Metrische Vektorräume und quadratische Formen

Der Isomorphiesatz von Witt-Lenz

Witts Beweis der Sätze von Artin-Springer und Knebusch

Ina Kersten

Abstract. Dies ist eine Seminarausarbeitung zweier kurzer bisher unveröffentlichter Manuskripte [11, 12], die im Nachlaß von Ernst Witt gefunden wurden. Das erste beinhaltet eine Verallgemeinerung der euklidischen Kongruenzsätze, und in dem zweiten werden die Sätze von Springer [9] und Knebusch [3] ganz kurz mit Hilfe ein und derselben Beweisidee gezeigt. In dieser Seminarausarbeitung werden außerdem Grundbegriffe aus der Theorie der quadratischen Formen bereitgestellt.

1991 Mathematics Subject Classification. 11E04, 11E39, 14L35.

Einleitung. Wenn zwei Dreiecke in zwei Seiten und dem eingeschlossenen Winkel übereinstimmen, sind sie kongruent (lassen sich also durch eine Bewegung ineinander überführen). Dieser euklidische Kongruenzsatz wird durch den Satz von Witt [10] verallgemeinert: Ein Isomorphismus zweier Teilräume eines metrischen Vektorraumes läßt sich zu einem Automorphismus des ganzen Raumes fortsetzen. Vorausgesetzt ist hierbei, daß die Räume endlich dimensional und regulär sind und daß der zugrundegelegte Körper nicht die Charakteristik 2 hat. Im allgemeinen ist eine Fortsetzbarkeit nicht uneingeschränkt möglich. Da der Satz von Witt fundamental ist für die Theorie der quadratischen und hermiteschen Formen, sowie für das Studium der klassischen Gruppen, ist es wünschenswert, möglichst allgemein ein Kriterium für die Fortsetzbarkeit von Isometrien zu finden. In dem bisher unveröffentlichen, nur fünf Seiten langen Manuskript [11] wird ein solches Kriterium angegeben, vgl. Abschnitt 4 unten. Obwohl das Manuskript [11] aus dem Jahre 1957 stammt, ist dieses Kriterium bis heute noch nicht bekannt. Besonders interessant ist hierbei der Beweis und die Definition der Ableitung $\dot{\varphi}$ einer metrischen Abbildung φ, die zu einer originellen allgemeinen Beschreibung orthogonaler und unitärer Gruppen führt (vgl. 3.1 und 3.2 unten).

Der Satz von Springer [9] besagt, daß eine anisotrope quadratische Form anisotrop bleibt bei Grundkörpererweiterung ungeraden Grades. In [12] wird hierfür ein kurzer eleganter Beweis gegeben, dessen "additive Variante" einen Beweis von Knebusch's Normprinzip [3] ergibt.

Die Darstellung in [11] und [12] ist kurz, klar und ausgesprochen elegant. Ich habe daraus eine Textvorlage für ein Seminar gemacht, das ich im Sommer 1994 in Regensburg abgehalten habe und in dem ich kaum mehr als Lineare Algebra an Vorkenntnissen vorausgesetzt habe. Die hier vorliegende Fassung ist aus der Textvorlage und den gehaltenen Vorträgen entstanden, und ich möchte allen Teilnehmern und Teilnehmerinnen herzlich für ihre Mitarbeit danken, ganz besonders auch dem Assistenten Dr. G. Seibert.

Diese Ausarbeitung ist in die folgenden Abschnitte gegliedert.

1. Skalarprodukt und Orthogonalität 2
2. Quadratische Formen 5
3. Metrische Abbildungen von Teilräumen 8
4. Der Isomorphiesatz 11
5. Der Kürzungssatz 16
6. Der Wittring 18
7. Die Sätze von Artin-Springer und Knebusch 21

Die Abschnitte 5 und 6 enthalten Ergebnisse aus Witts berühmter Arbeit [10] von 1937, die heutzutage als Standard in die Lehrbuchliteratur über quadratische Formen eingegangen sind, vgl. z. B. [4,5,7,8]. In den übrigen Abschnitten werden über den bekannten Stoff hinaus Definitionen und Resultate aus [11] und [12] vorgestellt.

1. Skalarprodukt und Orthogonalität

Ein *Schiefkörper* ist ein assoziativer Ring mit $1 \neq 0$, in dem jedes Element $\neq 0$ invertierbar ist. Es müssen also alle Körperaxiome erfüllt sein mit Ausnahme der Kommutativität der Multiplikation, die nicht gefordert wird.

Beispiel für einen Schiefkörper (Hamilton 1843). Sei $\mathbb{H}$ die Menge der Matrizen

$$\begin{pmatrix} \alpha & -\bar\beta \\ \beta & \bar\alpha \end{pmatrix}$$

mit $\alpha, \beta \in \mathbb{C}$, wobei $\bar\alpha$ die zu α konjugiert komplexe Zahl bedeute. $\mathbb{H}$ ist bezüglich Matrizenaddition und Matrizenmultiplikation ein Ring und –betrachtet als Vektorraum über $\mathbb{R}$– vier-dimensional mit Basis

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathfrak{i} = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \qquad \mathfrak{j} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \mathfrak{k} = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},$$

wobei $\mathrm{i} \in \mathbb{C}$ die Gleichung $\mathrm{i}^2 = -1$ erfüllt. $\mathbb{H}$ ist nicht kommutativ, denn es gilt $\mathfrak{ij} = -\mathfrak{k}$ und $\mathfrak{ji} = \mathfrak{k}$. Ist $\lambda = \begin{pmatrix} \alpha & -\bar\beta \\ \beta & \bar\alpha \end{pmatrix} \neq 0$ in $\mathbb{H}$, so ist $\lambda^{-1} = \det(\lambda)^{-1} \begin{pmatrix} \bar\alpha & \bar\beta \\ -\beta & \alpha \end{pmatrix}$ in $\mathbb{H}$. Also ist $\mathbb{H}$ ein Schiefkörper, genannt *Quaternionenschiefkörper*.

Sei nun K ein beliebiger Schiefkörper. Auf der Additionsgruppe von K sei ein involutorischer Automorphismus $\alpha \mapsto \bar\alpha$ gegeben, der also die Bedingungen $\overline{\alpha + \beta} = \bar\alpha + \bar\beta$ und $\bar{\bar\alpha} = \alpha$ für alle α, $\beta \in K$ erfüllt. Bezüglich der Multiplikation fordern wir gemäß [11] die Regel

$$\overline{\alpha\beta\gamma} = \bar\gamma\bar\beta\bar\alpha. \tag{1}$$

Es folgt $\bar1\bar1\bar\alpha = \overline{\alpha 1 1} = \overline{1\alpha 1} = \bar1\bar\alpha\bar1$ und daraus $\bar1\bar\alpha = \bar\alpha\bar1$ für alle $\alpha \in K$, d.h. $\bar1$ ist im Zentrum von K. Weiter folgt $\bar1 = \overline{111} = \bar1^2\,\bar1$ und also $1 = \bar1^2$, d.h. $\bar1 = \pm1$. Definiert man $\alpha^* = \bar1\bar\alpha$, so erhält man einen involutorischen Antiautomorphismus $\alpha \mapsto \alpha^*$ von K, für den dann also gilt $(\alpha\beta)^* = \beta^*\alpha^*$. Wie in [11] setzen wir

$$\alpha + \bar\alpha = \ \mathrm{sp}\ \alpha, \quad \alpha - \bar\alpha = \delta\alpha$$

und definieren die *Spur* $\operatorname{sp} K = \{ \operatorname{sp} \alpha \mid \alpha \in K \}$, analog δK.

Ein Linksvektorraum E über K heißt *metrischer Raum*, wenn ein *Skalarprodukt* $xy \in K$ für je zwei Vektoren $x, y \in E$ erklärt ist mit den Regeln

$$(\lambda x)y = \lambda(xy), \quad (x+y)z = xz + yz, \quad \overline{xy} = yx \quad (\lambda \in K;\, x,y,z \in E). \tag{2}$$

Es gilt dann $z(x+y) = zx + zy$ und $x(\mu y) = (xy)\mu^*$ (denn $x(\mu y) = \overline{(\mu y)x} = \overline{1\mu(yx)} = \overline{yx}\bar{\mu}\bar{1} = (xy)\mu^*$.) Diese Definition eines metrischen Raumes E schließt die folgenden Fälle ein, die wir später simultan behandeln werden:

I. Es ist $\bar{1} = 1$ und nach (1) daher $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$ für alle $\alpha, \beta \in K$. Dann heißt E ein *hermitescher Raum* und das Skalarprodukt eine *hermitesche Form* auf E.

Ia. Es ist $\delta K = 0$ (d.h. $\bar{\alpha} = \alpha$ für alle $\alpha \in K$). Dann ist $xy = yx$ für alle $x, y \in E$, und man spricht von *symmetrischen Bilinearform* auf E.

II. Es ist $\bar{1} = -1$ und nach (1) daher $\overline{\alpha\beta} = -\bar{\beta}\bar{\alpha}$ für alle $\alpha, \beta \in K$. Dann heißt E ein *schiefhermitescher Raum* und das Skalarprodukt eine *schiefhermitesche Form* auf E.

IIa. Es ist $\operatorname{sp} K = 0$ (d.h. $\bar{\alpha} = -\alpha$ für alle $\alpha \in K$). Dann ist $xy = -yx$ für alle $x, y \in E$, und man spricht von einer *symplektischen Form* auf E.

