THE HILBERT SYMBOL

This lecture is based on the book *A course in Arithmetic* by Serre, all the omitted proofs can be found there.

In the whole lecture, let $k = \mathbb{Q}_v$ for some $v \in V = \{\infty\} \cup \{p \text{ prime}\}$, where $\mathbb{Q}_\infty = \mathbb{R}$.

Definition. *For any $a, b \in k^*$, the Hilbert symbol of a and b relative to $\mathbb{Q}_v$ is defined as*

$$(a,b)_v := \begin{cases} +1 & \text{if } z^2 - ax - by^2 = 0 \text{ has a nontrivial solution in } k^3, \\ -1 & \text{otherwise.} \end{cases}$$

Remark. *If a and b are multiplied by squares, $(a,b)_v$ doesn't change, thus $(\ \ ,\ \ )_v$ defines a map*

$$k^*/k^{*2} \times k^*/k^{*2} \longrightarrow \{\pm 1\}.$$

Proposition 1. *Let $a, b \in k^*$ and $k_b = k(\sqrt{b})$. We have $(a,b)_v = 1$ if and only if $a \in N(k_b^*)$, the group of norms of elements of k_b^*.*

Proof. Easy. □

Proposition 2. *Let $a, a', b, c \in k$. We have:*

i) $(a,b)_v = (b,a)_v$ *and* $(a,c^2)_v = 1$,
ii) $(a,-a)_v = (a,1-a)_v = 1$,
iii) $(a,b)_v = 1 \Rightarrow (a,b)_v = (aa',b)_v$,
iv) $(a,b)_v = (a,-ab)_v = (a,(1-a)b)_v$,

Proof. $i)$ and $ii)$ are trivial and $iv)$ is implied by $ii)$ and $iii)$. To prove $iii)$, apply Proposition 1. □

Lemma 1. *All quadratic forms in at least 3 variables over a finite fields have a nontrivial zero.*

Proof. See Serre's book. □

Lemma 2. *Let x be a zero of the reduction modulo p of a polynomial $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$. Then, if x is simple (i.e. $\partial f/\partial X_i(x) \neq 0$ for some i), it lifts to a zero of f with coefficients in Z_p.*

Proof. See Serre's book. Anyway, it's nothing deep, it's just a simple application of Taylor's formula. □

Lemma 3. *Let $v \in \mathbb{Z}_p^*$ a p-adic unit. If the equation $z^2 - px^2 - wy^2 = 0$ has a nontrivial solution in $\mathbb{Q}_p$, it has a solution (z,x,y) with $z, y \in \mathbb{Z}_p^*$ and $x \in \mathbb{Z}_p$.*

Proof. See Serre's book. □

Theorem 1. *If $k = \mathbb{R}$, we have*

$$(a,b)_\infty = \begin{cases} +1 & \text{if } a \text{ or } b > 0, \\ -1 & \text{otherwise.} \end{cases}$$

If $k = \mathbb{Q}_p$ and if we write $a = p^\alpha u$, $b = p^\beta w$, with $u, w \in \mathbb{Z}_p^*$, we have

$$(a,b)_p = (-1)^{\alpha\beta\frac{(p-1)}{2}} \left(\frac{\overline{u}}{p}\right)^\alpha \left(\frac{\overline{w}}{p}\right)^\beta \qquad \text{if } p > 2,$$

$$(a,b)_2 = (-1)^{\frac{\overline{u}-1}{2}\frac{\overline{w}-1}{2}+\alpha\frac{\overline{w}^2-1}{8}+\beta\frac{\overline{u}^2-1}{8}} \left(\frac{\overline{u}}{p}\right)^\alpha \left(\frac{\overline{w}}{p}\right)^\beta.$$

Proof. If k=$\mathbb{R}$ the assertion is trivial. Let $k = \mathbb{Q}_p$ with $p > 2$. We can split the problem in three cases:

(1) $\alpha \equiv \beta \equiv 0 \pmod 2$. We must check that $(u,w)_p = 1$. By lemma 1, the equation
$$z^2 - ux^2 - wy^2 = 0$$
has a nontrivial zero mod p. By lemma 2, this lifts to $\mathbb{Z}_p$ and so $(u,v)_p = 1$.

(2) $\alpha \equiv 1$, $\beta \equiv 0 \pmod 2$. We must check that $(pu,w)_p = \left(\frac{\overline{w}}{p}\right)$ and this, by 1) and *iii*) of Proposition 2, is equivalent to $(p,w)_p = \left(\frac{\overline{w}}{p}\right)$. If w is a square, both sides are clearly equal to 1, otherwise $\left(\frac{\overline{w}}{p}\right) = -1$ and so is $(p,w)_p$ by Lemma 3.

(3) $\alpha \equiv \beta \equiv 1 \pmod 2$. We must check that
$$(pu,pw)_p = (-1)^{(p-1)/2} \left(\frac{\overline{u}}{p}\right)\left(\frac{\overline{w}}{p}\right).$$
By *iv*) of Proposition 2, we have
$$(pu,pw)_p = (pu, -p^2uw)_p = (pu, -uw)_p$$
and, by 2), this is
$$\left(\frac{\overline{uw}}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\overline{u}}{p}\right)\left(\frac{\overline{w}}{p}\right) = (-1)^{(p-1)/2}\left(\frac{\overline{u}}{p}\right)\left(\frac{\overline{w}}{p}\right)$$

For the case $p = 2$, see Serre's book. □

Theorem 2. *The Hilbert symbol is a bilinear form on the $\mathbf{F}_2$-vector space k^*/k^{*2}. That is,*
$$(aa', b)_v = (a,b)_v(a',b)_v,$$
for all $a, a', b \in k^*$. Moreover the Hilbert symbol is nondegenerate, i.e. if $b \in k^*$ is such that $(a,b)_v = 1$ for all $a \in k^*$, then $b \in k^{*2}$.

Proof. The bilinearity is clear form Theorem 1. To prove the nondegeneracy, see Serre's book. □

Theorem 3. *If $a, b \in \mathbb{Q}^*$, we have $(a, b)_p = 1$ for almost all primes p and*

$$\prod_{v \in V} (a, b)_p = 1.$$

Proof. Since the Hilbert symbols are bilinear, we just need to consider the case when a, b are equal to a prime or to -1. Theorem 1 and the quadratic reciprocity law allow us to do explicitly the computations and to prove the theorem. □

Theorem 4. *Let $(a_i)_{i \in I}$ a finite family of elements of $\mathbb{Q}^*$ and let $(\varepsilon_{i,v})_{i \in I, v \in V}$ a family of numbers equal to ± 1. Then, there exists an $x \in \mathbb{Q}^*$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$ and all $v \in V$ if and only if*

(1) $\varepsilon_{i,v} = 1$ for almost all $v \in V$.
(2) $\prod_v \varepsilon_{i,v} = 1$ for all $i \in I$.
(3) For all $v \in V$ there exists $x_v \in \mathbb{Q}_v^*$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$.

Proof. See Serre's book (the proof uses Dirichlet theorem on the infinity of primes in any arithmetic progression and the density of $\mathbb{Q}$ in $\prod_v \mathbb{Q}_v$). □