Lokale Eigenschaften des Hilbert-Symbols

(Nach J.P. Serre: *A Course in Arithmetic*)

Bettina Böhme, Karin Loch

24.05.2007

Im Folgenden bezeichnet k entweder den Körper $\mathbb{R}$ der reellen Zahlen oder den Körper $\mathbb{Q}_p$ der p -adischen Zahlen (p prim).
Außerdem sei $\mathbb{U} := \mathbb{Z}_p^*$.
Zur Definition der Homomorphismen ϵ und ω vgl. [1], II, §3.

1 Definition und erste Eigenschaften

Definition 1 (Das Hilbert Symbol)**.** *Seien $a, b \in k^*$. Es sei:*

$$(a,b) = \begin{cases} +1 & falls\ z^2 - ax^2 - by^2 = 0\ für\ ein\ k^3 \ni (z,x,y) \neq (0,0,0) \\ -1 & sonst \end{cases}$$

$(a,b) = \pm 1$ heißt *HilbertSymbol* von a und b bezüglich k.

Bemerkung: Das Hilbert Symbol (a,b) ändert sich nicht, wenn a oder b mit Quadraten multipliziert werden, d.h. mit $c, d \in k^*$ gilt $(ac^2, bd^2) = (a,b)$.

Beweis der Bemerkung: Ist (z,x,y) eine Lösung von $z^2 - ac^2x^2 - bd^2y^2 = 0$, dann ist offensichtlich (z, cx, dy) eine Lösung von $z^2 - ax^2 - by^2 = 0$, und ist umgekehrt (z,x,y) eine Lösung von $z^2 - ax^2 - by^2 = 0$, dann ist offensichtlich $(z, x/c, y/d)$ eine Lösung von $z^2 - ac^2x^2 - bd^2y^2 = 0$.
Das Hilbertsymbol definiert also eine Abbildung $k^*/k^{*2} \times k^*/k^{*2} \to \{\pm 1\}$, wobei $k^{*2} = \{a^2 | a \in k^*\}$.

Proposition 1. *Seien $a, b \in k^*$ und sei $k_b = k(\sqrt{b})$. Dann gilt $(a,b) = 1 \Leftrightarrow a \in Nk_b^*$.*

Beweis: Falls b Quadrat in k, d.h. falls es ein $c \in k^*$ gibt mit $c^2 = b$, dann ist $(c, 0, 1)$ eine Lösung von $z^2 - ax^2 - by^2 = 0$, also ist $(a,b) = 1$. In diesem Fall ist die Aussage klar, denn dann ist $k_b = k$ und $Nk_b^* = k^*$.
Sei also b kein Quadrat in k. Dann ist k_b quadratische Erweiterung von k. Es gilt $k_b = \{z + \beta y | z, y \in k\}$ mit $\beta^2 = b$ für ein $\beta \in k_b$. Für die Norm von k_b gilt: $N(\xi) = z^2 - by^2$ für $\xi \in k_b$, $\xi = z + \beta y$.
$\Leftarrow$)Ist $a \in Nk_b^*$, dann existieren $y, z \in k$ mit $a = z^2 - by^2$. Also ist $(z, 1, y)$ eine Lösung von $z^2 - ax^2 - by^2 = 0$ und somit ist $(a,b) = 1$.
$\Rightarrow$) Ist $(a,b) = 1$, dann existiert eine Lösung $(z,x,y) \neq (0,0,0)$ von $z^2 - ax^2 - by^2 = 0$. Es gilt $x \neq 0$, denn sonst wäre $by^2 = z^2$ und wegen $y \neq 0$ (sonst

wäre auch $z = 0$) wäre $b = (z/y)^2$, aber b ist kein Quadrat in k. Sei also $\xi = (z/x) + \beta(y/x)$, dann ist $N(\xi) = z^2/x^2 - by^2/x^2 = a$, also $a \in Nk_b^*$.

