El símbolo de Hilbert

Índice

1 El Lema de Hensel

Fijamos un cuerpo (conmutativo) local no arquimedeano F y denotamos por $\mathfrak{o}$ su anillo de enteros y por $\mathfrak{p}$ el ideal maximal. Fijamos, además, un uniformizador, $\pi_{\mathfrak{p}}$. Denotamos por $v(x)$ la valuación de $x \in F^{\times}$.

Lema 1.1. *Sea $f \in \mathfrak{o}[X]$ con derivada f'. Si $x \in \mathfrak{o}$ y $n, k \in \mathbb{Z}$ cumplen:*

- $0 \leq 2k < n$,
- $f\,x \equiv 0 \,(\mathsf{mod}\, \pi^n)$ y
- $v(f'\,x) = k$.

Entonces, existe $y \in \mathfrak{o}$ tal que

- $f\,y \equiv 0 \,(\mathsf{mod}\, \pi^{n+1})$,
- $y \equiv x \,(\mathsf{mod}\, \pi^{n-k})$ y
- $v(f'\,y) = k$.

Demostración. Eligiendo $y = x + \pi^{n-k} z$, $z \in \mathfrak{o}$,

$$f\,y \;=\; f\,x \;+\; \pi^{n-k}\, z\, f'\,x \;+\; \pi^{2(n-k)}\, a \;,$$

para cierto $a \in \mathfrak{o}$. Pero $f\,x = \pi^n\, b$, para cierto $b \in \mathfrak{o}$ y $f'\,x = \pi^k\, c$, $c \in \mathfrak{o}^{\times}$. Entonces,

$$f\,y \;=\; \pi^n \left((b + cz) + \pi^{n-2k}\, a \right) \;,$$

con lo cual,

$$f\,y \;\equiv\; 0 \,(\mathsf{mod}\, \pi^{n+1}) \qquad \Leftrightarrow \qquad b + cz \;\equiv\; 0 \,(\mathsf{mod}\, \pi) \;.$$

Ahora, para cierto $a' \in \mathfrak{o}$,

$$f'\,y \;=\; f'x \;+\; \pi^{n-k}\, a' \;.$$

Como $n - k > k = v(f'\,x)$, se verifica que $v(f'\,y) = v(f'\,x) = k$. □

Teorema 1.2. *Sea $f \in \mathfrak{o}[X_1, \ldots, X_m]$. Si $x \in \mathfrak{o}^m$, $n, k \in \mathbb{Z}$ y $1 \leq j \leq m$ cumplen*

- $0 \leq 2k < n$,
- $f\,x \equiv\; 0 \,(\mathsf{mod}\, \pi^n)$ y
- $v\big(\frac{\partial f}{\partial X_j}(x)\big) = k$,

entonces existe $y \in \mathfrak{o}^m$ tal que

- $f\,y = 0$ e
- $y \equiv x \,(\mathsf{mod}\, \pi^{n-k})$.

Demostración. Si $m = 1$, definimos una secuencia de la siguiente manera: tomamos $x^{(0)} = x$, solución módulo π^n, y, para $q \geq 0$, una solución módulo π^{n+q+1}, $x^{(q+1)}$, congruente con $x^{(q)}$ módulo π^{n-k+q} (Lema 1.1). Si $y = \lim_{q\to\infty} x^{(q)}$, entonces $f\,y = 0$, por continuidad de f. Además, $y \equiv x \,(\mathsf{mod}\, \pi^{n-k})$ y $v(f'\,y) = v(f'\,x) = k$. En general, si $m \geq 1$ y j es tal que $v\big(\frac{\partial f}{\partial X_j}(x)\big) = k$, definimos

$$\tilde{f}(X) \,=\, f(x_1, \,\ldots,\, x_{j-1},\, X,\, x_{j+1},\, \ldots,\, x_m) \,\in\, \mathfrak{o}[X] \;,$$

reduciendo el problema al caso anterior. □

Corolario 1.3. *Si $x \in \mathfrak{o}^m$ es un cero simple de $f \in \mathfrak{o}[X_1, \ldots, X_m]$ módulo π, entonces existe un (único) cero de f en $\mathfrak{o}^m$ (congruente con x módulo π).*

