Alexandra Merz, Christian Semrau **WS 2002/03**

Kapitel III. Das Hilbert-Symbol

aus: Jean Pierre Serre: A course in arithmetics

Vortrag zum Seminar
"Quadratische Formen über p-adischen Zahlen"
an der LMU München

1 Lokale Eigenschaften

k bezeichne in diesem Abschnitt $\mathbb{R}$ oder ein $\mathbb{Q}_p$ (p prim).

1.1 Definition und erste Eigenschaften

Definition. Seien $a, b \in k^*$. Falls die Gleichung

$$ax^2 + by^2 = z^2 \quad \text{(H)}$$

eine Lösung $(x, y, z) \neq (0, 0, 0)$ in k^3 hat, setze $(a, b) = 1$, sonst setze $(a, b) = -1$.
(a, b) heisst das *Hilbert-Symbol von a und b* bezüglich k.

Bemerkung. Sind $c, d \in k^*$, dann ist $(ac^2, bd^2) = (a, b)$, denn hat $ac^2x^2 + bd^2y^2 = z^2$ eine Lösung (x, y, z), dann ist (cx, dy, z) eine Lösung von $ax^2 + by^2 = z^2$, hat $ax^2 + by^2 = z^2$ eine Lösung (x, y, z), dann ist $(x/c, y/d, z)$ eine Lösung von $ac^2x^2 + bd^2y^2 = z^2$.
Bezeichnet $k^{*2} = \{a^2 : a \in k^*\}$ die multiplikative Gruppe der Quadrate in k^*, dann definiert also das Hilbertsymbol eine Abbildung $k^*/k^{*2} \times k^*/k^{*2} \to \{\pm 1\}$. (Sprich k^*/k^{*2} als "k Stern modulo Quadrate").

Erinnerung. Folgende Aussagen aus der Algebra werden als bekannt vorausgesetzt:
Sei K ein Körper und $b \in K$. Sei $L := K(\sqrt{b})$ und $N\colon L \to K$ die Norm von L über K.
Falls b ein Quadrat in K ist, dann ist $L = K$, $N(x) = x$ und $N(L^*) = K^*$.
Falls b kein Quadrat in K ist, dann ist L eine quadratische Erweiterung von K. Sei $\beta \in L$ mit $\beta^2 = b$. Es ist $L = \{x + \beta y : x, y \in K\}$ und $N(x + \beta y) = (x + \beta y)(x - \beta y) = x^2 - by^2$.
$N(L^*)$ ist eine Untergruppe von K^*.

Satz 1. Seien $a, b \in k^*, k_b := k(\sqrt{b})$. Dann ist $(a, b) = 1 \Leftrightarrow a \in N(k_b^*)$.

Beweis. 1. Fall: b ist ein Quadrat in k. $b = c^2, c \in k^*$. Dann ist $k_b = k$, $N(k_b^*) = k^* \ni a$ und (H) hat die Lösung $(0, 1, c)$. Damit sind beide Seiten der Behauptung erfüllt.

2. Fall: b ist kein Quadrat in k. Sei $\beta \in k_b$ mit $\beta^2 = b$. Es ist $N(z + \beta y) = z^2 - by^2$.

"$\Leftarrow$": Ist $a \in N(k_b^*)$, dann $\exists y, z \in k : a = z^2 - by^2$ und es ist $a \cdot 1^2 + by^2 = z^2$, also $(a, b) = 1$.

"$\Rightarrow$": Ist $(a, b) = 1$, dann $\exists (0, 0, 0) \neq (x, y, z) \in k^3 : ax^2 + by^2 = z^2$. Wäre $x = 0$, dann wäre $by^2 = z^2$, und weil $y \neq 0$ (sonst wäre auch $z = 0$) wäre $b = (z/y)^2 \in k^{*2}$, aber b ist kein Quadrat. Also ist $x \neq 0$ und mit $\xi = (z/x) + \beta(y/x)$ ist $N(\xi) = z^2/x^2 - by^2/x^2 = a$. □

Satz 2. Seien $a, a', b, c \in k^*$, $a \neq 1$ in Formel ii)2) und iv)2).

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) $(a,b) = (a,-ab)$, $(a,b) = (a,(1-a)b)$

Beweis. i) 1) klar nach Def., 2) $(0,1,c)$ ist Lsg. von (H)
ii) 1) $(1,1,0)$, 2) $(1,1,1)$ sind Lsg. von (H)
iii) $(a,b) = 1 \Rightarrow a \in N(k_b^*)$. Weil $N(k_b^*) \subseteq k^*$ eine Untergruppe ist, ist $a' \in N(k_b^*) \Leftrightarrow aa' \in N(k_b^*)$. Die Behauptung folgt mit Satz 1.
iv) 1) $(-a,a) = 1 \Rightarrow (b,a) = (-ab,a)$, 2) $((1-a),a) = 1 \Rightarrow (b,a) = ((1-a)b,a)$ □

Bemerkung. Formel iii) ist ein Spezialfall von

v) $(aa',b) = (a,b)(a',b)$.

Diese Formel (zusammen mit der Symmetrie) bedeutet die Bilinearität des Hilbert-Symbols und wird gleich bewiesen.

1.2 Berechnung des Hilbert-Symbols (a,b)

Wir geben zunächst eine Berechnungsvorschrift für das Hilbert-Symbol in $\mathbb{R}$ an (Satz 3), dann für $\mathbb{Q}_p, p > 2$ (Lemma 2 bis 4, Satz 4) und schließlich für $\mathbb{Q}_2$ (Lemma 5 bis 7, Satz 5), alle Berechnungsvorschriften vereint sollen dann Theorem 1 bilden.

