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

Quadratische Formen

Manuela Ernst
ernst-manuela@web.de

Margrit Kasper
margritkasper@web.de

14. Juni 2007

Inhaltsverzeichnis

Quadratische Formen

1 Definitionen

Definition 1.1 (Quadratische From)**.** *Sei V ein Modul über einem kommutativen Ring A. Eine Funktion $Q : V \longrightarrow A$ heißt Quadratische Form auf V, wenn*

1. $Q(ax) = a^2Q(x), a \in A, x \in V$
2. $(x, y) \longmapsto Q(x + y) - Q(x) - Q(y)$ *eine Bilinearform ist.*

Definition 1.2 (Quadratischer Modul)**.** *Das Paar (V, Q) heißt Quadratischer Modul.*

Im Folgenden betrachten wir den Fall, in dem A ein Körper K mit $char(K) \neq 2$ ist und der A-Modul V ein endlichdimensionaler K-Vektorraum ist.

Definition 1.3 (Skalarprodukt)**.** *Wir setzen:*

$$x.y = \tfrac{1}{2}(Q(x + y) - Q(x) - Q(y))$$

Die Abbildung $(x, y) \longmapsto x.y$ ist eine symmetrische Bilinearform auf V und heißt Skalarprodukt bzgl. Q.

Bemerkung 1.4. *Das Skalarprodukt bzgl. Q ist nicht positiv definit.*

Es gilt $Q(x) = x.x$. Damit haben wir eine bijektive Beziehung zwischen Quadratischen Formen und symmetrischen Bilinearformen.

Definition 1.5 (metrischer Morphismus)**.** *Wenn (V, Q) und (V', Q') Quadratische Moduln sind und $f : V \longrightarrow V'$ eine lineare Abbildung mit $Q' \circ f = Q$, die metrischer Morphismus genannt wird, dann ist $f(x).f(y) = x.y$ für alle $x, y \in V$.*

Die Matrix von Q bzgl. einer Basis $(e_i)_{1 \leq i \leq n}$ von V ist die symmetrische Matrix $A = (a_{ij})$, wobei $a_{ij} = e_i.e_j$. Für $x = \sum x_i e_i$ aus V ist $Q(x) = \sum_{i,j} a_{ij} x_i x_j$, dies ist eine Quadratische Form in $x_1, \ldots, x_n$ im gewöhnlichen Sinn.

Wenn man einen Basiswechsel mit einer invertierbaren Matrix X durchführt, erhält man aus der Matrix A eine neue Matrix der Quadratischen Form $A' = XAX^T$.

Bemerkung 1.6. *Insbesondere gilt:*

$$\det(A) = \det(A) \cdot \det(X)^2$$

Beweis. $\det(A') = \det(XAX^T) = \det(X) \cdot \det(A) \cdot \det(X^T) = \det(A) \cdot \det(X)^2$ □

Definition 1.7 (Diskriminante)**.** *Man nennt* $\det(A)$ *Diskriminante von* Q *und bezeichnet sie mit* $\operatorname{disc}(Q)$.

Bemerkung 1.8. *Die Diskriminante ist bis auf Multiplikation mit einem Element aus* K^{*2} *eindeutig bestimmt.*

2 Orthogonalität

Sei (V, Q) ein Quadratischer Modul über K.

Definition 2.1 (ortholgonal)**.** *Zwei Elemente* $x, y \in V$ *heißen orthogonal, wenn* $x.y = 0$.

Definition 2.2 (orthogonales Komplement)**.** *Sei* $H \leq V$ *ein Untervektorraum. Die Menge aller Elemente, die orthogonal zu* H *sind, ist das orthogonale Komplement von* H*. Es wird mit* H^0 *bezeichnet.*

$$H^0 = \{v \in V \mid v.h = 0, \forall h \in H\}$$

Definition 2.3 (ortholgonal)**.** *Zwei Untervektorräume* $V_1, V_2 \leq V$ *heißen orthogonal, wenn* $V_1 \subset V_2^0$.

Insbesondere gilt für $x \in V_1$ und $y \in V_2$ ist $x.y = 0$.

Definition 2.4 (Radikal)**.** *Das orthogonale Komplement* V^0 *von* V *heißt Radikal und wird mit* $\operatorname{rad}(V)$ *bezeichnet.*

$$\operatorname{rad}(V) = \{v \in V \mid v.w = 0, \forall w \in V\}$$

Definition 2.5 (Rang)**.** *Die Kodimension des Radikals heißt Rang von* Q.

Bemerkung 2.6. $\operatorname{codim}(V^0) = \dim(V) - \dim(V^0)$

Definition 2.7 (nichtausgeartet)**.** Q *ist nichtausgeartet, wenn* $V^0 = 0$.

Bemerkung 2.8. *Das* Q *nichtausgeartet ist, ist äquivalent dazu dass* $\operatorname{disc}(Q) \neq 0$.

Beweis. Sei A die Matrix der Quadratischen Form Q.

$$\begin{aligned}
&K^*/K^{*2} \ni \operatorname{disc}(Q) = \det(Q) \neq 0 \\
&\Leftrightarrow \det(A) \text{ ist invertierbar, d. h. } A \text{ ist injektiv} \\
&\Leftrightarrow \nexists v \neq 0 : Av = 0 \\
&\Leftrightarrow \nexists v \neq 0 : w^T Av = 0, (\forall w \in V; w \neq 0) \\
&\Leftrightarrow \nexists v \neq 0 : v \in V^0 \\
&\Leftrightarrow V^0 = 0 \\
&\Leftrightarrow Q \text{ ist nichtausgeartet.}
\end{aligned}$$

□

Sei $U \leq V$ ein Untervektorraum und U^* der Dualraum zu U. Die Abbildung q_U ordnet jedem $x \in V$ eine Linearform zu:

$$q_U : V \longrightarrow U^*$$
$$q_U : x \longmapsto f, \text{ mit } f : y \longmapsto y.x \, (y \in U)$$

Bemerkung 2.9. *Der Kern von q_U ist U^0.*

Beweis.

$$\begin{aligned} V \supseteq \text{Kern}(q_U) &= \{v \in V \mid q_U(v) = 0\} \\ &= \{v \in V \mid f(v) = 0\} \\ &= \{v \in V \mid u.v = 0, \forall u \in U\} \\ &= \{v \in V \mid v \perp u\} \\ &= U^0 \end{aligned}$$

□

Bemerkung 2.10. *Q ist genau dann nichtausgeartet, wenn $q_V : V \longrightarrow V^*$ ein Isomorphismus ist.*

Beweis.

