Ruprecht-Karls-Universität Heidelberg
Fakultät für Mathematik und Informatik
Seminar: Quadratische Formen über den rationalen Zahlen
Sommersemester 2007
Prof. Dr. Kay Wingberg
05. Juli 2007

Klassifikation quadratischer Formen über $\mathbb{Q}$ und Quadratsätze

Tamara Döringer
ta-doe@gmx.de

Tobias Schultz
Tobias.Schultz@stud.uni-heidelberg.de

Im Folgenden seien alle quadratischen Formen nichtausgeartet und mögen nur Koeffizienten aus $\mathbb{Q}$besitzen.

1 Klassifikation quadratischer Formen über $\mathbb{Q}$

In diesem Abschnitt werden viele Ergebnisse der vorangengenen Kapitel benötigt. Es lässt sich daher nicht vermeiden, sich in Beweisen auf Sätze dieser Kaptiel zu beziehen. Diese werden aber an entsprechender Stelle nochmals als *Hilfsmittel* rezitiert.
Wir beginnen mit einer Äquivalenzaussage für quadratische Formen in $\mathbb{Q}$ zu solchen in $\mathbb{Q}_\nu$. Eine umfassende Aussage hierüber gibt das folgende

Theorem 9. *Seien f und f' zwei quadratische Formen über $\mathbb{Q}$. Es sind f und f' genau dann über $\mathbb{Q}$ äquivalent, wenn sie über jedem Körper $\mathbb{Q}_\nu$ äquivalent sind.*

Beweis. Zum Beweis des Theorems benötigen wir zwei Hilfsmittel.

Hilfsmittel 1. *Sei $a \in \mathbb{Q}^*$. Damit eine quadratische Form f ein a aus $\mathbb{Q}^*$ repräsentiert, ist es notwendig und hinreichend, dass sie dieses in jedem $\mathbb{Q}_\nu$ repräsentiert.*

Hilfsmittel 2. *Seien $f = g + h$ und $f' = g' + h'$ zwei nichtausgeartete quadratische Formen. Wenn $f \backsim f'$ und $g \backsim g'$, dann ist auch $h \backsim h'$.*

Nun zum Beweis des Theorems:
„⇒“:
Seien f und f' über $\mathbb{Q}$ äquivalent. Da $\mathbb{Q} \subset \mathbb{Q}_\nu$ für alle $\nu \in V$, ist diese Richtung trivialerweise erfüllt.
„⇐“:
Seien nun f und f' äquivalent über jedem $\mathbb{Q}_\nu$. Wir beweisen das Theorem per vollständiger Induktion über die Anzahl n der Variablen. Im Fall $n = 0$ ist nichts zu zeigen. Sei also $n \geq 1$ und das Theorem bereits für Formen mit $n - 1$ Variablen gezeigt. Da f nichtausgeartet ist, existiert ein $a \in \mathbb{Q}^*$, welches durch f repräsentiert wird. Da f und f' äquivalent sind, wird a auch von f' repräsentiert. Nach Hilfsmittel 1 wird $a \in \mathbb{Q}^*$ bereits von f und f' über $\mathbb{Q}$ repräsentiert. Somit können wir f und f' in der Form

$$f \backsim aZ^2 + g, \quad f' \backsim aZ^2 + g'$$

darstellen. Nach Hilfsmittel 2 ist $g \backsim g'$ über $\mathbb{Q}_\nu$ für alle $\nu \in V$. Da g und g' Formen in $n - 1$ Variablen sind, sind diese nach Induktionsannahme äquivalent über $\mathbb{Q}$. Folglich ist auch $f \backsim f'$ über $\mathbb{Q}$. □

Korollar. *Seien (r, s) und (r', s') die Signaturen von f und f'. f und f' sind genau dann äquivalent, wenn folgendes gilt:*

