Ruprecht-Karls-Universität Heidelberg
Institut für Mathematik
Sommersemester 2007
Seminar: Quadratische Formen über den rationalen Zahlen
Dozent: Prof. Dr. Kay Wingberg

9. Vortrag. Quadratische Formen über $\mathbb{Q}$[1]

Wir verwenden die Notationen der vergangenen beiden Vorträge und machen folgende Generalvoraussetzungen:

- alle quadratischen Formen haben Koeffizienten aus $\mathbb{Q}$ und seien nicht ausgeartet
- $V = \mathbb{P} \cup \{\infty\}$, $\mathbb{Q}_\infty = \mathbb{R}$

1. Invarianten

Sei $f \sim a_1X_1^2 + \ldots + a_nX_n^2$ eine quadratische Form vom Rang n. Dann gibt es drei wichtige Invarianten:

1. Die Diskriminante $d(f) \in \mathbb{Q}^*/\mathbb{Q}^{*^2}$ mit $d(f) = \prod_{i=1}^{n} a_i$. Sei $\nu \in V$. Vermöge $\mathbb{Q} \hookrightarrow \mathbb{Q}_\nu$ lässt sich f als quadratische Form f_ν über $\mathbb{Q}_\nu$ interpretieren. $d_\nu(f)$ ist das Bild von $d(f)$ unter $\mathbb{Q}^*/\mathbb{Q}^{*^2} \to \mathbb{Q}_\nu^*/\mathbb{Q}_\nu^{*^2}$.
2. $\varepsilon_\nu(f) = \prod_{i<j} (a_i, a_j)_\nu$. Nach dem Theorem von Hilbert[2] gilt $\prod_{\nu \in V} \varepsilon_\nu(f) = 1$.
3. Die (Sylvester-)Signatur (r, s) der reellen quadratischen Form f (bekannt aus der Linearen Algebra) gibt die Anzahl der positiven und negativen Eigenwerte der der quadratischen Form f zugehörigen Matrix A an.

Die Invarianten $d_\nu(f), \varepsilon_\nu(f)$ und (r, s) heißen **lokale Invarianten** von f.

2. Das Theorem von Hasse-Minkowski

Von nun an soll die Aussage, dass eine quadratische Form f_K über einem Körper K 0 repräsentiert bedeuten, dass es ein $x \in K - \{0\}$ gibt mit $f(x) = 0$. Im Zentrum des Vortrags steht folgendes Theorem.

Satz 1 (Theorem von Hasse-Minkowski)

$$f \text{ repräsentiert } 0 \Leftrightarrow \bigwedge_{\nu \in V} f_\nu \text{ repräsentiert } 0.$$

Beweis:

$\Rightarrow$ Trivial.

$\Leftarrow$ Zunächst schreibe man f in der Form $f = a_1X_1^2 + \ldots + a_nX_n^2$, $a_i \in \mathbb{Q}^*$. Ohne Einschränkung kann $a_1 = 1$ angenommen werden. Sonst ersetzt man f durch $a_1 f$. Der Beweis wird durch eine Fallunterscheidung geführt.

1. Fall: $n = 2$**.**

$$f = X_1^2 - aX_2^2 \overset{f_\infty \text{ repr. } 0}{\Longrightarrow} a > 0$$

[1] nach Jean-Pierre Serre: A Course in Arithmetic, GTM 7, pp. 41-44
[2] Chap. III Theorem 3

Primzerlegung von a: $a = \prod_{p\in\mathbb{P}} p^{\nu_p(a)} \overset{f_p \text{ repr. } 0}{\Longrightarrow} a$ ist Quadrat in $\mathbb{Q}_p$. $\bigwedge_{p\in\mathbb{P}} 2|\nu_p(a) \Rightarrow a$ ist Quadrat in $\mathbb{Q} \Rightarrow f$ repräsentiert 0 via $(\sqrt{a}, 1)$.

