-adic version of squares in $\mathbb{Q}_p^\times$. Hensel's lemma also admits a version for $\mathbb{F}_p((t))$, indeed, any nonarchimedean complete field.) In particular, the squares in $\mathbb{F}_p((t))$ form an open subgroup (of finite index). By contrast, the squares in $\mathbb{F}_2((t))$ do *not* form an open subgroup (why?).

(2) Check that any five-dimensional quadratic form over $\mathbb{Q}_2$ is isotropic. Check that the quadratic form $\langle 1, -5, 2, -10\rangle$ over $\mathbb{Q}_2$ is anisotropic.

   Use the following ingredients. The previous lecture's exercises showed that the squares in $\mathbb{Z}_2^\times$ are exactly those elements which are $\equiv 1$ modulo 8. To see the present claim, look at congruences modulo 8 and 2-adic valuations. Show that if $x, y \in \mathbb{Z}_2^\times$, then the 2-adic valuation of $x^2 - 5y^2$ is 2.)

(3) Show that if $x, y \in \mathbb{Z}_2^\times$, then the Hilbert symbol $(x, y)_2$ is given by $(-1)^{\epsilon_x \epsilon_y}$ where $\epsilon_x = \frac{x-1}{2} \bmod 2, \epsilon_y = \frac{y-1}{2} \bmod 2$. In particular, if both $x, y \equiv 1 \bmod 4$, then $(x, y)_2 = 1$.