Christian Semrau **SS 2003**

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

§2. Quadratische Formen über $\mathbb{Q}_p$

...

2.3. Klassifikation

Theorem 7. *Zwei quadratische Formen über $\mathbb{Q}_p$ sind äquivalent gdw. sie den gleichen Rang, die gleiche Diskriminante und die gleiche Invariante ε haben.*

Beweis. Dass zwei äquivalente quadr. Formen die gleichen Invarianten haben, ist klar nach ihren Definitionen. Die Umkehrung beweisen wir mit Induktion nach dem (nach Vor.) gemeinsamen Rang n der quadr. Formen f und g.
Der Fall $n = 0$ ist trivial ($f = 0 = g$ ist die einzige quadr. Form).
Ist $n \geq 1$, dann folgt aus Th. 6, Kor., dass f und g dieselben Elemente von k^*/k^{*2} repräsentieren, es gibt also ein $a \in k^*$ das von f und von g repräsentiert wird. Deshalb haben wir (nach 1.6, 3', Kor. 1)

$$f \sim aZ^2 \dotplus f' \text{ und } g \sim aZ^2 \dotplus g'$$

mit quadr. Formen f', g' vom Rang $n-1$. Es ist $d(f') = d(f)/a = d(g)/a = d(g')$ und $\varepsilon(f') = \varepsilon(f)/(a, d(f')) = \varepsilon(g)/(a, d(g')) = \varepsilon(g')$. Also haben f', g' die gleichen Invarianten und nach Induktionsvoraussetzung ist $f' \sim g'$, also auch $f \sim g$. ♣

Korollar. *Bis auf Äquivalenz existiert genau eine quadr. Form vom Rang 4 die nicht die 0 repräsentiert. Seien $a, b \in \mathbb{Q}_p$ mit $(a, b) = -1$, dann ist das die Form $z^2 - ax^2 - by^2 + abt^2$.*

Beweis. Nach Theorem 6 wird eine solche Form durch die Invarianten $d = 1, \varepsilon = -(-1, -1)$ charakterisiert. Nachrechnen zeigt, dass $f = z^2 - ax^2 - by^2 + abt^2$ diese Invarianten hat ($\varepsilon(f) = (-a, -b)(ab, ab) = (-1, -1)(a, b) = -(-1, -1)$). ♣

Bemerkung. Diese quadr. Form ist die reduzierte Norm des (bis auf Isomorphie eindeutig bestimmten) Schiefkörpers vom Grad 4 über $\mathbb{Q}_p$, dem "Quaternionenkörper über $\mathbb{Q}_p$" mit der Basis $B = \{1, i, j, k\}$, wobei $i^2 = a, j^2 = b, ij = k = -ji, (a, b) = -1$.
(Ist $\alpha = z + xi + yj + tk$ ein Quaternion über $\mathbb{Q}_p$, dann ist $N(\alpha) := \det(M_B(\ell_\alpha)) = (z^2 - ax^2 - by^2 + abt^2)^2$.)

Satz 6. *Sei $n > 1, d \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}, \varepsilon = \pm 1$. Es existiert eine quadr. Form f vom Rang n mit $d(f) = d, \varepsilon(f) = \varepsilon$ genau dann, wenn $n = 1, \varepsilon = 1$ oder $n = 2, d \neq -1$ oder $n = 2, \varepsilon = 1$ oder $n \geq 3$.*

Beweis. Der Fall $n = 1$ ist trivial ($\varepsilon(f) = 1$ und $d(f) = d$ für $f \sim dX^2$).
Ist $n = 2$, dann ist $f \sim aX^2 + bY^2$, und es gilt $d(f) = -1 \Rightarrow \varepsilon(f) = (a, b) = (a, -ab) = 1$, also kann nicht gleichzeitig $d(f) = -1$ und $\varepsilon(f) = -1$ sein (das zeigt "⇒"). Falls umgekehrt $d = -1, \varepsilon = 1$, hat $f = X^2 - Y^2$ diese Invarianten, ist aber $d \neq -1$, dann existiert ein $a \in \mathbb{Q}_p^*$ mit $(a, -d) = \varepsilon$ und $f = aX^2 + adY^2$ leistet das Gewünschte.
Ist $n = 3$, dann sei $-d \neq a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Wie eben gezeigt wurde, existiert eine quadr. Form g vom Rang 2 mit $d(g) = ad, \varepsilon(g) = \varepsilon(a, -d)$. Dann hat $f = aZ^2 \dot{+} g$ die Invarianten d und ε.
Ist schliesslich $n \geq 4$, dann gibt es ein g vom Rang 3 mit den vorgegebenen Invarianten und $f = g(X_1, X_2, X_3) + X_4^2 + \cdots + X_n^2$ hat dieselben Invarianten. ♣