- $d(f) = d(f')$
- $\epsilon_\nu(f) = \epsilon_\nu(f')$ *für alle* $\nu \in V$
- $(r, s) = (r', s')$

Beweis. Wir benötigen hierzu das

Hilfsmittel 3. *Zwei quadratische Formen über $\mathbb{Q}_p$ sind genau dann äquivalent, wenn sie den gleichen Rang, die gleiche Diskriminante und das gleiche $\epsilon_p = \prod_{i<j}(a_i, a_j)$ besitzen.*

Wir betrachten zuerst den Fall, dass die quadratischen Formen nicht reell sind. Aus dem Hilfsmittel folgt mit $d(f) = d(f')$ und $\epsilon_p(f) = \epsilon_p(f')$ für alle $p \in P$, dass f und f' äquivalent über jedem $\mathbb{Q}_p$ sind.
Seien die Formen nun reell. Aus dem *Sylvesterschen Trägheitssatz* folgt, dass zwei quadratische Formen genau dann äquivalent sind, wenn $(r, s) = (r', s')$.
Somit folgt die Behauptung für alle $\mathbb{Q}_\nu$. Das Theorem 9 impliziert, dass diese dann auch über $\mathbb{Q}$ äquivalent sind. □

Im der folgenden Bemerkung sind wichtige Eigenschafen von Invarianten quadratischer Formen aus den vorherigen Vorträgen zusammengefasst.

Bemerkung. *Die Invarianten $d = d(f)$, $\epsilon_\nu = \epsilon_\nu(f)$ und die Signatur (r, s) sind nicht frei wählbar. Sie erfüllen die folgenden Eigenschaften.*

(i) $\epsilon_\nu = 1$ *für fast alle* $\nu \in V$ *und* $\prod_{\nu \in V} \epsilon_\nu = 1$

(ii) $\epsilon_\nu = 1$, *falls* $n = 1$

(iii) $\epsilon_\nu = 1$, *falls* $n = 2$ *und das Bild* d_ν *von* d *in* $\mathbb{Q}_\nu^*/\mathbb{Q}_\nu^{*2}$ *sei gleich* -1

(iv) $r, s \geq 0$ *und* $r + s = n$

(v) $d_\infty = (-1)^s$

(vi) $\epsilon_\infty = (-1)^{s(s-1)/2}$

Mit diesen Forderungen zeigen wir die Existenz quadratischer Formen, die d, $(\epsilon_\nu)_{\nu \in V}$ und (r, s) als Invarianten besitzen.

Proposition 7. *Es erfüllen d, $(\epsilon_\nu)_{\nu \in V}$ und (r, s) die Bedingungen aus der Bemerkung oben. Dann existiert eine quadratische Form vom Rang n über $\mathbb{Q}$, die als Invarianten d, $(\epsilon_\nu)_{\nu \in V}$ und (r, s) besitzt.*

Beweis. Im Beweis benötigen wir

Hilfsmittel 4. *Sei $(a_i)_{i \in I}$ eine endliche Familie von Elementen in $\mathbb{Q}^*$ und sei $(\epsilon_{i,\nu})_{i \in I, \nu \in V}$ eine Familie von Zahlen, die ± 1 sind. Damit ein $x \in \mathbb{Q}^*$ mit $(a_i, x)_\nu = \epsilon_{i,\nu} \quad \forall i \in I, \quad \forall \nu \in V$ existiert, ist es notwendig und hinreichend, dass die folgenden Bedingungen erfüllt sind:*

(i) Fast alle $\epsilon_{i,\nu}$ sind 1.

(ii) Für alle $i \in I$ gilt $\prod_{\nu \in V} \epsilon_{i,\nu} = 1$.

(iii) Für alle $\nu \in V$ existiert ein $x_\nu \in \mathbb{Q}_\nu^*$ mit $(a_i, x_\nu) = \epsilon_{i,\nu} \quad \forall i \in I$.

