Mario Romsy, Holger Blasum, Michael Helbig **WS 2002/03**

Kapitel IV. 1-2 Quadratische Formen

basierend auf: Jean Pierre Serre[4]

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

1 Quadratische Formen

Bemerkung 1. Bei Verweisen der Form (n) [p.q Def/Prop/Thm m] bezieht sich die Zahl n in runden Klammern auf die Numerierung in unserer Bearbeitung, der Gehalt der eckigen Klammern auf Abschnitt $(p.q)$ und Numerierung (m) in [4].

1.1 Definitionen

Erinnerung 2. Eine *Bilinearform* ist eine Funktion F von $V \times V \to A$, so dass:
$F(x + x', y) = F(x, y) + F(x', y)$
$F(x, y + y') = F(x, y) + F(x, y')$
$F(\alpha x, y) = \alpha F(x, y) = F(x, \alpha y)$ für alle $x, x', y, y' \in V$ und $\alpha \in A$.

Eine aus der linearen Algebra bekannte Bilinearform ist das Skalarprodukt (mit Tupeln oder Funktionen als Vektoren).

Definition 3 (Def 1). Sei V ein Modul über einem kommutativen Ring A. Eine Funktion $Q\colon V \to A$ heißt *quadratische Form* auf V, genau dann wenn $\forall \alpha \in A, \forall x, y \in V$:
$(Q1)$ $\quad Q(\alpha x) = \alpha^2 Q(x)$
$(Q2)$ $\quad (x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ ist eine Bilinearform.

Ein Paar (V, Q) mit V Modul über einem kommutativen Ring und einer quadratischen Form Q auf V heißt *quadratischer Modul*.

Bemerkung 4. In diesem Kapitel beschränken wir uns auf den Fall $A = K$. Ein Körper mit Charakteristik (Elementzahl) $\neq 2$, d.h. V ist dann ein K-Vektorraum. Des weiteren sei $dim(V) = n < \infty$.

Definition 5 (Polarisation).

$$\cdot : (x, y) \mapsto x \cdot y := \frac{1}{2}(Q(x+y) - Q(x) - Q(y))$$

$\cdot$ (Also Q2 von der vorhergehenden Definition multipliziert mit $\frac{1}{2}$) ist eine symmetrische Bilinearform auf V und wird *mit Q assoziiertes Skalarprodukt* genannt, es muss im Gegensatz zum uns aus der linearen Algebra bereits bekannten Skalarprodukt nicht positiv definit sein.

Bemerkung 6. Damit ist die Beschränkung auf $char(k) \neq 2$ motiviert, sonst ist im Falle $2 = 0 \ (mod\ k)$ der Wert $\frac{1}{2}$ nicht definiert.

Es gilt: $Q(x) = x \cdot x$, dies erzeugt eine Bijektion zwischen quadratischen Formen und symmetrischen Bilinearformen.

Definition 7. Seien (V, Q) und (V', Q') zwei quadratische Moduln. Eine lineare Abbildung $f : V \to V'$, bestimmt durch die Anforderung $Q = Q' \circ f$, also

$$\forall x \in V, x' \in V' : Q(x) = Q'(f(x'))$$

heißt *Morphismus* (oder: *metrischer Morphismus*) von (V, Q) nach (V', Q'). Zwei Moduln heißen *isomorph*, wenn ihre Vektorraüme isomorph sind und es zwischen ihnen einen metrischen Morphismus gibt.

Bemerkung 8. Es gilt $f(x) \cdot f(y) = x \cdot y \quad \forall x, y \in V$ (für f metrischer Morphismus).

Überlegung 9. Sei $(e_i)_{1 \leq i \leq n}$ eine Basis von V. Die Matrix von Q bzgl. dieser Basis ist die Matrix $A = (a_{ij})$ mit $a_{ij} = e_i \cdot e_j$. A ist symmetrisch. $x = \sum x_i e_i$ sei ein Element von V, dann ist

$$Q(x) = \sum_{i,j} a_{ij} x_i x_j \quad Q(x) = x \cdot x$$

was zeigt, dass $Q(x)$ eine "quadratische Form" in $x_1, \ldots, x_n$ im üblichen Sinn ist.

Überlegung 10. Basiswechsel bewirkt: $A' = X * A * X^t$ wobei $X \in GL_n(k)$, A' die Matrix von Q bzgl. der neuen Basis ist.

Beweis. Seien $(e_i)_{1\leq i\leq n}$, $(e'_i)_{1\leq i\leq n}$ Basen, $\alpha_{ij} = e_i \cdot e_j$. Die Transformation kann dann dargestellt werden als: $e'_i = \sum_{j=1}^{n} \xi_{kj} e_j$, $X = (\xi_{ij})$, $X^t = (\xi_{ji})$ Dann gilt:

$$\begin{aligned}\alpha'_{ij} = e'_k \cdot e'_l &= \sum_j \xi_{kj} e_j \cdot \sum_m \xi_{lm} e_m \\ &= \sum_{j,m} \xi_{kj} * \xi_{lm} * (e_j \cdot e_m) = \sum_{j,m} \xi_{kj} * \xi_{lm} * \alpha_{jm} \\ &= \sum_{j,m} \xi_{kj} * \alpha_{jm} * \overset{(=\xi_{lm})}{\xi_{ml}} = (XAX^t)_{k,l}\end{aligned}$$

Damit gilt dann auch $A' = XAX'$. □

Definition 11. Insbesondere $det(A') = det(A) * det(X)^2$ (Determinantenmultiplikationssatz) was zeigt, dass $det(A)$ festgelegt ist bis auf Multiplikation mit $x \in k^{*^2}$. Ein Repräsentant der so (Invarianz unter Basiswechsel) induzierten Restklassenstruktur wird die *Diskriminante von* Q, $disc(Q)$, genannt. Es ist also $disc(Q)$ entweder 0 oder ein Element von k^*/k^{*^2}.

1.2 Orthogonalität

Definition 12. Sei (V, Q) ein quadratischer Modul über k. Zwei *Elemente* x, y aus V heißen *orthogonal*, wenn $x \cdot y = 0$. Sei $H \subset V$: Dann ist

$$H^\perp := \{v \in V \mid v \cdot h = 0 \quad \forall h \in H\}$$

Unterraum in V. $V_1, V_2 \subset V$ *Unterräume* heißen *orthogonal* ($V_1 \perp V_2$), wenn $V_1 \subset V_2^\perp$, äquivalent dazu: $x \in V_1, y \in V_2 \Rightarrow x \cdot y = 0$. Der Unterraum $H^\perp$, der zu dem Vektorraum H orthogonal ist, wird als *orthogonales Komplement* bezeichnet. Das orthogonale Komplement $V^\perp$ von V (also dem trivialen Unterraum) heißt *Radikal* (Merkhilfe: Nullstellen("radix")erzeuger oder *Kern*) von V, $rad(V)$.

$$rad(V) = V^\perp = \{v \in V \mid \forall w \in V : v \cdot w = 0\}.$$

Seine Kodimension heißt *Rang* von Q, geschrieben $rank(Q)$.
$rank(Q) = dim(V) - dim(V^\perp)$. Ist $V^\perp = 0$, ist Q *nicht ausgeartet*. (Erinnerung: σ n.a. $\Leftrightarrow \forall x \neq 0 : \sigma(x, v) \neq 0 \neq \sigma(v, x)$).