Korollar. *Die Anzahl der Äquivalenzklassen quadr. Formen vom Rang n über $\mathbb{Q}_p$ ist*

für n	*falls $p \neq 2$*	*falls $p = 2$*
$= 1$	4	8
$= 2$	7	15
≥ 3	8	16

Beweis. $d(f)$ kann 4 Werte annehmen für $p \neq 2$ und 8 Werte für $p = 2$, $\varepsilon(f)$ kann 2 Werte annehmen. Mit den Einschränkungen aus Satz 6 ergeben sich die Anzahlen. ♣

2.4. Der reelle Fall

Sei f eine quadr. Form vom Rang n über $\mathbb{R}$. f ist äquivalent zu

$$X_1^2 + \cdots + X_r^2 - Y_1^2 - \cdots - Y_s^2$$

mit $r, s \in \mathbb{N}_0$ und $r + s = n$. Das Paar (r, s) hängt nur von f ab, es heißt die Signatur von f. f heißt definit, falls $r = 0$ oder $s = 0$, sonst indefinit (genau in diesem Fall repräsentiert f die 0).
Die Invarianten $\varepsilon(f)$ und $d(f)$ sind definiert wie im Fall $\mathbb{Q}_p$, und wegen $(-1, -1) = -1$ ergeben sich die Formeln

$$\varepsilon(f) = (-1)^{s(s-1)/2} = \begin{cases} 1 & \text{falls } s \equiv 0, 1 \pmod 4 \\ -1 & \text{falls } s \equiv 2, 3 \pmod 4 \end{cases}$$

$$d(f) = (-1)^s = \begin{cases} 1 & \text{falls } s \equiv 0 \pmod 2 \\ -1 & \text{falls } s \equiv 1 \pmod 2 \end{cases}$$

Die Werte von $d(f)$ und $\varepsilon(f)$ bestimmen also den Wert von s mod 4, insbesondere ist f im Fall $n \leq 3$ bis auf Äquivalenz eindeutig durch $d(f)$ und $\varepsilon(f)$ bestimmt.
Man sieht leicht, dass die Teile i), ii), iii) von Theorem 6 und seinem Korollar auch für $\mathbb{R}$ gelten (denn in den Beweisen wurde nur die Regularität des Hilbert-Symbols benutzt), und dass Teil iv) nicht für $\mathbb{R}$ zutrifft.

§3. Quadratische Formen über $\mathbb{Q}$

Alle quadratischen Formen f die wir in diesem Abschnitt betrachten, sollen Koeffizienten in $\mathbb{Q}$ haben und nichtdegeneriert sein.

3.1. Invarianten einer quadr. Form

Wie in Kapitel III, Abschnitt 2 bezeichnen wir mit V die Menge der Primzahlen zusammen mit dem Symbol ∞ und setzen $\mathbb{Q}_\infty = \mathbb{R}$.
Sei $f \sim a_1X_1^2 + \cdots + a_nX_n^2$ nichtdegeneriert. Wir ordnen dieser quadr. Form folgende Invarianten zu:

a) Die Diskriminante $d(f) = a_1 \cdots a_n \in \mathbb{Q}^*/\mathbb{Q}^{*2}$

b) Sei $v \in V$. Dann sei f_v die quadr. Form über $\mathbb{Q}_v$ mit denselben Koeffizienten wie f (wobei man die Injektion $\mathbb{Q} \to \mathbb{Q}_v$ benutzt). Die Invarianten von f_v bezeichnen wir mit $d_v(f)$ und $\varepsilon_v(f)$. Es ist klar, dass $d_v(f)$ das Bild von $d(f)$ ist unter der kanonischen Abbildung $\mathbb{Q}/\mathbb{Q}^{*2} \to \mathbb{Q}_v/\mathbb{Q}_v^{*2}$. Es ist $\varepsilon_v(f) = \prod_{i<j}(a_i, a_j)_v$ und die Produktformel aus (III, 2.1, Theorem 3) liefert $\prod_{v\in V} \varepsilon_v(f) = 1$.

c) Die Signatur (r, s) der reellen quadr. Form f.

Die Invarianten $d_v(f), \varepsilon_v(f), (r, s)$ heißen lokale Invarianten von f.