Weiterhin erinnern wir uns daran, dass eine quadratische Form in zwei Variablen genau dann die Null repräsentiert, wenn ihre Diskrimante $d = -1, \quad d \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ ist. Wir führen den Beweis per Induktion über n.
Der Fall $n = 1$ ist trivial. Sei also $n = 2$ und $\nu \in V$. Wir betrachten $(x_\nu, -d)_\nu = \epsilon_\nu$. Wir zeigen, dass ein $x_\nu \in \mathbb{Q}_\nu^*$ für alle $\nu \in V$ existiert, sodass dieser Ausdruck gilt. Dann nämlich können wir Hilfsmittel 4 anwenden und ein $x \in \mathbb{Q}^*$ mit $(x, -d)_\nu = \epsilon_\nu$ finden. Im Fall $\epsilon_\nu = 1$ wählen wir $x_\nu = d$. Damit folgt mit der Definition der Diskriminante $d = x_\nu \cdot (-d) = -x_\nu \cdot d = -d^2 = -1$. Für $\epsilon_\nu = -1$ wählen wir $x_\nu = -d$, da dann $d = x_\nu \cdot (-d) = -x_\nu \cdot d = +d^2 = 1$ gilt. Aus Hilfsmittel 4 folgt die Existenz eines $x \in \mathbb{Q}^*$, sodass $\epsilon_\nu = (x, -d)_\nu$ für alle $\nu \in V$ gilt. Die quadratische Form $xX^2 + xdY^2$ besitzt die vorgegebenen Invarianten, die der Bemerkung genügen:

$$\begin{aligned} d &= x \cdot xd = x^2 d = d \\ \epsilon_\nu &= (x, xd)_\nu = (x, x)_\nu \cdot (x, d)_\nu = (-1, x)_\nu \cdot (x, d)_\nu = (x, -d)_\nu \end{aligned}$$

Sei $n = 3$ und sei $S := \{\nu \in V \quad | \quad (-d, -1)_\nu = -\epsilon_\nu\}$ eine Menge. S ist endlich. Für ein $\nu \in S$ wählen wir uns ein Element $c_\nu \in \mathbb{Q}_\nu^*/\mathbb{Q}_\nu^{*2}$, welches sich von dem Bild d_ν der Diskriminante d in dieser Untergruppe unterscheidet.

Hilfsmittel 5 (Approximationstheorem)**.** *Sei S eine endliche Teilmenge von V. Das Bild von $\mathbb{Q}$ in $\prod_{\nu \in V} \mathbb{Q}_\nu$ liegt dicht in diesem Produkt.*

Das Approximationstheorem liefert die Existenz eines $c \in \mathbb{Q}^*$ dessen Bild in allen Quotientengruppen $\mathbb{Q}_\nu^*/\mathbb{Q}_\nu^{*2}$ c_ν ist. Aus dem im Induktionsschritt für $n = 2$ bewiesenen folgt die Existenz einer quadratischen Form g vom Rang 2 mit

$$d_g = cd, \quad e_{\nu,g} = (c, -d)_\nu \epsilon_\nu \quad \forall \nu \in V$$

als Invarianten. Die Form $f = cZ^2 + g$ besitzt nun die geforderten Invarianten:

$$\begin{aligned} d &= d_g \cdot c = c \cdot d \cdot c = c^2 \cdot d = d \\ \epsilon_\nu &= \epsilon_{\nu,g} \cdot (c, cd)_\nu = \epsilon_\nu \cdot (c, -d)_\nu \cdot (c, cd)_\nu = \epsilon_\nu \cdot (c, -cd^2)_\nu = \epsilon_\nu \cdot (c, -c)_\nu = \epsilon_\nu \end{aligned}$$

Bis zu $n \leq 3$ mussten wir Signatur der Form nicht gesondert beachten, da diese bereits durch die letzten drei Bedingungen in der Bemerkung eindeutig festgelegt ist.