In den Fällen Ia und IIa ist K stets kommutativ (wie aus (1) mit $\gamma = 1$ folgt).

Beispiel (Fall I):

Es sei E der $\mathbb{C}$-Vektorraum der im Intervall $0 \le \alpha \le 2\pi$ definierten stetigen komplexwertigen Funktionen und $^-$ die komplexe Konjugation. Definiert man für zwei Funktionen f, g ein Skalarprodukt durch $fg = \int_0^{2\pi} f(\alpha)\,\overline{g(\alpha)}\;d\alpha$, so ist (2) erfüllt. Es ist E dann ein sogenannter Prä-Hilbert-Raum; derartige Räume werden in der Physik und in der Funktionalanalysis betrachtet.

Beschreibung des Skalarproduktes bezüglich einer Basis:

Sei $x = \sum_i \lambda_i e_i$ und $y = \sum_j \mu_j e_j$ mit einer fest gewählten Basis $\{e_i\}$ von E über K. Dann ist $xy = \sum_{i,j} (\lambda_i e_i)(\mu_j e_j) = \sum_{i,j} ((\lambda_i e_i) e_j)\mu_j^* = \sum_{i,j} \lambda_i (e_i e_j) \mu_j^*$. Ist $\dim_K E = n$, so ist das Skalarprodukt bekannt, wenn man die n^2 Produkte $e_i e_j$ und also die Matrix $\big(e_{ij}\big) = \big(e_i e_j\big)$ kennt; und umgekehrt kann man durch Vorgabe einer $n \times n$-Matrix $\big(e_{ij}\big)$ mit $e_{ij} = \bar{e}_{ji}$ und der Definition $xy = \sum_{i,j} \lambda_i\, e_{ij}\, \mu_j^*$ auf E ein Skalarprodukt mit den Eigenschaften (2) erklären; es gilt dann $e_{ij} = e_i e_j$ für alle i, j.

Beispiel einer symplektischen Metrik (Fall IIa):

Sei $E = \mathbb{R}^2$ und $(e_{ij}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Für $x = (\lambda_1, \lambda_2)$ und $y = (\mu_1, \mu_2)$ ist dann $xy = \lambda_1\mu_2 - \lambda_2\mu_1$, z.B. $(3,5)(1,2) = 6 - 5 = 1$ und $(3,5)(3,5) = 15 - 15 = 0$.

Die euklidische Metrik (Fall Ia):

Sei E ein metrischer $\mathbb{R}$-Vektorraum mit $\delta K = 0$. Gilt dann neben (2) zusätzlich

$$xx \ge 0 \quad \text{und} \quad = 0 \text{ nur für } x = 0,$$

so heißt E ein *euklidischer Vektorraum*, und das Skalarprodukt heißt *positiv definit*. In einem euklidischen Vektorraum definiert man die *Länge* eines Vektors x als $|x| := \sqrt{xx}$ und den *Winkel* θ zwischen zwei Vektoren $x, y \neq 0$ durch $\cos\theta = \frac{xy}{|x||y|}$ oder durch $xy = |x||y|\cos\theta$. Die Vektoren x, y stehen senkrecht aufeinander, wenn $\theta = 90^0$, also $\cos\theta = 0$ und damit $xy = 0$ gilt. Es ist $(x-y)(x-y) = xx-xy-yx+yy = xx+yy-2xy$ (das letzte Gleichheitszeichen gilt, weil $\delta K = 0$ ist). Hieraus folgt der Kosinussatz, nämlich $|x-y|^2 = |x|^2 + |y|^2 - 2|x||y|\cos\theta$. In einem euklidischen Vektorraum gilt also die gewöhnliche Trigonometrie, denn die Formeln der Trigonometrie lassen sich aus dem Kosinussatz herleiten.

Beispiel für einen euklidischen Vektorraum:

Sei E ein n-dimensionaler $\mathbb{R}$-Vektorraum und $\{e_i \,|\, i = 1, \ldots, n\}$ eine Basis von E. Für zwei Vektoren $x = \sum_i \lambda_i e_i$ und $y = \sum_j \mu_j e_j$ setzt man $xy = \lambda_1\mu_1 + \cdots + \lambda_n\mu_n$ und erhält dadurch eine euklische Metrik auf E, die man auch die Standardmetrik oder die gewöhnliche euklidische Metrik nennt. Es ist dann $|x| = \sqrt{xx} = \sqrt{\lambda_1^2 + \cdots + \lambda_n^2}$.

Inspiriert durch die euklidische Metrik werden wir uns im folgenden auch im Falle eines ganz beliebigen metrischen Raumes von der Vorstellung leiten lassen, daß durch xx die Länge eines Vektors x bestimmt wird und daß durch xy der Winkel zwischen zwei Vektoren $x \neq y$ gegeben wird. Wie das Beispiel der symplektischen Metrik gezeigt hat, kann es dann Vektoren $\neq 0$ der Länge 0 geben. Im Fall IIa ist $xx = -xx$, also $2xx = 0$. Ist die Charakteristik von K ungleich 2, so folgt dann $xx = 0$ für alle $x \in K$.

Sei nun E ein beliebiger metrischer Vektorraum über K. Wir sagen dann, daß zwei Vektoren $x, y \in E$ *senkrecht* aufeinander stehen oder *orthogonal* sind, wenn ihr Skalarprodukt $xy = 0$ ist. Wie sich aus (2) ergibt, ist die Orthogonalitätsrelation $xy = 0$ symmetrisch d.h. aus $xy = 0$ folgt $yx = 0$.

Für einen Teilraum A von E sei $A^\perp = \{\, e \in E \,|\, ex = 0 \;\forall\, x \in A \,\}$, also $A^\perp$ die Menge derjenigen Vektoren aus E, die auf allen Vektoren aus A senkrecht stehen. Man schreibt dafür auch $A^\perp = \{\, e \in E \,|\, eA = 0 \,\}$. Es ist $A^\perp$ ein Teilraum von E. Wir verwenden durchgehend die Abkürzung

$$A_B = A \cap B^\perp \quad (\text{Teilräume } A, B \subseteq E)$$

für die Menge aller Vektoren $a \in A$ mit $aB = 0$. Den Raum $E_E = E^\perp$ nennt man das *Radikal* von E. Sei C ein Teilraum von E.

1.1 SATZ [11]. *Es gilt die Regel* $A_{B_{C+Ka}} = A_{B_C} + Ka \quad (a \in A)$.

Beweis: Allgemein gilt für $D \subseteq D'$ die Regel $A_{D'} \subseteq A_D$. Da $C \subseteq C + Ka$ ist, gilt $B_{C+Ka} \subseteq B_C$ und also $A_{B_C} \subseteq A_{B_{C+Ka}}$. Es ist $aB_{C+Ka} = a(B_C \cap B_{Ka}) \subseteq aB_{Ka} = 0$, also $a \in A_{B_{C+Ka}}$.

Es ist B_{C+Ka} der Kern der nach (2) linkslinearen Abbildung $B_C \to K, b \mapsto ba$. Ist $aB_C = 0$, so folgt $B_{C+Ka} = B_C$ und somit $A_{B_{C+Ka}} = A_{B_C} = A_{B_C} + Ka$.

Da B_{C+Ka} höchstens von der Kodimension 1 in B_C ist, gibt es ein $x \in B_C$ so, daß $B_C = B_{C+Ka} + Kx$ und also $A_{B_C} = A_{B_{C+Ka}} \cap A_{Kx}$ gilt. Es sei nun $aB_C \neq 0$. Da

$aB_{C+Ka} = 0$ ist, gilt dann $ax \neq 0$, und wir können ohne Einschränkung annehmen, daß $ax = 1$ gilt. Man hat dann eine exakte Sequenz

$$\begin{array}{ccccccccc} 0 & \to & A_{B_C} & \to & A_{B_{C+Ka}} & \xrightarrow{\varphi} & K & \to & 0 \\ & & & & d & \mapsto & dx, & & \end{array}$$

wobei $\psi : K \to A_{B_{C+Ka}}$, $\lambda \mapsto \lambda a$, ein Schnitt von φ ist, d.h. $\varphi \circ \psi = \mathrm{id}_K$. Es folgt $A_{B_{C+Ka}} = A_{B_C} \oplus Ka$. □

Der folgende Satz wurde im Nachlaß von Witt unter seinen handschriftlichen Aufzeichnungen gefunden.