Proposition 2. *Seien $a, a', b, c \in k^*$, dann genügt das Hilbert-Symbol folgenden Formeln (wobei man davon ausgeht, dass $a \neq 1$, überall dort, wo der Ausdruck $1 - a$ auftaucht):*

$$\begin{array}{ll} i) & (a,b) = (b,a), (a,c^2) = 1 \\ ii) & (a,-a) = 1, (a,1-a) = 1 \\ iii) & (a,b) = 1 \Rightarrow (a',b) = (aa',b) \\ iv) & (a,b) = (a,-ab), (a,b) = (a,(1-a)b) \end{array}$$

Beweis:
i) 1) Folgt direkt aus der Definition.
2) $(c, 0, 1)$ ist Lösung von $z^2 - ax^2 - c^2y^2 = 0$
ii) 1) $(0, 1, 1)$ ist Lösung von $z^2 - ax^2 + ay^2 = 0$.
2) $(1, 1, 1)$ ist Lösung von $z^2 - ax^2 - (1-a)y^2 = 0$
iii) $(a, b) = 1 \Rightarrow a \in Nk_b^*$. Da $Nk_b^* \subseteq k*$ Untergruppe ist, gilt: $a' \in Nk_b^* \Leftrightarrow aa' \in Nk_b^*$. Die Behauptung folgt somit aus Proposition 1.
iv)1) $(-a, a) = 1 \overset{\text{(iii)}}{\Rightarrow} (b, a) = (-ab, a)$ 2) $((1-a), a) = 1 \overset{\text{(iii)}}{\Rightarrow} (b, a) = ((1-a)b, a)$

Bemerkung: Die Formel unter *iii*) ist ein Spezialfall der folgenden Formel:

$$v) \quad (aa', b) = (a, b)(a', b)$$

Diese Formel drückt, wenn man die Symmetrie des Hilbert-Symbols beachtet, dessen Bilinearität aus. Diese soll im Folgenden bewiesen werden.

2 Berechnung des Hilbert-Symbols

Satz 1. *Seien $a, b \in \mathbb{R}^*$, dann gilt:*

$$(a,b) = \begin{cases} +1 & \textit{falls} \quad (a > 0) \vee (b > 0) \\ -1 & \textit{sonst} \end{cases}$$

Seien $a, b \in \mathbb{Q}_p$ mit $a = p^\alpha u, b = p^\beta v$ wobei $u, v \in \mathbb{U}, \alpha, \beta \in \mathbb{Z}$, dann gilt:

$$(a,b) = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \quad p \neq 2$$

$$(a,b) = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} \quad p = 2$$

Wir beweisen zunächst nur den Fall $k = \mathbb{R}$.

Beweis für den Fall $k = \mathbb{R}$: Falls $a > 0$, dann ist a Quadrat in $\mathbb{R}$, und somit ist $(a, b) = 1$ wegen Eigenschaft *i*) aus Proposition 2. Analog ist $(a, b) = 1$ für $b > 0$. Falls $a < 0$ und $b < 0$, ist $(a, b) = (-1, -1) = -1$, denn $-a$ und $-b$ sind Quadrate in $\mathbb{R}$, und die Gleichung $z^2 = -x^2 - y^2$ hat in $\mathbb{R}$ nur die triviale Lösung.

Zum Beweis des Satzes für $\mathbb{Q}_p$ benötigen wir noch folgendes Lemma.

Lemma 1. *Sei $v \in \mathbb{U}$ p-adische Einheit. Falls die Gleichung $z^2 - px^2 - vy^2 = 0$ eine nichttriviale Lösung in $\mathbb{Q}_p$ besitzt, dann hat sie auch eine Lösung (x, y, z), so dass $z, y \in \mathbb{U}$ und $x \in \mathbb{Z}_p$.*

Beweis: Nach [1], Prop. 6, II, §2.1 besitzt die Gleichung eine *primitive* Lösung in $\mathbb{Z}_p^3$. Diese Lösung erfüllt die gewünschten Eigenschaften. Wäre dies nicht so, dann wäre entweder $y \equiv 0 \bmod p$ oder $z \equiv 0 \bmod p$. Außerdem gilt $z^2 - vy^2 \equiv 0 \bmod p$ und $v \not\equiv 0 \bmod p$, also würde folgen $y \equiv 0 \bmod p$ und $z \equiv 0 \bmod p$. Dann wäre $px^2 \equiv 0 \bmod p^2$, also auch $x \equiv 0 \bmod p$, im Widerspruch zur Primitivität der Lösung.

Wir können jetzt mit dem Beweis von Satz 1 fortfahren.