Satz 3. Seien $a, b \in \mathbb{R}^*$, dann ist $(a,b) = \begin{cases} 1 & \text{falls } a > 0 \text{ oder } b > 0 \\ -1 & \text{falls } a < 0 \text{ und } b < 0 \end{cases}$.

Beweis. Es ist $\mathbb{R}^{*2} = \{x \in \mathbb{R} : x > 0\}$.
Falls $a > 0$ oder $b > 0$, dann ist $(a,b) = 1$ nach Satz 2.i). Falls $a < 0$ und $b < 0$, dann ist $(a,b) = (-1,-1) = -1$, denn $-x^2 - y^2 = z^2$ hat (in $\mathbb{R}$) nur die triviale Lösung. □

Theorem (Chevalley-Warning). Seien $0 \neq f_1, \ldots, f_n \in \mathbb{F}_p[X_1, \ldots X_r]$ Polynome mit $\sum_{i=1}^n \deg f_i < r$. Sei $L := \{x \in (\mathbb{F}_p)^r : \forall i\colon f_i(x) = 0\}$. Dann ist $|L| \equiv 0 \pmod p$.
Daraus folgt, dass $f = aX^2 + bY^2 + cZ^2 \in \mathbb{F}_p[X,Y,Z]$ eine nichttriviale Nullstelle hat.

Lemma 1. Sei $v \in \mathbb{Z}_p^*$. Wenn $(p,v) = 1$, dann hat $px^2 + vy^2 = z^2$ auch eine Lösung (x,y,z) bei der $x \in \mathbb{Z}_p$ und $y, z \in \mathbb{Z}_p^*$.

Beweis. Wenn $(p,v) = 1$, dann hat nach Satz 6 (a⇒b) aus Kapitel II, 2.1 die Gleichung $px^2 + vy^2 = z^2$ eine primitive Lösung $(x,y,z) \in (\mathbb{Z}_p)^3$. Wir zeigen, dass (x,y,z) die gewünschte Eigenschaft hat.
Wenn nicht $y, z \in \mathbb{Z}_p^*$ wären, dann wäre $y \equiv 0 \pmod p$ oder $z \equiv 0 \pmod p$. Wegen $vy^2 \equiv z^2 \pmod p$ und $v \not\equiv 0 \pmod p$ wäre dann $y \equiv 0 \equiv z \pmod p$, also $px^2 \equiv 0 \pmod{p^2}$. Damit wäre $x^2 \equiv 0 \pmod p$ und also $x \equiv 0 \pmod p$, im Widerspruch zur Primitivität der Lösung. □

Lemma 2. Seien $p > 2$, $u, v \in \mathbb{Z}_p^*$. Dann ist $(u,v) = 1$.

Beweis. Die Gleichung $ux^2 + vy^2 - z^2 = 0$ hat nach dem Korollar zum Theorem von Chevalley-Warning eine nichttriviale Lösung modulo p. Weil die Diskriminante dieser quadratischen Form eine p-adische Einheit $(-uv)$ ist, folgt aus (Kor.2 zu Th.1 in II,2.2), dass es eine p-adische Lösung gibt, also ist $(u, v) = 1$. □

Definition. Ist $p > 2$, $u \in \mathbb{Z}_p^*$, dann sei $\left(\frac{u}{p}\right) := \left(\frac{u \bmod p}{p}\right) \in \{-1, 1\}$.

Lemma 3. Seien $p > 2$, $u, v \in \mathbb{Z}_p^*$. Dann ist $(pu, v) = \left(\frac{v}{p}\right)$.

Beweis. Wegen $(u, v) = 1$ (nach Lemma 2) gilt nach Satz 2.iii) $(pu, v) = (p, v)$.
Falls v ein Quadrat ist, dann ist $(p, v) = 1 = \left(\frac{v}{p}\right)$ nach Satz 2.i).
Falls v kein Quadrat ist, dann ist $\left(\frac{v}{p}\right) = -1$. Wäre nun $(p, v) = 1$, dann gäbe es nach Lemma 1 eine primitive Lösung, bei der y und z Einheiten sind. Es wäre dann $v \equiv (z/y)^2 \pmod{p}$, aber v ist hier kein Quadrat. Also muss $(p, v) = -1$ sein. □

Lemma 4. Seien $p > 2$, $u, v \in \mathbb{Z}_p^*$. Dann ist $(pu, pv) = (-1)^{(p-1)/2}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$.

Beweis. Nach Satz 2.iv) ist $(pu, pv) = (pu, -pupv) = (pu, -uv)$.
Aus Lemma 3 folgt $(pu, -uv) = \left(\frac{-uv}{p}\right)$ (setze die Einheit $-uv$ für v).
Wegen $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ zerfällt $\left(\frac{-uv}{p}\right)$ in die rechte Seite und wir sind fertig. □

Satz 4. Sei $p > 2$, $a, b \in \mathbb{Q}_p^*$, $a = p^\alpha u, b = p^\beta v$, wobei $\alpha, \beta \in \mathbb{Z}$, $u, v \in \mathbb{Z}_p^*$, dann gilt

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

Dabei ist $\varepsilon(p) = \frac{p-1}{2} \bmod 2 \in \mathbb{Z}/2\mathbb{Z}$.

Beweis. Auf beiden Seiten der Gleichung ist nur wichtig, ob α und β gerade oder ungerade sind. Man kann also zu ihren Resten modulo 2 übergehen. Durch die Symmetrie des Hilbert-Symbols und der rechten Seite sind nur noch drei Fälle zu unterscheiden.