„ $\Leftarrow$ “:

q_V ist Isomorphismus, d. h. insbesondere auch injektiv $\Rightarrow$ $\text{Kern}(q_V) = 0$

nach der vorherigen Bemerkung ist $\text{Kern}(q_V) = V^0 \Rightarrow V^0 = 0 \Rightarrow Q$ ist nichtausgeartet

„ $\Rightarrow$ “:

$V^0 = 0 \Rightarrow \text{disc}(Q) \neq 0 \Rightarrow \det(A) \neq 0 \Rightarrow A$ ist invertierbar, also auch injektiv

$\Rightarrow$ q_V injektiv $\Rightarrow$ Bijektivität, da $\dim(V) = \dim(V^*)$

□

Definition 2.11 (orthogonale direkte Summe)**.** *Seien $U_1, \ldots, U_m \leq V$ Unterräume von V. Man bezeichnet V als die orthogonale direkte Summe von U_i, wenn diese paarweise orthogonal zueinander sind und V ihre direkte Summe ist.*
Schreibweise: $V = U_1 \hat{\bigoplus} \cdots \hat{\bigoplus} U_m$

Bemerkung 2.12. *Wenn $x \in V$ Komponenten $x_i \in U_i$ hat, gilt*

$$Q(x) = Q_1(x_1) + \cdots + Q_m(x_m)$$

wobei $Q_i = Q \mid_{U_i}$ die Einschränkung von Q auf U_i ist. Die gemischten Terme sind aufgrund der Orthogonalität gleich Null und fallen somit raus.
Umgekehrt ergibt sich aus obiger Formel für eine Familie (U_i, Q_i) von Qudratischen Moduln $V = \bigoplus U_i$ mit einer Quadratischen Form, die als direkte Summe aus Q_i bezeichnet wird, und es gilt $V = U_1 \hat{\bigoplus} \cdots \hat{\bigoplus} U_m$.

Proposition 2.13. *Wenn $U \subseteq V$ ein ergänzender Unterraum zu $\text{rad}(V)$ ist, dann ist $V = U \hat{\bigoplus} \text{rad}(V)$.*

Beweis. Die Summe ist direkt, da die Unterräume sich gegenseitig ergänzen, und sie ist orthogonal, da alle Elemente aus $\mathrm{rad}(V)$ orthogonal zu allen Elementen aus V sind, also insbesondere auch zu denen aus U. □

Proposition 2.14. *Sei (V, Q) nichtausgeartet. Dann:*

(i) sind alle metrischen Morphismen von V in einen Quadratischen Modul (V', Q') injektiv.

(ii) Für alle Untervektorräume U von V gilt:

(a) $\dim(U) + \dim(U^0) = \dim(V)$

(b) $U^{00} = U$

(c) $\mathrm{rad}(U) = \mathrm{rad}(U^0) = U \cap U^0$

(d) Der Quadratische Modul U ist nichtausgeartet, genau dann wenn U^0 nichtausgeartet ist. In diesem Fall ist $V = U \hat{\bigoplus} U^0$.

(iii) Wenn V die orthogonale direkte Summe von zwei Unterräumen ist, dann sind diese nichtausgeartet und orthogonal zueinander.

Beweis. (i) Sei $f : V \longrightarrow V'$ ein metrischer Morphismus

z. z.: nur die Null wird auf Null abgebildet

$f(x) = 0$

$x.y = f(x).f(y) = 0 \, \forall y \in V \Rightarrow x \in V^0$

Da (V, Q) nichtausgeartet, ist $V^0 = 0 \Rightarrow x = 0$.

(ii) $U \leq V$ Untervektorraum. Wir betrachten:

$$V \xrightarrow[bijektiv]{q_V} \quad V^* \xrightarrow[kanon.Surj.]{} U^*$$

Der Homomorphismus $q_U : V \longrightarrow U^*$ ist surjektiv und wir erhalten die exakte Sequenz:

$$0 \longrightarrow U^0 \longrightarrow V \longrightarrow U^* \longrightarrow 0$$

(a) Da dies eine exakte Sequenz ist, gilt: $\dim(V) = \dim(U^*) + \dim(U^0)$. Da $\dim(U) = \dim(U^*)$, folgt $\dim(V) = \dim(U) + \dim(U^0)$.

(b)

$\dim(V) = \dim(U) + \dim(U^0)$ gilt für beliebige Untervektorräume, also insbesondere auch fürU^0 :

$\dim(V) = \dim(U^0) + \dim(U^{00})$

Daraus folgt, dass $\dim(U) = \dim(U^{00})$, und da nach Definition des orthogonalen Komplements $U \subseteq U^{00}$ ist $U = U^{00}$.