Beweis. $V^\perp = 0 \Leftrightarrow \forall 0 \neq v \in V \quad \exists v' \in V : v \cdot v' \neq 0. \quad v = \sum_i \alpha_i e_i, v' = \sum_i \alpha'_i e_i. \quad \forall(\alpha_1, \alpha_n) \in k^n \quad \exists(\alpha'_1, \alpha'_n) \in k^n :$

$$\begin{aligned} v \cdot v' &= \sum_{i,j} \alpha_i \alpha'_j \alpha_{ij} \text{ mit } \alpha_{ij} = e_i \cdot e_j \\ &= \sum_{i,j} \alpha_i \alpha_{ij} \alpha'_j \\ &= (\alpha_1, \ldots, \alpha_n) A \begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix}. \end{aligned}$$

$\forall 0 \neq (\alpha_1, \ldots, \alpha_n) \in k^n \quad \exists(\alpha'_1, \ldots, \alpha'_n)$:

$$(\alpha_1, \ldots, \alpha_n) A \begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix} \neq 0 \Rightarrow (\alpha_1, \ldots, \alpha_n) A \neq 0 \Leftrightarrow rank(A) = n. \qquad \square$$

Bemerkung 13. $disc(Q) \neq 0$ (d.h. $disc(Q) \in k^*/k^{*^2}$)) $\overset{\text{Determinantenmultiplikationssatz}}{\Leftrightarrow}$ Q *n.a.*

Bemerkung 14. Sei $U \subset V$ ein Unterraum, U^* der Dualraum, $q_U \colon V \to U^*$ die Funktion, die jedem $x \in V$ die Linearform $(y \in U \mapsto x \cdot y)$ zuordnet. $Ker(q_U) = U^\perp$ (Def $U^\perp$!). Wir sehen: Q nicht ausgeartet $\Leftrightarrow$ $q_V \colon V \to V^*$ Isomorphismus. $U \subset V$ Unterraum: $rad(U) = \{u \in U \mid \forall w \in U : u \cdot w = 0\}$.

Definition 15 (Def 2). Seien $U_1, \ldots, U_m \subset V$ Unterräume: V ist *direkte orthogonale Summe* der U_i, wenn die U_i paarweise orthogonal sind und V direkte Summe der U_i ist. $V = U_1 \hat{\oplus} \ldots \hat{\oplus} U_m$.

Bemerkung 16. Hat $x \in V$ Komponenten $x_i \in U_i$, so ist

$$Q(x) = (\sum_{i=1}^m x_i, \sum_{j=1}^n x_j) = \sum_{i,j=0}^m (x_i, x_j) = \sum_{i=1}^n (x_i, x_i) = Q_1(x_1) + \ldots + Q_m(x_m)$$

wobei $Q_i = Q \mid U_i$ die Einschränkung von Q auf U_i bezeichnet.

Satz 17 (Prop 1). Ist U ein orthogonales Komplement zu $rad(V)$ in V, so ist $V = U \hat{\oplus} rad(V)$.

Beweis. Klar. $\square$

Satz 18 (Zerlegung von (V,Q), Prop 2). Sei (V,Q) nicht ausgeartet. $\Rightarrow$

1. Alle metrischen Morphismen von V in einem quadratischen Modul (V',Q') sind injektiv.
2. $\forall U \subset V$ Unterraum gilt:
   (a) $dim(U) + dim(U^\perp) = dim(V)$
   (b) $U^{\perp\perp} = U$
   (c) $rad(U) = rad(U^\perp) = U \cap U^\perp$
   (d) Der quadratische Modul $(U, Q \mid U)$ ist nicht ausgeartet $\Leftrightarrow U^\perp$ ist nicht ausgeartet. In diesem Fall ist $V = U \hat{\oplus} U^\perp$.
3. $V = U \hat{\oplus} W \Rightarrow U, W$ nicht ausgeartet und $U \perp W$

Beweis. 1. Sei $f\colon V \to V$ Morphismus,

$$f(x) = 0 \Rightarrow x \cdot y = f(x) \cdot f(y) = 0 \quad \forall y \in V \quad \text{(einsetzen).}$$

$\Rightarrow x = 0$ da (V,Q) nicht ausgeartet. $\Rightarrow Ke(f) = \{0\}$

2. $q_U\colon V \to U^*$ surjektiv wg. $q_V\colon V \to V^*$ surjektiv (bijektiv), und $s : V^* \to U^*$ Einbettung und damit surjektiv.

$$0 \xrightarrow{a} U^\perp \xrightarrow{j} V \xrightarrow{q_U} U^* \xrightarrow{b} 0$$

ist kurze exakte Folge, da $0 = Im(a) = Ke(j) = 0$, da j injektiv.
$U^\perp = Im(j) = Ke(q_U)$ da (s.o. $Ke(q_U) = U^\perp$)
$Im(q_U) = Ke(b) = U^*$ klar.
$\Rightarrow$

   (a) $dim(V) \overset{\text{Dimensionsformel}}{=} dim(Im(q_U)) + dim(Ke(q_U)) = dim(U^\perp) + dim(U^*) \overset{\text{endl. dim.}}{=} dim(U^\perp) + dim(U)$
   (b) $\forall$ Unterräume U: $dim(V) = dim(U^\perp) + dim(U^{\perp\perp}) \Rightarrow dim(U) = dim(U^{\perp\perp})$ mit $U \subset U^{\perp\perp} \Rightarrow U = U^{\perp\perp}$
   (c) $rad(U) = U \cap U^\perp$ klar (Definition!) $\Rightarrow rad(U^\perp) = U^\perp \cap U^{\perp\perp} = U^\perp \cap U = rad(U) \Rightarrow$
   (d) U n.a. $\Leftrightarrow rad(U) = 0 \Leftrightarrow rad(U^\perp) = 0 \Leftrightarrow U^\perp$ n.a.

3. $V = U \hat{\oplus} W \Rightarrow U \perp W$; $\overset{V \text{ n.a.; 2(d)}}{\Rightarrow} rad(U) = 0 = rad(W) \overset{V \text{ n.a.}}{\Rightarrow} U, W$ n.a.

□

1.3 Isotrope Vektoren

Definition 19 (Def 3). (V, G) quadratische Moduln, $x \in V$ *isotrop* $\Leftrightarrow Q(x) = 0$. $U \subset V$ Unterraum heißt *isotrop* $\Leftrightarrow \forall u \in U$: U isotrop. Offensichtlich gilt: U isotrop $\Leftrightarrow U \subset U^{\perp} \Leftrightarrow Q \mid U = 0$.

Definition 20 (Def 4). Ein quadratischer Modul heißt *hyperbolische Ebene*, wenn der Modul eine Basis aus zwei isotropen Vektoren x und y mit $x \cdot y \neq 0$ besitzt.

Bemerkung 21. Multipliziert man y mit $\frac{1}{x \cdot y}$, so kann man annehmen, dass $x \cdot y = 1$ ist. Bezüglich x und y ist die Matrix der quadratischen Form dann $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ mit mit $disc \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$. Sie ist nicht ausgeartet.

Beispiel 22. Siehe Tabelle 1.

Vorbemerkung: Anschaulich sind quadratische Formen Polynome. Werden als Vektoren 2-Tupel verwendet, so sind quadratische Formen über dem Vektorraum der 2-Tupel Polynome, in denen nur Terme vom Grad 2 vorkommen, nicht aber Konstanten (ungleich 0) oder lineare Argumente (*Homogenität*). Über $\mathbb{C}$ als Grundkörper sind dann z.B. alle quadratischen Formen der Art

$$a * x^2 + b * x * y + c * y^2.$$

Ein Beispiel ist $5x^2 - 2x * y + 4x^2$.

Bemerkung 23. "Messung": Im letzten Beispiel der Tabelle ($\mathbb{F}_5$) sind genau 40 der 125 Belegungen für $\alpha_1 * x_1^2 + \alpha_2 * x_1 * x_2 + \alpha_3 * x_2^2$ isotrop, 85 anisotrop, für $\mathbb{F}_3, \mathbb{F}_7, \mathbb{F}_{11}$ sowohl für Vektorbestandteile als auch Skalare liegen die Werte bei 6 vs. 21, 126 vs. 217, 550 vs. 781.

Theorem 24 (Prop 3). Sei (V, Q) ein nicht ausgearteter quadratischer Modul, $x \in V$ isotrop mit $x \neq 0$. Dann existiert $U \subset V$ Unterraum mit $x \in U$ und U ist hyperbolische Ebene.