2. Fall: $n = 3$. (Legendre)

$$f = X_1^2 - aX_2^2 - bX_3^2.$$

OE kann man a, b als quadratfreie ganze Zahlen annehmen (sonst: Multiplikation der Koeffizienten mit geeigneten Quadratzahlen), i.e. $\bigwedge_{p\in\mathbb{P}} \nu_p(a), \nu_p(b) \in \{0, 1\}$. *OE* $|a| \leq |b|$. Der Beweis wird nun durch Induktion nach $m = |a| + |b|$ geführt.

Induktionsanfang. $m = 2$.
$f = X_1^2 \pm X_2^2 \pm X_3^2 \overset{f_\infty \text{ repr. } 0}{\Longrightarrow} f \neq X_1^2 + X_2^2 + X_3^2$. Also *o.B.d.A.* $f = X_1^2 - X_2^2 \pm X_3^2$ mit Lösung $(a, a, 0)$ $(a \in \mathbb{Q}^*)$.

Induktionsschritt. $m - 1 \Rightarrow m$.
$m > 2$, $|b| \geq 2$. b besitzt eindeutige Primzerlegung $b = \pm \prod_{i=1}^{k} p_i$ $(p_i \neq p_j)$ falls $i \neq j$ (b war quadratfrei gewählt).

Sei nun $p \in \{p_i,\ i = 1, \ldots, k\}$.

Behauptung: a ist Quadrat modulo p.

Der Fall $a \equiv 0\ mod\ p$ ist trivial. Also $a \neq\ 0\ mod\ p\ \Rightarrow\ a\ mod\ p \in (\mathbb{Z}/p\mathbb{Z})^*$.

Voraussetzung $\bigvee_{(x,y,z)\in\mathbb{Q}_p^3} z^2 - ax^2 - by^2 = 0,\ oE(x, y, z)$ primitiv [3].

$p|b \Rightarrow z^2 - ax^2 \equiv\ 0\ mod\ p$. Annahme: $x \equiv 0\ mod\ p \Rightarrow z \equiv 0\ mod\ p \Rightarrow by^2 \equiv 0\ mod\ p^2\ \Rightarrow y \equiv 0\ mod\ p$. Widerspruch, denn (x, y, z) war nach Voraussetzung primitiv. Also $x \neq 0\ mod\ p \overset{x\in(\mathbb{Z}/p\mathbb{Z})^*}{\Longrightarrow} a$ Quadrat modulo p.

Chinesischer Restsatz: $\mathbb{Z}/b\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/p_i\mathbb{Z} \Rightarrow\ a$ ist Quadrat $mod\ b$.

$\Rightarrow \bigvee_{t,\acute{b}\in\mathbb{Z}} t^2 = a + b\acute{b}$ mit $|t| \leq \frac{|b|}{2}$. Also $b\acute{b} = t^2 - a$. Letzteres ist jedoch eine Norm in der Körpererweiterung $k(\sqrt{a})/k$ für $k = \mathbb{Q}$ bzw. $k = \mathbb{Q}_\nu$. Denn: $\mathcal{N}_{k(\sqrt{a})/k}(t+\sqrt{a}) = t^2 - a$ (allgemein: $\mathcal{N}_{k(\sqrt{a})/k}(\alpha+\beta\sqrt{a}) = \alpha^2 - a\beta^2$).

Mit Prop. 1 aus Chapter III folgt nun: f repräsentiert $0 \Leftrightarrow \acute{f} = X_1^2 - aX_2^2 - \acute{b}X_3^2$ repräsentiert 0.[4]

$\bigwedge_{\nu\in V} \acute{f}_\nu\ repr.\ 0$. Weiterhin gilt:

$$\left|\acute{b}\right| = \left|\frac{t^2 - a}{b}\right| \leq \frac{|b|}{4} + 1 < |b| \qquad (|b| \geq 2).$$

Setze $\acute{b} = \tilde{b} \cdot u$ mit $\tilde{b}$ quadratfrei und wende die Induktionsannahme auf die quadratische Form $\tilde{f} = X_1^2 - aX_2^2 - \tilde{b}X_3^2$ an, welche zu $\acute{f}$ äquivalent ist.