Beweis Satz 1, Fall $p \neq 2$: Man überlegt sich zunächst, dass für den Einfluss der Exponenten α und β nur entscheidend ist, ob sie gerade oder ungerade sind. Deswegen betrachten wir sie nur hinsichtlich ihrer Restklasse modulo 2. Aufgrund der Symmetrie des Hilbert-Symbols führt dies zu drei Fällen, die betrachtet werden müssen:

Fall 1) $\alpha = 0, \beta = 0$. Zu zeigen ist: $(u, v) = 1$. Wegen [1], I, §2, Cor. 2 zu Th. 3 hat die Gleichung

$$z^2 - ux^2 - vy^2 = 0$$

eine nichttriviale Lösung modulo p. Da die zu dieser quadratischen Form dazugehörige Determinante invertierbar ist, lässt sich diese Lösung zu einer p-adischen Lösung hochheben (vgl. [1], II, §2.2, Cor. 2 zu Th. 1). Also ist $(u, v) = 1$.
Fall 2) $\alpha = 1, \beta = 0$. Zu zeigen ist: $(pu, v) = \left(\frac{v}{p}\right)$. Da wie gesehen $(u, v) = 1$ ist, gilt $(pu, v) = (p, v)$ aufgrund von Proposition 2 iii). Es genügt also zu zeigen, dass $(p, v) = \left(\frac{v}{p}\right)$. Wenn v ein Quadrat ist, sind beide Seiten der Gleichung gleich 1, also ist sie erfüllt. Wenn v kein Quadrat ist, dann ist (nach [1], II, §3.3, Th. 3) $\left(\frac{v}{p}\right) = -1$. Wäre $(p, v) = 1$, dann gäbe es aufgrund von Lemma 1 eine primitive Lösung der Gleichung

$$z^2 - px^2 - vy^2 = 0$$

mit $y, z \in \mathbb{U}$. Es wäre also $v \equiv (\frac{z}{y})^2 \bmod p$, im Widerspruch zu v kein Quadrat. Also ist $(p, v) = -1$.
Fall 3) $\alpha = 1, \beta = 1$ Zu zeigen ist: $(pu, pv) = (-1)^{\frac{p-1}{2}} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)$.
Wegen Proposition 2 iv) gilt: $(pu, pv) = (pu, -p^2uv) = (pu, -uv)$. Da $-uv$ eine Einheit ist, gilt nach Fall 2): $(pu, pv) = (pu, -uv) = \left(\frac{-uv}{p}\right)$.
Es gilt: $\left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)$ und $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Also ist das Gewünschte bewiesen.

Beweis Satz 1, Fall $p = 2$: Auch in diesem Fall spielen die Exponenten α und β nur hinsichlich ihrer Restklasse modulo 2 eine Rolle, und es lassen sich wieder drei Fälle unterscheiden:
Fall 1) $\alpha = 0, \beta = 0$. Zu zeigen ist: $(u, v) = 1$, falls $u \equiv 1 \bmod 4$ oder $v \equiv$