Beweis. (V, Q) nicht ausgeartet. $\Rightarrow \exists \tilde{z} \in V$ mit $x \cdot \tilde{z} = \alpha \neq 0$. Konstruiere daraus $z \in V$ mit $x \cdot z = 1$ ($z := \frac{\tilde{z}}{\alpha}; x \cdot z = x \cdot \frac{\tilde{z}}{\alpha} = \frac{x \cdot \tilde{z}}{\alpha} = \frac{\alpha}{\alpha}$). Dann ist auch $y = 2z - (z \cdot z)x$ isotrop:

$$\begin{aligned} y \cdot y &= (2z - (z \cdot z)x) \cdot (2z - (z \cdot z)x) \\ &= 4(z \cdot z) - 4(z \cdot z) * (z \cdot x) + (z \cdot z)^2 (x \cdot x) \\ &= 4(z \cdot z) - 4(z \cdot z) + (z \cdot z)^2 (x \cdot x) \overset{x \text{ isotr.}}{=} 0. \end{aligned}$$

Tabelle 1: Isotropie - Unabhängigkeit der Ausgabebeobachtung über einen Eingabebereich

Objektklasse	Versuchsparameter	Isotropiekriterium	Bsp (isotrop)	Gegenbsp (anisotrop)
Kristalle, Minerale	Betrachtungsrichtung 3-dim. (x, y, z)	Lichtausbreitung, Farbe konstant ?	NaCl, Glas	$CaCO_3$ (Doppelspat), SiO_2
A (Körper des VR) $= \mathbb{R}, V = \mathbb{R} \times \mathbb{R}$	$x := (x_1, x_2)$ aus V	$x \neq 0$ s.d. $Q(x) \equiv 0 \forall \alpha \in A$?	$x_1 * x_2, x_1^2 + 3 * x_1 * x_2 + x_2^2$	$x_1^2 + x_2^2$, $x_1^2 + 1 * x_1 * x_2 + x_2^2$
A (Körper des VR) $= \mathbb{F}_5$, $V = \mathbb{F}_5 \times \mathbb{F}_5$	$x := (x_1, x_2)$ aus V	$\exists x \neq 0$ s.d. $Q(x) \equiv 0 \forall \alpha \in A$?	$x_1 * x_2, x_1^2 + x_2^2$ (Z.B. $x_1 = 3, x_2 = 4$)	$x_1^2 + 2 * x_2^2$

Ferner ist das Produkt der beiden isotropen Basisvektoren $x \cdot y \neq 0$:

$$x \cdot y = x \cdot (2z - (z \cdot z)x) \overset{x \text{ isotr.}}{=} 2(x \cdot z) - 0 = 2.$$

$\Rightarrow$ Der Unterraum $U = kx + ky$ hat die gewünschten Eigenschaften. □

Satz 25 (Prop 3+). (V, Q) n.a. q.M., $U \subset V$, $0 \neq x \in rad(U)$ (d.h. U ausgeartet)
$\Rightarrow$ zerlegt man U in $U = U' \oplus kx$, so $\exists y \in U'^{\perp} \setminus U^{\perp}$ mit $y \cdot y = 0$, $x \cdot y = 1$ (damit gilt: $kx \oplus ky$ ist hyperbolische Ebene).

Beweis. Sei $U = U' \oplus kx$, $0 \neq x \in rad(U)$
$\Rightarrow$ da V n.a. gilt $dim(U) + dim(U^{\perp}) \overset{\text{[1.2 Prop 2.2 (a)]}}{=} dim(V)$,
weiter gilt $dim(U') = dim(U) - 1$, also wegen $dim(U') + dim(U'^{\perp}) = dim(V)$:

$dim(U'^{\perp}) = dim(U^{\perp}) + 1$,
zusammen mit $U' \subsetneq U \Rightarrow U'^{\perp} \setminus U^{\perp} \neq \emptyset \quad (U^{\perp} \subsetneq U'^{\perp})$.
Sei $z \in U'^{\perp} \setminus U^{\perp} \Rightarrow z \cdot x \neq 0$, o.E. $z \cdot x = 1$. $z_1 = 2z - (z \cdot z)x$.
Wie in (24) [Prop 3]: $z_1 \cdot z_1 = 0$ und $x \cdot z_1 = 2$. Sei $y = \frac{1}{2} z_1 = z - \frac{1}{2}(z \cdot z)x$. Es gilt: $y \cdot y = 0, x \cdot y = 1, y \in U'^{\perp} \setminus U^{\perp}$ (da $x \in U$ und $x \cdot y = 1 \Rightarrow y \notin U^{\perp}$. Aber $x \in U'^{\perp}$ und $z \in U'^{\perp} \Rightarrow y \in U'^{\perp}$ da $U'^{\perp} \subset V$ Unterraum). Damit erfüllt y die Bedingungen. □

Korollar 26. Sei (V, Q) nicht ausgeartet und enthalte ein isotropes Element $\neq 0 \Rightarrow Q(V) = k$, d.h $\forall a \in k \quad \exists v \in V$ mit $Q(v) = a$.

Beweis. Nach (24) [Prop 3] reicht es, den Fall zu betrachten, in dem V eine hyperbolische Ebene ist, mit Basis x und y, wobei $x \cdot y = 1$ und x, y isotrop. Sei $a \in k$, dann ist $a = Q(x + \frac{a}{2}y) \quad (char(k) \neq 2!)$. (Komponenten von $x + \frac{a}{2}y$ bzgl x, y: 1 und $\frac{a}{2}$, in $Q(x) = \sum_{i,j} a_{i,j}(x_i \cdot x_j) = 0 * 1 + 1 * \frac{a}{2} + 1 * \frac{a}{2} + 0 * 1 = a$). $\square$

1.4 Orthogonale Basis

Definition 27 (Def 5). Eine Basis $(e_1, \ldots, e_n)$ eines quadratischen Moduls (V, Q) heißt *orthogonal*, wenn ihre Elemente paarweise orthogonal sind,
d.h. $V = ke_1 \hat{\oplus} \ldots \hat{\oplus} ke_n$. Das bedeutet, dass die Matrix von Q Diagonalform hat:

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

Ist $x = \sum x_i e_i$, so ergibt sich $Q(x) = a_1 x_1^2 + \ldots + a_n x_n^2$.

Theorem 28 (Orthogonaler Basisergänzungssatz, Thm 1). Jeder quadratische Modul hat eine orthogonale Basis.

Beweis. Wir unterscheiden nach Isotropie von V.

1. Fall: V isotrop: V isotrop $\Rightarrow Q(x) = x \cdot x = 0 \quad \forall x$
   $\Rightarrow Q(x + y) = 0 \quad \forall x, y \Rightarrow x \cdot y = 0 \quad \forall x, y$
   $\Rightarrow$ alle Basen von V sind orthogonal.

2. Fall: V nicht isotrop: Induktion über $n = dim(V)$.

   Basis: $n = 0$ ist trivial (0-Basis ist 0).

   Schritt:

   Annahme: Alle (U, Q) mit $dim(U) \leq n-1$ haben orthogonale Basis.

   Schluss: Wähle $e_1 \in V$ mit $e_1 \cdot e_2 \neq 0$. $H = (ke_1)^{\perp}$ ist eine Hyperebene (18) [1.2 Prop 2 (4)] und da $e_1 \notin H$ folgt $V = ke_1 \hat{\oplus} H$. Nach Induktionsannahme hat H eine orthogonale Basis $(e_2, \ldots, e_n)$, damit ist $(e_1, \ldots, e_n)$ orthogonale Basis von V.

$\square$

Definition 29 (Verwandtschaft, Def 6). Zwei orthogonale Basen $e = (e_1, \ldots, e_n)$ und $e' = (e'_1, \ldots, e'_n)$ von V heißen *verwandt* (angrenzend, berührend, contiguous), wenn $\exists i, j \in \{1, \ldots, n\}$ mit $e_i = e'_j$.

Theorem 30 (Entfernte Verwandtschaft, Thm2). Sei (V, Q) ein quadratischer Modul mit $dim(V) \geq 3$ und seien $e = (e_1, \ldots, e_n)$ und $e' = (e'_1, \ldots, e'_n)$ zwei orthogonale Basen von V.