Demostración. Es el caso $n = 1$ y $k = 0$. □

Nos interesa aplicar estos resultados al caso en que f representa una forma cuadrática. Si

$$f \,=\, \sum_{i\leq j} a_{ij}\, X_i X_j \,\in\, \mathfrak{o}[X_1, \,\ldots,\, X_m] \tag{1}$$

es un polinomio homogéneo de grado 2, las derivadas parciales están dadas por:

$$\frac{\partial f}{\partial X_j} \,=\, \sum_{i<j} a_{ij}\, X_i \,+\, 2\, a_{jj}\, X_j \,+\, \sum_{j<k} a_{jk}\, X_k \;. \tag{2}$$

Sea $N = [\,a_{ij}\,]$, la matriz de coeficientes; esta matriz es triangular superior. Entonces, el sistema de ecuaciones $\frac{\partial f}{\partial X_j} = 0$ está representado por la matriz

$$N \,+\, {}^t\!N \,=\, \begin{bmatrix} 2\,a_{11} & a_{12} & \cdot & a_{1m} \\ a_{12} & 2\,a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1m} & a_{2m} & \cdots & 2\,a_{mm} \end{bmatrix} \;. \tag{3}$$

La matriz (3) es el doble de la matriz asociada a la forma cuadrática correspondiente a f. Sea $Q : F^m \to F$ la forma cuadrática representada por f en la base canónica.[1] Dado que f tiene coeficientes enteros, también podemos interpretar que f representa una forma cuadrática en sobre el cuerpo residual $\mathfrak{o}/\mathfrak{p}$; denotamos por $\tilde{Q} : \big(\mathfrak{o}/\mathfrak{p}\big)^m \to \mathfrak{o}/\mathfrak{p}$ la forma cuadrática reducida. Una *solución primitiva* de $Q(x) = a$ o, más en general, de $Q(x) \equiv a \,(\mathsf{mod}\, \pi^n)$, es un vector $x \in \mathfrak{o}^m$ que verifica $Q(x) = a$, o bien $Q(x) \equiv a \,(\mathsf{mod}\, \pi^n)$, y, además, alguna de sus coordenadas es una unidad. Es decir, x es una solución primitiva, si, al reducir coordenadas módulo π, no es el vector nulo. Una solución primitiva de $Q(x) = a$ módulo π es lo mismo que una solución no trivial de $\tilde{Q}(x) = a$.

[1] Si la característica del cuerpo de base es distinta de 2, asociamos, a una forma cuadrática Q, la forma bilineal simétrica $B(x, y) = \frac{Q(x+y)-Q(x)-Q(y)}{2}$. Así, si M denota la matriz asociada a B en la base canónica, vale que $2\,M = N + {}^t\!N$. Si la característica del cuerpo de base es 2, entonces la forma bilineal *alternada* asociada es $B(x, y) = Q(x + y) + Q(x) + Q(y)$. La matriz correspondiente es igual a $N + {}^t\!N$, pero esta matriz pierde la información de la diagonal.

Definición 1.4. El *discriminante* de la forma cuadrática $Q : F^m \to F$ asociada al polinomio f dado por (1) es el determinante de la matriz $N + {}^tN$ definida en (3):

$$\mathsf{disc}(Q) \;=\; \mathsf{det}\big(N + {}^tN\big) \;.$$

Corolario 1.5. *Si* $\mathsf{disc}(Q) \in \mathfrak{o}^\times$*, toda solución primitiva de* $Q(x) = a$ *módulo* π *da lugar a una solución de* $Q(x) = a$*; precisamente, si* $x \in \mathfrak{o}^m$ *cumple que* $Q(x) \equiv a \,(\mathsf{mod}\,\pi)$*, entonces existe* $y \in \mathfrak{o}^m$ *tal que* $y \equiv x \,(\mathsf{mod}\,\pi)$ *y* $Q(y) = a$*.*