Beispiel. *Im Fall $n = 2$ geben wir uns $d = 1$ und $\epsilon_\nu = -1$ vor. Aus der ersten Vorgabe folgt $s = 0, 2$, aus der zweiten $s = 2$. Somit ist die Signatur der Form $(0, 2)$.*

Falls $n \geq 4$ ist, führen wir die Induktion über n aus. Als erstes betrachten wir den Fall $r \geq 1$. Die Induktionsannahme liefert eine quadratische Form g vom Rang $n-1$, die d, $(\epsilon_\nu)_{\nu \in V}$ und die Signatur $(r-1, s)$ als Invarianten besitzt. Die Form $X^2 + g$ besitzt dann die geforderten Invarianten. Sein nun $r = 0$. Nach Induktionsannahme existiert wieder eine Form h vom Rang $n-1$ mit den Invarianten $-d$, $\epsilon_\nu(-1, -d)_\nu$ und der Signatur $(0, n-1)$. Die Form $-X^2 + h$ besitzt die geforderten Invarianten:

$$\begin{aligned} d &= d_h \cdot (-1) = d \\ \epsilon_\nu &= \epsilon_\nu \cdot (-1, -d)_\nu \cdot (-1, -d)_\nu = \epsilon_\nu \end{aligned}$$

□

2 Quadratsätze

In diesem Abschnitt können wir mit Hilfe quadratischer Formen Quadratsätze sehr elegant beweisen, die ohne diese Kenntnisse umständlich und lang zu beweisen wären.

Definition (Summe von p Quadraten)**.** *Seien $n, p \in \mathbb{N}$. Man sagt n* ist die Summe von p Quadraten*, wenn n über $\mathbb{Z}$ durch die quadratische Form $X_1^2 + X_2^2 + \cdots + X_p^2$ repräsentiert wird, d. h. es gibt ganze Zahlen $n_1, n_2, \ldots, n_p$ mit*

$$n = n_1^2 + n_2^2 + \cdots + n_p^2.$$

Theorem 10 (Gauß)**.** *Eine natürliche Zahl a ist Summe von drei Quadraten genau dann, wenn sie nicht von der Form $4^n(8m-1)$ mit $n, m \in \mathbb{N}_0$ ist.*

Beispiel. *Falls a nicht durch 4 teilbar ist, ist a genau dann Summe von drei Quadraten, wenn $a \equiv 1, 2, 3, 5, 6$ mod 8.*

Zum Beweis dieses Theorems benötigen wir zwei Lemmata.

Lemma 1. *Sei $a \in \mathbb{Q}^*$. Es wird a in $\mathbb{Q}$ genau dann durch die Form $f = X_1^2 + X_2^2 + X_3^2$ repräsentiert, wenn $a > 0$ und $-a$ kein Quadrat in $\mathbb{Q}_2$ ist.*

Beweis. Zum Beweis benötigen wir

Hilfsmittel 6. *Sei $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ und f eine quadratische Form vom Rang 3 über $\mathbb{Q}_p$. Dann repräsentiert f a genau dann, wenn entweder $a \neq -d_p$ oder $[a = -d_p$ und $(-1, -d_p)_p = \epsilon_p]$.*

Gemäß Hilfsmittel 1 müssen wir zeigen, dass a durch f in allen $\mathbb{Q}_\nu$ repräsentiert wird. Im reellen Fall sieht man sofort, dass $a > 0$ gelten muss. Es bleibt der p-adische Fall zu zeigen. Die lokalen Invarianten $d_p(f)$ und $\epsilon_p(f)$ sind 1. Für $p \neq 2$ gilt:

$$(-1, -d_p(f))_p = (-1, -1)_p = 1 = \epsilon_p(f)$$

Aus Hilfsmittel 6 folgt, dass a durch f in $\mathbb{Q}_p$ für $p \neq 2$ repräsentiert wird. Sei schließlich $p = 2$. Es folgt:

$$(-1, -d_2(f))_2 = -1 \neq \epsilon_2(f)$$

Aus Hilfsmittel 6 folgt, dass a genau dann durch f in $\mathbb{Q}_2$ repräsentiert wird, wenn $a \neq -d_2 = -1$ in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ gilt. D. h. $-a$ ist kein Quadrat in $\mathbb{Q}_2$. □