$\Rightarrow \exists$ eine endliche Folge $e^{(0)}, e^{(1)}, \ldots, e^{(m)}$ von orthogonalen Basen von V mit $e^{(0)} = e, e^{(m)} = e'$ und $e^{(i)}$ grenzt an $e^{(i+1)} \quad \forall 0 \leq i < m$. Es bezeichne $(e^{(0)}, \ldots, e^{(m)})$ eine solche Kette orthogonaler Basen, die e und e' angrenzend verbinden.

Beweis. Wir unterscheiden, ob (V, Q) ausgeartet ist:

(V, Q) ausgeartet: (V, Q) ausgeartet $\Leftrightarrow \exists 0 \neq b \in V^\perp \Rightarrow \exists e_i$ und e'_j so dass $e^{(1)} = (e_1, \ldots, b_i, \ldots, e_n)$ und $e^{(2)} = (e'_1, \ldots, b_j, \ldots, e'_n)$ Basis. Da $b \in V^\perp \Rightarrow$ sogar orthonormale Basis $\Rightarrow e \to e^{(1)} \to e^{(2)} \to e'$.

(V, Q) nicht ausgeartet: $\to \forall i \in \{1, \ldots n\} : (e_i \cdot e_i) \neq 0$. (Matrix

$$A = \begin{pmatrix} e_1e_1 & 0 & \ldots & 0 \\ 0 & e_2e_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & e_ne_n \end{pmatrix}, det(A) \neq 0).$$

1. Fall: Sei die Ebene $P = ke_1 + ke'_1$ nicht ausgeartet. Dann sind e_1 und e'_1 linear unabhängig und:

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

Es existieren (nach (28) [1.4 Thm 1]) ε_2 und ε'_2 so, dass

$$P = ke_1 \hat{\oplus} k\varepsilon_2 \text{ und } P = ke'_1 \hat{\oplus} k\varepsilon'_2.$$

Sei $H = P^\perp$. Da P nicht ausgeartet ist, folgt nach (18) [Prop 2], dass $V = H \hat{\oplus} P$. Sei $(e''_3, \ldots, e''_n)$ eine orthogonale Basis von H. Somit erhält man eine verbindende Kette:

$$e \to (e_1, \varepsilon_2, e''_3, \ldots, e''_n) \overset{n \geq 3}{\to} (e'_1, \varepsilon'_2, e''_3, \ldots, e''_n) \to e'.$$

2. Fall:

$$(e_1 \cdot e_1)(e_2' \cdot e_2') - (e_1 \cdot e_2')^2 \neq 0$$

Analog zum 1. Fall durch Vertauschen von e_1' mit e_2'.

3. Fall:

$$(e_1 \cdot e_1)(e_i' \cdot e_i') - (e_1 \cdot e_i')^2 = 0 \quad i = 1, 2$$

Die Ebene P ist also ausgeartet. Wir unterbrechen den Beweis für ein Lemma:

□

Lemma 31. Es existiert $x \in k$ mit $e_x = e_1' + xe_2'$ nicht isotrop und $E = ke_1 \hat{\oplus} ke_x$ nicht ausgeartete Ebene.

Beweis. Zwei Bedingungen müssen erfüllt sein:

(a) e_x nicht isotrop,

(b) $e_x \cdot e_1$ bilden n.a. Ebene.

Damit nicht isotrop (a) erfüllt ist, muss gelten:

$$e_x \cdot e_x = e_1' \cdot e_1' + x^2(e_2' \cdot e_2') \overset{!}{\neq} 0 \tag{1}$$

Damit e_x, e_1 eine nicht-ausgeartete Ebene bilden (b), muss gelten:

$$(e_1 \cdot e_1)(e_x \cdot e_x) - (e_1 \cdot e_x)^2 \overset{!}{\neq} 0 \tag{2}$$

Also muss auch die Einsetzung (1) in (2) gelten:

$$\begin{aligned}
&(e_1 \cdot e_1)(e_1' \cdot e_1') + (e_1 \cdot e_1)(e_2' \cdot e_2')x^2 - (e_1 \cdot e_x)^2 \\
&= (e_1 \cdot e_1)(e_1' \cdot e_1') + (e_1 \cdot e_1)(e_2' \cdot e_2')x^2 - (e_1 \cdot (e_1' + xe_2'))^2 \\
&= (e_1 \cdot e_1)(e_1' \cdot e_1') + (e_1 \cdot e_1)(e_2' \cdot e_2')x^2 - ((e_1 \cdot e_1') + x(e_1 \cdot e_2'))^2 \\
&= (e_1 \cdot e_1)(e_1' \cdot e_1') + (e_1 \cdot e_1)(e_2' \cdot e_2')x^2 \\
&- ((e_1 \cdot e_1')^2 + 2x(e_1 \cdot e_1')(e_1 \cdot e_2') + x^2(e_1 \cdot e_2')^2) \\
&\overset{Orthog.}{=} (e_1 \cdot e_1)(e_1' \cdot e_1') + (e_1 \cdot e_1)(e_2' \cdot e_2')x^2 \\
&- (e_1 \cdot e_1)(e_1' \cdot e_1') - 2x(e_1 \cdot e_1')(e_1 \cdot e_2') - x^2(e_1 \cdot e_1)(e_2' \cdot e_2') \\
&= -2x(e_1 \cdot e_1)(e_1 \cdot e_2') \overset{!}{\neq} 0.
\end{aligned} \tag{3}$$

Da wegen Orthogonalität auch $(e_1 \cdot e_1)(e_i' \cdot e_i') - (e_1 \cdot e_i')^2 = 0$ gilt und soeben gezeigt, dass gelten muss $e_1 \cdot e_1 \neq 0$, sowie $e_i' \cdot e_i' \neq 0$, folgt also $(e_1 \cdot e_i')^2 = c \neq 0$, somit insbesondere: $(e_1 \cdot e_1') \neq 0 \neq (e_1 \cdot e_2')$. (1) und (3) ergeben die Bedingungen $x^2 \neq -(e_1' \cdot e_1')/(e_2' \cdot e_2')$ und $x \neq 0$, damit e_x die gewünschten Eigenschaften hat. Somit werden maximal 3 Werte für x festgelegt. Ist nun $char(k) \geq 4$, so finden wir sicher ein $x \in k$, mit welchem die Behauptungen für e_x erfüllt sind, also ist das Lemma bewiesen.

Fall $k = \mathbb{F}_3$ ($\mathbb{F}_2$ nicht, wegen $char(k) \neq 2$): Hier sind $1^2 = 1$ und $2^2 = 1$, also kann die Bedingung von Fall 3 geschrieben werden als $(e_1 \cdot e_1)(e_i' \cdot e_i') = (e_1 \cdot e_i')^2 = 1 \text{für} i = 1, 2$. Daher also $(e_1' \cdot e_1')/(e_2' \cdot e_2') = 1$ und damit genügt z.B. als Zeuge $x = 1$, d.h. $e_{x=1} = e_1' + e_2'$ erfüllt die Bedingung: $x^2 \neq -(e_1' \cdot e_1')/(e_2' \cdot e_2') = -1 = 2$. □

Zurück zum Beweis von Fall 3 in (30) [Thm 2]:

Beweis. Wähle $e_x = e_1' + xe_2'$ wie im Lemma. e_x ist nicht isotrop, also existiert e_2'', so dass $(e_x \cdot e_2'')$ eine Orthogonalbasis von $ke_1' + ke_2'$ ist. Mit dem Basisergänzungssatz (28) [1.4 Thm 1] folgt: $e'' = (e_x, e_2'', e_3', \ldots, e_n')$ Orthogonalbasis von V. □

$ke_1 + ke_x$ ist eine nicht ausgeartete Ebene (Lemma!), deshalb folgt mit Fall 1, dass man e und e'' in einer Kette angrenzend verbinden kann. Da e' und e'' angrenzend sind $\Rightarrow$ Behauptung.

1.5 Satz von Witt

Bemerkung 32 (Motivation). Seien (V, Q) und (V', Q') zwei nicht-ausgeartete quadratische Moduln, $U \subset V$ Unterraum und sei $s : U \Rightarrow V'$ ein injektiver Morphismus von U nach V'. Wir wollen versuchen, s auf einen größeren Raum als U — womöglich ganz V— zu erweitern.