Demostración. Si $\mathsf{det}(N + {}^tN) \in \mathfrak{o}^\times$, entonces toda solución primitiva de $Q(x) \equiv a \,(\mathsf{mod}\,\pi)$ es simple. La condición $\mathsf{det}(N + {}^tN) \in \mathfrak{o}^\times$ equivale a

$$x \not\equiv 0 \pmod{\pi} \qquad \Rightarrow \qquad \frac{\partial f}{\partial X_j}(x) \not\equiv 0 \pmod{\pi} \text{ , para algún } j \;.$$

□

Supongamos que $f \in \mathfrak{o}[X_1, \ldots, X_m]$ está escrito de la siguiente manera:

$$f \;=\; \sum_{i,j} a_{ij}\, X_i X_j \;=\; \sum_{i<j} (a_{ij} + a_{ji})\, X_i X_j \;+\; \sum_{i=1}^{m} a_{ii}\, X_i^2 \;. \tag{4}$$

Entonces, si f es simétrico, es decir, $a_{ij} = a_{ji}$, las derivadas parciales están dadas por:

$$\frac{\partial f}{\partial X_j} \;=\; 2 \sum_{i=1}^{m} a_{ij}\, X_i \;. \tag{5}$$

Sea $A = [\, a_{ij} \,]$. El sistema $\frac{\partial f}{\partial X_j} = 0$ está representado por la matriz $A + {}^tA = 2\,A$.

Corolario 1.6. *Si la característica residual de* F *es impar y* $f \in \mathfrak{o}[X_1, \ldots, X_m]$ *es un polinomio homogéneo de grado* 2 *simétrico de la forma* (4) *y se cumple que* $\mathsf{det}(a_{ij}) \in \mathfrak{o}^\times$*, entonces toda solución primitiva de* $f\,x \equiv a \,(\mathsf{mod}\,\pi)$ *se levanta a una solución de* $f\,x = a$*.*

Demostración. Dado que, en este caso, $2 \in \mathfrak{o}^\times$, la condición $\mathsf{det}(A + {}^tA) \in \mathfrak{o}^\times$ equivale a $\mathsf{det}(A) \in \mathfrak{o}^\times$. Por lo tanto, f y x están en las condiciones del Corolario 1.3. □

Corolario 1.7. *Si la característica residual de* F *es par, sea* $e \geq 1$ *el grado de ramificación sobre* $\mathbb{Q}_2$*, es decir,* $\langle 2 \rangle = \langle \pi^e \rangle$*. Si* $f \in \mathfrak{o}[X_1, \ldots, X_m]$ *es un polinomio homogéneo de grado* 2 *simétrico de la forma* (4) *y* $x \in \mathfrak{o}^m$ *cumple*

- $f\,x \equiv a \,(\mathsf{mod}\,\pi^{2e+1})$ *y*
- $\frac{\partial f}{\partial X_j}(x) \not\equiv 0 \,(\mathsf{mod}\,\pi^{e+1})$,

entonces x *se levanta a una solución de* $f\,x = a$*. La condición en las derivadas se cumple, si* $\mathsf{det}(A) \in \mathfrak{o}^\times$ *y* x *es una solución primitiva de* $f\,x \equiv a$*, es decir,* $x \not\equiv 0 \,(\mathsf{mod}\,\pi)$*.*

Demostración. En cuanto a la primera parte, dado que $v(2) = e$, las derivadas parciales de f se anulan automáticamente con orden, al menos, e. Bajo las condiciones sobre f, x y las derivadas, se satisfacen las hipótesis del Teorema 1.2, con $k = e$ y $n = 2e + 1$. □

Lema 1.8. *Si $v \in \mathfrak{o}^\times$, la ecuación*

$$z^2 \,-\, \pi\, x^2 \,-\, v\, y^2 \,=\, 0 \tag{6}$$

admite solución no trivial en F, si y sólo si admite una solución (z, x, y) tal que $z, y \in \mathfrak{o}^\times$ y $x \in \mathfrak{o}$.