1.2 SATZ (WITT). *Ist A/A_B endlich dimensional, so gilt* $\dim(A/A_B) = \dim(B/B_A)$.

Beweis. Der Dualraum $A^* := \mathrm{Hom}(A, K)$ ist ein Linksvektorraum, wenn man λf definiert durch $(\lambda f)(x) = f(x)\lambda^*$ für $\lambda \in K$, $x \in A$ und $f \in A^*$. Die Abbildung $B \to A^*$, $b \mapsto \hat{b}$ mit $\hat{b}(a) = ab$, ist dann nach (2) linkslinear und induziert eine Injektion $B/B_A \hookrightarrow (A/A_B)^*$. Ist A/A_B endlich dimensional, so folgt $\dim(B/B_A) \leq \dim(A/A_B)$, und hieraus folgt aus Symmetriegründen die Behauptung. □

2. QUADRATISCHE FORMEN

Zunächst gelte $\alpha = \bar{\alpha}$ für alle $\alpha \in K$. Dann ist K kommutativ, und man definiert eine *quadratische Form* auf einem Vektorraum E als eine Abbildung $q : E \to K$ mit den Eigenschaften

(3) $$q(\lambda x) = \lambda^2 q(x) \quad \text{für alle } \lambda \in K,\ x \in E,$$

(4) $$f(x,y) := q(x+y) - q(x) - q(y) \text{ ist eine Bilinearform auf } E.$$

Es sei $q : E \to K$ eine quadratische Form. Dann ist die zugehörige Bilinearform $f(x,y)$ symmetrisch, d.h. $f(x,y) = f(y,x)$. Aus (4) und (3) folgt $f(x,x) = q(2x) - 2q(x) = 4q(x) - 2q(x) = 2q(x)$. Ist $\mathrm{Char}K \neq 2$, so setzen wir $xy := \frac{1}{2}f(x,y)$ und erhalten ein symmetrisches Skalarprodukt xy auf E mit $xx = q(x)$. Aus (3) und (4) folgt $q(x-y) = q(x) + q(y) - f(x,y)$, also $(x-y)(x-y) = xx + yy - 2xy$, und das ist der Kosinussatz. Ist $xy = 0$, stehen also die Vektoren x, y senkrecht auf einander, so folgt der Satz von Pythagoras. Man mache sich anhand einer Zeichnung klar, daß man für linear unabhängige Vektoren x, y den Vektor $x - y$ (bis auf Parallelverschiebung) als dritte Seite in einem Dreieck erhält, die dem von x und y eingeschlossenen Winkel gegenüber liegt.

Ist $\mathrm{Char}K = 2$, so ist $f(x,x) = 2q(x) = 0$ für alle $x \in E$. Es braucht dann kein symmetrisches Skalarprodukt xy zu geben mit der Eigenschaft $xx = q(x)$.

Beispiel [6, Kap. XXVI, §4]:

Die Abbildung $q : K^2 \to K, (\alpha, \beta) \mapsto \alpha\beta$, erfüllt die Regeln (3) und (4), ist also eine quadratische Form auf E. Ist $\mathrm{Char}K = 2$ und nimmt man an, daß es ein symmetrisches

Skalarprodukt xy mit $xx = q(x)$ gibt, so folgt $q(x+y) - q(x) - q(y) = (x+y)(x+y) - xx - yy = 2xy = 0$; aber für $x = (1,0)$, $y = (0,1)$ ist $q(x+y) - q(x) - q(y) = 1 - 0 - 0 = 1 \neq 0$, und man hat einen Widerspruch.

Es sei nun K ein Schiefkörper beliebiger Charakteristik und E ein metrischer Vektorraum über K. Auf E ist also ein Skalarprodukt xy gegeben, das die Bedingungen (2) erfüllt. Wie in §1 sei $\mathrm{sp}K = \{\alpha + \bar{\alpha} \mid \alpha \in K\}$.

2.1 SATZ [11]. *Ist* $\mathrm{sp}K \neq 0$, *so ist die Funktion* xy *bereits durch ihre Spezialisierung* xx *festgelegt.*

Beweis. Wir betrachten die durch $f_\alpha(\xi) = \mathrm{sp}\xi\alpha$ definierte additive Abbildung $\alpha \mapsto f_\alpha$ von K auf einen $\mathbb{Z}$-Modul, der aus Funktionen der Variablen ξ besteht, und wir zeigen zunächst, daß diese Abbildung injektiv ist: Nach Voraussetzung gibt es ein $\gamma \in K$ mit $\mathrm{sp}\gamma \neq 0$. Ist $\alpha \neq 0$ in K, so setze man $\beta = \gamma\alpha^{-1}$. Dann ist $f_\alpha(\beta) = \mathrm{sp}\beta\alpha = \mathrm{sp}\gamma \neq 0$, also $f_\alpha \neq 0$, woraus die Injektivität folgt.

Man rechnet mit Hilfe von (2) mühelos nach, daß für alle $a, b \in E$ und $\xi \in K$ gilt $f_{ab}(\xi) = \mathrm{sp}(\xi ab) = (\xi a + b)(\xi a + b) - (\xi a)(\xi a) - bb$. Sind also die Quadrate xx mit $x = \xi a + \eta b$ für alle $\xi, \eta \in K$ bekannt, so erhält man ab durch Umkehrung des oben betrachteten Isomorphismus $\alpha \mapsto f_\alpha$. □

Ein Vektor x mit $xx \in \mathrm{sp}K$ d.h. mit $xx = \alpha + \bar{\alpha}$ wird *gerade* genannt (in Verallgemeinerung des Falles $\alpha = \bar{\alpha}$). Die geraden Vektoren bilden einen Unterraum H von E, denn ist $xx = \mathrm{sp}\alpha$ und $y = \mathrm{sp}\beta$, so ist $(x+y)(x+y) = \mathrm{sp}(\alpha + \beta + xy)$ und $(\lambda x)(\lambda x) = \lambda(xx)\lambda^* = \mathrm{sp}(\lambda\alpha\lambda^*)$, wie man mit Hilfe von (2) ermittelt. Auch die Teilräume von H werden *gerade* genannt. Für Char $K \neq 2$ ist $H = E$ wegen $xx = \mathrm{sp}\frac{1}{2}xx$.

2.2 LEMMA [11]. *Der Raum* H *besteht aus allen Differenzen* $x - y$ *mit* $xx = yy$.

Beweis. Gilt $xx = yy$ für $x, y \in E$, so ist $(x-y)(x-y) = \mathrm{sp}(xx - xy)$. Ist $h \in H$, so ist entweder $hh = 0$ und $h = h - 0$ eine passende Differenz, oder es gilt $hh = \mathrm{sp}\ \alpha = \beta^{-1}$, und $h = x - y$ mit $x = \alpha\beta h$ und $y = (\alpha\beta - 1)h$ ist eine passende Differenz, wie man mit Hilfe von (1) und (2) leicht nachrechnet. □

Wie in [11] verallgemeinern wir nun den Begriff der quadratischen Form auf den Fall, daß K ein beliebiger Schiefkörper ist. Wie in §1 ist $\delta K = \{\alpha - \bar{\alpha} \mid \alpha \in K\}$. Der Vektorraum E sei mit einem Skalarprodukt xy mit den Eigenschaften (2) versehen, und es sei h_i eine total geordnete Basis von H. Wählt man $\eta_i \in K$ mit $h_i h_i = \mathrm{sp}\eta_i$, so ist durch

$$N\Big(\sum_i \lambda_i h_i\Big) = \sum_i \lambda_i \eta_i \lambda_i^* + \sum_{i<k} \lambda_i (h_i h_k) \lambda_k^* \tag{5}$$

eine Abbildung $N : H \to K$ erklärt mit den Eigenschaften

$$N(\lambda x) = \lambda N(x) \lambda^* \text{ für alle } \lambda \in K,\ x \in H, \tag{3'}$$

$$N(x+y) - N(x) - N(y) \equiv xy \bmod \delta K \text{ für alle } x, y \in H. \tag{4'}$$

Wir nennen daher N eine *quadratische Form.* (Man beachte, daß $xy \equiv yx \bmod \delta K$ gilt wegen $xy - yx = xy - \overline{xy} \in \delta K$, daß also $xy \bmod \delta K$ symmetrisch ist.)

Ist umgekehrt eine Funktion N auf H gegeben, die (3′) und (4′) erfüllt, so gilt $N(\sum_i \lambda_i h_i) \equiv \sum_i \lambda_i N(h_i) \lambda_i^* + \sum_{i<k} \lambda_i (h_i h_k) \lambda_k^* \bmod \delta K$, und es ist $hh \equiv 2\,N(h) = N(h) + \overline{N(h)} + N(h) - \overline{N(h)} \equiv$ sp $N(h) \bmod \delta K$ für alle $h \in H$. Man rechnet nun leicht nach, daß allgemein gilt:

2.3 BEMERKUNG. Ist eine Abbildung $N : H \to K$ durch (5) erklärt, so ist $hh = N(h) + \overline{N}(h)$ für alle $h \in H$.

Hierdurch wird der vorher durch (3) und (4) gegebene Begriff einer quadratischen Form verallgemeinert. Denn ist $\delta K = 0$ und $q : E \to K$ eine quadratische Form auf einem Vektorraum E, so setze man $xy = f(x,y)$ und erhält aus (3) und (4) die Bedingungen (3′) und (4′) für $N = q$. Es ist dann $H = E$ wegen $xx = f(x,x) = 2q(x) = q(x) + \overline{q(x)} \in \mathrm{sp}K$.

Im allgemeinen kann es aber vorkommen, daß $H \neq E$ gilt. Es ist dann notwendig $\mathrm{Char}K = 2$. Wir geben hier zwei Beispiele für den Fall, daß $\delta K = 0$ ist. Es ist dann $\mathrm{sp}K = 0$ (da $\mathrm{sp}K = \delta K$ bei Charakteristik 2 gilt), und die geraden Vektoren sind genau die Vektoren h mit $hh = 0$. Für $E = Ka_1 \oplus Ka_2$ mit der durch die Matrix $(a_i a_k) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ definierten Metrik gilt dann $H = Ka_2$, also $H \neq E$, und für $E = Ka_1 \oplus Ka_2 \oplus Ka_3$ mit der durch die Matrix

$$(a_i a_k) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

definierten Metrik gilt dann $H = Ka_1 \oplus Ka_3$, also auch $H \neq E$.