Fall 1: $\alpha = 0, \beta = 0$ Das ist Lemma 2.
Fall 2: $\alpha = 1, \beta = 0$ Das ist Lemma 3.
Fall 3: $\alpha = 1, \beta = 1$ Das ist Lemma 4. □

Lemma 5. Seien $u, v \in \mathbb{U} = \mathbb{Z}_2^*$, dann ist $(u, v) = 1 \Leftrightarrow u \equiv 1 \pmod 4 \vee v \equiv 1 \pmod 4$.

Beweis. „⇒“: Sei $ux^2 + vy^2 = z^2$ nichttrivial lösbar. Es gibt dann (nach Satz 6 aus Kapitel II, 2.1) eine primitive Lösung $(x, y, z) \in (\mathbb{Z}_2)^3$. Nehmen wir nun an, es wäre $u \equiv -1 \pmod 4$ und $v \equiv -1 \pmod 4$. Die primitive Lösung erfüllt dann $0 \equiv z^2 + x^2 + y^2 \pmod 4$. Weil aber $0, 1$ die Quadrate von $\mathbb{Z}/4\mathbb{Z}$ sind, kann diese Kongruenz nur erfüllt sein, wenn alle drei Variablen kongruent 0 modulo 2 sind, was der Primitivität widerspricht. Also ist $u \equiv 1 \bmod 4$ oder $v \equiv 1 \bmod 4$.

„⇐“: Sei $u \equiv 1 \pmod 4$, dann ist $u \equiv 1 \pmod 8$ oder $u \equiv 5 \pmod 8$. Im ersten Fall ist u ein Quadrat (Th.4 in II,3.3), also $(u, v) = 1$, im zweiten Fall ist $u + 4v \equiv 1 \pmod 8$, also $u + 4v$ ein Quadrat, und es gibt ein $w \in \mathbb{Z}_2$ mit $w^2 = u + 4v$. Die Gleichung $ux^2 + vy^2 = z^2$ hat also die Lösung $(1, 2, w)$. Damit ist $(u, v) = 1$. Analog folgt aus $v \equiv 1 \pmod 4$, dass $(u, v) = 1$. □

Lemma 6. Sei $v \in \mathbb{Z}_2^*$. Dann ist $(2, v) = 1 \Leftrightarrow v \equiv \pm 1 \pmod 8$.

Beweis. „⇒“: Falls $(2, v) = 1$, dann ist $2x^2 + vy^2 = z^2$ nichttrivial lösbar und nach Lemma 1 existiert eine Lösung $x, y, z \in \mathbb{Z}_2$ mit $y, z \not\equiv 0 \pmod 2$. Für diese Lösung gilt $y^2 \equiv z^2 \equiv 1 \pmod 8$, und damit $v \equiv 1 - 2x^2 \pmod 8$. Weil $0, 1, 4$ die Quadrate von $\mathbb{Z}/8\mathbb{Z}$ sind, folgt daraus, dass $v \equiv \pm 1 \pmod 8$.

„⇐“: Falls $v \equiv 1 \pmod 8$, dann ist v ein Quadrat und $(2, v) = 1$. Falls $v \equiv -1 \pmod 8$, dann hat $2x^2 + vy^2 = z^2$ modulo 8 die Lösung $(1, 1, 1)$ und nach (Kor.3 zu Th.1 in II,2.2) liefert diese Näherungslösung eine exakte Lösung. Damit ist $(2, v) = 1$. □

Lemma 7. Seien $u, v \in \mathbb{Z}_2^*$, dann ist $(2u, v) = (2, v)(u, v)$.

Beweis. Wegen Satz 2.iii) [1] ist das nur noch im Fall $(2, v) = (u, v) = -1$ zu beweisen, also falls $v \equiv \pm 3 \pmod 8$ (nach Lemma 6) und $u, v \equiv 3 \pmod 4$ (nach Lemma 5). Da beide Bedingungen gleichzeitig erfüllt sind, gilt $u \equiv 3 \pmod 8$ oder $u \equiv 7 \pmod 8$ und $v \equiv 3 \pmod 8$.

Falls $u \equiv 3 \pmod 8, v \equiv 3 \pmod 8$, dann sind $u' := 3/u \equiv 1 \pmod 8$ und $v' := -5/v \equiv 1 \pmod 8$ Quadrate in $\mathbb{Q}_2^*$, damit ist $uu' = 3$, $vv' = -5$ und $(2u, v) = (6, -5)$. $6x^2 - 5y^2 = z^2$ hat die Lösung $(1, 1, 1)$, also ist $(2u, v) = 1$.

Falls $u \equiv 7 \pmod 8, v \equiv 3 \pmod 8$, dann sind $u' := -1/u \equiv 1 \pmod 8$ und $v' := 3/v \equiv 1 \pmod 8$ Quadrate in $\mathbb{Q}_2^*$, damit ist $uu' = -1$, $vv' = 3$ und $(2u, v) = (-2, 3)$. $-2x^2 + 3y^2 = z^2$ hat die Lösung $(1, 1, 1)$, also ist $(2u, v) = 1$. □

Definition. Für $u \in \mathbb{Z}_2^*$ sei $\varepsilon(u) := \frac{u-1}{2} \bmod 2$, $\omega(u) := \frac{u^2-1}{8} \bmod 2 \in \mathbb{Z}/\mathbb{Z}_2$.
ε und ω sind Homomorphismen von $\mathbb{Z}_2^*$ nach $\mathbb{Z}/2\mathbb{Z}$, d.h. $\varepsilon(xy) = \varepsilon(x) + \varepsilon(y), \omega(xy) = \omega(x) + \omega(y)$.