Demostración. Por homogeneidad, si (6) tiene una solución no trivial en F, existe una solución primitiva, es decir, existe una solución $(z, x, y) \in F^3$, donde $x, y, z \in \mathfrak{o}$ y

$$\min\big\{v(x), v(y), v(z)\big\} \,=\, 0\ .$$

Dado que $v \in \mathfrak{o}^\times$, vale $v(y) \geq 1$ si y sólo $v(z) \geq 1$. Pero, en ese caso, $v(\pi\, x^2) \geq 2$ y, en consecuencia, $v(x) \geq 1$. Es decir, si la solución $(z, x, y) \in \mathfrak{o}^3$ es primitiva, debe cumplirse $y, z \in \mathfrak{o}^\times$. □

2 Definición y propiedades

En esta sección, F denota un cuerpo (conmutativo) arbitrario. Fijamos F^{a}/F una clausura algebraica de F. Dados $a, b \in F^\times$, nos interesa saber bajo qué condiciones la forma cuadrática $Q : F^3 \to F$ dada por

$$Q(z, x, y) \,=\, z^2 \,-\, a\, x^2 \,-\, b\, y^2$$

es isotrópica sobre F, es decir, bajo qué condiciones,

$$Q(z, x, y) \,=\, 0 \tag{7}$$

admite una solución no trivial en F.

Definición 2.1. Dados $a, b \in F^\times$, el *símbolo de Hilbert (de a y b respecto de F)* es

$$(a, b)_F \,=\, (a, b) \,=\, \begin{cases} 1\ , & \text{si (7) admite solución no trivial en } F\ , \\ -1\ , & \text{si no.} \end{cases}$$

Proposición 2.2. *Si $b \notin (F^\times)^2$, sea $E = F(\sqrt{b}) \subset F^{\mathsf{a}}$. Entonces,*

$$(a, b) \,=\, 1 \qquad \Leftrightarrow \qquad a \,\in\, \mathsf{Nm}(E^\times)\ ,$$

donde $\mathsf{Nm} : E^\times \to F^\times$ es la norma de la extensión E/F.

Demostración. La norma $\mathsf{Nm} : E^\times \to F^\times$ está dada por $\mathsf{Nm}(z + \sqrt{b}\, y) = z^2 - b\, y^2$. Si $a = \mathsf{Nm}(z + \sqrt{b}\, y)$, entonces $(z, 1, y)$ es una solución no trivial de (7). Recíprocamente, si $(z, x, y) \in F^3$ es solución no trivial, necesariamente $x \neq 0$ (pues $b \notin (F^\times)^2$) y, por lo tanto, $a = \mathsf{Nm}((z/x) + \sqrt{b}\,(y/x))$. □

Observación 2.3. El símbolo de Hilbert tiene las siguientes propiedades:

(i) $(a,b) = (b,a)$,

(ii) $\big(a, c^2\big) = 1$,

(iii) $(a,-a) = (a,1-a) = 1$,

(iv) si $(a,b) = 1$, entonces $(aa',b) = (a',b)$,

(v) $(a,b) = (a,-ab) = (a,(1-a)\,b)$.

En particular, de (ii), se deduce que el símbolo de Hilbert induce una aplicación

$$F^\times/(F^\times)^2 \times F^\times/(F^\times)^2 \to \big\{\pm 1\big\}\ . \tag{8}$$

Más adelante veremos que el símbolo de Hilbert tiene la siguiente propiedad:

$$\big(aa',b\big) \;=\; (a,b)\ \big(a',b\big)\ . \tag{9}$$

El conjunto $\big\{\pm 1\big\}$ es una realización del cuerpo de dos elementos; el cociente $F^\times/(F^\times)^2$ es un espacio vectorial sobre $\big\{\pm 1\big\}$. La igualdad (9) es la bilinealidad de (8)

3 Cálculo local en característica 0

En esta sección, F denota un cuerpo (conmutativo) local, arquimedeano o no arquimedeano.