(c)

$$U^0 = \{u \in V \mid u.v = 0, \forall v \in U\}$$
$$\mathrm{rad}(U) = \{u \in U \mid u.v = 0, \forall u \in U\}$$

$\Rightarrow \mathrm{rad}(U) = U \cap U^0$

Da $U = U^{00}$, gilt: $\mathrm{rad}(U^0) = U^0 \cap U^{00} = U^0 \cap U = \mathrm{rad}(U)$

(d) U ist nichtausgeartet $\iff \mathrm{rad}(U) = 0 \iff \mathrm{rad}(U^0) = 0 \iff U^0$ ist nichtausgeartet.

(iii) $V = U_1 \hat{\bigoplus} U_2$, d. h. dass $U_1 \perp U_2$, und da die Summe auch direkt ist, gilt $\mathrm{rad}(U_i) = 0 \Rightarrow U_i$ ist nichtausgeartet $(i = 1; 2)$.

□

3 Isotrope Vektoren

Definition 3.1 (isotrop)**.** *Ein Element x aus einem Quadratischen Modul heißt isotrop, wenn $Q(x) = x.x = 0$.*
Ein Unterraum $U \leq V$ heißt isotrop, wenn alle seine Elemente isotrop sind, d. h. $\forall x \in U : Q(x) = 0$.

Bemerkung 3.2. *U isotrop $\iff U \subset U^0 \iff Q\mid_U = 0$*

Definition 3.3 (Hyperbolische Ebene)**.** *Ein Quadratischer Modul, der eine Basis aus zwei isotropen Elementen x, y hat, so dass $x.y \neq 0$, heißt hyperbolische Ebene.*

Nach Multiplikation von y mit $1/x.y$, kann man annehmen, dass $x.y = 1$. Die Matrix der Quadratischen Form bezüglich x und y ist $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ mit $\mathrm{disc}(Q) = -1$. Also ist die hyperbolische Ebene nichtausgeartet.

Proposition 3.4. *Sei $x \neq 0$ ein isotropes Element eines nichtausgearteten Quadratischen Moduls (V,Q). Dann existiert ein Unterraum $U \leq V$, der x enthält und eine hyperbolische Ebene ist.*

Beweis. Da V nichtausgeartet ist, existiert ein $z \in V$, so dass $x.z = 1$.
Das Element $y = 2z - (z.z)x$ ist isotrop, denn nachrechnen ergibt:

$$\begin{aligned} y.y &= (2z - (z.z)x).(2z - (z.z)x) \\ &= 4z.z - 2(z.z)\underbrace{(z.x)}_{=1} - 2(z.z)\underbrace{(z.x)}_{=1} + \underbrace{(z.z)^2(x.x)}_{=0,\text{ da } x \text{ isotrop}} \\ &= 4z.z - 4z.z \\ &= 0 \end{aligned}$$

Ebenso berechnet man: $y.x = (2z - (z.z)x).x = 2z.x - \underbrace{(z.z)(x.x)}_{=0,\text{ da } x \text{ isotrop}} = 2$. Somit hat der Unterraum $U = xK + yK$ die gewünschte Eigenschaft. □

Korollar 3.5. *Wenn (V, Q) nichtausgeartet ist und ein isotropes Element ungleich Null enthält, gilt $Q(V) = K$, d.h. $\forall a \in K : \exists v \in V : Q(v) = a$.*

Beweis. Aus vorheriger Proposition folgt, dass V eine hyperbolische Ebene enthält. Zum Beweis des Korollars genügt es den Fall zu zeigen, in dem V eine hyperbolische Ebene mit Basis x, y ist, wobei

x, y isotrop und $x.y = 1$. Wenn $a \in K$, gilt $a = Q(x + \frac{a}{2}y)$. Dies kann man leicht nachrechnen: $Q(x + \frac{a}{2}y) = (x + \frac{a}{2}y).(x + \frac{a}{2}y) = \underbrace{(x.x)}_{=0} + \frac{a}{2}\underbrace{(y.x)}_{=1} + \frac{a}{2}\underbrace{(x.y)}_{=1} + \frac{a}{2}^2\underbrace{(y.y)}_{=0} = a.$

Also ist $Q(V) = K$. □

4 Orthogonalbasis

Definition 4.1 (Orthogonalbasis)**.** *Eine Basis $(e_1, \ldots, e_n)$ eines Quadratischen Moduls (V, Q) heißt orthogonal, wenn ihre Elemente paarweise orthogonal sind.*

Beispiel 4.2. $V = e_1K \hat{\bigoplus} \cdots \hat{\bigoplus} e_nK$

Daraus folgt, dass die Matrix von Q bezüglich dieser Basis eine Diagonalmatrix ist:

$$\begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & & \ddots & 0 \\ 0 & \ldots & & a_n \end{pmatrix}$$

Wenn $x = \sum x_i e_i$ ist, dann ist $Q(x) = a_1x_1^2 + \cdots + a_nx_n^2$.

Theorem 4.3. *Jeder Quadratische Modul (V, Q) hat eine Orthogonalbasis.*

Beweis. Beweis durch Induktion nach $n = \dim(V)$: Die Aussage gilt für den Fall $n = 0$. Falls V isotrop ist, sind alle Basen von V orthogonal. Falls V nicht isotrop, wählt man ein Element $e_1 \in V$, so dass $e_1.e_1 \neq 0$ ist. Das orthogonale Komplement H von e_1 hat $\dim(H) = n - 1$, ist also eine Hyperebene. Nach Induktionsannahme hat H eine orthogonale Basis $(e_2, \ldots, e_n)$. Da e_1 nicht zu H gehört, ist $V = e_1K \hat{\bigoplus} H$ und $(e_1, \ldots, e_n)$ ist eine Orthogonalbasis von V. □

Definition 4.4 (benachbart)**.** *Zwei Orthogonalbasen $\boldsymbol{e} = (e_1, \ldots, e_n)$ und $\boldsymbol{e'} = (e'_1, \ldots, e'_n)$ von V heißen benachbart, wenn sie ein gemeinsames Element haben, d. h. $\exists i$ und $j : e_i = e'_j$.*