Erläuterung zur Definition (5):

Es sei $\dim H = 2$ und zunächst $\delta K = 0$. Wir betrachten den binomischen Ausdruck $(h_1 + h_2)^2 = h_1 h_1 + 2h_1 h_2 + h_2 h_2$. Da h_1 und h_2 gerade sind, also $h_1 h_1 = 2\eta_1$ und $h_2 h_2 = 2\eta_2$, hat man $(h_1 + h_2)^2 = 2(\eta_1 + h_1 h_2 + \eta_2)$ und $N(h_1 + h_2) = \eta_1 + \eta_2 + h_1 h_2$. Durch die Definition (5) wird also erreicht, daß der Faktor 2, der bei Charakteristik 2 alles zu 0 machen würde, impliziert gekürzt wird. Ist δK beliebig, so haben wir $(h_1 + h_2)^2 = h_1 h_1 + h_1 h_2 + h_2 h_1 + h_2 h_2 = \eta_1 + \overline{\eta_1} + h_1 h_2 + \overline{h_1 h_2} + \eta_2 + \overline{\eta_2}$ und $N(h_1 + h_2) = \eta_1 + \eta_2 + h_1 h_2$. Hier ist also quasi auch nur die Hälfte genommen worden.

Die Definition von N ist von Witt aus dem Jahre 1957, die er leider nicht veröffentlicht hat. In ihr steckt die Idee des sogenannten Formparameters, wie er z.B. in [2] und [4] zu finden ist. Tatsächlich hat Witt damals auf einem Notizzettel allgemeiner die Bedingungen (3′) und (4′) mod Λ_0 betrachtet, wobei $\delta K \subseteq \Lambda_0$ gilt und Λ_0 eine Gruppe ist mit $\lambda \Lambda_0 \lambda^* \subseteq \Lambda_0$ und $\mathrm{sp}\Lambda_0 = 0$.

3. Metrische Abbildungen von Teilräumen

Metrische Abbildungen sind winkel- und längenerhaltende Abbildungen, genauer: Sind A, B Teilräume eines metrischen Raumes E über einem Schiefkörper K, so heißt eine linkslineare Abbildung $\varphi : A \to B$ *metrisch*, wenn $\varphi x \varphi y = xy$ für alle $x, y \in A$ gilt.

Ist $\varphi : A \to B$ eine metrische Abbildung und ist das Radikal A_A von A gleich $\{0\}$, so ist φ injektiv. Denn andernfalls gäbe es einen Vektor $a \neq 0$ mit $\varphi a = 0$ und einen Vektor $b \in A$ mit $ab \neq 0$, aber es wäre $\varphi a \varphi b = 0$.

Für eine metrische Abbildung $\varphi : A \to E$ werde $(\varphi - 1)A = \{\varphi(a) - a \mid a \in A\}$ die *Bahn* von φ genannt; sie liegt in H (vgl. Lemma 2.2).

Es sei nun E metrischer Raum, N eine durch (5) gegebene Funktion auf H und $\varphi : A \to E$ eine metrische Abbildung. Für $x \in A$ ist dann $\varphi(x) - x =: h \in H$, und wir definieren nach Witt, vgl. [11], die Restklasse $xh + N(h)$ mod δK in $K/\delta K$ als *Ableitung* $\dot\varphi(x)$. Aus (3′) und (4′) folgt dann

$$\dot\varphi(\lambda x) = \lambda \dot\varphi(x) \lambda^*, \qquad \dot\varphi(x+y) = \dot\varphi(x) + \dot\varphi(y), \qquad (\varphi \circ \psi)^\cdot = \dot\varphi \circ \psi + \dot\psi.$$

Die letzte Regel ist eine Art additiver Kettenregel für zusammengesetzte Abbildungen $\varphi \circ \psi$. Falls $x \in H$ ist, gilt $\dot\varphi(x) = N(x+h) - N(x)$ mod δK nach (4′). Ist $\dot\varphi(x) = 0$, so gilt dann also $N(\varphi x) \equiv N(x)$ mod δK (da $x + h = \varphi(x)$). Das führt uns zu der folgenden Definition.

3.1 Definition [11]. Eine linkslineare Abbildung $\varphi : A \to B$ zweier Teilräume A, B von E heißt eine *Isometrie*, wenn $\varphi x \varphi y = xy$ und $\dot\varphi(x) = 0$ für alle $x, y \in A$ gilt. Ein *Isomorphismus* ist eine bijektive Isometrie, und entsprechend ist ein *Automorphismus* definiert.

3.2 Bemerkung a) Ist $\delta K = 0$ und $A \subseteq H$, so folgt die Bedingung $\varphi(x)\varphi(y) = xy$ aus der Bedingung $\dot\varphi = 0$; denn ist $\dot\varphi(x) = 0$ für alle $x \in A$, so ist dann $N(\varphi x) = N(x)$ für alle $x \in A$ und also $xy = N(x+y) - N(x) - N(y) = N(\varphi x + \varphi y) - N(\varphi x) - N(\varphi y) = \varphi x \varphi y$ nach (4′) für alle $x, y \in A$.

b) Ist $\dot\varphi = 0 = \dot\psi$, so ist nach der Kettenregel auch $(\varphi \circ \psi)^\cdot = 0$.) Die Automorphismen eines metrischen Vektorraumes E bilden also eine Gruppe Aut$E$ bezüglich der Zusammensetzung $\varphi \circ \psi : E \to E, x \mapsto \varphi(\psi x)$.

Es ist eine interessant Aufgabe, den Zusammenhang zwischen den klassischen Gruppen und der Gruppe Aut$E$ zu studieren. Vielleicht erhält man sogar durch diese Definition von Aut$E$ bisher nicht bekannte Gruppen (z.B. wenn die Dimension von E nicht endlich ist). Unsere Betrachtungsweise hat auch den Vorteil, daß man dadurch einerseits die klassische Theorie der quadratischen Formen und andererseits die Theorie der metrischen Vektorräume als Spezialfälle erhält. Letztere erhält man einfach dadurch, daß man alle Aussagen über N und die Ableitung $\dot\varphi$ sinngemäß fortläßt. Grundlegend für diese Theorien ist der Isomorphiesatz von Witt, den wir im nächsten Abschnitt in sehr allgemeiner Form beweisen werden. Diesen Isomorphiesatz kann man als Verallgemeinerung der euklidischen Kongruenzsätze ansehen, wie wir noch ausführen werden.

Das Radikal E_E besteht aus denjenigen Vektoren z, die auf allen Vektoren in E senkrecht stehen, für die also $zE = 0$ gilt. E_E ist ein gerader Teilraum von E. Ist $E_E = 0$, so heißt E *regulär*. Es sei

$$Z = \{z \in E_E \mid N(z) \in \delta K\}.$$

Dann ist Z ein Teilraum von E. Die Produkte xy und die Werte $N(h)$ mod δK hängen nur von den Restklassen der Vektoren mod Z ab (denn $(x+z)(y+z') = xy$ und $N(h+z) \equiv N(h)$ mod δK nach (4′) für alle $z, z' \in Z$).

3.3 Lemma [11]. *Für die Bahn Q einer Isometrie gilt $Q_E = Q \cap Z$.*

Beweis. Es sei $\varphi : A \to E$ eine Isometrie eines Teilraumes A in E und $Q = (\varphi - 1)A$. Ist $q \in Q_E$, also $q = \varphi(a) - a$ für ein $a \in A$ und $eq = 0$ für alle $e \in E$, so ist $0 = \dot{\varphi}(a) = aq + N(q) = N(q)$ mod δK und daher $q \in Z$. Umgekehrt ist offensichtlich $Q \cap Z \subseteq Q_E$. □

3.4 Lemma [11]. *Es sei σ ein Automorphismus von E mit Bahn $Q = (\sigma - 1)E$. Ist $Q_E = 0$, so ist* $\mathrm{kern}(\sigma - 1) = E_Q$.

Beweis. Sei $e \in \mathrm{kern}(\sigma - 1)$, also $\sigma e - e = 0$. Da σ eine metrische Abbildung ist, folgt dann $0 = (e - \sigma e)\sigma x = e(\sigma x - x)$ für alle $x \in E$, also $e \in E_Q$. Sei umgekehrt $e \in E_Q$ gegeben, also $0 = e(\sigma x - x) = (e - \sigma e)\sigma x$ für alle $x \in E$. Dann ist $(e - \sigma e)E = 0$, da σ bijektiv ist. Weil $Q_E = 0$ ist, folgt $\sigma e - e = 0$, also $e \in \mathrm{kern}(\sigma - 1)$. □

Ist σ ein Automorphismus von E mit endlich dimensionaler Bahn Q und ist $Q_E = 0$, so folgt aus Lemma 3.4, daß $\sigma - 1$ einen Vektorraum-Isomorphismus $E/E_Q \to Q$ induziert. Wir wählen Elemente $a_i \in E$ so, daß deren Restklassen mod E_Q eine Basis von E/E_Q bilden. Sie gehen dann unter $\sigma - 1$ in eine Basis $\{q_i\}$ von Q über: $q_i = \sigma a_i - a_i$.