Teorema 3.1. *Sea F un cuerpo local arquimedeano, $F = \mathbb{R}$ o $F = \mathbb{C}$, y sean $a, b \in F^\times$. Si $F = \mathbb{C}$, entonces $(a,b) = 1$; si $F = \mathbb{R}$, entonces*

$$(a,b) \;=\; \begin{cases} 1\ , & \text{si } a>0 \text{ o } b>0\ , \\ -1\ , & \text{si } a<0 \text{ y } b<0\ . \end{cases}$$

Demostración. Si $F = \mathbb{C}$, entonces $\mathbb{C}^\times = (\mathbb{C}^\times)^2$. Si $F = \mathbb{R}$, entonces $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \big\{\pm 1\big\}$. □

Lema 3.2. *Sean p un primo racional impar y $F = \mathbb{Q}_p$. Si $u, v \in \mathbb{Z}_p^\times$,*

- $(u,v) = 1$,
- $(pu,v) = \left(\dfrac{v}{p}\right)$ *y*
- $(pu,pv) = (pu,-uv) = \left(\dfrac{-uv}{p}\right)$

Demostración. Dado que el cuerpo residual $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$ es finito, la ecuación $c^2 - u\,x^2 - v\,y^2$ tiene solución para todo $c \in \mathbb{F}_p$. En particular, eligiendo $z = c \not\equiv 0 \,(\mathsf{mod}\, p)$, $Q(z,x,y) = 0$ tiene soluciones primitivas módulo p. Como $\mathsf{disc}(Q) = 8uv \in \mathbb{Z}_p^\times$, por el Corolario 1.5, toda solución primitiva módulo p da lugar a una solución no trivial en $\mathbb{Q}_p$. En particular, $(u,v) = 1$.

Por la Observación 2.3 (iv), como $(u,v) = 1$,

$$(pu, v) \;=\; (p, v) \;\; .$$

Si $(v/p) = 1$, esto quiere decir que v es un cuadrado módulo p, luego, por el Teorema 1.2, es un cuadrado en $\mathbb{Z}_p^\times$ y, por la Observación 2.3 (ii), $(p,v) = 1$, también. Recíprocamente, si $(p,v) = 1$, la ecuación $z^2 - p\,x^2 - v\,y^2 = 0$ admite una solución de la forma $(z,x,y) \in \mathbb{Z}_p$, $y, z \in \mathbb{Z}_p^\times$, con lo que v es un cuadrado en $\mathbb{Z}_p$ y $(v/p) = 1$.

Finalmente, por la Observación 2.3 (v) y el caso anterior,

$$(pu, pv) \;=\; \big(pu, -p^2uv\big) \;=\; (pu, -uv) \;=\; \left(\frac{-uv}{p}\right) .$$

□

Teorema 3.3. *Sean p un primo racional impar y $F = \mathbb{Q}_p$ y sean $a, b \in \mathbb{Q}_p^\times$. Si $a = p^m\, u$ y $b = p^n\, v$, donde $u, v \in \mathbb{Z}_p^\times$, entonces*

$$(a,b) \;=\; (-1)^{mn\frac{p-1}{2}} \left(\frac{u}{p}\right)^n \left(\frac{v}{p}\right)^m \;\; .$$

En particular,

$$(a,b) \;:\; F^\times/(F^\times)^2 \;\times\; F^\times/(F^\times)^2 \;\to\; \big\{\pm 1\big\}$$

es una forma bilineal no degenerada.

Demostración. Por la Observación 2.3 (ii) y (iv), basta considerar los casos $m, n \in \big\{0, 1\big\}$. Por (i), podemos suponera $m \geq n$. Entonces, el resultado es consecuencia del Lema 3.2.