Theorem 4.5. *Sei (V, Q) ein nichtausgearteter Quadratischer Modul mit Dimension $\geqq 3$ und seien $\boldsymbol{e} = (e_1, \ldots, e_n)$ und $\boldsymbol{e'} = (e'_1, \ldots, e'_n)$ zwei Orthogonalbasen von V. Dann existiert eine endliche Folge $\boldsymbol{e}^{(0)}, \boldsymbol{e}^{(1)}, \ldots, \boldsymbol{e}^{(m)}$ von Orthogonalbasen von V, so dass $\boldsymbol{e}^{(0)} = \boldsymbol{e}, \boldsymbol{e}^{(m)} = \boldsymbol{e'}$ und $\boldsymbol{e}^{(i)}$ benachbart zu $\boldsymbol{e}^{(i+1)}$ ist für $0 \leqq i < m$.*

Anmerkung 4.6. *Man nennt $\boldsymbol{e}^{(0)}, \boldsymbol{e}^{(1)}, \ldots, \boldsymbol{e}^{(m)}$ eine Kette von Orthogonalbasen, die $\boldsymbol{e}$ und $\boldsymbol{e'}$ benachbart verbindet.*

Beweis. Man unterscheidet drei Fälle:

(i) $(e_1.e_1)(e'_1.e'_1) - (e_1.e'_1)^2 \neq 0$

Das heißt e_1 und e'_1 sind linear unabhängig und die Ebene $P = e_1K + e'_1K$ ist nichtausgeartet, da $\det(Q\mid_P) = (e_1.e_1)(e'_1.e'_1) - (e_1.e'_1)^2 \neq 0$. Dann existieren ε_2 und ε'_2, so dass $P = e_1K \hat{\bigoplus} \varepsilon_2K$ und $P = e_1K \hat{\bigoplus} \varepsilon'_2K$.

Sei P^0 das orthogonale Komplement zu P in V. Da P nichtausgeartet folgt aus Proposition 2.14,

dass $V = P\hat{\bigoplus}P^0$. Sei $(e_3'', \ldots, e_n'')$ eine Orthogonalbasis von P^0. Nun kann man **e** und **e'** durch folgende Kette benachbart miteinander verbinden:

$$\mathbf{e} \to (e_1, \varepsilon_2, e_3'', \ldots, e_n'') \to (e_1', \varepsilon_2', e_3'', \ldots, e_n'') \to \mathbf{e'}.$$

(ii) $(e_1.e_1)(e_2'.e_2') - (e_1.e_2')^2 \neq 0$
analog zu (i), wenn man e_1' durch e_2' ersetzt.

(ii) $(e_1.e_1)(e_i'.e_i') - (e_1.e_i')^2 = 0$ für $i = 1; 2$
Dafür wird zunächst Lemma 4.7 bewiesen:

Lemma 4.7. *Es existiert ein $x \in K$, so dass $e_x = e_1' + xe_2'$ nicht isotrop ist und mit e_1 eine nichtausgeartete Ebene aufspannt.*

Beweis. Für das gesuchte x soll e_x nicht isotrop sein, d.h. es muss gelten $e_x.e_x = (e_1'+xe_2').(e_1'+xe_2') = e_1'.e_1' + x^2(e_2'.e_2') \neq 0 \iff x^2 \neq -(e_1'.e_1')/(e_2'.e_2')$. Um eine nichtausgeartete Ebene zu erhalten muss gelten $(e_1.e_1)(e_x.e_x) - (e_1.e_x)^2 \neq 0$. Setzt man $e_x.e_x = e_1'.e_1' + x^2(e_2'.e_2')$ und $e_x = e_1' + xe_2'$ in die zweite Gleichung ein, ergibt sich:

$$\begin{aligned}
&(e_1.e_1)(e_x.e_x) - (e_1.e_x)^2 \\
=&(e_1.e_1)(e_1'.e_1' + x^2(e_2'.e_2')) - (e_1.(e_1' + xe_2')^2 \\
=&(e_1.e_1)(e_1'.e_1') + x^2(e_1.e_1)(e_2'.e_2') - (e_1.(e_1' + xe_2')^2 \\
=&(e_1.e_1)(e_1'.e_1') + x^2(e_1.e_1)(e_2'.e_2') - ((e_1.e_1') + x(e_1.e_2'))^2 \\
=&(e_1.e_1)(e_1'.e_1') + x^2(e_1.e_1)(e_2'.e_2') - ((e_1.e_1')^2 + 2x(e_1.e_1')(e_1.e_2') + x^2(e_1.e_2')^2) \\
=&(e_1.e_1)(e_1'.e_1') + x^2(e_1.e_1)(e_2'.e_2') - (e_1.e_1)(e_1'.e_1') - 2x(e_1.e_1')(e_1.e_2') - x^2(e_1.e_1)(e_2'.e_2') \\
=&-2x(e_1.e_1')(e_1.e_2') \neq 0
\end{aligned}$$