Beweis. Seien $x, y \equiv 1 \pmod 2$, dann ist $(x-1), (y-1) \equiv 0 \pmod 2$, also $(x-1)(y-1) = xy-(x+y)+1 = (xy-1)-(x+y-2) \equiv 0 \pmod 4$, damit ist $\varepsilon(xy) = \frac{xy-1}{2} \equiv \frac{x+y-2}{2} = \varepsilon(x) + \varepsilon(y) \pmod 2$. Es ist $(x^2-1), (y^2-1) \equiv 0 \pmod 8$, also $(x^2-1)(y^2-1) = x^2y^2-(x^2+y^2)+1 = (x^2y^2-1)-(x^2+y^2-2) \equiv 0 \pmod{16}$, damit ist $\omega(xy) = \frac{x^2y^2-1}{8} \equiv \frac{x^2+y^2-2}{8} = \omega(x) + \omega(y) \pmod 2$. □

Satz 5. Seien $a, b \in \mathbb{Q}_2^*$, $a = 2^\alpha u, b = 2^\beta v$, wobei $\alpha, \beta \in \mathbb{Z}$, $u, v \in \mathbb{U}$, dann gilt

$$(a, b) = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}$$

Beweis. Auch hier kann man zu den Resten von α und β modulo 2 übergehen, und auch hier sind beide Seiten symmetrisch.

Fall 1: $\alpha = 0, \beta = 0$ Zu zeigen ist $(u, v) = (-1)^{\varepsilon(u)\varepsilon(v)}$.
Das ist Lemma 5, denn $(-1)^{\varepsilon(u)\varepsilon(v)} = 1 \Leftrightarrow u \equiv 1 \pmod 4 \vee v \equiv 1 \pmod 4$.

Fall 2: $\alpha = 1, \beta = 0$ Zu zeigen ist $(2u, v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}$.
Wegen $(-1)^{\omega(v)} = 1 \Leftrightarrow v \equiv \pm 1 \pmod 8$ und Lemma 6 wissen wir $(2, v) = (-1)^{\omega(v)}$.
Mit Lemma 7 haben wir $(2u, v) = (2, v)(u, v) = (-1)^{\omega(v)}(-1)^{\varepsilon(u)\varepsilon(v)}$.

Fall 3: $\alpha = 1, \beta = 1$ Zu zeigen ist $(2u, 2v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)+\omega(u)}$.

[1] $(2, v) = 1 \Rightarrow (u, v) = (2u, v)$, $(u, v) = 1 \Rightarrow (2, v) = (2u, v)$

Nach Satz 2.iv) ist $(2u, 2v) = (2u, -4uv) = (2u, -uv)$. Gerade gezeigt wurde $(2u, -uv) = (-1)^{\varepsilon(u)\varepsilon(-uv)+\omega(-uv)}$ (nimm $-uv$ für v in Fall 2).
Es ist $\varepsilon(xy) = \varepsilon(x) + \varepsilon(y), \omega(xy) = \omega(x) + \omega(y)$, ausserdem ist $\varepsilon(-1) = 1, \varepsilon(u)(1 + \varepsilon(u)) = 0, \omega(-1) = 0$. Also ist $\varepsilon(u)\varepsilon(-uv) + \omega(-uv) = \varepsilon(u)\varepsilon(v) + \omega(u) + \omega(v)$. □

Theorem 1. Wir fassen die Aussagen der Sätze 3, 4 und 5 zusammen zum Theorem 1.

Theorem 2. Das Hilbert-Symbol ist eine reguläre Bilinearform des $\mathbb{F}_2$-Vektorraums k^*/k^{*2} in den $\mathbb{F}_2$-Vektorraum $\{\pm 1\}$.

Die Bilinearform (a, b) nach $\{\pm 1\}$ heisst *regulär* (oder *nicht ausgeartet*), wenn für jedes $b \in k^*$ mit $\forall a \in k^* \colon (a, b) = 1$ gilt, dass $b \in k^{*2}$ ist. Das ist gleichbedeutend damit, dass es zu jedem Nichtquadrat $b \in k^* \setminus k^{*2}$ ein $a \in k^*$ gibt mit $(a, b) = -1$.

Beweis. k^*/k^{*2} ist ein $\mathbb{F}_2$ -Vektorraum, denn:
Man prüft leicht nach, dass jede (additiv geschriebene) abelsche Gruppe G mit der Eigenschaft $a + a = 0 \forall a \in G$ mit der Skalarmultiplikation $0a = 0, 1a = a$ einen $\mathbb{F}_2$ -Vektorraum bildet.
k^*/k^{*2} erfüllt diese Bedingung (mit der Multiplikation der Restklassen als Vektoraddition), denn $\forall u \in k^* : u^2 \in k^{*2}$, also ist k^*/k^{*2} ein $\mathbb{F}_2$ -Vektorraum (mit der Skalarmultiplikation a^λ für $a \in k^*/k^{*2}, \lambda \in \mathbb{F}_2$).

$\mathbb{R}^*/\mathbb{R}^{*2}$ hat die Repräsentanten $\{1, -1\}$ und bildet einen eindimensionalen $\mathbb{F}_2$ -Vektorraum mit der einzigen Basis $\{-1\}$. Die Bilinearität ist nur noch im Fall $(a, b) = (a', b) = -1$ zu zeigen (die anderen Fälle sind in Satz 2.iii) gezeigt): $1 = (1, -1) = (-1, -1)(-1, -1) = -1 \cdot -1$. Dass das Hilbert-Symbol für $\mathbb{R}$ regulär ist, folgt aus $(-1, -1) = -1$.