3. Fall. $n = 4$. $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$.

[3] vgl. Chap. II Prop. 6

[4] Chap. III Prop. 1 wurde dort nur für die Körper $\mathbb{R}$ bzw. $\mathbb{Q}_p$ gezeigt, gilt aber auch in $\mathbb{Q}$. Am Beweis ändert sich nichts. Nutze dann aus, dass $(a, b\acute{b}) = (a, b) \cdot (a, \acute{b})$

f_ν repräsentiert $0 \Longrightarrow$ [5] $\bigvee_{x_\nu \in \mathbb{Q}_\nu^*} x_\nu$ wird von $aX_1^2 + bX_2^2$ und von $cX_3^2 + dX_4^2$. Nach dem Korollar 2 zu Theorem 6 in Chap. IV ist dies gleichbedeutend mit

$$\bigwedge_{\nu \in V} (x_\nu, -ab)_\nu = (a,b)_\nu \; und \; (x_\nu, -cd)_\nu = (c,d)_\nu$$

.

Hilberts Theorem: $\prod_{\nu \in V} (a,b)_\nu = \prod_{\nu \in V} (c,d)_\nu = 1 \implies$ [6] $\bigvee_{x \in \mathbb{Q}^*} \bigwedge_{\nu \in V} (x, -ab)_\nu = (a,b)_\nu \; \wedge \; (x, -cd)_\nu = (c,d)_\nu$.

$aX_1^2 + bX_2^2 - xZ^2$ repräsentiert 0 für jedes $\mathbb{Q}_\nu$ und nach dem Fall $n = 3$ somit auch in $\mathbb{Q}$. Also wird x durch $aX_1^2 + bX_2^2$ repräsentiert. Wende das analoge Argument auf $cX_3^2 + dX_4^2$ an $\Rightarrow$ Behauptung.

4. Fall. $n \geq 5$**.**
Wiederum erfolgt der Beweis durch Induktion. Den Induktionsanfang haben wir bereits durch die obigen Untersuchungen. $f = h - g$ mit $h = a_1X_1^2 + a_2X_2^2$ und $g = -(a_3X_3^2 + \ldots + a_nX_n^2)$.

$$S := \{2, \infty\} \cup \left\{ p \in \mathbb{P} \mid \bigvee_{i \geq 3} \nu_p(a_i) \neq 0 \right\}$$

ist eine endliche Menge.

$\nu \in S$. f_ν repräsentiert $0 \Rightarrow \bigvee_{a_\nu \in \mathbb{Q}_\nu^*} a_\nu$ wird von h und g dargestellt, i.e. $\bigvee_{x_i^\nu \in \mathbb{Q}_\nu} h(x_1^\nu, x_2^\nu) = a_\nu = g(x_3^\nu, \ldots, x_n^\nu)$.

$(\mathbb{Q}_\nu^*)^2 \subset \mathbb{Q}_\nu^*$ offen nach Chap. II.

Approximationssatz: [7] $\Rightarrow \bigvee_{x_1, x_2 \in \mathbb{Q}} a = h(x_1, x_2)$ mit $\bigwedge_{\nu \in S} \frac{a}{a_\nu} \in \mathbb{Q}_\nu^{*^2}$.

Wir betrachten nun die Form $f_1 = aZ^2 - g$.

- $\nu \in S \Rightarrow$ g repräsentiert a_ν in $\mathbb{Q}_\nu \Rightarrow$ g repräsentiert a in $\mathbb{Q}_\nu$ wegen $\frac{a}{a_\nu} \in \mathbb{Q}_\nu^{*^2} \Rightarrow$ f_1 stellt 0 in $\mathbb{Q}_\nu$ dar.
- $\nu \notin S \Rightarrow$ $-a_3, \ldots, -a_n$ sind ν-adische Einheiten $\Rightarrow$ $d_\nu(g)$ ist ν-adische Einheit. $\nu \neq 2 \Rightarrow$ $\varepsilon_\nu(g) = 1$ nach Theorem I aus Kapitel III.

f_1 stellt 0 dar in $\mathbb{Q}_\nu \Rightarrow$ f_1 stellt 0 in $\mathbb{Q}$ dar $\Rightarrow$ g stellt a in $\mathbb{Q}$ dar. h stellt a dar $\Rightarrow$ f stellt 0 dar.

