18.786 PROBLEM SET 1

Due February 11, 2016

Let K be a finite extension of $\mathbb{Q}_p$. Let $\mathcal{O}_K$ be its ring of integers with maximal ideal $\mathfrak{p}$, and let $k = \mathcal{O}_K/\mathfrak{p}$ be the residue field. Let $v_\mathfrak{p}$ denote the valuation on K, normalized so that the valuation of a uniformizer is 1.

(1) (a) Show that the subgroup $(K^\times)^2 \subseteq K^\times$ of squares contains an open neighborhood of the identity, i.e., every element of $1+\mathfrak{p}^N$ is a square for N large enough. Give an upper bound on N.

(b) Show that $(K^\times)^2 \subseteq K^\times$ is a subgroup of index $4|k|^{v_\mathfrak{p}(2)}$.

(c) Show that $x \in \mathbb{Q}_2^\times$ is a square if and only if $v_2(x) \in 2\mathbb{Z} \subseteq \mathbb{Z}$, and $2^{-v_2(x)} \cdot x \in \mathbb{Z}_2$ is equal to 1 modulo $8\mathbb{Z}_2$.

(2) (a) For $a, b \in K^\times$, show that $\frac{a^{v_\mathfrak{p}(b)}}{b^{v_\mathfrak{p}(a)}} \in \mathcal{O}_K^\times$.

(b) Define the *tame symbol* as the pairing:

$$K^\times \times K^\times \to k^\times$$

$$(a,b) \mapsto \mathrm{Tame}(a,b) := (-1)^{v_\mathfrak{p}(a)\cdot v_\mathfrak{p}(b)} \frac{a^{v_\mathfrak{p}(b)}}{b^{v_\mathfrak{p}(a)}} \mod \mathfrak{p}.$$

For $p \neq 2$, show that the Hilbert symbol is computed by composing the tame symbol with the unique non-trivial character $k^\times \to \{1,-1\}$.

(c) If $a \in \mathbb{Z}_2^\times$, define $\varepsilon(a) \in \mathbb{Z}/2\mathbb{Z} = \{0,1\}$ as the reduction of a mod $4\mathbb{Z}_2$ under the isomorphism $(\mathbb{Z}/4\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z}$ (i.e., $\varepsilon(a) = 0$ if $a \in 1+4\mathbb{Z}_2$ and $\varepsilon(a) = 1$ if $a \in 3+4\mathbb{Z}_2$).

If $a, b \in \mathbb{Z}_2^\times$, show that their Hilbert symbol is computed as:

$$(a,b) = (-1)^{\varepsilon(a)\varepsilon(b)}.$$

(d) Further show that $(2,2) = 1$, and that for $a \in \mathbb{Z}_2^\times$:

$$(a,2) = (-1)^{\theta(a)}.$$

Here $\theta(a) \in \mathbb{Z}/2\mathbb{Z}$ is the reduction of a^2 mod $16\mathbb{Z}_2$ under the isomorphism between the squares in $(\mathbb{Z}/16\mathbb{Z})^\times$ (which are 1 and 9) and $\mathbb{Z}/2\mathbb{Z}$.

Using bimultiplicativity, deduce an explicit formula for the 2-adic Hilbert symbol (which could be deduced using similarly elementary methods and some more work).

(3) Let $\ldots \subseteq F_2A \subseteq F_1A \subseteq F_0A = A$ and $\ldots \subseteq F_2B \subseteq F_1B \subseteq F_0B = B$ be abelian groups with complete filtrations.

Let $f : A \to B$ be a map that is *not necessarily a homomorphism*, but preserves the filtration in the sense that for every $x \in A$, f maps $x + F_nA$ to $f(x) + F_nB$.

Date: February 3, 2016.

(a) For every $x \in A$, show that the *symbol map*:

$$F_nA/F_{n+1}A \xrightarrow{y \mapsto f(x+y)-f(x)} F_nB/F_{n+1}B$$

is well-defined.

(b) Suppose that for all $x \in A$, the associated symbol map is surjective. Show that f is surjective.

(c) Deduce Hensel's lemma: for $f(t) \in \mathcal{O}_K[t]$ a polynomial with $f(\mathfrak{p}) \subseteq \mathfrak{p}$ and $f'(\mathfrak{p}) \subseteq \mathcal{O}_K^\times$, f has a zero. (Then look up Hensel's lemma on Wikipedia and make sure you understand why this statement is equivalent to that one. E.g., use it to show that -1 is a square in $\mathbb{Q}_5$.)

Now let K be any local field of characteristic $\neq 2$.[1] You may assume the bimultiplicativity of the Hilbert symbol in the next problems.

(4) For $a, b, \lambda \in K^\times$, so that $ax^2 + by^2 = \lambda$ has a solution if and only if we have the Hilbert symbol equality $(-ab, \lambda) = (a, b)$.

(5) For $a, b \in K^\times$, define the *quaternion algebra* $H_{a,b}$ to be the (unital, associative) K-algebra generated by elements i, j and with relations

$$i^2 = a, j^2 = b, ij = -ji.$$

(a) Show that $H_{a,b}$ is 4-dimensional as a K-vector space, with basis $\{1, i, j, ij\}$.

(b) Show that the Hilbert symbol (a, b) equals 1 if and only $H_{a,b}$ is isomorphic to $M_2(K)$, the algebra of 2×2-matrices over K.

[1] This means we do not allow $\mathbb{F}_{2^n}((t))$, but e.g. $\mathbb{Q}_2$ is still allowed.