Für $p \geq 2$ folgt die Bilinearität des Hilbert-Symbols in $\mathbb{Q}_p$ aus Satz 4 und 5.

Nach (Kor. zu Th.3 in II,3.3) hat $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ für $p > 2$ die Repräsentanten $1, p, u, pu$ mit $u \in \mathbb{Z}_p^*$, $\left(\frac{u}{p}\right) = -1$. $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ ist ein 2-dimensionaler $\mathbb{F}_2$-Vektorraum, eine Basis ist $\{p, u\}$. Es folgt aus $(u, p) = (u, pu) = -1$, dass das Hilbert-Symbol regulär ist.

Nach (Kor. zu Th.4 in II,3.3) hat $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ die Repräsentanten $u, 2u$ mit $u = \pm 1, \pm 5$. $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ ist ein 3-dimensionaler $\mathbb{F}_2$-Vektorraum, eine Basis ist $\{2, -1, 5\}$. Aus $(-1, -1) = (-1, -5) = (2u, 5) = -1$ folgt, dass (a, b) regulär ist. □

Korollar 1. Wenn b kein Quadrat ist, dann ist $N(k_b^*)$ eine Untergruppe mit Index 2.

Beweis. Die Abbildung $\phi_b \colon k^* \to \{\pm 1\}$, $\phi_b(a) = (a, b)$ ist ein Homomorphismus (das folgt aus der Bilinearität von (a, b)), hat nach Satz 1 den Kern $N(k_b^*)$, und ist surjektiv, da (a, b) regulär ist. Also definiert ϕ_b einen Isomorphismus $k^*/N(k_b^*) \to \{\pm 1\}$. Damit ist $[k^* : N(k_b^*)] = 2$. □

Bemerkung. Wenn wir $(a, b) = (-1)^{[a,b]}$ schreiben 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 von $\mathbb{F}_2$-Vektorräumen, die wir nach Wahl einer Basis B durch eine Multiplikation mit der darstellenden Matrix beschreiben können: $[x, y] = \hat{x}^t A \hat{y}$, wobei $\hat{x}$ der Koordinatenvektor (in $(\mathbb{F}_2)^{\dim}$) des Vektors x (in k^*/k^{*2}) ist.

- Für $k = \mathbb{R}$ ist $B = \{-1\}$ die einzige Basis von k^*/k^{*2} und $A = \big(1\big)$.

- Für $k = \mathbb{Q}_p, p \neq 2$ und die Basis $B = \{p, u\}$ ist $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ falls $p \equiv 1 \pmod 4$ und $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ falls $p \equiv 3 \pmod 4$.
- Für $k = \mathbb{Q}_2$ und die Basis $\{2, -1, 5\}$ ist $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

2 Globale Eigenschaften

$\mathbb{Q}$ lässt sich als Teilkörper in jedes $\mathbb{Q}_p$ und in $\mathbb{R}$ einbetten. Seien $a, b \in \mathbb{Q}^*$, dann bezeichne $(a, b)_p$ ihr Hilbert-Symbol bezüglich $\mathbb{Q}_p$ und $(a, b)_\infty$ ihr Hilbert-Symbol bezüglich $\mathbb{R}$. Sei $\mathbb{P}$ die Menge der Primzahlen, $V := \mathbb{P} \cup \{\infty\}$, und $\mathbb{Q}_\infty := \mathbb{R}$. Dann ist $\mathbb{Q}$ dicht in $\mathbb{Q}_v$ für alle $v \in V$.

2.1 Produktformel

Theorem 3 (Hilbert). Seien $a, b \in \mathbb{Q}^*$. Dann ist $(a, b)_v = 1$ für fast alle $v \in V$ (alle bis auf endlich viele) und es ist $\prod_{v \in V} (a, b)_v = 1$.

Beweis. Durch Multiplikation mit rationalen Quadraten kann man a, b als ganze Zahlen darstellen, ohne irgendeines der Hilbert-Symbole zu ändern: $a = \prod_{i=1}^n p_i$, $b = \prod_{j=1}^m q_j$ mit $p_i, q_j \in \mathbb{P} \cup \{-1\}$ (nicht notwendig verschieden).
Wegen der Bilinearität des Hilbert-Symbols genügt es, das Theorem für den Fall zu beweisen, dass a und b selbst Primzahlen oder -1 sind. Denn sei $M(x, y) := \{v \in V : (x, y)_v = -1\}$. Dann folgt aus $(a, b)_v = \prod_{i=1}^n \prod_{j=1}^m (p_i, q_j)_v$ die Beziehung $M(a, b) \subseteq \bigcup_{i=1}^n \bigcup_{j=1}^m M(p_i, q_j)$ (denn wenn $(a, b)_v = -1$, dann muss mindestens eines der $(p_i, q_j)_v = -1$ sein). Wenn nun alle $M(p_i, q_j)$ als endlich nachgewiesen sind, dann ist $M(a, b)$ als endliche Vereinigung endlicher Mengen auch endlich. Damit ist $\prod_{v \in V} (a, b)_v = \prod_{v \in V} \prod_{i=1}^n \prod_{j=1}^m (p_i, q_j)_v = \prod_{i=1}^n \prod_{j=1}^m \prod_{v \in V} (p_i, q_j)_v$, (weil nur noch endliche Produkte auftreten,) und wenn $\prod_{v \in V} (p_i, q_j)_v = 1$, dann gilt auch $\prod_{v \in V} (a, b)_v = 1$.