3.2. Repräsentation einer Zahl durch eine quadr. Form

Theorem 8 (Hasse-Minkowski). *f repr $0 \Leftrightarrow \forall\, v \in V$: f_v repr 0. (D.h. f hat eine "globale" Nullstelle gdw. f "überall lokal" eine Nullstelle hat.)*

Beweis. "$\Rightarrow$": Klar.
"$\Leftarrow$": Schreibe $f = a_1X_1^2 + \cdots + a_nX_n^2, a_i \in \mathbb{Q}^*$. Indem man $a_1 f$ statt f betrachtet, kann man zusätzlich $a_1 = 1$ annehmen. Wir unterscheiden mehrere Fälle.

i) $n = 2$.
Es ist $f = X_1^2 - aX_2^2$ und weil f_∞ *repr* 0 ist $a > 0$. Zerlege a in der Form $a = \prod_p p^{v_p(a)}$. Da f_p die 0 repräsentiert, ist $a \in \mathbb{Q}_p^{*2}$, also ist $v_p(a)$ gerade. Weil das für alle p gilt, ist a ein Quadrat in $\mathbb{Q}$ und f *repr* 0.

ii) $n = 3$ (Legendre).
Es ist $f = X_1^2 - aX_2^2 - bX_3^2$. Indem wir a und b mit Quadraten multiplizieren, können wir annehmen, dass a und b quadratfreie ganze Zahlen sind, und oBdA sei $|a| \leq |b|$. Wir verwenden Induktion nach $m = |a| + |b| \in \mathbb{N}$.
Ist $m = 2$, dann ist $f = X_1^2 \pm X_2^2 \pm X_3^2$. Der Fall $f = X_1^2 + X_2^2 + X_3^2$ entfällt, weil f_∞ *repr* 0, in allen anderen Fällen repräsentiert f die 0.
Ist $m > 2$, dann ist $|b| \geq 2$ und wir schreiben $b = \pm p_1 \cdots p_k$ mit pw. versch. Primzahlen p_i. Sei p eine dieser p_i, wir werden zeigen, dass a ein Quadrat modulo p ist.
Das ist klar, wenn $a \equiv 0 \pmod p$. Andernfalls ist a eine p-adische Einheit. Nach Voraussetzung existiert ein Tupel $(x, y, z) \in (\mathbb{Q}_p)^3 \setminus \{0\}$ mit $z^2 - ax^2 - by^2 = 0$ und wir können annehmen, dass es primitiv ist (II, 2.1, Satz 6). Wir haben dann $z^2 - ax^2 \equiv 0 \pmod p$ (weil $p \mid b$).

Falls nun $x \equiv 0 \pmod{p}$, dann wäre auch $z \equiv 0 \pmod{p}$, und dann wäre $by^2 \equiv 0 \pmod{p^2}$. Weil aber $v_p(b) = 1$, heißt dass $y \equiv 0 \pmod{p}$, im Widerspruch zur Primitivität der Lösung. Es ist also $x \not\equiv 0 \pmod{p}$, und deshalb ist a ein Quadrat modulo p.
Nach dem Chin. Restsatz ist dann a auch ein Quadrat modulo b.
Es existieren also ganze Zahlen t, b' mit $|t| \leq |b|/2$ und $t^2 = a + bb'$. Die Gleichung $bb' = t^2 - a$ zeigt, dass bb' eine Norm der Erweiterung $k(\sqrt{a})/k$ ist für $k = \mathbb{Q}$ und alle $\mathbb{Q}_v$ (egal ob $\sqrt{a} \in \mathbb{Q}_v$ [dann $bb' = N(t^2 - a)$] oder nicht [dann $bb' = N(t + \sqrt{a})$]). Analog zum Beweis von III, 1.1, Satz 2 iii) folgt $b \in Nk(\sqrt{a})^* \Leftrightarrow b^2 b' \in Nk(\sqrt{a})^*$ und analog zu III, 1.1, Satz 1 folgt daraus, dass mit

$$f' = X_1^2 - aX_2^2 - b'X_3^2$$

gilt

$$f \; repr \; 0 \text{ in } k \iff f' \; repr \; 0 \text{ in } k \text{ für } k = \mathbb{Q}, \mathbb{Q}_v, v \in V$$

Insbesondere repräsentiert f' nach Vorauss. die 0 in allen $\mathbb{Q}_v$.
Es ist $|b'| = |(t^2 - a)/b| \leq |t^2/b| + |a/b| \leq |b|/4 + 1 < |b|$ (wegen $|b| \geq 2$). Zerlege $b' = b''u^2$ mit $b'', u \in \mathbb{Z} \setminus \{0\}$ und b'' quadratfrei. $|b''| \leq |b'| < |b|$ ist klar. Wir können nun die Induktionsvoraussetzung auf die zu f' äquivalente quadr. Form

$$f'' = X_1^2 - aX_2^2 - b''X_3^2$$

anwenden. Weil diese nun die 0 in $\mathbb{Q}$ repräsentiert, trifft das auch auf f' und damit auch auf f zu.