Para ver que la forma es no degenerada, elegimos representantes de ${\mathbb{Q}_p}^\times/({\mathbb{Q}_p}^\times)^2$: $\{1, p, u_0, u_0p\}$, donde $u_0 \in \mathbb{Z}_p^\times$ no es cuadrado, es decir, $(u_0/p) = -1$. Entonces, mirando módulo p, o bien usando la fórmula, para cada $a \in \{u_0, p, u_0p\}$, existe b tal que $(a,b) = -1$. □

Si $p = 2$, $\mathbb{Z}_2^\times = 1 + 2\,\mathbb{Z}_2$ y

$$\big(\mathbb{Z}_2^\times\big)^2 \;\subset\; 1 \;+\; 8\,\mathbb{Z}_2 \;\; .$$

Por el Teorema 1.2, vale la igualdad. Dado $u \in \mathbb{Z}_2^\times$, definimos

$$\epsilon(u) \;=\; \frac{u-1}{2} \qquad \text{y} \qquad \omega(u) \;=\; \frac{u^2-1}{8} \;\; .$$

Observación 3.4. Si $u \in \mathbb{Z}_{\geq} 1$ es un entero impar positivo,

$$(-1)^{\epsilon(u)} \,=\, \left(\frac{-1}{u}\right) \qquad \text{y} \qquad (-1)^{\omega(u)} \,=\, \left(\frac{2}{u}\right) \,,$$

donde $(\cdot/u)$ denota el símbolo de Jacobi. $u \mapsto (-1/u)$ y $u \mapsto (2/u)$ definen caracteres del grupo de unidades $\big(\mathbb{Z}/8\mathbb{Z}\big)^{\times}$. El isomorfismo

$$\frac{\big(1+2\,\mathbb{Z}_2\big)}{\big(1+8\,\mathbb{Z}_2\big)} \,\simeq\, \big(\mathbb{Z}/8\mathbb{Z}\big)^{\times}$$

dado por reducir módulo 8 permite trasladar estos caracteres a caracteres de $\mathbb{Z}_2^{\times} = 1+2\,\mathbb{Z}_2$. Definimos

$$\chi_4(u) \,=\, \left(\frac{-1}{\tilde{u}}\right) \qquad \text{y} \qquad \chi_8(u) \,=\, \left(\frac{2}{\tilde{u}}\right) \,,$$

donde $\tilde{u} \in \{1,3,5,7\}$ denota la clase correspondiente a u módulo 8. Se cumple que

$$\chi_4(-1) \,=\, -1 \qquad \text{y} \qquad \chi_8(-1) = 1 \,.$$

Lema 3.5. *Sea $F = \mathbb{Q}_2$. Si $u, v \in \mathbb{Z}_2^{\times}$,*

- $(u,v) = (-1)^{\epsilon(u)\,\epsilon(v)}$,
- $(2,v) = \chi_8(v) = (-1)^{\omega(v)}$,
- $(2u,v) = (2,v)\;(u,v) = \chi_8(v)\;(u,v)\;$ *y*
- $(2u,2v) = (2u,-uv) = \chi_8(uv)\;(u,v)$.

Observación 3.6. Si $p, q \in \mathbb{Z}_{\geq 1}$ son enteros impares positivos y coprimos entre sí,

$$(p,q)_{\mathbb{Q}_2} \,=\, (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}} \,=\, \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \,,$$

que es el factor en la Ley de reciprocidad cuadrática.

Demostración. Si $u \equiv 1 \,(\mathsf{mod}\, 4)$, entonces $u \in 1+8\,\mathbb{Z}_2$ o bien $u \in 5+8\,\mathbb{Z}_2$. En el primer caso, u es un cuadrado y $(u,v) = 1$. En el segundo caso, $u+4\,v \in 1+8\,\mathbb{Z}_2$ y es un cuadrado, $w^2 = u+4\,v$, con lo que $z^2 - u\,x^2 - v\,y^2$ admite la solución no trivial $(w,1,2)$ y $(u,v) = 1$, también. Si $u, v \in 3+4\,\mathbb{Z}_2$, entonces

$$z^2 \,-\, u\,x^2 \,-\, v\,y^2 \,=\, 0 \quad \Rightarrow \quad z^2 \,+\, x^2 \,+\, y^2 \,\equiv\, 0 \,(\mathsf{mod}\, 4) \quad \Rightarrow \quad x, y, z \,\equiv\, 0 \,(\mathsf{mod}\, 2) \,,$$

con lo cual, (7) no admite soluciones primitivas y $(u,v) = -1$. Esto prueba la primera afirmación: el símbolo de Hilbert es 1, si y sólo si al menos uno de u y v es congruente a 1 módulo 4.