Fall 1: $a = -1, b = -1$ Es ist $(-1, -1)_\infty = (-1, -1)_2 = -1$ und $(-1, -1)_v = 1$ für $v \neq 2, \infty$ (Lemma 2 in Abschnitt 1.2), das Produkt ist gleich 1.

Fall 2: $a = -1, b = l, l$ prim Wenn $l = 2$, dann ist $(-1, 2)_v = 1$ für alle $v \in V$ ($(-1, 2)_2 = 1$ nach Lemma 6, $(-1, 2)_\infty = 1$ nach Satz 3, restliche v mit Lemma 2).
Wenn $l \neq 2$, dann ist $(-1, l)_v = 1$ für $v \neq 2, l$ (Lemma 2 und Satz 3), $(-1, l)_2 = (-1)^{\varepsilon(-1)\varepsilon(l)} = (-1)^{\varepsilon(l)}$ (Fall 2 in Satz 5), $(-1, l)_l = \left(\frac{-1}{l}\right) = (-1)^{\varepsilon(l)}$ (Lemma 3). Das Produkt ist gleich 1.

Fall 3: $a = l, b = l', l, l'$ prim Wenn $l = l'$, dann folgt aus Satz 2.iv) dass $(l, l')_v = (-1, l)_v$ $\forall v \in V$ und wir sind im zweiten Fall.
Wenn $l \neq l'$ und $l' = 2$, dann ist $(l, 2)_v = 1$ für $v \neq 2, l$ (Lemma 2), $(l, 2)_2 = (-1)^{\omega(l)}$ (Fall 2 in Satz 5), $(l, 2)_l = \left(\frac{2}{l}\right) = (-1)^{\omega(l)}$ (Lemma 3). Das Produkt ist gleich 1.
Wenn l, l' verschieden und ungleich 2 sind, dann ist $(l, l')_v = 1$ für $v \neq 2, l, l'$ (Lemma 2) und $(l, l')_2 = (-1)^{\varepsilon(l)\varepsilon(l')}$ (Fall 1 in Satz 5), $(l, l')_l = \left(\frac{l'}{l}\right)$, $(l, l')_{l'} = \left(\frac{l}{l'}\right)$ (Lemma 3). Nach dem Reziprozitätsgesetz ist $\left(\frac{l'}{l}\right)\left(\frac{l}{l'}\right) = (-1)^{\varepsilon(l)\varepsilon(l')}$, also ist das Produkt gleich 1. □

2.2 Existenz rationaler Zahlen mit vorgegebenen Hilbert-Symbolen

Theorem 4. Sei I eine endliche Menge, $(a_i)_{i\in I}$ mit $a_i \in \mathbb{Q}^*$, und sei $(\varepsilon_{i,v})_{i\in I, v\in V}$ mit $\varepsilon_{i,v} \in \{\pm 1\}$. Dann sind die folgenden Aussagen äquivalent:

(a) Es gibt ein $x \in \mathbb{Q}^*$, so dass $\forall i \in I, v \in V\colon (a_i, x)_v = \varepsilon_{i,v}$.

(b) Die folgenden drei Bedingungen sind erfüllt:

(1) Fast alle $\varepsilon_{i,v}$ sind gleich 1.
(2) Für alle $i \in I$ ist $\prod_{v\in V} \varepsilon_{i,v} = 1$.
(3) $\forall v \in V\colon \exists x_v \in \mathbb{Q}_v^*\colon \forall i \in I\colon (a_i, x_v)_v = \varepsilon_{i,v}$.

"(a)⇒(b)": Die Gültigkeit der Bedingungen (1) und (2) folgt aus Theorem 3, und mit $x_v := x$ ist Bedingung (3) erfüllt. Zum Nachweis der anderen Richtung brauchen wir drei Lemmas.

Lemma 1 (Chinesischer Restsatz). Seien $a_1, \ldots, a_n \in \mathbb{Z}$ und $m_1, \ldots, m_n \in \mathbb{Z}$ paarweise teilerfremd. Dann gibt es ein $a \in \mathbb{Z}$ mit $a \equiv a_i \pmod{m_i}$ für $i = 1, \ldots, n$.

Lemma 2 (Näherungssatz). Sei $S \subsetneq V$ endlich. Dann ist das Bild von $\mathbb{Q}$ dicht in $\prod_{v\in S} \mathbb{Q}_v$.