$1 \bmod 4$ und $(u,v) = -1$ sonst. Nehmen wir zunächst an, dass $u \equiv 1 \bmod 4$. Also $u \equiv 1 \bmod 8$ oder $u \equiv 5 \bmod 8$. Im ersten Fall ist u ein Quadrat (nach [1], II, §3.3, Th. 4) und daher ist $(u,v) = 1$. Im zweiten Fall gilt $u + 4v \equiv 1 \bmod 8$, also gibt es ein $w \in \mathbb{U}$ mit $w^2 = u + 4v$. Die Gleichung $z^2 - ux^2 - vy^2 = 0$ hat also die Lösung $(w, 1, 2)$ und somit ist $(u,v) = 1$. Analog ist $(u,v) = 1$, falls $v \equiv 1 \bmod 4$.
Sei nun umgekehrt $u \equiv v \equiv -1 \bmod 4$. Wäre $(u,v) = 1$, dann gäbe es eine primitive Lösung (z,x,y) der Gleichung $z^2 - ux^2 - vy^2 = 0$ (wegen [1], Prop. 6, II, §2.1). Also müsste gelten: $z^2 + x^2 + y^2 \equiv 0 \bmod 4$. Da 0 und 1 die einzigen Quadrate modulo 4 sind, ist dies nur möglich, wenn $x \equiv y \equiv z \equiv 0 \bmod 4$ und somit $x \equiv y \equiv z \equiv 0 \bmod 2$, im Widerspruch zur Primitivität der Lösung. Also ist $(u,v) = -1$.
Fall 2) $\alpha = 1, \beta = 0$. Zu zeigen ist: $(2u,v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)}$.
Zunächst zeigen wir: $(2,v) = (-1)^{\omega(v)}$, also $(2,v) = 1 \Leftrightarrow v \equiv \pm 1 \bmod 8$. Falls $(2,v) = 1$ existieren nach Lemma 1 $x, y, z \in \mathbb{Z}_2$ mit $z^2 - 2x^2 - vy^2 = 0$ und $y, z \not\equiv 0 \bmod 2$. Für diese Lösung gilt: $y^2 \equiv z^2 \equiv 1 \bmod 8$ und damit auch $1 - 2x^2 - v \equiv 0 \bmod 8$. Die einzigen Quadrate modulo 8 sind 0,1 und 4, also ist $v \equiv \pm 1 \bmod 8$.
Ist umgekehrt $v \equiv 1 \bmod 8$, dann ist v Quadrat (nach [1], II, §3.3, Th. 4) und $(2,v) = 1$. Ist $v \equiv -1 \bmod 8$, dann hat die Gleichung $z^2 - 2x^2 - vy^2 = 0$ modulo 8 die Lösung $(1,1,1)$. Wegen [1], II, §2.2, Cor. 3 zu Th. 1 lässt sich diese primitive Lösung modulo 8 zu einer exakten Lösung hochheben. Also $(2,v) = 1$.
Als nächstes zeigen wir: $(2u,v) = (2,v)(u,v)$. Nach Propisition 2 *iii)* ist dies der Fall, falls $(2,v) = 1$ oder $(u,v) = 1$. Wir betrachten also den Fall $(2,v) = (u,v) = -1$. Das heißt $v \equiv \pm 3 \bmod 8$ (wie eben gesehen) und $u, v \equiv 3 \bmod 4$ (vgl. Fall 1). Beides kann nur gleichzeitig erfüllt sein für $v \equiv 3 \bmod 8$ und $u \equiv 3$ oder $u \equiv -1 \bmod 8$.
Betrachte zunächst $u, v \equiv 3 \bmod 8$. Setze $u' := \frac{3}{u}$ und $v' := \frac{-5}{v}$. Es gilt: $u', v' \equiv 1 \bmod 8$, also nach [1], II, §3.3, Th. 4 Quadrate in $\mathbb{Q}_2^*$. Es gilt $uu' = 3$, $vv' = -5$ und $(2u,v) = (2uu', vv') = (6,-5)$. Die Gleichung $z^2 - 6x^2 + 5y^2 = 0$ hat die Lösung $(1,1,1)$, also ist $(2u,v) = 1$.
Betrachte jetzt $u \equiv -1$, $v \equiv 3 \bmod 8$. Setze $u' := \frac{-1}{u}$ und $v' := \frac{3}{v}$. Es gilt: $u', v' \equiv 1 \bmod 8$, also u', v' Quadrate in $\mathbb{Q}_2^*$. Es gilt $uu' = -1$, $vv' = 3$ und $(2u,v) = (2uu', vv') = (-2,3)$. Die Gleichung $z^2 + 2x^2 - 3y^2 = 0$ hat die Lösung $(1,1,1)$, also ist $(2u,v) = 1$.
Zusammenfassend ergibt sich:

$$(2u,v) = (2,v)(u,v) = (-1)^{\omega(v)}(u,v) = (-1)^{\omega(v)}(-1)^{\epsilon(u)\epsilon(v)} = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)}$$

Fall 3) $\alpha = 1, \beta = 1$. Zu zeigen ist: $(2u,2v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(u)+\omega(v)}$. Nach Proposition 2 *iv)* gilt: $(2u,2v) = (2u,-4uv) = (2u,-uv)$. Nach Fall 2 wissen wir, dass $(2u,-uv) = (-1)^{\epsilon(u)\epsilon(-uv)+\omega(-uv)}$. Also ist zu zeigen:

$$\epsilon(u)\epsilon(v) + \omega(u) + \omega(v) = \epsilon(u)\epsilon(-uv) + \omega(-uv)$$

Diese Gleichheit ergibt sich durch Umformen, wenn man beachtet, dass

- ϵ, ω sind Homomorphismen, d.h. $\epsilon(xy) = \epsilon(x) + \epsilon(y)$, analog für ω
- $\epsilon(-1) = 1$
- $\omega(-1) = 0$

- $\epsilon(u)(1+\epsilon(u)) = 0$

Satz 2. *Das Hilbert-Symbol ist eine reguläre Bilinearform vom $\mathbb{F}_2$-Vektorraum k^*/k^{*2} in den $\mathbb{F}_2$-Vektorraum $\{-1, 1\}$.*