Lemma 2 (Davenport-Cassels)**.** *Sei $f(X) = \sum_{i,j=1}^p a_{ij} X_i X_j$ eine positiv definite quadratische Form. Die zugehörige Matrix $(a_{ij}) \in \mathbb{Z}^{p \times p}$ sei symmetrisch. Wir machen folgende Annahme:*

$$\textit{Zu jedem } x \in \mathbb{Q}^p \textit{ existiert ein } y \in \mathbb{Z}^p, \textit{ sodass } f(x - y) < 1.$$

Wird $n \in \mathbb{Z}$ durch f in $\mathbb{Q}$ repräsentiert, so wird n durch f in $\mathbb{Z}$ repräsentiert.

Beweis. Wenn $x = (x_1, \ldots, x_p)$ und $y = (y_1, \ldots, y_p)$ zwei Elemente in $\mathbb{Q}^p$ sind, bezeichnen wir deren Skalarprodukt durch $x.y$ mit $x.y = \sum a_{ij} x_i y_j$. Es gilt: $x.x = f(x)$. Sei $n \in \mathbb{Z}$ durch f in $\mathbb{Q}$ repräsentiert. Dann existiert ein $t \in \mathbb{N}$, sodass $t^2 n = x.x$ mit $x \in \mathbb{Z}^p$. Wir wählen t und x derart, dass t minimal ist (t wurde als Hauptnenner der Komponenten des Vektors x gewählt). Zu zeigen bleibt $t = 1$, da dann aus $t^2 n = x.x \Rightarrow x \in \mathbb{Z}^p$. Somit wird n bereits durch f in $\mathbb{Z}$ repräsentiert.
Nach unserer Annahme existiert ein $y \in \mathbb{Z}^p$, sodass

$$\frac{x}{t} = y + z \quad \text{mit } z.z < 1,$$

denn wir können ein z derart wählen, dass $z = \frac{x}{t} - y, \quad f(z) = z.z < 1$. Für $z.z = 0$ folgt $z = 0$, deswegen besitzt der Vektor $\frac{x}{t}$ nur ganze Komponenten. Die Minimalität von t impliziert $t = 1$.
Sei also $z.z \neq 0$ und sei

$$\begin{aligned} a &= y.y - n \\ b &= 2(nt - x.y) \\ t' &= at + b \\ x' &= ax + by \end{aligned}$$

mit $a, b, t' \in \mathbb{Z}$. Betrachte

$$\begin{aligned} x'.x' &= a^2 x.x + 2abx.y + b^2 y.y \\ &= a^2 t^2 n + ab(2nt - b) + b^2(n + a) \\ &= n(a^2 t^2 + 2abt + b^2) \\ &= t'^2 n. \end{aligned}$$

Weiterhin gilt

$$\begin{aligned} tt' = at^2 + bt &= t^2 y.y - nt^2 + 2nt^2 - 2tx.y \\ &= t^2 y.y - 2tx.y + x.x = (ty - x).(ty - x) \\ &= t^2 z.z, \end{aligned}$$

also $t' = tz.z$. Da jedoch $0 < z.z < 1$, gilt $0 < t' < t$, was einen Widerspruch zur Minimalität von t darstellt. □

Beweis von Theorem 10. Wir benötigen

Hilfsmittel 7. *Ein Element $x = p^n u \in \mathbb{Q}_2^*$ ist genau dann ein Quadrat, wenn n gerade und $u \equiv 1 \mod 8$ ist.*