Beweis. Sei $(\widetilde{x}_v)_{v\in S} \in \prod_{v\in S} \mathbb{Q}_v$, dann ist zu jedem $\varepsilon > 0$ ein $\widetilde{x} \in \mathbb{Q}$ zu finden, so dass $d(\widetilde{x}, \widetilde{x}_v) \le \varepsilon$ für alle $v \in S$. Das ist für $v = p$ prim gleichbedeutend mit $v_p(\widetilde{x} - \widetilde{x}_p) \ge N$ für ein geeignetes N.
Falls $\infty \notin S$, dann fügen wir ∞ zu S hinzu und beweisen mehr als nötig ist.
Sei $(\widetilde{x}_\infty, \widetilde{x}_1, \ldots, \widetilde{x}_n) \in \mathbb{R} \times \mathbb{Q}_{p_1} \times \ldots \times \mathbb{Q}_{p_n}$ und seien $\varepsilon > 0$ und $\widetilde{N} \in \mathbb{N}$ beliebig vorgegeben. Es ist nun ein $\widetilde{x} \in \mathbb{Q}$ zu finden, so dass $|\widetilde{x} - \widetilde{x}_\infty| \le \varepsilon$ und $v_{p_i}(\widetilde{x} - \widetilde{x}_i) \ge \widetilde{N}$ für alle i.
Durch Multiplikation des Tupels mit einer geeigneten natürlichen Zahl [2] $m \ge 1$ erhalten wir $x_i := m\widetilde{x}_i \in \mathbb{Z}_{p_i}$ für $i = 1, \ldots, n$ und $x_\infty := m\widetilde{x}_\infty$.
Setze $M := \max\{v_{p_i}(m)\}$ und $N := \widetilde{N} + M \in \mathbb{N}$. (Denn $0 \le M \in \mathbb{Z}$.) Nach Lemma 1 (mit $m_i = p_i^N, a_i \equiv x_i \pmod{p_i^N}$) existiert ein $x_0 \in \mathbb{Z}$, so dass $v_{p_i}(x_0 - x_i) \ge N$ für alle i.
Sei nun $q \ge 2$ eine zu allen p_i teilerfremde Zahl (z.B. eine weitere Primzahl). Die rationalen Zahlen $\left\{\frac{a}{q^r} : a \in \mathbb{Z}, r \in \mathbb{N}\right\}$ liegen dicht in $\mathbb{R}$.[3] Wähle eine Zahl $u = \frac{a}{q^r}$ mit $\left|x_0 - x_\infty + u(p_1 \ldots p_n)^N\right| \le \varepsilon$.
Wir setzen $x := x_0 + u(p_1 \ldots p_n)^N$. Für alle $i = 1, \ldots, n$ gilt $q \in \mathbb{Z}_{p_i}^*$, also ist $u \in \mathbb{Z}_{p_i}$ und

$$\begin{aligned} v_{p_i}(x - x_i) &= v_{p_i}(x_0 + u(p_1 \ldots p_n)^N - x_i) \\ &\ge \inf\{\underbrace{v_{p_i}(x_0 - x_i)}_{\ge N}, \underbrace{v_{p_i}(u)}_{\ge 0} + \underbrace{v_{p_i}((p_1 \ldots p_n)^N)}_{= N}\} \ge N \end{aligned}$$

Setzen wir $\widetilde{x} := \frac{x}{m}$, dann haben wir $|\widetilde{x} - \widetilde{x}_\infty| = \left|\frac{x - x_\infty}{m}\right| \le \frac{\varepsilon}{m} \le \varepsilon$ und

$$v_{p_i}(\widetilde{x} - \widetilde{x}_i) = v_{p_i}(\frac{x - x_i}{m}) = v_{p_i}(x - x_i) - v_{p_i}(m) \ge N - M = \widetilde{N}$$

□

[2] z.B. $m := \prod_{i=1}^n p^{-\inf\{v_{p_i}(x_i), 0\}} \in \mathbb{N}$
[3] $x \in \mathbb{R}, \varepsilon > 0, q \in \mathbb{N} \Rightarrow \exists r \in \mathbb{N} : q^{-r} < \varepsilon, \exists a \in \mathbb{Z} : |q^r x - a| < 1$, also $|x - a/q^r| < \varepsilon$.

Lemma 3 (Dirichlet). Wenn $a, b \in \mathbb{N}$ teilerfremd sind, dann gibt es unendlich viele Primzahlen der Form $an + b$. Wird in Kapitel VI bewiesen ohne Verwendung von Resultaten aus den vorigen Kapiteln.

Beweis von Theorem 4. "(b)⇒(a)": Seien die drei Bedingungen erfüllt. Ohne die Hilbert-Symbole zu verändern, können wir die a_i mit den Quadraten ihrer Nenner multiplizieren und deshalb annehmen, dass alle a_i in $\mathbb{Z}$ liegen.
Sei $S = \{2, \infty\}$ vereinigt mit der Menge der Primteiler der a_i.
Sei $T = \{v \in V : \exists i \in I \colon \varepsilon_{i,v} = -1\}$.
$S, T \subseteq V$. Beide Mengen sind endlich (S klar, T nach Bedingung (1)).

1. Fall: $S \cap T = \emptyset$. Dann ist $\infty \notin T$. Setze $a := \prod T$, $m := 8 \prod (S \setminus \{2, \infty\})$.
Weil $S \cap T = \emptyset$ sind a und m teilerfremd. Nach Lemma 3 existiert eine Primzahl $p \equiv a \pmod m$ mit $p \notin S \cup T$. Wir werden zeigen, dass $x := ap$ die gewünschte Eigenschaft $(a_i, x)_v = \varepsilon_{i,v}\ \forall i \in I, v \in V$ hat. Seien dazu $i \in I$ und $v \in V$ beliebig vorgegeben.

I. $v \in S$: Dann ist $v \notin T$ und deshalb $\varepsilon_{i,v} = 1$. Ist $v = \infty$, dann ist $(a_i, x)_\infty = 1$ wegen $x > 0$. Ist $v = l$ eine Primzahl, dann ist $x = ap \equiv a^2 \pmod m$, also $x \equiv a^2 \pmod 8$ und $x \equiv a^2 \pmod l$. Das zeigt, dass x ein Quadrat in $\mathbb{Q}_l^*$ ist (s. II,3.3), also ist $(a_i, x)_v = 1$.