Daraus und aus der Bedingung $(e_1.e_1)(e_i'.e_i') - (e_1.e_i')^2 = 0$ für $i = 1; 2$ folgt, dass $e_1.e_1 \neq 0$ und $e_1.e_i' \neq 0$. Das gesuchte x nuss also $x \neq 0$ und $x^2 \neq -(e_1'.e_1')/(e_2'.e_2')$ sein, d. h. dass man höchstens drei Werte ausschließen muss, für einen Körper mit mindestens vier Elementen, gibt es daher immer ein solches gesuchtes x. Da $char(K) \neq 2$ ist der Fall $K = \mathbb{F}_2$ ausgeschlossen. Es bleibt also nur noch der Fall $K = \mathbb{F}_3$ zu betrachten: $(e_1.e_1)(e_i'.e_i') - (e_1.e_i')^2 = 0 \iff (e_1.e_1)(e_i'.e_i') = (e_1.e_i')^2 \equiv 1$, da alle Quadrate ungleich Null in $\mathbb{F}_3$ gleich Eins sind. Aus der letzten Gleichung gewinnt man auch $\underbrace{\overbrace{\frac{(e_1.e_1)(e_1'.e_1')}{(e_1.e_1)(e_2'.e_2')}}^{=1}}_{=1} = \frac{(e_1'.e_1')}{(e_2'.e_2')} = 1$. Da $x \neq 0$ und $x \neq -1$, muss $x = 1$ sein. □

Nun wählt man $e_x = e_1' + xe_2'$, so dass es die Bedingungen aus dem Lemma erfüllt. Da e_x nicht isotrop ist, gibt es ein e_2'', so dass (e_x, e_2'') eine Orthogonalbasis von $e_1'K\hat{\bigoplus}e_2'K$ ist. Denn um mit einer Orthogonalbasis eine nichtausgeartete Ebene aufzuspannen, müssen e_x und e_2'' nicht isotrop sein: $(e_x.e_x)(e_2''.e_2'') - \underbrace{(e_x.e_2'')^2}_{=0,\text{ da orthogonal}} \neq 0 \implies (e_x.e_x) \neq 0 \wedge (e_x.e_2'') \neq 0.$

Man setzt **e"** $= (e_x, e_2'', e_3', \ldots, e_n')$. **e"** ist eine Orthogonalbasis von V. Da $e_1K + e_xK$ eine nichtausgeartete Ebene ist, gilt nach (i), dass man **e** und **e"** durch eine Kette benachbarter Basen verbinden kann. Da **e'** benachbart zu **e"** ist, folgt das Theorem. □

5 Theorem von Witt

Seien (V, Q) und (V', Q') zwei nichtausgeartete Quatratische Moduln; sei $U \in V$ ein Untervektorraum von V und sei $s : U \to V'$ ein injektiver metrischer Morphismus von U nach V'. Wir wollen s zu einem Unterraum erweitern, der größer ist als U, falls möglich sogar ganz V. Wir beginnen mit dem Fall, dass U ausgeartet ist:

Lemma 5.1. *Ist U ausgeartet kann man s zu einem injektiven metrischen Morphismus $s_1 : U_1 \to V'$ erweitern, wobei U als Hyperebe in U_1 enthalten ist.*

Beweis. Sei $0 \neq x \in \mathrm{rad}(U)$ (d.h. x ist isotrop). Sei l eine Linearform auf U mit $l(x) = 1$.
Da V nichtausgeartet ist folgt, dass ein $y \in V$ existiert mit $l(u) = u.y \quad \forall u \in U$
Außerdem gilt: $y.y = 0$, da:

$$u.(y - \lambda x) = u.y - \lambda \underbrace{u.x}_{=0} = u.y, \quad \lambda = \frac{1}{2} y.y$$

$$\Rightarrow y.y = (y - \lambda x).(y - \lambda x) = y.y - 2 \cdot (\frac{1}{2} y.y) \underbrace{y.x}_{=1} + \lambda^2 \underbrace{x.x}_{=0} = y.y - y.y = 0$$

Proposition 3.4 angewendet liefert:

$0 \neq x \in U_1$ isotrop, U_1 nichtausgeartet $\Rightarrow \exists U \subset U_1$, wobei U Hyperebene von U_1 mit $x \in U$

Da $y \notin U$ gilt nun: $U_1 = U \oplus ky$
Anschließend definieren wir: $\quad U' = s(U), \quad x' = s(x), \quad l' = l \circ s^{-1}$
Da $\quad 0 = x.u = s(x).s(u) = x'.s(u) \quad \forall u \in U$ gilt: $\quad x' \in \mathrm{rad}(s(U))$
Da V' nichtausgeartet ist, gibt es auch hier ein $y' \in V'$ mit $l'(u') = u'.y' \quad \forall u' \in U'$
Mit der gleichen Folgerungskette wie oben erhält man: $\quad U_1' = U' \oplus ky'$
Die Abbildung

$s_1 : U_1 \to V'$ mit $u + \alpha y \mapsto s(u) + \alpha y'$ ist der gesuchte Morphismus.

(Er bildet U_1 auf U_1' ab, und bildet zwischen diesen einen Isomorphismus, mit $s_1|U = s$) □

Theorem 5.2 (Witt)**.** *Seien (V, Q) und (V', Q') isomorph und nichtausgeartet. Jeder injektive metrische Morphismus $s : U \to V'$ eines Untervektorraumes U von V kann zu einem metrischen Isomorphismus von V nach V' fortgesetzt werden.*

Beweis. Da $V \cong V'$ können wir $V = V'$ annehmen.
Man unterscheidet zwei Fälle:

(i) U ausgeartet $\Rightarrow$ Lemma

(ii) U nichtausgeartet $\Rightarrow$ Beweis durch Induktion nach $\dim(U) = n$
Induktionsannahme: $n = 1$

$\dim(U) = 1 \quad \Rightarrow \quad U =< x >, \quad x.x \neq 0$ (da U nicht ausgeartet)

Definiere: $y = s(x) \quad \Rightarrow \quad y.y = x.x$

Wähle $z = x + \epsilon y \in V$ mit $\epsilon = \{+1, -1\}$

z ist nicht isotrop, da sonst folgendes gelten würde:

$$0 = (x+y).(x+y) = x.x + 2x.y + y.y = 2x.x + 2x.y$$

$$0 = (x-y).(x-y) = x.x - 2x.y + y.y = 2x.x - 2x.y$$

die beiden Gleichungen addiert ergibt: $0 = 4x.x \Rightarrow x.x = 0$

$\Rightarrow$ Widerspruch dazu, dass U nicht ausgeartet ist.