Die Matrix $\big(a_i q_k\big) = \big(\lambda_{ik}\big)$ ist invertierbar, weil ihre Zeilen linkslinear unabhängig sind, wie die folgende Überlegung zeigt: Es sei $\sum_i \lambda_i(a_i q_1, \dots, a_i q_n) = 0$ mit $\lambda_i \in K$. Dann folgt $0 = \sum_i \lambda_i(a_i q_j) = \big(\sum_i \lambda_i a_i\big) q_j$ für alle j nach (2). Da die q_j eine Basis von Q bilden, folgt $\sum_i \lambda_i a_i \in E_Q$. Es ist $E = (Ka_1 \oplus \cdots \oplus Ka_n) \oplus E_Q$, und dies erzwingt nun $\sum_i \lambda_i a_i = 0$ und damit $\lambda_i = 0$ für alle i, da die a_i linear unabhängig sind.

Wir ermitteln nun notwendige und hinreichende Bedingungen dafür, daß σ ein Automorphismus von E ist. Es gilt: $\sigma a_i\, \sigma a_k = a_i a_k \iff \sigma a_i\; q_k = \sigma a_i(\sigma a_k - a_k) = a_i a_k - \sigma a_i\; a_k = -q_i a_k = -\overline{a_k q_i} = -\bar{\lambda}_{ki}$ nach (2). Die Bedingung $\sigma a_i\; q_k = -\bar{\lambda}_{ki}$ impliziert $q_i q_k = (\sigma a_i - a_i) q_k = -\bar{\lambda}_{ki} - \lambda_{ik}$. Damit erhalten wir

$$(*) \qquad \sigma a_i\; \sigma a_k = a_i a_k \iff q_i q_k = -\lambda_{ik} - \bar{\lambda}_{ki}\ .$$

Weiter gilt nach Definition der Ableitung $\dot{\sigma}(a_i) = a_i q_i + N(q_i)$ mod δK und also

$$(**) \qquad \dot{\sigma}(a_i) = 0 \iff N(q_i) \equiv -\lambda_{ii} \bmod \delta K.$$

Dafür, daß σ ein Automorphismus von E sei, findet man also die Bedingungen

$$(6) \qquad q_i q_k = -\lambda_{ik} - \bar{\lambda}_{ki}, \quad N(q_i) \equiv -\lambda_{ii} \bmod \delta K.$$

Damit haben wir Bedingungen dafür gefunden, wann ein vorgegebener endlich dimensionaler Teilraum Q von E die Bahn eines Automorphismus ist. Es gilt nämlich:

3.5 SATZ [11]. *Sei Q ein Teilraum von E mit einer endlichen Basis $q_1, \ldots, q_n$ und (λ_{ik}) eine invertierbare Matrix, die (6) erfüllt. Ist $Q_E = 0$, so gibt es* mod E_Q *genau eine Basis $\{a_i\}$ von E* mod E_Q *mit $a_i q_k = \lambda_{ik}$, und der Ansatz*

$$\sigma a_i = a_i + q_i, \quad (\sigma - 1)E_Q = 0 \tag{7}$$

liefert einen Automorphismus σ von E mit $(\sigma - 1)E = Q$.

Beweis. Da $Q_E = 0$ ist, ist $\dim(E/E_Q) = n$ nach 1.2. Wir wählen Elemente $b_1, \ldots b_n \in E$ so, daß deren Restklassen mod E_Q eine Basis von E/E_Q bilden. Wie oben sieht man, daß die Zeilen der Matrix $(b_i q_k)$ linkslinear unabhängig sind, und also die Matrix invertierbar ist. Wir setzen nun $(\alpha_{ik}) = (\lambda_{ik})\,(b_i q_k)^{-1}$ und $a_i = \sum_j \alpha_{ij} b_j$. Dann gilt $a_i q_k = \lambda_{ik}$, die a_i sind linear unabhängig in E (da mit (λ_{ik}) auch die Matrix (α_{ik}) invertierbar ist), und ihre Restklassen mod E_Q bilden eine Basis von E/E_Q. Ist $\{c_i \bmod E_Q\}$ eine weitere Basis von E/E_Q mit $a_i q_k = \lambda_{ik} = c_i q_k$ für alle i, k, so folgt $(a_i - c_i)q_k = 0$ für alle k, also $a_i - c_i \in E_Q$ und damit $a_i \equiv c_i \bmod E_Q$, womit die Eindeutigkeitsaussage bewiesen ist.

Wir zeigen nun, daß der Ansatz (7) eine Isometrie σ von E liefert. Aus den Bedingungen (6) folgt nach $(*)$ und $(**)$, daß $\sigma a_i\ \sigma a_k = a_i a_k$ und $\dot\sigma(a_i) = 0$ gilt für alle i, k. Nach (7) ist σ die Identität auf E_Q, also $\sigma x\ \sigma y = xy$ und $\dot\sigma(x) = 0$ für alle $x, y \in E_Q$. Weiter ist $0 = q_i x = (\sigma a_i - a_i)x$, also $(\sigma a_i)x = a_i x$ und entsprechend $x\,\sigma a_i = x a_i$. Da jedes Element $e \in E$ die Gestalt $e = \sum_i \lambda_i a_i + z$ mit $z \in E_Q$ hat, folgt $\sigma e\ \sigma e' = ee'$ für alle $e, e' \in E$. Wegen $\dot\sigma(e) = \sum_i \lambda_i\,\dot\sigma(a_i)\,\lambda_i^* = 0$ folgt, daß σ eine Isometrie ist.

Wir zeigen nun, daß σ bijektiv ist. Sei $e = \sum_i \lambda_i a_i + z \in E$ mit $z \in E_Q$. Dann ist $\sigma e = \sum_i \lambda_i(a_i + q_i) + z$. Ist $\sigma e \in E_Q$, so folgt $0 = q_k\ \sigma e = \sum_i q_k(\lambda_i a_i) + q_k(\lambda_i q_i) = \sum_i (q_k a_i)\lambda_i^* + (q_k q_i)\lambda_i^* = \sum_i (\bar\lambda_{ik}\lambda_i^* - \lambda_{ki}\lambda_i^* - \bar\lambda_{ik}\lambda_i^*) = -\sum_i \lambda_{ki}\lambda_i^*$ nach (6), das heißt $\sum_i \lambda_{ki}\lambda_i^* = 0$ für alle k. Da die Matrix $\big(\lambda_{ik}\big)$ nach Voraussetzung invertierbar ist, sind ihre Spalten rechtslinear unabhängig, also impliziert $\sum_i (\lambda_{1i}, \ldots, \lambda_{ni})\lambda_i^* = \big(\sum_i \lambda_{1i}\lambda_i^*, \ldots, \sum_i \lambda_{ni}\lambda_i^*\big) = 0$, daß $\lambda_i^* = 0$ für alle i gilt und damit $\lambda_i = 0$ für alle i. Wenn $\sigma e \in E_Q$ ist, so ist also auch $e \in E_Q$. Hieraus folgt sofort, daß σ injektiv ist, denn ist $\sigma(e) = 0$, so ist $\sigma(e) \in E_Q$, da $0 \in E_Q$, also $e = \sigma(e) = 0$. Weiter induziert σ einen injektiven Homomorphismus $\tilde\sigma : E/E_Q \to E/E_Q$, $e \bmod E_Q \mapsto \sigma(e) \bmod E_Q$, denn ist $\tilde\sigma(e \bmod E_Q) = 0$, so ist $\sigma(e) \in E_Q$, also $\sigma(e) = e \in E_Q$. Da E/E_Q endlichdimensional ist, ist $\tilde\sigma$ auch surjektiv. Sei nun $e \in E$. Dann gibt es ein $e' \in E$ mit $\tilde\sigma(e' \bmod E_Q) = e \bmod E_Q$. Es folgt $\sigma(e') = e + y$ mit $y \in E_Q$ und daher $\sigma(e' - y) = \sigma(e') - y = e$. Also ist σ surjektiv.

Es ist $(\sigma - 1)e = \sum_i \lambda_i q_i \in Q$, und ist umgekehrt $q = \sum_i \lambda_i q_i \in Q$, so folgt $q = \sum_i \lambda_i(\sigma a_i - a_i) = (\sigma - 1)\sum_i \lambda_i a_i$, also $q \in (\sigma - 1)E$. Damit gilt $(\sigma - 1)E = Q$. □

3.6 DEFINITION. Sei σ ein Automorphismus von E mit Bahn $Q = (\sigma - 1)E$, und es gelte $Q_E = 0$. Wenn $\dim Q = 1$ bzw. $= 2$ ist, werde σ eine *Spiegelung* bzw. eine *Rotation* längs Q genannt.

Beispiel: Es sei $\alpha = \bar{\alpha}$ für alle $\alpha \in K$ und $\mathrm{Char} K \neq 2$. Die Voraussetzungen von Satz 3.5 seien für einen eindimensionalen Teilraum $Q = Kq_1$ erfüllt. Wie sieht dann die Spiegelung längs Q aus, die durch den Ansatz (7) gegeben ist? Es ist $a_1 q_1 = \lambda_{11} \neq 0$, also $q_1 q_1 = -\lambda_{11} - \lambda_{11} = -2\lambda_{11} \neq 0$. Setzt man nun für $x \in E$

$$\sigma(x) = x - 2\,\frac{xq_1}{q_1 q_1}\,q_1,$$

so ist $\sigma(q_1) = -q_1$ und $\sigma(x) = x$ für alle $x \in E_Q$, da $E_Q = E_{Kq_1} = \{x \in E \mid xq_1 = 0\}$. Weiter gilt $\sigma(a_1) = a_1 + q_1$ (wegen $-2\frac{a_1 q_1}{q_1 q_1} = 1$), also ist (7) erfüllt.