II. $v \notin S$, $v = l$ prim : Dann gilt $\forall k \in I : a_k \in \mathbb{Z}_l^*$ (denn $l \nmid a_k$). Da $l \neq 2$ folgt aus Theorem 1

$$\forall k \in I, b \in \mathbb{Q}_l^* \colon (a_k, b)_l = \left(\frac{a_k}{l}\right)^{v_l(b)}$$

II.1. $l \notin T \cup \{p\}$: Dann gilt $x = ap \in \mathbb{Z}_l^*$ (denn $l \nmid p$, $l \nmid a = \prod T$), also $v_l(x) = 0$ und wir haben $(a_i, x)_l = \left(\frac{a_i}{l}\right)^0 = 1$, und wegen $l \notin T$ ist $\varepsilon_{i,l} = 1$.

II.2. $l \in T$: Dann ist $v_l(x) = 1$ (denn $x = ap$ ist ein Produkt verschiedener Primzahlen, $l \mid a$). Wegen Bedingung (3) existiert ein $x_l \in \mathbb{Q}_l^*$ mit $\forall k \in I \colon (a_k, x_l)_l = \varepsilon_{k,l}$. Wegen $l \in T$ gibt es ein $j \in I$ für das $\varepsilon_{j,l} = -1$ und wir haben $(a_j, x_l)_l = -1 = \left(\frac{a_j}{l}\right)^{v_l(x_l)}$, deshalb muss $v_l(x_l) \equiv 1 \pmod 2$ sein, also gilt $(a_i, x)_l = \left(\frac{a_i}{l}\right)^{v_l(x)} = \left(\frac{a_i}{l}\right) = \left(\frac{a_i}{l}\right)^{v_l(x_l)} = (a_i, x_l)_l = \varepsilon_{i,l}$.

II.3. $l = p$: Dann ist nach Theorem 3, den Fällen I, II.1, II.2 sowie Bedingung (2)

$$(a_i, x)_p = \prod_{v \neq p} (a_i, x)_v = \prod_{v \neq p} \varepsilon_{i,v} = \varepsilon_{i,p}$$

2. Fall: $S \cap T \neq \emptyset$. Aus Kapitel II,3.3 wissen wir, dass die Quadrate in $\mathbb{Q}_v^*$ eine offene Untergruppe bilden (auch in $\mathbb{R}^*$). Es gibt also (wegen der Endlichkeit von S) ein $N \in \mathbb{N}$, so dass für alle Primzahlen $p \in S$ gilt: Ist $x \in \mathbb{Q}_p^*$ mit $v_p(x - 1) \geq N$, dann ist x ein Quadrat in $\mathbb{Q}_p^*$.
Von der Bedingung (3) haben wir ein Tupel $(x_v)_{v \in S} \in \prod_{v \in S} \mathbb{Q}_v$ (dabei ist jedes $x_v \in \mathbb{Q}^*$). Setze $M := \max \{v_p(x_p) : p \in S \text{ prim}\} \in \mathbb{Z}$. Nach Lemma 2 existiert ein $x' \in \mathbb{Q}^*$ mit $v_p(x' - x_p) \geq N + M$ für alle Primzahlen $p \in S$ und $|x' - x_\infty| \leq |x_\infty / 2|$ in $\mathbb{R}$. Dann ist $v_p(x'/x_p - 1) = v_p(x' - x_p) - v_p(x_p) \geq N + M - M = N$ und $|x'/x_\infty - 1| \leq 1/2$, also ist für alle $v \in S$ die Zahl x'/x_v ein Quadrat in $\mathbb{Q}_v^*$.
Setzen wir für alle $i \in I, v \in V$

$$\eta_{i,v} := \varepsilon_{i,v} (a_i, x')_v$$

dann erfüllt die Familie $(\eta_{i,v})$ die Bedingungen (1),(2),(3) und es ist $\eta_{i,v} = 1\ \forall i \in I, v \in S$. Denn nach den Bedingungen für $\varepsilon_{i,v}$ und Theorem 3 gilt:

(1) Fast alle $\eta_{i,v} = \varepsilon_{i,v}(a_i, x')_v$ sind gleich 1.

(2) Für alle $i \in I$ ist $\prod_{v\in V} \eta_{i,v} = \prod_{v\in V}(\varepsilon_{i,v}(a_i, x')_v) = \prod_{v\in V} \varepsilon_{i,v} \prod_{v\in V}(a_i, x')_v = 1$.

(3) $\forall v \in V\colon \exists x'_v \in \mathbb{Q}_v^*\colon \forall i \in I\colon (a_i, x'_v)_v = \eta_{i,v}$. Setze $x'_v := x'/x_v$, dann ist $(a_i, x'/x_v)_v = (a_i, x_v)_v(a_i, x')_v = \varepsilon_{i,v}(a_i, x')_v = \eta_{i,v}$.

Falls $v \in S$, dann ist $x'/x_v \in \mathbb{Q}_v^{*2}$, also $\forall i \in I\colon \eta_{i,v} = (a_i, x'/x_v)_v = 1$.

Auf die Familie $\eta_{i,v}$ ist nun Fall 1 anwendbar, denn $\widetilde{T} := \{v \in V : \exists i \in I\colon \eta_{i,v} = -1\}$ ist disjunkt zu S. Es existiert also ein $y \in \mathbb{Q}^*$ mit $\forall i \in I, v \in V\colon (a_i, y)_v = \eta_{i,v}$. Setzen wir $x := yx'$, dann ist $\forall i \in I, v \in V\colon (a_i, x)_v = (a_i, y)_v(a_i, x')_v = \eta_{i,v}(a_i, x')_v = \varepsilon_{i,v}$. □