Definiere: $H = (Kz)^0$ orthogonales Komplement von z

$\Rightarrow V = Kz \oplus H$

Definiere: $\sigma =$ Spiegelung an H

d.h. $\sigma : V \to V, \quad \alpha z + h \mapsto -\alpha z + h$ (d.h. $\sigma(H) = H, z \mapsto -z$)

Es gilt: $x - \epsilon y \in H$, da $(x - \epsilon y).y = (x - \epsilon y).(x + \epsilon y) = x.x - \underbrace{\epsilon^2}_{=1} y.y = x.x - y.y = 0$

$\Rightarrow \sigma(x - \epsilon y) = x - \epsilon y \quad$ (da $\in H$)

$\sigma(x + \epsilon y) = -x - \epsilon y$

Weiter gilt: $\sigma(x - x + \epsilon y) = \sigma(x) - \sigma(x - \epsilon y) = \sigma(x) - (x - \epsilon y) = \sigma(x) - x + \epsilon y$

$\sigma(-x + x + \epsilon y) = \sigma(-x) + \sigma(x - \epsilon y) = -\sigma(x) - x - \epsilon y$

nach Gleichsetzen folgt: $\sigma(x) - x + \epsilon y = -\sigma(x) - x - \epsilon y$

$\Leftrightarrow 2\sigma(x) = -2\epsilon y$

$\Leftrightarrow \sigma(x) = -\epsilon y$

$\Rightarrow s(x) = y = -\epsilon\sigma(x)$ (da $\epsilon \in \{+1, -1\}$)

$\Rightarrow -\epsilon\sigma$ ist der gesuchte Isomorphismus.

Induktionsschritt: $n \to n + 1$

Zerlege U: $U = U_1 \hat{\oplus} U_2$ mit $U_1, U_2 \neq 0$

Da $\dim(U_1) \leq n$ gilt nach Induktionsannahme:

$s_1 = s|U$ wird zu einem Automorphismus σ_1 von V fortgesetzt

Durch Ersetzen von s durch $\tilde{s} = \sigma^{-1} \circ s$ sieht man:

$\tilde{s}|U_1 = id|U_1$

$\tilde{s}|U_2 : U_2 \to V_1 = U_1^0$

Nach Induktionsannahme gilt wieder:

$\tilde{s}|U_2$ wird zu einem Automorphismus σ_2 von V_1 fortgesetzt.

Wähle nun als Erweiterung von $\tilde{s}|U$:

$\sigma : U_1 \hat{\oplus} V_1 = V \to V = U_1 \hat{\oplus} V_1$ mit $u + v \mapsto u + \sigma_2(v)$

$\Rightarrow$ Erweiterung von s: $\quad \sigma_1 \circ \sigma$

□

Korollar 5.3. *Zwei isomorphe Unterräume eines nichtausgearteten Quadratischen Moduls haben isomorphe orthogonale Komplemente.*

Beweis. Sei (V, Q) nichtausgearteter Quadratischer Modul.

Seien $U, W \subset V$ Unterräume mit $U \cong W$. Sei $s : U \to W$ Isomorphismus.

$\overset{Theorem}{\Rightarrow}$ s kann zu einem metrischen Isomorphismus $\sigma : V \to V'$ fortgesetzt werden.

$\Rightarrow$ Einschränkung $\sigma|U^0 : U^0 \to W^0$ metrischer Isomorphismus $\square$

Bemerkung 5.4 (Wittscher Kürzungssatz)**.** $V \oplus W \cong V' \oplus W', \quad V \cong V' \quad \Rightarrow \quad W \cong W'$

6 Translationen

Sei $f(X) = \sum_{i=1}^{n} a_{ii} {X_i}^2 + \sum_{i<j} a_{ij} X_i X_j$ eine Quadratische Form über K in n Variablen; wir setzen $a_{ij} = a_{ji}$ für $i > j$, so dass die Matrix $A = (a_{ij})$ symmetrisch ist. Das Paar (K^n, f) ist ein Quadratischer Modul, der f (oder der Matrix A) zugeordnet ist.

Definition 6.1 (Äquivalent)**.** *Zwei Quadratische Formen f und f' heißen äquivalent, wenn die zugehörigen Moduln isomorph sind.*

Bezeichnung: $f \sim f'$.

Wenn A und A' die Matrizen von f und f' sind, folgt daraus, dass eine invertierbare Matrix X existiert, so dass $A' = X.A.X^t$.

Seien $f(X_1, \ldots, X_n)$ und $g(X_1, \ldots, X_m)$ zwei Quadratische Formen; wir ordnen $f \dot{+} g$ (oder einfach $f+g$, falls keine Verwechslung möglich ist) die Quadratische Form $f(X_1, \ldots, X_n)+g(X_{n+1}, \ldots, X_{n+m})$ in $n + m$ Variablen zu. Dies Operation korrespodiert zu der orthogonalen Summe.

Wir schreiben ähnlich $f \dot{-} g$ (oder einfach $f - g$) für $f + (-g)$.