Nach Hiflsmittel 7 ist die Aussage „a ist von der Form $4^n(8m - 1)$“ äquivalent zu der Aussage „$-a$ ist ein Quadrat in $\mathbb{Q}_2^*$“, denn $-a = \underbrace{4^n}_{2^{2n}} \underbrace{(-8m + 1)}_{u} \quad \Rightarrow u \equiv 1 \mod 8$, also ist $-a$ ein Quadrat in $\mathbb{Q}_2^*$.
Wir müssen nun zeigen, dass a genau dann als Summe von drei Quadraten darstellbar ist, wenn $-a$ kein Quadrat in $\mathbb{Q}_2$ ist. Für rationale Quadrate ist dies genau die Aussage von Lemma 1. Da $a \in \mathbb{N}$ und zusätzlich die Annahme erfüllt ist, folgt aus Lemma 2 sofort, dass diese Quadrate ganz sein müssen. Wir überprüfen die Annahme: Zu jedem $x \in \mathbb{Q}^3$ existiert ein $y \in \mathbb{Z}^3$, sodass $|x_i - y_i| \leq \frac{1}{2}$ für $i = 1, 2, 3$. Also gilt $\sum (x_i - y_i)^2 \leq \frac{3}{4} < 1$. □

Korollar (Lagrange)**.** *Jede natürliche Zahl ist Summe von vier Quadraten.*

Beweis. Sie $n \in \mathbb{N}$. In diesem Beweis nutzen wir das Theorem 10 aus. Deshalb schreiben wir n in der Form $4^a m$, wobei $a \in \mathbb{N}_0, m \in \mathbb{N}$, m aber nicht durch 4 teilbar ist. Wenn $m \equiv 1, 2, 3, 5, 6 \mod 8$ ist, ist m Summe von drei Quadraten nach Gauß. Dann ist auch n Summe von drei Quadraten.
Wenn $m \equiv -1 \mod 8$ ist, ist $m - 1$ Summe von drei Quadraten (denn $m - 1 \equiv -2 \equiv 6 \mod 8$). In diesem Fall ist m Summe von vier Quadraten und folglich ist auch n Summe von vier Quadraten. □

Definition (Dreieckszahl)**.** *Man nennt eine natürliche Zahl n Dreieckszahl, wenn sie von der Form $n = \frac{m(m+1)}{2}$ mit $m \in \mathbb{Z}$.*

Korollar (Gauß)**.** *Jede natürliche Zahl ist Summe dreier Dreieckszahlen.*

Beweis. Sei $n \in \mathbb{N}$. Nach dem Theorem 10 gibt es ganze Zahlen x_1, x_2, x_3 mit

$$x_1^2 + x_2^2 + x_3^2 = 8n + 3$$

Es gilt

$$x_1^2 + x_2^2 + x_3^2 \equiv 3 \bmod 8.$$

Die einzigen Quadrate in $\mathbb{Z}/8\mathbb{Z}$ sind $0, 1, 4$. Die Summe von drei Quadraten in $\mathbb{Z}/8\mathbb{Z}$ kann lediglich 3 sein, wenn jeder der Terme kongruent 1 ist. Folglich sind die x_i mit $i = 1, 2, 3$ ungerade und man kann sie in der Form $2m_i + 1$ mit $m_i \in \mathbb{Z}$ schreiben. Wir erhalten also für die Summe von drei Dreieckszahlen

$$\sum_{i=1}^{3} \frac{m_i(m_i+1)}{2} = \frac{1}{8}\sum_{i=1}^{3} 4m_i(m_i+1) = \frac{1}{8}\sum_{i=1}^{3}((2m_i+1)^2 - 3) = \frac{1}{8}\sum_{i=1}^{3}(x_i^2 - 3) = \frac{1}{8}(8n + 3 - 3) = n$$

Also ist n Summe dreier Dreieckszahlen. □