iii) $n = 4$.
Es ist $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. Sei $v \in V$. Weil $f_v \; repr \; 0$ existiert nach 1.6, Satz 3', Kor. 2 (a⇒b) ein $x_v \in \mathbb{Q}_v^*$, das repräsentiert wird von $aX_1^2 + bX_2^2$ und von $cX_3^2 + dX_4^2$. Nach Th.6, Kor. ii) heißt das, dass

$$(x_v, -ab)_v = (a, b)_v \text{ und } (x_v, -cd)_v = (c, d)_v \text{ für alle } v \in V.$$

Wir können nun III, 2.2, Theorem 4 anwenden und erhalten ein $x \in \mathbb{Q}^*$ mit

$$(x, -ab)_v = (a, b)_v \text{ und } (x, -cd)_v = (c, d)_v \text{ für alle } v \in V$$

Die quadr. Form $aX_1^2 + bX_2^2 - xZ^2$ repräsentiert 0 in jedem $\mathbb{Q}_v$ nach Theorem 6, Kor. ii) und deshalb nach Fall ii): $aX_1^2 + bX_2^2 - xZ^2 \; repr \; 0$ in $\mathbb{Q}$. Analog zeigt man, dass $cX_3^2 + dX_4^2 - xZ^2 \; repr \; 0$ in $\mathbb{Q}$, und mit 1.6, Satz 3', Kor. 2 (c⇒a) folgt, dass f die 0 repräsentiert.

iv) $n \geq 5$.
Wir verwenden Induktion nach n. Wir setzen $f = h \dot{-} g$ mit $h = a_1X_1^2 + a_2X_2^2$ und $g = -(a_3X_3^2 + \cdots + a_nX_n^2)$. Sei $S = \{2, \infty\} \cup \{p \in \mathbb{P} : v_p(a_i) \neq 0 \text{ für ein } i \geq 3\}$. S ist endlich. Sei $v \in S$. Weil $f_v \; repr \; 0$ existiert ein $a_v \in \mathbb{Q}_v$ das repräsentiert wird von h und g. Für jedes $v \in S$ gibt es also $a_v, x_{v,i} \in \mathbb{Q}_v, i = 1, \ldots n$ mit

$$h(x_{v,1}, x_{v,2}) = a_v = g(x_{v,3}, \ldots, x_{v,n}).$$

Die Menge der Quadrate von $\mathbb{Q}_v^*$ ist offen, die Abbildung $\mathbb{Q}_v \times \mathbb{Q}_v \to \mathbb{Q}_v, (x_1, x_2) \mapsto h(x_1, x_2)/a_v$ ist stetig für jedes $v \in S$, also folgt aus dem Näherungssatz (III, 2.2, Lemma 2) die Existenz von $x_1, x_2 \in \mathbb{Q}, a := h(x_1, x_2)$ so dass $a/a_v \in \mathbb{Q}_v^{*2}$ für alle $v \in S$.

Sei $f_1 = aZ^2 \dot{-} g$. Ist $v \in S$, dann repräsentiert g a_v, also auch a (weil a/a_v ein Quadrat ist), also repräsentiert f_1 die 0 in $\mathbb{Q}_v$. Ist $v \notin S$, (also $v \in \mathbb{P} \setminus S$) dann sind die Koeffizienten $-a_3, \ldots, -a_n$ von g v-adische Einheiten, ebenso wie $-d_v(g)$ (nach Def. von S), und weil $v \neq 2$ ($2 \in S$) ist $\varepsilon_v(g) = 1$ (Berechnungsformel in III, 1.2, Lemma 2). Damit ist $(-1, -d_v(g)) = 1 = \varepsilon_v(g)$, also nach Th. 6, Kor. iii), iv) repräsentiert g a.
Für jedes $v \in V$ repräsentiert f_1 die 0 in $\mathbb{Q}_v$, und da der Rang von f_1 gleich $n - 1$ ist, repräsentiert f_1 nach Induktionsvoraussetzung die 0 auch in $\mathbb{Q}$. Also repräsentiert g a in $\mathbb{Q}$, und weil h *repr* a nach Def. von a, repräsentiert f die 0.

♣