Die Spiegelung σ ist involutorisch (d.h. $\sigma^2 = \mathrm{id}$), da $E = Ka_1 \oplus E_Q$ und $\sigma^2(a_1) = \sigma(a_1 + q_1) = a_1$ gilt. (Dies braucht bei $\mathrm{Char} K = 2$ oder $\delta(K) \neq 0$ nicht immer erfüllt zu sein.) Gespiegelt wird an der Hyperebene E_Q längs der Geraden $Q = Kq_1$. Diese Gerade steht senkrecht zur Hyperebene, und jeder Punkt λq_1 auf der Geraden geht bei Spiegelung in sein Negatives über, während die Hyperebene invariant bleibt. Man veranschauliche sich dies durch eine Zeichnung, falls $\dim E = 3$ gilt und also $\dim E_Q = 2$ ist.

4. Der Isomorphiesatz

Im folgenden wird untersucht, unter welchen Umständen sich ein Isomorphismus zweier Teilräume von E zu einem Automorphismus von E fortsetzen läßt. Der unten stehende Isomorphiesatz läßt sich als Verallgemeinerung des Satzes von EUKLID auffassen, daß zwei Dreiecke kongruent sind, wenn sie in zwei Seiten und dem eingeschlossenen Winkel übereinstimmen. Ist $\mathrm{sp} K \neq 0$, so wird durch Satz 2.1 die Verbindung zu dem anderen Kongruenzsatz hergestellt, der sich auf die Übereinstimmung in drei Dreiecksseiten bezieht. Kongruenz bedeutet hierbei, daß sich die Dreiecke durch eine Bewegung des Raumes, in dem sie beide liegen, ineinander überführen lassen. Es seien $A = Ka_1 + Ka_2$ und $B = Kb_1 + Kb_2$ zwei 2-dimensionale Teilräume von E und $\varphi : A \to B$ ein Isomorphismus (Def. 3.1). Wir betrachten das Dreieck, das die Seiten a_1 und a_2 hat und als dritte Seite $a_1 - a_2$, die dem von a_1 und a_2 eingeschlossenen Winkel gegenüber liegt, und entsprechend betrachten wir ein Dreieck in B. Da φ ein Isomorphismus ist, bleiben die Seitenlängen und die Winkel bei Anwendung von φ erhalten. Die Fortsetzbarkeit von φ zu einem Automorphismus σ von E bedeutet dann, daß es eine Bewegung σ gibt, welche die Dreiecke ineinander überführt.

Es sei nun E ein metrischer Vektorraum, auf dem gemäß (5) eine quadratische Form $N : H \to K$ gegeben sei. Wie in §3 (oberhalb von Lemma 3.3) sei

$$Z = \{z \in E_E \mid N(z) \in \delta K\},$$

wobei allgemein $A_B = \{a \in A \mid aB = 0\}$ gilt. Wir beweisen den Isomorphiesatz [11], der von Witt und Lenz 1957 gefunden wurde, zunächst für $Z = 0$ und erhalten dann daraus den berühmten Satz von Witt [10] aus dem Jahre 1937. Danach werden wir einen Reduktionssatz beweisen, aus dem sich die allgemeine Fassung für beliebiges Z von selbst ergibt. Wir werden durchgehend folgende Bezeichnungen benutzen.

Bezeichnungen: Es sei $\varphi : A \to B$ ein Isomorphismus zweier Teilräume von E, und es sei C ein Teilraum von A. Wer nur an metrischen Räumen interessiert ist, möge sich im folgenden einen Isomorphismus $\varphi : A \to B$ vorstellen als eine bijektive lineare Abbildung, die $\varphi x \varphi y = xy$ für alle $x, y \in A$ erfüllt; (an die Stelle von Z tritt dann E_E und alle Aussagen über $\dot{\varphi}$ können dann ignoriert werden). Wer gleichzeitig auch die quadratischen Formen mit behandelt sehen möchte, benutze die Definition 3.1 für einen Isomorphismus (d.h. es gilt stets auch $\dot{\varphi}(x) = 0$ für alle $x \in A$). Diesen Standpunkt werden wir hier einnehmen.

Die Schreibweise $(\varphi - 1)C \subseteq D$ bedeutet, daß $\varphi(x) - x \in D$ gilt für alle $x \in C$. Die Schreibweise $(\varphi - 1)C = 0$ bedeutet, daß $\varphi(x) = x$ für alle $x \in C$ gilt. In diesem Fall sagen wir auch, daß C ein Teilraum von Invarianten von φ ist.

D sei ein gerader Teilraum von E, also $D \subseteq H$. Es sei $G = G(D)$ die Gruppe derjenigen Automorphismen von E, deren Bahnen in D liegen,

$$G(D) := \{\sigma \in \mathrm{Aut}E \mid (\sigma - 1)E \subseteq D\}.$$

Speziell für $D = H$ ist G die Gruppe aller Automorphismen von E, wie aus Lemma 2.2 folgt.

Isomorphiesatz von Witt und Lenz für $Z = 0$. *Es sei C ein Teilraum von A mit* dim $A/C = n < \infty$. *Weiter gelte $(\varphi - 1)C = 0$ und $(\varphi - 1)A \subseteq D$. Dann läßt sich $\varphi : A \to B$ genau dann zu einem Automorphismus $\sigma \in G$ fortsetzen, wenn $A_{D_C} = B_{D_C}$ und $(\varphi - 1)A_{D_C} = 0$.*

σ kann als Produkt von höchstens n Rotationen oder Spiegelungen $\sigma_i \in G(D_C)$ mit $(\sigma_i - 1)C = 0$ dargestellt werden.

Beweis. Es sei $\sigma \in G(D)$ eine Fortsetzung von φ, und es sei $Q := (\sigma - 1)E \subseteq D$ die Bahn von σ. Nach Lemma 3.3 ist $Q_E = 0$, da $Z = 0$ ist. Dies impliziert nach Lemma 3.4, daß $\mathrm{kern}(\sigma - 1) = E_Q$ gilt. Die Voraussetzung $(\varphi - 1)C = 0$ ergibt $C \subseteq \mathrm{kern}(\sigma - 1)$, also $C \subseteq E_Q$. Es folgt $cQ = 0$ für alle $c \in C$ und also $qC = 0$ für alle $q \in Q$. Da $Q \subseteq D$ ist, ergibt sich nun $Q \subseteq D_C$, d.h. $\sigma \in G(D_C)$. Es folgt weiter

$$A_{D_C} \subseteq E_{D_C} \subseteq E_Q = \mathrm{kern}(\sigma - 1),$$

also $(\varphi - 1)A_{D_C} = 0$ und $A_{D_C} \subseteq B_{D_C}$. Aus Symmetriegründen, indem man φ durch φ^{-1} und σ durch σ^{-1} ersetzt, ergibt sich auch $B_{D_C} \subseteq A_{D_C}$.

Wir zeigen nun umgekehrt, die Bedingungen $A_{D_C} = B_{D_C}$ und $(\varphi - 1)A_{D_C} = 0$ eine Fortsetzung $\in G(D_C)$ von φ liefern.

Für jedes $\tau \in G(D_C)$ gilt $(\tau\varphi - 1)A_{D_C} = 0$ (denn es ist $Q' := (\tau - 1)E \subseteq D_C$, und analog wie oben erhalten wir, daß $A_{D_C} \subseteq E_{D_C} \subseteq E_{Q'} = \mathrm{kern}(\tau - 1)$ gilt. Wegen $(\varphi - 1)A_{D_C} = 0$ folgt dann $\tau\varphi a - a = \tau a - a = 0$ für alle $a \in A_{D_C}$). Nach der Voraussetzung $(\varphi - 1)C = 0$ besteht C nur aus Invarianten von φ. Ist $a \in A$ eine weitere Invariante von φ, so erfüllt auch $C + Ka$ die obigen Voraussetzungen, d.h. es ist $A_{D_{C+Ka}} = B_{D_{C+Ka}}$ und $(\varphi - 1)A_{D_{C+Ka}} = 0$; (dies ergibt sich aus Satz 1.1, da nach Voraussetzung $A_{D_C} + Ka = \varphi(A_{D_C}) + Ka = B_{D_C} + Ka$). Wegen $\dim A/C < \infty$ dürfen wir nun annehmen, daß C aus allen Invarianten von φ besteht und also $C = \mathrm{kern}(\varphi - 1)$ gilt. Für $C \neq A$ wird nun eine Spiegelung oder Rotation $\sigma \in G(D_C)$

angegeben, für welche $\sigma^{-1}\varphi$ noch mehr Invarianten hat als φ, etwa zusätzlich a_1. Höchstens n-malige Wiederholung dieses Verfahrens führt dann auf den trivialen Fall der identischen Abbildung, und die gewünschte Fortsetzung von φ ist dann gefunden.