Lemma 33 (Wittsche Erweiterbarkeit für ausgeartete Moduln). Wenn U ausgeartet ist, können wir s zu einem injektiven Morphismus $s_1 \colon U_1 \to V'$ erweitern, wobei U_1 den Unterraum U als Hyperebene enthält, also $s_1|U = s$, wobei $dim(U_1) = 1 + dim(U)$.

Beweis. Da U ausgeartet $\exists x \in rad(U), x \neq 0$ ($\Rightarrow x$ insbes. isotrop). Sei $U = U' \oplus kx$. Nach (25) [Prop 3+]: $\exists y \in V$, so dass $y \cdot y = 0, x \cdot y = 1, y \in U'^{\perp} \setminus U^{\perp}$. Da s ein metr. Morphismus ist, gilt $\forall u \in U : s(x) \cdot s(u) = x \cdot u = 0$, d.h. $s(x) \in rad(s(U))$. Sei $s(U) = ks(x) \oplus s(U')$. Nach (25) [Prop 3+] $\exists y' \in V'$ mit $y' \cdot y' = 0, s(x) \cdot y' = 1, y' \in s(U')^{\perp} \setminus s(U)^{\perp}$.

Definiere s_1:
$s_1 : U \oplus ky \to V$:
$u + \alpha y \mapsto s(u) + \alpha y'$
s_1 erfüllt das Lemma, denn:

s_1 injektiv klar (s injektiv, $y' \notin s(U)$),

s_1 linear klar (s ist linear),

s_1 Morphismus (Erhaltung des Skalarprodukts): Sei $(u + \alpha y) \in U \oplus ky$:

Skalarprodukt des Bildes:
$s_1(u + \alpha y) \cdot s_1(u + \alpha y)$
$\overset{\text{Def. } s_1}{=} (s(u) + \alpha y') \cdot (s(u) + \alpha y')$
$= s(u) \cdot s(u) + 2\alpha(s(u) \cdot y') + \alpha^2(y' \cdot y') \overset{y' \text{isotr.}}{=} u \cdot u + 2\alpha(s(u) \cdot y')$
$\overset{u=\tilde{u}+\beta x}{=} u \cdot u + 2\alpha(s(\tilde{u} + \beta x) \cdot y') =$
$u \cdot u + 2\alpha(s(\tilde{u}) \cdot y') + 2\alpha\beta(s(x) \cdot y')$
$\overset{y' \in s(U')^\perp \text{ und } s(x) \cdot y' = 1 \text{ nach Def.}}{=} u \cdot u + 2\alpha\beta.$

Skalarprodukt des Urbildes:
$(u + \alpha y) \cdot (u + \alpha y)$
$= u \cdot u + 2\alpha(u \cdot y) + \alpha^2(y \cdot y)$
$\overset{\text{wie oben}}{=} u \cdot u + 2\alpha((\tilde{u} + \beta x) \cdot y)$
$= u \cdot u + 2\alpha(\tilde{u} \cdot y) + 2\alpha\beta(x \cdot y) = u \cdot u + 2\alpha\beta$

□

Theorem 34 (Wittsche Erweiterbarkeit für beliebige Moduln, Thm 3). Seien (V, Q) und (V', Q') zwei nicht ausgeartete quadratische Moduln, $U \subset V$ Unterraum und sei $s\colon U \to V'$ ein injektiver metrischer Morphismus. Dann kann s zu einem Isomorphismus $s+\colon V \to V'$ erweitert werden.

Beweis. Da $V \cong V'$, können wir annehmen, dass $V = V'$. Mit (33) wurde bereits der ausgeartete Fall behandelt. Noch zu zeigen, dass die Erweiterbarkeit auch gilt, wenn U nicht ausgeartet ist. Dazu Beweis durch Induktion über $dim(U)$:

Basis: $dim(U) = 1 \Rightarrow U =< x >, x \cdot x \neq 0$ (da n.a.). Sei $y = s(x) \Rightarrow y \cdot y = x \cdot x$. Entweder $x + y$ nicht isotrop ($\varepsilon = 1$) oder $x - y$ nicht isotrop ($\varepsilon = -1$),

denn sonst:

$(x+y)\cdot(x+y) = x\cdot x + 2x\cdot y + y\cdot y = 2x\cdot x + 2x\cdot y$
$(x-y)\cdot(x-y) = x\cdot x - 2x\cdot y + y\cdot y = 2x\cdot x - 2x\cdot y$
Addition der beiden Zeilen gibt: $4x\cdot x = 0$, also $x\cdot x = 0$ $\Leftrightarrow$

Wähle ε dementsprechend aus $\{-1,+1\}$. $z := x+\varepsilon y; H = (kz)^{\perp}$
$\Rightarrow V = kz\hat{\oplus}H$.

Wir definieren σ als Spiegelung am Unterraum H, d.h. als Automorphismus von V, der die Identität auf H ist, und der z in $-z$ umwandelt.

$$\sigma : V \to V, kz\hat{\oplus}H \to kz\hat{\oplus}H, \alpha z + h \mapsto -\alpha z + h$$

$$\begin{aligned} &x-\varepsilon y \in H : (\sigma(x+\varepsilon y)\cdot(x-\varepsilon y) \\ &= \sigma[(x\cdot x) - \varepsilon(x\cdot y) + \varepsilon(y\cdot x) - (y\cdot y)] = 0 \\ &\Rightarrow x-\varepsilon y \in H \perp x+\varepsilon y \in z \\ &\Rightarrow \sigma(x-\varepsilon y) = x-\varepsilon y, \sigma(x+\varepsilon y) = -x-\varepsilon y. \qquad (*) \end{aligned}$$

Somit $\sigma(x) = -\varepsilon y$, da

$$\begin{aligned} &\sigma(x-x+\varepsilon y) \overset{\text{lin.}}{=} \sigma(x) - \sigma(x-\varepsilon y) \overset{(*)}{=} \sigma(x) - x + \varepsilon y \qquad (**) \\ &= \sigma(-x) + \sigma(x+\varepsilon y) = -\sigma(x) - x - \varepsilon y \qquad (***) \end{aligned}$$

Durch Gleichsetzen der rechten Terme in (**) und (***): $2\sigma(x) = -2\varepsilon y$.

Damit ist $-\varepsilon\sigma$ eine geeignete Erweiterung von s auf $s+$:
(Linearität und Injektivität sind klar, $-\varepsilon\sigma \mid U = s$ klar, da $-\varepsilon\sigma(x) = y = s(x)$). Morphismus (Erhaltung des Skalarprodukts) klar mit
$Q'(-\varepsilon\sigma(\alpha z+h)) = (-\varepsilon\sigma(\alpha z+h))\cdot(-\varepsilon\sigma(\alpha z+h)) = (\varepsilon\alpha z-\varepsilon h)\cdot(\varepsilon\alpha z-\varepsilon h) = \varepsilon^2(\alpha z-h)\cdot(\alpha z-h) = (\alpha z-h)\cdot(\alpha z-h) \overset{kz\perp H}{=} (\alpha z+h)\cdot(\alpha z+h) = Q(\alpha z+h)$.

Schritt: $dim(U) > 1$

Induktionsannahme: $U = U_1\hat{\oplus}U_2$ mit $U_1 \neq 0 \neq U_2$, σ_1 bezeichne die Erweiterung auf V von $s_1 = s|U_1$, dies ist ein Automorphismus auf V.