Hier einige Beispiele für Translationen:

Definition 6.2 (Definition 3.3')**.** *Eine Form $f(X_1, X_2)$ in zwei Variablen heißt hyperbolisch, wenn gilt*

$f \sim X_1 X_2 \sim {X_1}^2 - {X_2}^2$

(D.h. der Modul (K^2, f) korrespondiert zu einer hyperbolischen Ebene)

Beweis. Nach Definition 3.3 gilt: Matrix einer hyperpolischen Quadratischen Form $= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$\Rightarrow$ zugehörige Form: $X_1 X_2$

$\Rightarrow f \sim X_1 X_2$

Umformung: $\begin{pmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$\Rightarrow$ zugehörige Form $X_1 - X_2$

$\Rightarrow f \sim X_1 X_2 \sim X_1 - X_2$ $\square$

Eine Form $f(X_1, \ldots, X_n)$ repräsentiert ein Element a von K, wenn ein $x \in K^n$, $x \neq 0$, existiert, so dass $f(x) = a$. Insbesondere gilt f repr 0, genau dann wenn der korrespondierende Quadratische Modul ein isotropes Element ungleich 0 enthält.

Proposition 6.3. *Wenn f repr 0 und nichtausgeartet ist, erhält man $f \sim f_2 \dot{+} g$, wobei f_2 hyperbolisch ist. Außerdem repräsentiert f alle Elemente von K.*

Das ist eine Translation von Proposition 3.4 und ihrem Korollar.

Beweis. Da f nichtausgeartet ist, ist auch (K^n, f) nichtaugeartet

f repr $0 \quad \Rightarrow \quad \exists x \in K^n : f(x) = 0 \quad$ (d.h. x isotrop)

$\overset{Prop.3.4}{\Rightarrow} x \in (K^n, f_2) \subset (K^n, f)$ mit K^2 hyperbolische Ebene

$\Rightarrow (K^n, f) = (K^2, f_2) \oplus (K^{n-2}, g)$

$\Rightarrow f \sim f_2 + g$ □

Korollar 6.4. *Sei $g = g(X_1, \ldots, X_{n-1})$ eine nicht ausgeartete Quadratische Form und sei $a \in K^*$. Die folgenden Eigentschaften sind äquivalent:*

1. *g repräsentiert a*
2. *es gilt $g \sim h \dot{+} aZ^2$, wobei h eine From in $n-2$ Variablen ist*
3. *die Form $f = g \dot{-} aZ^2$ repräsentiert 0*

Beweis. (ii) $\rightarrow$ (i): $h(0, \ldots, 0) + aZ^2(1) = a$

(Erinnerung: $f \sim g$ heißt f und g stellen dieselben Werte aus dem Grundkörper dar)

(i) $\rightarrow$ (ii): Sei (K^{n-1}, g) der zu g assoziierte Modul

g repr $a \quad \overset{Def.}{\Rightarrow} \quad \exists x \in (K^{n-1}, g) : g(x) = x.x = a$

$H := (kx)^0 \quad \Rightarrow \quad V = H \oplus kx \quad \Rightarrow \quad g \sim h \dot{+} aZ^2$

(i) $\rightarrow$(iii): g repr a $\quad \Rightarrow \quad \exists x \in K^{n-1} : g(x) = a$

$f(x, 1) = g(x) - aZ^2(1) = a - a = 0$

(iii) $\rightarrow$(i): $f = g \dot{-} aZ^2$ repr $0 \quad \Rightarrow \quad \exists x \in K^n, z \in K : (x, z) \neq 0$ mit g repr az^2

Fall 1: $z = 0 \quad \Rightarrow \quad x \neq 0$ und $g(x) = 0$

$\Rightarrow$ g repr 0

Fall 2: $z \neq 0 \quad \Rightarrow \quad f(x, z) = 0 = g(x) - az^2$

$\Rightarrow g(x) = az^2 \quad \Rightarrow \quad a = \frac{1}{z^2} g(x)$

$\overset{gQuadr.Form}{\Rightarrow} a = g(\frac{1}{z} x)$

$\overset{KKörper}{\Rightarrow} a = g(\frac{x_1}{z}, \ldots, \frac{x_{n-1}}{z})$

$\Rightarrow g$ repr a

□

Korollar 6.5. *Seien g und h zwei nicht ausgeartete Formen mit Rang ≥ 1 und sei $f = g \dot{-} h$. Die folgenden Eigenschaften sind äquivalent:*

1. *f repräsentiert 0*
2. *es existiert ein $a \in K^*$, welches durch g ung h repräsentiert wird.*

3. es existiert ein $a \in K^*$, so dass $g \dot{-} aZ^2$ und $h \dot{-} aZ^2$ 0 repräsentieren.

Beweis. (ii) $\leftrightarrow$(iii): g repr $a \overset{Kor.1}{\Rightarrow} g \dot{-} aZ^2$ repr 0
h repr $a \overset{Kor.1}{\Rightarrow} h \dot{-} aZ^2$ repr 0

(ii) $\rightarrow$(i): $\exists a, x_1, x_2 : a = g(x_1) = h(x_2)$
$\Rightarrow f(x_1, x_2) = g(x_1) - h(x_2) = 0 \quad ((x_1, x_2) \neq 0$, da $x_1 \neq 0, x_2 \neq 0)$
$\Rightarrow f$ repr 0

(i) $\rightarrow$ (ii): f repr $0 \quad \Rightarrow \quad \exists a, x_1, x_2 : a = g(x_1) = h(x_2)$
Fall 1: $a \neq 0 : g(x_1) = a, \quad h(x_2) = a \quad \Rightarrow$ fertig
Fall 2: $a = 0$ ($\Rightarrow x_1, x_2$ sind isotrop)
o.E. $x_1 \neq 0$ (da $(x_1, x_2) \neq 0$ muss entweder $x_1 \neq 0$ oder $x_2 \neq 0$ sein)
$\Rightarrow g$ repr 0
$\overset{Prop6.3'}{\Rightarrow} \forall y$: g repr y
da h nichtausgeartet $\Rightarrow \exists z, a_2 : h(z) = a_2 \Rightarrow$ h repr a_2
da g alle Elemente aus K^* repräsentiert $\Rightarrow g$ repr a_2