□

Anmerkung 1 *Das Theorem behält seine Gültigkeit in jedem Zahlkörper K, wobei die Beweisstruktur im wesentlichen gleich bleibt. Allerdings baut unser Seminar auf einem relativ elementaren Beweis des quadratischen Reziprozitätsgesetzes auf. Im allgemeinen Fall braucht man jedoch einen Spezialfall der Artin Reziprozität, welche man z. B. in einer Vorlesung über Klassenkörpertheorie kennenlernt.*[8]

3. Korollare und Bemerkungen

Korollar 1 *Sei $a \in \mathbb{Q}^*$. f stellt a in $\mathbb{Q}$ dar $\Leftrightarrow \bigwedge_{\nu \in V} f$ stellt a in $\mathbb{Q}_\nu$ dar.*

Beweis: Wende das Theorem von Hasse-Minkowski auf die quadratische Form $aZ^2 - f$ an. □

[5] Prop. 3', Kor. 2
[6] Chap. III Theorem 4
[7] $\mathbb{Q} \hookrightarrow \prod_{\nu \in S} \mathbb{Q}_\nu$ liegt dicht für endliche $S \subset V$
[8] Diese Anmerkung habe ich entnommen aus dem englischsprachigen Skript Algebraic Number Theory von James Milne, im Netz unter http://www.jmilne.org/math/CourseNotes/math631a.pdf

Korollar 2 (Meyer) *Eine quadratische Form vom Rang ≥ 5 stellt 0 dar genau dann, wenn sie indefinit ist.*

Beweis: Sofort aus Theorem 6. □

Korollar 3 *Sei n der Rang von f. Annahme: $n = 3$ (bzw. $n = 4$ und $d(f) = 1$). Wenn f die 0 in allen $\mathbb{Q}_\nu$ bis auf höchstens eines darstellt, dann stellt f 0 dar.*

Beweis:

- $n = 3$. Theorem 6 $\Rightarrow$ f repräsentiert 0 in $\mathbb{Q}_\nu$ dann und nur dann, wenn

  $$(-1, -d(f))_\nu = \varepsilon_\nu(f).$$

  Augrund der Produktformel müssen linke und rechte Seite schon dann für alle ν übereinstimmen, wenn sie für alle ν bis auf eines übereinstimmen. Dann repr. f aber 0 nach dem Satz von Hasse-Minkowski.

- $n = 4$ analog für die Gleichung $(-1, -1)_\nu = \varepsilon_\nu(f)$.

□

Anmerkung 2 *Man kann die Bedingungen im Theorem für den Fall $n = 2$ weiter abschwächen, eine Verallgemeinerung auf homogene Polynome höheren Grades ist allerdings nicht möglich. Genauer gilt:*

- *Es reicht im Fall $n = 2$ bereits aus vorauszusetzen, dass f die 0 für alle $\nu \in V$ bis auf endlich viele Ausnahmen darstellt.*
- *Das Theorem von Hasse-Minkowski lässt sich nicht auf homogene Polynome mit Grad > 2 ausweiten. Selmer hat gezeigt, dass die Gleichung $3X^3 + 4Y^3 + 5Z^3$ eine von $(0, 0, 0)$ verschiedene Lösung in jedem $\mathbb{Q}_\nu$ hat, aber nicht in $\mathbb{Q}$.*

***

Heidelberg, Juni 2007
Martin Kroll
martin.kroll@urz.uni-heidelberg.de

Literaturverzeichnis

[1] Jean-Pierre Serre: *A Course in Arithmetic,* GTM 7, New York, Springer-Verlag (1973)

[2] James Milne: *Algebraic Number Theory,* http://www.jmilne.org/math/CourseNotes/math631a.pdf