Es sei $\varphi a_1 = a_1 + q_1 = b_1$. Dann ist $q_1 \in D_C$, da nach Voraussetzung $(\varphi - 1)A \subseteq D$ und da $c(\varphi a_1 - a_1) = (c - \varphi c)\varphi a_1 = 0$ für alle $c \in C$ gilt (wegen $C \subseteq \mathrm{kern}(\varphi - 1)$). Es ist $Kq_1 = (\varphi - 1)Ka_1$, also $(Kq_1)_E = Kq_1 \cap Z = 0$ nach 3.3. Wegen $A_{D_C} = B_{D_C} \subseteq \mathrm{kern}(\varphi - 1)$ ist $a_1 D_C \neq 0$ und $b_1 D_C \neq 0$, also gibt es $s, t \in D_C$ mit $a_1 s = b_1 t = 1$. Für einen der Vektoren $q_2 = s, t$ oder $s + t$ ist dann zugleich $a_1 q_2 \neq 0$ und $b_1 q_2 \neq 0$. Es ist dann $q_2 \in D_C \subseteq H$. Man rechnet nun mit Hilfe von 2.3 nach, daß (6) erfüllt ist für die Matrix

$$\begin{pmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{pmatrix} = \begin{pmatrix} a_1 q_1 & a_1 q_2 \\ -q_2 b_1 & -N(q_2) \end{pmatrix}.$$

Ist $\lambda_{11} \neq 0$, so ergibt Satz 3.5 angewandt auf Kq_1 eine Spiegelung σ mit $\sigma a_1 = \varphi a_1$ und $(\sigma - 1)E_{Kq_1} = 0$. Letzteres impliziert, daß $\sigma^{-1}\varphi(a) = a$ auch für alle $a \in \mathrm{kern}(\varphi - 1)$ gilt. Im Falle $\lambda_{11} = 0$ ist die Matrix (λ_{ik}) invertierbar, und für $Q = Kq_1 + Kq_2$ gilt $Q_E = (Q_{Ka_1})_E = (Kq_1)_E = 0$. Der Ansatz (7) ergibt nun eine Rotation σ mit $\sigma a_1 = \varphi a_1$ und $(\sigma - 1)E_Q = 0$. Da q_1, q_2 beide in D_C sind, ist $q_1 C = 0 = q_2 C$, und es folgt $\mathrm{kern}(\varphi - 1) = C \subseteq E_Q \subseteq \mathrm{kern}(\sigma - 1)$. Also hat $\sigma^{-1}\varphi$ auch in diesem Falle mehr Invarianten als φ. □

Wir betrachten nun folgenden Spezialfall des Isomorphiesatzes für $Z = 0$. Es seien E regulär (d.h. $E_E = 0$), der Raum A endlich dimensional, $C = 0$ und $D = H = E$. Dann gilt $A_{D_C} = A_E = 0 = B_{D_C}$, und die letzten beiden Bedingungen in dem Satz sind automatisch erfüllt. Wir erhalten dann den berühmten Satz von Witt [10].

SATZ VON WITT. *Es seien E ein gerader regulärer Raum und A, B Teilräume von E. Ist A endlich dimensional, so läßt sich jeder Isomorphismus $\varphi : A \to B$ zu einem Automorphismus von E fortsetzen.*

Beispiel [6, S. 340]: Die Bedingung, daß A endlich dimensional ist (oder allgemeiner A/C endlich dimensional ist), ist wirklich notwendig. Es sei E ein ∞-dimensionaler $\mathbb{R}$-Vektorraum mit abzählbarer Basis $\{a_i\}$ und mit einem Skalarprodukt, das durch $a_i a_j = \delta_{ij}$ definiert sei. Es gelte $N(x) = \frac{1}{2}xx$ für $x \in E$. Ist $A = E$ und $B = < a_2, a_3, \ldots >$, so ist die durch $\varphi(a_i) = a_{i+1}$ definierte lineare Abbildung ein Isomorphismus (im Sinne von Definition 3.1), aber φ hat offensichtlich keine Fortsetzung zu einem Automorphismus von E.

Beispiel [11]: Es sei E zweidimensional mit der Multiplikationstafel

$$(a_i a_k) = \begin{pmatrix} \nu & 1 \\ \bar{1} & 0 \end{pmatrix}, \quad (\nu \notin \text{ sp K}),$$

und es sei N die Nullabbildung. Setzt man $A = Ka_2 = B$ und definiert $\varphi : A \to B$ durch $\varphi(a_2) = \lambda a_2$ mit $\lambda \neq 0, 1$, dann ist φ ein Isomorphismus. Es ist $H = Ka_2 = E_H = A_H$ und $Z = 0 = E_E$. Weiter ist $C = 0$ und $(\varphi - 1)A_H \neq 0$, da φ nicht konstant ist. Nach dem Isomorphiesatz für $Z = 0$ hat φ keine Fortsetzung zu einem $\sigma \in \mathrm{Aut}E$.

Aus dem Isomorphisatz folgt der *Kürzungssatz* [10] von Witt (vgl §5 unten). Er bildet die Grundlage zur Definition eines Ringes von quadratischen Formen, den man den *Wittring* nennt. Dieser Ring ist heutzutage Forschungsgegenstand von Mathematikern in aller Welt. Den Wittring zu einem gegebenem Grundkörper zu bestimmen, ist eine im Allgemeinen noch ungelöste Aufgabe.

Der allgemeine Isomorphiesatz (ohne die Voraussetzung $Z = 0$) ergibt sich aus dem unten stehenden Reduktionssatz von Witt. Es sei π eine Projektion von E so, daß

$$E = Z \oplus \pi E \text{ und } D = (D \cap Z) \oplus \pi D$$

gilt. (Dazu wähle man Elemente $a_i \in E$ so, daß deren Restklassen mod $D \cap Z$ eine Basis von $D/D \cap Z$ bilden. Man ergänze diese Basis zu einer Basis $(a_j \bmod Z)_{j\in J}$ von E/Z und setze dann $\pi(z + \sum \lambda_j a_j) = \sum \lambda_j a_j$.) Für jedes $e \in E$ ist $e = z + \pi e$ mit einem $z \in Z$, also ist $\pi e - e \in Z$ für alle $e \in E$. Hieraus folgt, daß π eine Isometrie im Sinne von Definition 3.1 ist, denn es gilt $ee' = ee' + e(\pi e' - e') = e(\pi e') = e(\pi e') + (\pi e - e)\pi e' = (\pi e)(\pi e')$ und $\dot{\pi}(e) = e(\pi e - e) + N(\pi e - e) = N(\pi e - e) \equiv 0 \bmod \delta K$.

Seien A und B Teilräume von E und $\varphi : A \to B$ ein Isomorphismus. Wenn $\varphi(A \cap Z) \subseteq Z$ gilt, so induziert φ eine Abbildung $\varphi_\pi : \pi A \to \pi B$ vermöge $\varphi_\pi(\pi a) = \pi\varphi(a)$ für alle $a \in A$. Denn ist $\pi a = \pi a'$ für $a, a' \in A$, so ist $a = a' + z$ mit einem $z \in A \cap Z$, und es folgt dann $\pi\varphi(a) = \pi\varphi(a' + z) = \pi(\varphi(a') + \varphi(z)) = \pi\varphi(a')$, also ist φ_π wohldefiniert.

REDUKTIONSSATZ [11]. *Ein Isomorphismus $\varphi : A \to B$ mit $(\varphi - 1)A \subseteq D$ ist genau dann zu einem Automorphismus $\sigma \in G(D)$ fortsetzbar, wenn*

1. *φ eine Abbildung $\varphi_Z : A \cap Z \to B \cap Z$ induziert, die auf ein $\sigma_Z \in G(D \cap Z)$ fortsetzbar ist,*
2. *die induzierte Abbildung $\varphi_\pi : \pi A \to \pi B$ auf ein $\sigma_\pi \in G(\pi D)$ fortsetzbar ist.*

Beweis. Es sei φ zu einem $\sigma \in G(D)$ fortsetzbar. Für $z \in Z$ und $e \in E$ gilt $\sigma(z)e = \sigma(z)\,\sigma(\sigma^{-1}e) = z\,\sigma^{-1}e = 0$ und $0 = \dot{\sigma}(z) = z(\sigma z - z) + N(\sigma z - z) = N(\sigma z - z) \equiv N(\sigma z) + N(-z) \bmod \delta K$ nach (4′), also ist (da $N(-z) \in \delta K$) auch $N(\sigma z) \in \delta K$. Es folgt $\sigma(Z) \subseteq Z$, und $\sigma_Z := \sigma|_Z \oplus 1 \in G(D \cap Z)$ setzt $\varphi_Z = \varphi|_{A\cap Z}$ fort. Ist $e \in E$, so ist $e = z + \pi e$ mit einem $z \in Z$, also $\sigma(e) = \sigma(z) + \sigma(\pi e)$ und $\pi\sigma(e) = \pi\sigma(\pi e)$. Hieraus folgt, daß $\sigma_\pi := 1 \oplus \pi\sigma \in G(\pi D)$ eine Fortsetzung von φ_π ist.

Seien nun umgekehrt die Bedingungen 1. und 2. erfüllt. Dann induziert σ_π auf Z und σ_Z auf E/Z die Identität. Für $\psi = \sigma_Z^{-1}\sigma_\pi^{-1}\varphi - 1$ gilt dann $\psi(A \cap Z) = 0$ und $\psi(A) \subseteq D \cap Z$. Sei $(e_i)_{i\in I}$ eine Basis von A über K. Wir ergänzen diese Basis zu einer Basis $(e_i)_{i\in J}$ von E über K. Setzt man dann $\psi(e_i) = 0$ für alle $i \in J \setminus I$, so erhält man eine lineare Abbildung $\psi : E \to E$, die $\psi(Z) = 0$ und $\psi(E) \subseteq D \cap Z$ erfüllt. Es ist dann $(\psi + 1) \in G(D \cap Z)$ und $\sigma_\pi\sigma_Z(\psi + 1) \in G(D)$ eine Fortsetzung von φ. □

Wir nennen $\sigma_Z(\psi + 1)$ eine *Abweichung*.