Schluss:

Betrachte jetzt $\tilde{s} = \sigma_1^{-1} \circ s$:

$$\Rightarrow \tilde{s}|U_1 = id|U_1 \text{ klar}$$
$$\Rightarrow \tilde{s}|U_2 \colon U_2 \to V_1 = U_1^{\perp}$$
$$\text{denn } \tilde{s}(u_2 \cdot u_1) = \tilde{s}(u_2) \cdot \tilde{s}(u_1) = u_2 \cdot u_1 = 0.$$

Wähle nun σ_2 als Erweiterung von $\tilde{s}|U_2$ auf V, die s ist nach Induktionsannahme ein Automorphismus auf V ($U_2 \subset V_1$ wg. $U = U_1 \hat{\oplus} U_2$). Wähle nun als Erweiterung von $\tilde{s}|U$

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

klar: σ linear und injektiv, σ Morphismus
$Q'(\sigma(u+v)) = \sigma(u+v) \cdot \sigma(u+v) = (u + \sigma_2(v)) \cdot (u + \sigma_2(v)) = u \cdot u + 2u \cdot \sigma_2(v) + \sigma_2^2(v) = u \cdot u + 0 + v \cdot v = (u+v) \cdot (u+v) = Q(u+v)$.
Damit ist $\sigma_1 \circ \sigma$ eine geeignete Erweiterung von s auf $s+$: σ_1 metr. Isomorphismus auf V und $\sigma_1 \circ \sigma \mid U = s$.

□

Korollar 35. $U \cong W$ Unterräume von (V, Q) nicht ausgeartete quadratische Moduln: $\Rightarrow U^{\perp} \cong W^{\perp}$.

Beweis. Die Einschränkung $\sigma \mid U = s \colon U \to W$ ist injektiver metrischer Unterraumisomorphismus, nach (34) [1.4 Thm 3] ist die Erweiterung auf ganz V: $\sigma \colon V \to V$ metrischer Isomorphismus, also auch die Einschränkung $\sigma \mid U^{\perp} \colon U^{\perp} \to W^{\perp}$ metrischer Isomorphismus. □

Bemerkung 36 (Wittscher Kürzungssatz). $V \hat{\oplus} W \cong V' \hat{\oplus} W'$, $V \cong V' \Rightarrow W \cong W'$ wird als *Wittscher Kürzungssatz* bezeichnet.

1.6 Übertragungen

Nachdem wir seit Abschnitt 1.2 alles aus der Modul-/ VR-Sicht betrachtet haben, wollen wir uns nun einige Ergebnisse in die (historisch ursprünglicheren) Form-/ Polynomsicht übertragen. Wir führen einen Äquivalenzbegriff quadratischer Formen ein, den wir dann zur Klassifikation verwenden können. Aus diesem und

den Ergebnissen der vorausgehenden Abschnitte können wir dann insbesondere einen Serviervorschlag für die mundgerechtere Zerlegung quadratischer Formen gewinnen.

Erinnerung 37 (Homogene Polynome haben symmetr. darst. Matrix). Matrix $\rightarrow$ Form: Eine symmetrische $n * n$ Matrix $A = (a_{ij})$ bestimmt eine Form f in n Variablen durch

$$f(X_1, \ldots, X_n) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i,j=1}^{n} a_{i<j} X_i X_j.$$

Form $\rightarrow$ Matrix: Eine quadratische Form in n Variablen über k bestimmt eine symmetrische Matrix, denn die bei naiver Verwendung einer vollständig ausmultiplizierten und termweise zusammengefaßten Form auftretende "untere Dreiecksmatrix" können wir durch Gleichsetzen von $a_{ij} = a_{ji}$ auch so balancieren, dass die Matrix $A = (a_{ij})$ symmetrisch ist.

Beispiel 38 (Def 4'). Wir kennen bereits einen Vertreter einer *hyperbolischen Form* in zwei Variablen, und zwar:

$$f(X_1, X_2) = 2 * X_1 X_2,$$

denn dies ist die Form zu der Matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ aus (20) [1.3 Def 4].

Erinnerung 39 (Modul). Das Paar (k^n, f) ist ein quadratischer Modul, der zu f (oder ihrer Matrix A) *assoziiert* ist, siehe auch (5).

Definition 40 (Def 7). Zwei quadratische Formen f und f' sind *äquivalent*, genau dann wenn die assoziierten Moduln isomorph sind: $f \sim f' \Leftrightarrow (k^n, f) \cong (k'^n, f')$. Bemerkung: In der Praxis ist $k = k'$. Kongruenzen verschiedener k, etwa $(\mathbb{R}^2, 0) = (\mathbb{F}_5^2, 0)$ sind uninteressant. Durch Betrachtung der Transformationsmatrizen X vergewissert man sich, dass die derart definierte Äquivalenzrelation reflexiv (Identität), transitiv (Matrizenmultiplikation) und symmetrisch ist (Inverse).

Bemerkung 41. Ist A Matrix von f, A' Matrix von f', so $f \sim f' \Leftrightarrow A' = X * A * X^t$ mit nicht-ausgearteter Matrix X, siehe auch (10) [1.1].

Beispiel 42. Ein Modul (k^2, f) ist eine hyperbolische Ebene, genau dann wenn: $f \overset{(38)}{\sim} 2 * X_1 X_2 \overset{(a)}{\sim} X_1 X_2 \overset{(b)}{\sim} X_1^2 + X_2^2$

(a) :

$$\begin{pmatrix} 0 & \frac{1}{2} \\ 1 & 0 \end{pmatrix} * \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} * \begin{pmatrix} 0 & 1 \\ \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}.$$

(b) :

$$\begin{pmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & -1 \end{pmatrix} * \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} * \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definition 43 (Def 7 ctd). Seien $f_1(X_1, \ldots, X_n)$ und $f_2(X_1, \ldots, X_m)$ zwei quadratische Formen, so werden wir mit $f_1 \overset{\circ}{+} f_2$ oder — falls keine Verwechslungsgefahr besteht — auch $f_1 + f_2$ die quadratische Form

$$f_1(X_1, \ldots, X_n) \overset{\circ}{+} f_2(X_{n+1}, \ldots, X_{n+m})$$

in $n + m$ Variablen bezeichnen. Das ist also genau die *orthogonale Summe* aus (15) [1.2 Def 2], die Operation $\overset{\circ}{+}$ ist kommutativ. Für $f \overset{\circ}{+} (-g)$ verwenden wir analog $\overset{\circ}{-}$. Beachte: um Variableneinfang zu vermeiden, kann es in der zweiten Form notwendig sein, Variablen zuvor geeignet umzubennen, Bsp. $f(X) = X^2$, $g(X) = X^2$, dann $f \overset{\circ}{+} g(X, Y) = X^2 + Y^2$.

Definition 44. Eine Form $f(X_1, \ldots, X_n)$ *stellt* ein Element a von k *dar*, $f\ repr\ a$, genau dann wenn es ein $x \in k^n$ gibt, $x \neq 0$, so dass $f(x) = a$ ("verallgemeinertes Wurzelziehen"). (Bsp. $(Q, V) = (\mathbb{F}_5, X^2)$: 1 wird dargestellt, 2 nicht.) Durch die Einschrankung $x \neq 0$ wird die 0 nur genau dann dargestellt, wenn der zugehörige quadratische Modul auch ein isotropes Element enthält.

Theorem 45 (Übertragung: Darstellung der $0 \Rightarrow$ Abspaltung einer hyperbolischen Ebene, Prop 3'). $f\ n.a.\ repr\ 0 \Rightarrow f \sim f_2 \overset{\circ}{+} g$ mit f_2 hyperbolische Ebene.

Beweis. f n.a. $\Rightarrow (k^n, f)$ n.a.

$f\ repr\ 0 \Rightarrow \exists x \in k^n : f(x) = 0$ (isotr. Element)
$\overset{(24)\ [1.3\ \text{Prop}\ 3]}{\Rightarrow} (k^2, f^2) \subset (k^n, f)$ (Unterraum, hyperbolische Ebene) $\overset{(25)\ [1.3\ \text{Prop}\ 3+]}{\Rightarrow}$ $(k^n, f) \cong (k^2, f_2) \oplus (k^{n-2}, g)$. Wähle Basen von (k^{n-2}) und (k^n) und wende f an. $\Rightarrow f \sim f_2 + g$. □

Theorem 46 (Übertragung: Darstellung der $0 \Rightarrow$ Bijektion, Prop 3' ctd).

$$f \text{ n.a. } repr\ 0 \Rightarrow \forall x \in k : f\ repr\ x$$

.