Si $(2, v) = 1$, por el Lema 1.8, existe una solución de $z^2 - 2\,x^2 - v\,y^2 = 0$ con $z, x, y \in \mathbb{Z}_2$ y $z, y \in \mathbb{Z}_2^\times$. Mirando esta solución módulo 8, $z^2 \equiv y^2 \equiv 1 \,(\mathsf{mod}\, 8)$ y

$$1 \,-\, 2\,x^2 \,-\, v \,\equiv\, 0 \,(\mathsf{mod}\, 8)\ ;$$

como x^2 es 0, 1 o 4 módulo 8, $v \equiv \pm 1 \,(\mathsf{mod}\, 8)$ y $\chi_8(v) = 1$. Recíprocamente, supongamos que $\chi_8(v) = 1$, es decir, que $v \equiv \pm 1 \,(\mathsf{mod}\, 8)$. Si $v \equiv 1 \,(\mathsf{mod}\, 8)$, entonces $v \in \left(\mathbb{Z}_2^\times\right)^2$ es un cuadrado y $(2, v) = 1$; si $v \equiv -1 \,(\mathsf{mod}\, 8)$ se cumple que $z^2 - 2\,x^2 - v\,y^2 = 0$ tiene a $(1, 1, 1)$ como solución primitiva módulo 8, que, por el Corolario 1.7, se levanta a una solución (no trivial) en $\mathbb{Z}_2^3$ y, así, $(2, v) = 1$, en este caso también.

La igualdad $(2u, v) = (2, v)\ (u, v)$ es un caso particularidad de la "bilinealidad" del símbolo de Hilbert. Si $(2, v) = 1$ o si $(u, v) = 1$, entonces, por la Observación 2.3 (iv), sabemos que se cumple dicha igualdad. Supongamos que $(2, v) = (u, v) = -1$; la afirmación es que $(2u, v) = 1$, en este caso. Entonces, $v \equiv 3 \,(\mathsf{mod}\, 8)$ y $u \equiv 3$ o $7 \,(\mathsf{mod}\, 8)$. Observando que $(1, 1, 1)$ es solución primitiva módulo 8 de $z^2 - 2u\,x^2 - v\,y^2 = 0$ y levantando,[2] se deduce que $(2u, v) = 1$.

Finalmente, $\chi_8(-1) = 1$, la Observación 2.3 (v) y el caso anterior implican

$$\begin{aligned}(2u, 2v) \,&=\, (2u, -4uv) \,=\, (2u, -uv) \,=\, (2, -uv)\ (u, -uv)\\ &=\, \chi_8(-uv)\ (u, v) \,=\, \chi_8(uv)\ (u, v)\end{aligned}\ .$$

□

Teorema 3.7. *Sea $F = \mathbb{Q}_2$ y sean $a, b \in \mathbb{Q}_p^\times$. Si $a = 2^m\,u$ y $b = 2^n\,v$, donde $u, v \in \mathbb{Z}_2^\times$, entonces*

$$(a, b) \,=\, (-1)^{\epsilon(u)\,\epsilon(v) + m\,\omega(v) + n\,\omega(u)}\ .$$

En particular,

$$(a, b)\ :\ F^\times/(F^\times)^2 \,\times\, F^\times/(F^\times)^2 \,\to\, \left\{\,\pm 1\right\}$$

es una forma bilineal no degenerada.

Demostración. Para ver que la forma es no degenerada, elegimos representantes de ${\mathbb{Q}_2}^\times/({\mathbb{Q}_2}^\times)^2$: $\{u, 2u\ :\ u \in \{\pm 1, \pm 5\}\}$. Mirando módulo 8, $(5, 2u) = -1$ y, también, $(-1, -5) = -1$. □

Observación 3.8. Siendo el símbolo de Hilbert $(a, b)_F$ una forma bilineal (simétrica) sobre el cuerpo $\mathbb{F}_2$, podemos asociarle una matriz, elegida una base de $F^\times/(F^\times)^2$.

