Christian Semrau

Zusatzdokument zu

Kapitel IV. Quadratische Formen über $\mathbb{Q}_p$ und über $\mathbb{Q}$

aus: Jean Pierre Serre: A course in arithmetics

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

In den Abschnitten IV, 2.3 und IV, 3 benutzte Sätze

Kapitel III

Definition. Seien $a, b \in k^*$. Falls die Gleichung $ax^2+by^2 = z^2$ 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.

Satz (III, 1.1, 1). *Seien $a, b \in k^*, k_b := k(\sqrt{b})$. Dann ist $(a, b) = 1 \Leftrightarrow a \in N(k_b^*)$.*

Satz (III, 1.1, 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) $(a, b) = (a, -ab)$, $(a, b) = (a, (1-a)b)$

Lemma (III, 1.2, 2). *Seien $p > 2$, $u, v \in \mathbb{Z}_p^*$. Dann ist $(u, v) = 1$.*

Definition. Sei $\mathbb{P}$ die Menge der Primzahlen, $V := \mathbb{P} \cup \{\infty\}$, und $\mathbb{Q}_\infty := \mathbb{R}$.

Lemma (Näherungssatz, III, 2.2, 2). *Sei $S \subsetneq V$ endlich. Dann ist das Bild von $\mathbb{Q}$ dicht in $\prod_{v\in S} \mathbb{Q}_v$.*

Bemerkung. Sei $(x_v)_{v\in S} \in \prod_{v\in S} \mathbb{Q}_v$, dann existiert zu jedem $\varepsilon > 0$ ein $x \in \mathbb{Q}$ mit $d(x, x_v) \leq \varepsilon$ für alle $v \in S$.

Theorem (III, 2.1, 3). *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 $\prod\limits_{v\in V} (a, b)_v = 1$.*

Theorem (III, 2.2, 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 $\forall i \in I, v \in V: (a_i, x)_v = \varepsilon_{i,v}$.*

(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) $\forall v \in V \colon \exists x_v \in \mathbb{Q}_v^* \colon \forall i \in I \colon (a_i, x_v)_v = \varepsilon_{i,v}$.

Kapitel IV

Satz (IV, 1.6, 3'). *Wenn* f *die* 0 *repräsentiert und nichtdegeneriert ist, dann ist* $f \sim f_2 \dot{+} g$ *mit* f_s *hyperbolisch. Ausserdem repräsentiert* f *alle Elemente von* k.

Korollar (IV, 1.6, 3', 2). *Seien* g, h *nichtdegenerierte quadr. Formen vom Rang* ≥ 1 *und sei* $f = g \dot{-} h$. *Dann ist äquivalent:*

(a) f *repr* 0

(b) *Es gibt ein* $a \in k^*$ *das von* g *und* h *repräsentiert wird*

(c) *Es gibt ein* $a \in k^*$ *so dass* $g \dot{-} aZ^2$ *und* $h \dot{-} aZ^2$ *die* 0 *repräsentieren*

Definition und Satz. Ist $f \sim a_1 X_1^2 + \cdots + a_n X_n^2$ eine quadr. Form über dem Körper k, dann sei $d(f) := a_1 \cdots a_n \in k^*/k^{*2}$, und $\varepsilon(f) := \prod_{i<j} (a_i, a_j) \in \{\pm 1\}$.
Ist f nichtdegeneriert, dann sind alle a_i in k^* und n ist der Rang von f.
Äquivalente quadr. Formen über $\mathbb{Q}_p$ haben dieselben Werte n, d, ε, die deshalb Invarianten heißen.
Für $f \sim aZ^2 \dot{+} g$ gilt $\varepsilon(f) = \varepsilon(g)(a, d(g))$ und $d(f) = ad(g)$.

Theorem (IV, 2.2, 6). *Eine quadr. Form* f *vom Rang* n *über* $\mathbb{Q}_p$ *mit den Invarianten* $d = d(f), \varepsilon = \varepsilon(f)$ *repräsentiert* 0 *genau dann wenn:*

i) $n = 2, d = -1$

ii) $n = 3, (-1, -d) = \varepsilon$

iii) $n = 4$ *und* $d \neq -1$ *oder* $d = 1, \varepsilon = (-1, -1)$

iv) $n \geq 5$

Korollar. *Eine quadr. Form* f *vom Rang* n *über* $\mathbb{Q}_p$ *mit den Invarianten* $d = d(f), \varepsilon = \varepsilon(f)$ *repräsentiert* $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ *genau dann wenn:*

i) $n = 1, d = a$

ii) $n = 2, (a, -d) = \varepsilon$

iii) $n = 3$ *und* $-d \neq a$ *oder* $-d = a, \varepsilon = (-1, -d)$

iv) $n \geq 4$