Beweis. f n.a. $repr\ 0 \overset{(38)\ [1.6\ \text{Def 4'}]}{\Rightarrow} (k^n, f)$ n.a. $\wedge\ \exists v \neq 0 : f(v) = 0$ (in (k^n, f) existiert isotroper Vektor!)
$\overset{(26)\ [1.3\ \text{Cor zu Prop 3}]}{\Rightarrow} \forall x \in k\ \exists v \in k^n : f(v) = x \overset{(38)\ [1.6\ \text{Def 4'}]}{\Rightarrow} \forall x \in k : f\ repr\ x.$ □

Theorem 47 (Zerlegung quadratischer Formen in Summen von Quadraten, Thm 1'). Sei f eine quadratische Form in n Variablen. Dann existieren $a_1, \ldots, a_n \in k$, so dass $f \sim a_1X^2 + \ldots + a_nX_n^2$.

Beweis. Der zu f assoziierte Modul (k^n, f) hat nach (28) [1.4 Thm 1] eine orthogonale Basis. $(k^n, f) \cong (ke_1 \hat{\oplus} \ldots \hat{\oplus} ke_n, f)$, $v = a_1e_n, \ldots, a_ne_n$. $f(v) = v \cdot v = \sum a_{ij}(e_i \cdot e_j) \overset{Orthogonalbasis}{=} \sum_{i=1}^n a_{ii}^2 * (e_i \cdot e_i) \Rightarrow f(X) = \sum_{i=1}^n (e_i \cdot e_i)X_i^2$. □

Die Existenz einer orthogonalen Basis zeigt auch, dass die hiermit berechnete Diskriminante $disc(f) = a_{11} * \ldots * a_{nn} \neq 0$.

Definition 48. Der *Rang von* f ist die Anzahl der Indizes i, so dass $a_i \neq 0$.

Korollar 49 (Abspaltung und Neutralisation eines Quadrates, Cor 1). Sei $g = g(X_1, \ldots, X_{n-1})$ eine nicht ausgeartete quadratische Form und sei $a \in k^*$. Dann sind äquivalent:

1. $g\ repr\ a$ (g Form in $n-1$ Variablen).
2. $g \sim h \overset{\circ}{+} aZ^2$ (h Form in $n-2$ Variablen, aZ^2 Form einer Variable).
3. $f = g \overset{\circ}{-} aZ^2\ repr\ 0$ (f Form in n Variablen).

Beweis. Sei (k^{n-1}, g) der zu g assoziierte Modul.

(2) $\Rightarrow$ (1): $g(X_1, \ldots, X_{n-1}) \sim h(X_1, \ldots, X_{n-2}) \overset{\circ}{+} aZ^2$. Erinnerung: $f \sim g$: f und g stellen dieselben Werte aus dem Grundkörper dar. $h(0, \ldots, 0) + aZ^2(1) = a$.

(1) $\Rightarrow$ (2): $g\ repr\ a \overset{(38\ [1.6\ \text{Def 4'}])}{\Rightarrow} \exists v \in (k^{n-1}, g) : g(v) = a$. Sei $H = (kv)^\perp$. $\overset{(28)\ [1.4\ \text{Thm 1}]}{\Rightarrow} H = kv_1 \hat{\oplus} \ldots \hat{\oplus} kv_{n-2}, y \in H = \sum_{i=1}^{n-2} \alpha_i v_i, g(y) = \sum_{i=1}^{n-2} \alpha_i^2 g(v_i), h = \sum_{i=1}^{n-2} g(v_i)X_i^2. H \hat{\oplus} kv = (k^{n-1}, h) \hat{\oplus} (k, aZ^2) \overset{(43)\ [1.6\ \text{Def 7}]}{\Rightarrow} g \sim h \overset{\circ}{+} aZ^2$.

(1) $\Rightarrow$ (3): $g\ repr\ a \Rightarrow \exists v \in k^{n-1} : g(v) = a. f(v, 1) = g(v) - a = 0$.

(3) $\Rightarrow$ (1): $f \sim g \overset{\circ}{-} aZ^2\ repr\ 0 \Rightarrow \exists v \in k^n, z \in k, (v,z) \neq 0, g\ repr\ aZ^2(z)$, betrachte z, entweder $z = 0$ oder $z \neq 0$:

Fall $z = 0$: $v \neq 0$ und $g(v) = 0$, $\overset{(45)\text{ [Prop 3'] isotr. Vektor}}{\Rightarrow} g\ repr\ a$.

Fall $z \neq 0$: $f(v,z) = 0 = g(v) - az^2 \Rightarrow az^2 = g(v) \Rightarrow$
$a = \frac{1}{z^2} g(v)$
$\overset{(g \text{ bilinear})}{=} g(\frac{1}{z} v)$
$\overset{(k \text{ Körper})}{=} g(x_1/z, \ldots, x_{n-1}/z) \overset{(38\text{ [1.6 Def 4']})}{\Rightarrow} g\ repr\ a$.

□

Korollar 50 (Cor 2, Lösbarkeit, Vorbereitung für Cor zu 2.2 Thm 6). Seien g und h zwei nicht ausgeartete Formen von Rang ≥ 1 und sei $f = g \overset{\circ}{-} h$. Dann sind äquivalent:

1. $f\ repr\ 0$.
2. $\exists a \in k^* : g\ repr\ a, h\ repr\ a$.
3. $\exists a \in k^* : g \overset{\circ}{-} aZ^2\ repr\ 0, h \overset{\circ}{-} aZ^2\ repr\ 0$.

Beweis. (2) $\Leftrightarrow$ (3) folgt aus der Anwendung (49) [1.6 Cor 1] (1) $\Leftrightarrow$ (3), je einmal auf g, h.

(2) $\Rightarrow$ (1) $\exists a \in k^*, \exists v_1 \in k^m, v_2 \in k^{n-m} : a = g(v_1) = h(v_2) \Rightarrow f(v_1, v_2) = g(v_1) - h(v_2 = a - a = 0, (v_1, v_2 \neq 0$, da $v_1 \neq 0$ und $v_2 \neq 0)$.

(1) $\Rightarrow$ (2) $f(X_1, \ldots, X_n), g(X_1, \ldots, X_m), h(X_{m+1}, \ldots, X_n) \Rightarrow \exists x \in k^m, y \in k^{n-m} : (x,y) \neq 0 \Rightarrow 0 = f(x,y) = g(x) - h(y) =: a$.

Fall $a = g(v_1) = h(v_2) \neq 0$: Wir nehmen dieses a als Zeugen für die Behauptung.

Fall $b := g(v_1) = h(v_2) = 0$: (Bem.: In diesem Fall sind v_1 und v_2 also isotrope Vektoren). O.E. $x \neq 0 \Rightarrow g\ repr\ 0 \overset{\text{[1.6 Prop 3']}}{\Rightarrow} \forall y \in k^* : g\ repr\ y$. Da h n.a. $\exists y \in k^{n-m}, a \in k^* : h(y) = a \overset{a \in k^*}{\Rightarrow} h\ repr\ a, g\ repr\ a$.

□

Theorem 51 (Kürzungssatz von Witt, Thm 4). Seien $f = g \overset{\circ}{+} h$ und $f' = g' \overset{\circ}{+} h'$ zwei n.a. quadratische Formen: $f \sim f' \wedge g \sim g' \Rightarrow h \sim h'$.

Beweis. $(k^n, f) \overset{\text{(16) [1.2 Def 2]}}{\cong} (k^m, g)\hat{\oplus}(k^{n-m}, h)$, $(k^n, f') \cong (k^m, g')\hat{\oplus}(k^{n-m}, h')$ und $(k^m, g') \cong (k^m, g) \overset{\text{(36) [1.5 Thm 3, Witt]}}{\Rightarrow} (k^{n-m}, h) \cong (k^{n-m}, h')$. □

Korollar 52 (Spalten, solange $h\ repr\ 0$). Wenn f nicht ausgeartet ist, so ist

$$f \sim g_1 \overset{\circ}{+} \ldots \overset{\circ}{+} g_m \overset{\circ}{+} h,$$

wobei $g_1, \ldots g_m$ hyperbolische Formen (38) [1.6 Def 4'] sind und h nicht $repr\ 0$. Diese Zerlegung ist bis auf Isomorphie eindeutig.