Bemerkung: *Regulär* bedeutet hier:

$$\forall b \in k^* : (\forall a \in k^* : (a, b) = 1 \Rightarrow b \in k^{*2})$$

Das ist gleichbedeutend mit:

$$\forall b \in k^*/k^{*2} - \{1\} : \exists a \in k^* : (a, b) = -1$$

Die Bilinearität ist genau das, was Formel v) in Abschnitt 1 ausdrückt.
k^*/k^{*2} bildet einen $\mathbb{F}_2$-Vektorraum mit der Multiplikation der Restklassen als Vektoraddition und der Skalarmultiplikation: a^λ für $a \in k^*/k^{*2}, \lambda \in \mathbb{F}_2$, wie man leicht nachprüft.

Beweis für den Fall $k = \mathbb{R}$:
Zu zeigen: $(aa', b) = (a, b)(a', b)$ für $a, a', b \in \mathbb{R}^*/\mathbb{R}^{*2}$. Der einzige Fall, der nicht von Proposition 2 *iii*) abgedeckt wird, ist: $(a, b) = (a', b) = -1$, was nur gilt wenn $a, a', b < 0$.$\{-1, 1\}$ sind Repräsentanten von $\mathbb{R}^*/\mathbb{R}^{*2}$. Also ist zu zeigen: $((-1)(-1), -1) = (-1, -1)(-1, -1)$, was nach Satz 1 erfüllt ist. Die Regularität des Hilbert-Symbols folgt aus $(-1, -1) = -1$.

Bilinearität für den Fall $k = \mathbb{Q}_p$:
Folgt aus der Bilinearität der Formeln aus Satz 1.

Regularität für den Fall $k = \mathbb{Q}_p, p \neq 2$:
$\{1, p, u, up\}$ mit $u \in \mathbb{U}$, so dass $\left(\frac{u}{p}\right) = -1$, sind Repräsentanten von $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Davon sind u, p und up keine Quadrate (nach [1], III, §3.3, Th. 3). Wir müssen also a, a', a'' in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ finden, so dass $(a, u) = -1$, $(a', p) = -1$ und $(a'', up) = -1$. Wähle $a = p$, $a' = u$ und $a'' = u$.

Regularität für den Fall $k = \mathbb{Q}_2$:
$\{u, 2u\}$ mit $u \in \{1, 5, -1, 5\}$ sind Repräsentanten von $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ (nach [1], III, §3.3, Cor. zu Th. 4). Für $b \in \{u, 2u\} - \{1\}$ (die Nichtquadrate) müssen wir je ein $a \in \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ finden mit $(a, b) = -1$. Es gilt $(5, 2u) = -1$ und $(-1, -1) = (-1, -5) = -1$.

Korollar: Wenn b kein Quadrat ist, ist Nk_b^* aus Proposition 1 Untergruppe von k^* mit Index 2.

Beweis: Zu zeigen: $\#(k^*/Nk_b^*) = 2$. Betrachte den Homomorphismus $\phi_b : k^* \to \{\pm 1\}$ mit $\phi_b(a) = (a, b)$. Nach Proposition 1 ist Nk_b^* der Kern dieser Abbildung. Sie ist surjektiv aufgrund der Regularität des Hilbertsymbols. Nach dem Isomorphiesatz induziert ϕ_b also einen Isomorphismus von k^*/Nk_b^* nach $\{\pm 1\}$.

Bemerkung: Schreibe (a, b) in der Form $(-1)^{[a,b]}$ mit $[a, b] \in \mathbb{F}_2$. Dann ist $[\cdot, \cdot] : k^*/k^{*2} \times k^*/k^{*2} \to \mathbb{F}_2$ eine symmetrische Bilinearform. Mithilfe von Satz

1 erhalten wir nach Wahl einer Basis von k^*/k^{*2} eine Matrixdarstellung dieser Bilinearform:

- Für $k = \mathbb{R}$ mit Basis $\{-1\}$ erhält man die Matrix (1).
- Für $k = \mathbb{Q}_p, p \neq 2$ mit Basis $\{p, u\}$, wobei $\left(\frac{u}{p}\right) = -1$, erhält man die Matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ für $p \equiv 1 \bmod 4$ und die Matrix $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ für $p \equiv 3 \bmod 4$.
- Für $k = \mathbb{Q}_2$ mit Basis $\{2, -1, 5\}$ erhält man die Matrix $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

Literatur

[1] Serre, J.P.: *A Course in Arithmetic.* Springer, 1973.