- Si $F = \mathbb{C}$, entonces $\mathsf{dim}\big(\mathbb{C}^\times/(\mathbb{C}^\times)^2\big) = 0$; no hay matriz –o la matriz tiene tamañõ 0 y hay una única opción– en este caso.
- Si $F = \mathbb{R}$, entonces $\mathsf{dim}\big(\mathbb{R}^\times/(\mathbb{R}^\times)^2\big) = 1$; en este caso, la matriz es $[\,1\,]$.

[2] O bien multiplicando u y v por cuadrados en $\mathbb{Z}_2^\times$ para obtener las ecuaciones $z^2 + 2\,x^2 - 3\,y^2 = 0$ o $z^2 - 6\,x^2 + 5\,y^2 = 0$

- Si $F = \mathbb{Q}_p$, $p \neq 2$, entonces $\mathsf{dim}\big({\mathbb{Q}_p}^{\times}/({\mathbb{Q}_p}^{\times})^2\big) = 2$; con respecto a la base $\big\{p, u_0\big\}$, donde $(u_0/p) = -1$, la matriz es

$$\begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \qquad \text{si } p \equiv 1 \,(\mathsf{mod}\, 4)\ ,$$
$$\begin{bmatrix} 1 & 1 \\ 1 & \end{bmatrix} \qquad \text{si } p \equiv 3 \,(\mathsf{mod}\, 4)\ .$$

- Si $F = \mathbb{Q}_2$, entonces $\mathsf{dim}\big({\mathbb{Q}_2}^{\times}/({\mathbb{Q}_2}^{\times})^2\big) = 3$; con respecto a la base $\big\{2, -1, 5\big\}$, la matriz es

$$\begin{bmatrix} & & 1 \\ & 1 & \\ 1 & & \end{bmatrix}\ .$$

Observación 3.9. Si $F/\mathbb{Q}_p$ es una extensión finita, $p \neq 2$, la demostración del Lema 3.2 se adapta. Sean $\mathfrak{o}$ el anillo de enteros, $\mathfrak{p}$ el ideal maximal, $q = |\mathfrak{o}/\mathfrak{p}|$ el cardinal del cuerpo residual y $\pi \in \mathfrak{o}$ un uniformizador. Si $u, v \in \mathfrak{o}^{\times}$, entonces

- $(u, v) = 1$,
- $(\pi u, v) = \left(\dfrac{v}{\pi}\right)$ y
- $(\pi u, \pi v) = (\pi u, -uv) = \left(\dfrac{-uv}{\pi}\right)$,

donde $(v/\pi) = \pm 1$, dependiendo de si v es o no un cuadrado en $\big(\mathfrak{o}/\mathfrak{p}\big)^{\times}$. En particular, se deduce el resultado análogo al Teorema 3.3: si $a = \pi^m\, u$ y $b = \pi^n\, v$, donde $u, v \in \mathfrak{o}^{\times}$, entonces[3]

$$(a, b) \ = \ (-1)^{mn\,\frac{q-1}{2}} \left(\frac{u}{\pi}\right)^n \left(\frac{v}{\pi}\right)^m\ .$$

La demostración del Lema 3.5, sin embargo, depende de la estructura del grupo de unidades $\mathbb{Z}_2^{\times}$. Concretamente, la caracterización $\big(\mathbb{Z}_2^{\times}\big)^2 = 1 + 8\,\mathbb{Z}_2$ es esencial en la demostración.

[3] En $\mathfrak{o}/\mathfrak{p}$, -1 es un cuadrado, si y sólo si $p \equiv 1 \,(\mathsf{mod}\, 4)$, o bien $p \equiv 3 \,(\mathsf{mod}\, 4)$ y $\mathfrak{o}/\mathfrak{p}$ es una extensión de grado par de $\mathbb{Z}/p\mathbb{Z}$; esto equivale a $q \equiv 1 \,(\mathsf{mod}\, 4)$.