□

Theorem 4.3 in die klassische Zerlegung von quadratischen Formen in „Summen von Quadraten“ übersetzt:

Theorem 6.6. *Sei f eine quadratische Form in n Variablen. Es existieren $a_1, \ldots, \alpha_n \in K$, so dass $f \sim a_1 {X_1}^2 + \ldots + a_n {X_n}^2$*

Beweis. Der zu f assoziierte Modul (K^n, f) hat nach Theorem 4.3 eine orth. Basis.
$(K^n, f) \cong (ke_1 \oplus \ldots \oplus ke_n, f)$
Sei $v = \alpha_1 e_1 + \ldots + \alpha_n e_n$
$f(v) = v.v = \sum(\alpha_i \cdot \alpha_j)(e_i.e_j) \overset{ONB}{=} \sum a_i^2 (e_i.e_i)$
$\Rightarrow f(X) = \sum(e_i.e_i) X_i^2$ □

Schließlich führt das Theorem von Witt auf folgendes „Kürzungstheorem“:

Theorem 6.7. *Seien $f = g + h$ und $f' = g' + h'$ zwei nichtausgeartete Quadratische Formen. Wenn $f \sim f'$ und $g \sim g'$ erhält man $h \sim h'$*

Korollar 6.8. *Wenn f nichtausgeartet ist, dann gilt $f \sim g_1 + \ldots + g_m + h$ wobei $g_1, \ldots, g_m$ hyperbolisch sind und h nicht 0 repräsentiert. Diese Zerlegung ist eindeutig bis auf Äquivalenz.*

Beweis. Existenz: folgt aus Prop 6.3 (solange angewandt, wie 0 repräsentiert wird).
Eindeutigkeit: folgt aus Theorem 6.7. □

7 Quadratische Formen über $\mathbb{F}_q$

Sei p eine Primzahl $\neq 2$ und sei $q = p^f$ eine Potenz von p; sei $\mathbb{F}_q$ ein Körper mit q Elementen.

Proposition 7.1. *Eine Quadratische Form über $\mathbb{F}_q$ von Rang ≥ 2 (bzw. von Rang ≥ 3) stellt alle Elemente von ${\mathbb{F}_q}^*$ (bzw. $\mathbb{F}_q$) dar.*

Beweis. Aus Serre: Kap 1 §2 Korollar 1 folgt die Aussage für Rang ≤ 3

Rang ≤ 2: Korollar 6.4: (i) $\rightarrow$ (iii)

Proposition 6.3: f repr $0 \Rightarrow f$ stellt alle Elemente von ${\mathbb{F}_q}^*$ dar $\square$

Wiederholung: Die Gruppe ${\mathbb{F}_q}^*/{{\mathbb{F}_q}^*}^2$ hat zwei Elemente.

Wir bezeichnen mit a ein Element von ${\mathbb{F}_q}^*$, welches keine Wurzel hat.

Proposition 7.2. *Jede nichtausgeartete Quadratische Form von Rang n über $\mathbb{F}_q$ ist äquivalent zu ${X_1}^2 + \ldots + {X_{n-1}}^2 + {X_n}^2$ oder ${X_1}^2 + \ldots + {X_{n-1}}^2 + a{X_n}^2$, abhängig davon, ob ihre Diskriminante ein Quadrat ist oder nicht.*

$\operatorname{disc}(f) \equiv 1 \pmod{{\mathbb{F}_q}^{*^2}} \Leftrightarrow$ Diskriminante ist Quadrat

Beweis. Induktion nach $Rang(f) = n$:

Induktionsanfang: $n = 1$:

Fall 1: $f \sim bX^2, b \in {\mathbb{F}_q}^{*^2} \quad \Leftrightarrow \quad (f \sim bX^2 \sim X^2 \Leftrightarrow \operatorname{disc}(f) \equiv 1)$

Fall 2: $f \sim bX^2, b \notin {\mathbb{F}_q}^{*^2}$

sei $b = c^2 + a$ mit $a \notin {\mathbb{F}_q}^{*^2}$ fest

$\Leftrightarrow f \sim bX^2 \sim aX^2$

$\Leftrightarrow \operatorname{disc}(f) \equiv a \pmod{{\mathbb{F}_q}^{*^2}}$

$\overset{a \notin {\mathbb{F}_q}^{*^2}}{\Leftrightarrow} \operatorname{disc}(f) \neq 1 \pmod{{\mathbb{F}_q}^{*^2}}$

Induktionsschritt: $n \Rightarrow n + 1$

Nach Proposition 7.1 gilt: $\forall y \in {\mathbb{F}_q}^* : f(x) = y$

$\Rightarrow \exists x : f(x) = 1$

$\overset{Kor.1}{\Rightarrow} f \sim g + {X_1}^2$

$\overset{I.A.}{\Rightarrow} g \sim {X_2}^2 + \ldots + {X_{n-1}}^2$ oder $g \sim {X_2}^2 + \ldots a{X_{n-1}}^2$

$\Rightarrow f \sim {X_1}^2 + {X_2}^2 + \ldots + {X_n}^2$ oder $f \sim {X_1}^2 + {X_2}^2 + \ldots + a{X_n}^2$

$\square$

Korollar 7.3. *Damit zwei nichtausgeartete Quadratische Formen über $\mathbb{F}_q$ äquivalent sind, ist es notwendig und hinreichend, dass sie den gleichen Rang und die gleiche Diskriminante haben.*
(Natürlich wird die Diskriminante als Element der Quotientengruppe ${\mathbb{F}_q}^*/{{\mathbb{F}_q}^*}^2$ angesehen.)

Beweis. folgt aus Proposition 7.1 und 7.2 $\square$