Beweis. Existenz: Wende (45) [1.6 Prop 3'] so lange an, wie $h\ repr\ 0$ (sei dabei m die Anzahl der dabei abgespaltenen hyperbolischen Formen). Die Eindeutigkeit folgt aus m-maliger Verwendung von (51) [1.6 Thm 4, Witt]. □

Bemerkung 53. Die Zahl $2 * m$ wird auch als die *Dimension der maximal isotropen Unterräume* des zu f assoziierten q.M. bezeichnet.

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

Erinnerung 54. p Primzahl $\neq 2$ und $q = p^f$ Potenz von $p \Rightarrow \mathbb{F}_q$ ist Körper mit q Elementen.

Theorem 55 (Prop 4). Eine quadratische Form über $\mathbb{F}_q$ von Rang ≥ 2 stellt alle Elemente von $\mathbb{F}_q^*$ dar. Eine Form vom Rang ≥ 3 stellt zusätzlich die 0 dar.

Beweis. Rang 2: Zu zeigen, dass

$$g(x,y) = h(x) \overset{\circ}{+} i(y)\ repr\ c, \text{ mit } h(x) = ax^2, i(y) = by^2$$

eine Lösung hat, mit $a \neq 0$, $b \neq 0$, $c \neq 0$.

Sei $A = \{\alpha \in F_q \mid \alpha = ax^2\}$, sei $B = \{\alpha \in F_q \mid \alpha = c - bx^2\}$.

$ord(\mathbb{F}_q^*) \overset{<\beta>:=\mathbb{F}_q^*}{=} q-1 \overset{char(\mathbb{F}_q)\neq 2}{\Rightarrow} 2|(q-1) \Rightarrow ord(\mathbb{F}_q^{*^2}) \overset{\mathbb{F}^{*^2}_q = <\beta^2>}{=} \frac{q-1}{2}$

$|\mathbb{F}_q^{*^2} \cup 0| = \frac{q-1}{2} + 1 = \frac{q+1}{2}$.

$\overset{\text{Multiplikation mit } a, b, \text{ Subtraktion } c - bx^2 \text{ über } \mathbb{F}_q \text{ bijektiv}}{\Rightarrow} |A| = |B| = \frac{q+1}{2}$

$\overset{Schubfachprinzip}{\Rightarrow} A \cap B \neq \emptyset$.

Aus der Existenz der Lösung c folgt:

$\Rightarrow \forall c \in \mathbb{F}_q^* : g(x,y)\ repr\ c$.

Rang 3: Sei $f \sim g \overset{\circ}{-} j(z)$. Da $g\ repr\ c$ (Rang 2) $\overset{\text{(49) [1.6 Cor 1] (1)⇒(3)}}{\Rightarrow}$ $f\ repr\ 0$.

□

Bemerkung 56. Alternativ (aufwändig, aber mit Wiedererkennungseffekt): verwende hier ein Korollar des Satzes von Chevalley-Warning [2] (bei [4] in 1.2) der Form: das Polynom $f = aX^2 + bY^2 + cZ^2 \in \mathbb{F}_p[X, Y, Z]$ hat eine nichttriviale Nullstelle. Dies ist die Aussage für Rang ≥ 3. Mit (49) [1.6 Cor 1] (3)⇒(1) folgt auch die Aussage des Satzes für $n \geq 2$.

Theorem 57 (Prop 5). Seien $a, b, c \in \mathbb{F}_q^*, a \notin \mathbb{F}_q^{*^2}$. Sei f n.a. quadratische Form von Rang n über $\mathbb{F}_q$. Dann gilt einer der beiden Fälle:

Fall 1: $f \sim X_1^2 + \ldots + X_{n-1}^2 + X_n^2 \Leftrightarrow disc(f) \equiv 1 \mod \mathbb{F}_q^{*^2}$,

Fall 2: $f \sim X_1^2 + \ldots + X_{n-1}^2 + aX_n^2 \Leftrightarrow disc(f) \not\equiv 1 \mod \mathbb{F}_q^{*^2}$.

Beweis. Induktion über Rang n.

Basis $n = 1$: Sei f n.a. q.F. von Rang 1.

Fall 1: $f \sim bX^2, b \in \mathbb{F}_q^{*^2} (\exists c : b = c^2) \Leftrightarrow f \sim bX^2 \sim X^2 \Leftrightarrow disc(f) \equiv 1 \mod \mathbb{F}_q^{*^2}$.

Fall 2: $f \sim bX^2, b \notin \mathbb{F}_q^{*^2}$, sei $b := c^2 * a \Leftrightarrow f \sim bX^2 \sim aX^2 \Leftrightarrow disc(f) \equiv a \mod \mathbb{F}_q^{*^2} \overset{a \notin \mathbb{F}_q^{*^2}}{\Leftrightarrow} disc(f) \not\equiv 1 \mod \mathbb{F}_q^{*^2}$.

Schritt $n - 1 \to n$: Sei f n.a. q.F. von Rang $n \geq 2$.

Hypothese (IH): $\forall g \in G := \{g \mid g \text{ n.a. quadr. Form}, rank(g) = n - 1\} : g \sim bX_1 + \ldots + X_{n-1}$. $disc(g) \in \mathbb{F}_q^*/\mathbb{F}_q^{*^2}$.

Schluss: $rank(f) \geq 2 \overset{\text{(55) [1.7 Prop 4]}}{\Rightarrow} f\ repr\ 1 \overset{\text{(49) [1.6 Cor 1] (1)⇒(2), a=1}}{\Rightarrow} \exists g \in G : f \sim g \overset{\circ}{+} X_n^2 \overset{IH}{\sim} bX_1 \overset{\circ}{+} X_2 \overset{\circ}{+} \ldots \overset{\circ}{+} X_n \overset{\text{(43) [1.6 Def 7]}}{\Leftrightarrow} (k^n, f) \cong (k^{n-1}, g) \hat{\oplus} (k, X_n^2) \Leftrightarrow disc(f) = disc(g) * 1 \overset{IH}{\in} \mathbb{F}_q^*/\mathbb{F}_q^{*^2}$.

□

Korollar 58. Zwei nicht-ausgeartete quadratische Formen über $\mathbb{F}_q$ sind genau dann äquivalent wenn sie denselben Rang und dieselbe Diskriminante haben.

Bemerkung 59. Im nicht-ausgearteten Fall ist die diskriminantenbeherbergende Quotientengruppe (11) [1.1] für endliche Körper mit $char(k) \neq 2$ der Form $\mathbb{F}_q^*/\mathbb{F}_q^{*^2}$ (Erinnerung: $|\mathbb{F}_q^*/\mathbb{F}_q^{*^2}| = 2$).

Bemerkung 60. Komplexität der Klassifikation:

Tabelle 2: Anzahl von nicht ausgearteten quadratischen Formen für Rang n bis auf Ähnlichkeit:

$\mathbb{C}$	$\mathbb{F}_q$ für festes $q \neq 2$	$\mathbb{R}$
1	2	n

Literatur

[1] A. Merz, C. Semrau, *Kapitel III. Das Hilbert-Symbol*, Seminarvortrag LMU München, Wintersemester 2002/03, online (zugegriffen 13.01.2003) http://www.chsemrau.de/studium/mathematik/chapter3.pdf.

[2] A. Merz, C. Semrau, *Der Satz von Chevalley-Warning*, Seminarvortrag LMU München, Wintersemester 2002/03, online (zugegriffen 13.01.2003) http://www.chsemrau.de/studium/mathematik/chevalley.pdf.

[3] W. Scharlau, *Quadratic and hermitian forms*, Springer, 1985.

[4] J.-P. Serre, *A course in arithmetic*, Springer, 1973.

(Elektronische Version dieses Dokuments via
http://www.blasum.net/holger/wri/math/al/nt/zimmermann2002/.)