Isomorphiesatz von Witt und Lenz. *D und $G = G(D)$ seien wie bisher erklärt. A, B seien Teilräume von E, und C sei ein Teilraum von A mit* $\dim A/C = n < \infty$.

Ein Isomorphismus $\varphi : A \to B$ mit $(\varphi - 1)C \subseteq Z$ und $(\varphi - 1)A \subseteq D$ läßt sich genau dann zu einem Automorphismus $\sigma \in G$ fortsetzen, wenn für passendes $\zeta \in G(D \cap Z)$

$$\varphi(A_{D_C}) = B_{D_C}, \quad (\varphi - 1)A_{D_C} \subseteq Z, \quad (\varphi - \zeta)(A \cap Z) = 0. \tag{8}$$

σ kann als Produkt von höchstens n Rotationen oder Spiegelungen $\sigma_i \in G(D_C)$ mit $(\sigma_i - 1)C = 0$ und einer Abweichung $\in G(D \cap Z)$ gewählt werden.

Beweis. Man beachte, daß allgemein für Teilräume U, V von E gilt $\pi(U_V) = \pi U_{\pi V}$. Sei $\sigma \in G(D)$ eine Fortsetzung von φ und also $\sigma_Z \in G(D \cap Z)$ und $\sigma_\pi \in G(\pi D)$ wie im Reduktionssatz gegeben. Dann ist die 3. Bedingung in (8) mit $\zeta = \sigma_Z$ erfüllt. Da $\pi Z = 0$ ist, ergibt der Isomorphiesatz für $Z = 0$ die Beziehungen

$$\varphi_\pi(\pi A_{D_C}) = \pi B_{D_C} \text{ und } (\varphi_\pi - 1)(\pi A_{D_C}) = 0.$$

Für $a \in A_{D_C}$ folgt $0 = (\varphi_\pi - 1)(\pi a) = \pi(\varphi a - a)$, also $\varphi a - a \in Z$, und daher gilt $(\varphi - 1)A_{D_C} \subseteq Z$. Sei $b \in B_{D_C}$. Dann gibt es ein $a \in A_{D_C}$ mit $\varphi_\pi(\pi a) = \pi b$. Es folgt $\pi(\varphi^{-1}b - b) = (\varphi_\pi^{-1} - 1)(\varphi_\pi(\pi a)) = \pi a - \varphi_\pi(\pi a) = \pi(a - \varphi a) = 0$ und daher $(\varphi^{-1} - 1)B_{D_C} \subseteq Z$. Nach Bemerkung b) unten implizieren die Bedingungen $(\varphi - 1)A_{D_C} \subseteq Z$ und $(\varphi^{-1} - 1)B_{D_C} \subseteq Z$ die ersten beiden Bedingungen in (8).

Es seien nun umgekehrt die drei Bedingungen in (8) erfüllt. Aus der letzten Bedingung in (8) folgt, daß 1. im Reduktionssatz erfüllt ist und daß φ einen Isomorphismus $\varphi_\pi : \pi A \to \pi B$ induziert. Wendet man π auf die ersten beiden Bedingungen in (8) an und berücksichtigt, daß $\pi Z = 0$ gilt, so ergibt der Isomorphiesatz für $Z = 0$ eine Fortsetzung $\sigma' : \pi E \to \pi E$ von φ_π, die sich aus Spiegelungen oder Rotationen $\sigma'_i \in G(\pi D_C)$ mit $(\sigma'_i - 1)(\pi C) = 0$ zusammensetzen läßt. Dann ist 2. im Reduktionssatz erfüllt mit $\sigma_\pi = 1 \oplus \sigma'$, und σ_π ist Produkt von höchstens n Spiegelungen oder Rotationen $\sigma_i \in G(\pi D_C)$, denn für $e = z + \pi ce \in E$ gilt $(\sigma_i - 1)(e) = ((1 \oplus \sigma'_i) - 1)(z + \pi e) = \sigma'_i(\pi e) - \pi e = (\sigma'_i - 1)(\pi e) \in \pi D_C$, insbesondere folgt $(\sigma_i - 1)(c) = (\sigma'_i - 1)(\pi c) = 0$ für alle $c \in C$. Man hat nun eine Fortsetzung $\sigma = \sigma_\pi \sigma_Z(\psi + 1)$ von φ, wobei die Abweichung $\sigma_Z(\psi + 1)$ in $G(D \cap Z)$ liegt. □

Bemerkung. a) Ist $(\varphi - 1)A_{D_C} \subseteq Z$, so ist $\varphi(A \cap Z) \subseteq B \cap Z$.

b) Die ersten beiden Bedingungen in (8) sind äquivalent zu $(\varphi - 1)A_{D_C} \subseteq Z$ und $(\varphi^{-1} - 1)B_{D_C} \subseteq Z$.

c) Für $D = H$ und $C = 0$ folgt die letzte Bedingung in (8) aus den ersten beiden.

Beweis. a) Es ist $A \cap Z \subseteq A \cap E_E = A_E \subseteq A_{D_C}$. Zu $a \in A \cap Z$ gibt es also ein $z \in Z$ mit $\varphi(a) = a + z \in Z$.

b) Sei $b \in B_{D_C}$ und $b = \varphi(a)$ mit $a \in A_{D_C}$. Dann ist $(\varphi^{-1} - 1)(b) = (\varphi^{-1} - 1)\varphi(a) = a - \varphi a \in Z$. Ist umgekehrt $a \in A_{D_C}$ und $(\varphi - 1)A_{D_C} \subseteq Z$, so ist $\varphi(a) \in A_{D_C} + Z \subseteq A_{D_C} + E_E \subseteq E_{D_C}$, also $\varphi(A_{D_C}) \subseteq B_{D_C}$. Analog impliziert $(\varphi^{-1} - 1)B_{D_C} \subseteq Z$, daß $\varphi^{-1}(B_{D_C}) \subseteq A_{D_C}$ gilt.

c) Da $Z \subseteq E_E$ gilt, ist jede lineare Abbildung $\sigma : Z \to Z$ metrisch, und wegen $N(Z) \subseteq \delta K$ gilt auch $\dot{\sigma}(z) = z(\sigma z - z) + N(\sigma z - z) = 0$ für alle $z \in Z$. Aus a) und b) folgt, daß φ einen Isomorphismus $A \cap Z \to B \cap Z$ induziert. Da A nach Voraussetzung endlich dimensional ist, läßt sich dieser Isomorphismus linear zu einem Automorphismus σ' von Z fortsetzen, und $\zeta := \sigma' \oplus 1$ ist in $G(Z)$. □

Für $D = H$ und $C = 0$ erhalten wir nun folgendes Korollar.

KOROLLAR. *Sei A ein endlich-dimensionaler Teilraum von E und $\varphi : A \to B$ ein Isomorphismus auf einen Teilraum B von E. Dann läßt sich φ genau dann zu einem Automorphismus σ von E fortsetzen, wenn $\varphi(A_H) = B_H$ und $(\varphi - 1)A_H \subseteq Z$.*

Der Isomorphiesatz von Witt und Lenz steht für $D = H$ und $(\varphi - 1)C = 0 = (\varphi^{-1} - 1)C$ in der ersten Auflage des Buches [6, S. 335f]. Das Korollar entspricht Satz 7 auf S. 335 l.c., wobei aber in [6] eine quadratische Form definiert ist als eine Abbildung $q : E \to K$, die $q(\lambda x) = \lambda^2 q(x)$ erfüllt und für die $q(x + y) - q(x) - q(y) = xy$ gilt mit einer vorgegebenen symmetrischen Bilinearform $(x, y) \mapsto xy$. In [6] wird σ soweit wie möglich aus Quasispiegelungen (das sind Automorphismen mit eindimensionaler Bahn) zusammengesetzt. Wenn $\delta K \neq 0$ ist, kann man das Auftreten von Rotationen ganz vermeiden [6, S. 340], im Allgemeinen aber nicht.

5. DER KÜRZUNGSSATZ

In diesem Abschnitt seien alle Vektorräume endlich dimensional. Es sei E ein metrischer Raum über einem Schiefkörper K und also E versehen mit einem Skalarprodukt, das (2) erfüllt. Für jeden Teilraum A von E benutzen wir wie bisher die folgenden Bezeichnungen

$$A^\perp = \{e \in E \,|\, eA = 0\} = E_A \quad \text{und} \quad \mathrm{Rad} A = A \cap A^\perp = A_A.$$

A heißt *regulär*, falls das Radikal Rad $A = 0$ ist.

5.1 DEFINITION. Es seien E_1 und E_2 zwei Teilräume von E mit den Eigenschaften
(i) $E = E_1 \oplus E_2$.
(ii) E_1 steht senkrecht auf E_2, d.h. $e_1 e_2 = 0$ für alle $e_1 \in E_1$ und $e_2 \in E_2$.
Wir schreiben dann $E = E_1 \perp E_2$ und nennen E die *orthogonale Summe* von E_1, E_2.

5.2 LEMMA. *Ist A ein regulärer Teilraum von E, so gilt $E = A \perp A^\perp$.*

Beweis. Der Dualraum $\mathrm{Hom}(A, K)$ von A ist ein Linksvektorraum, wenn man λf definiert durch $(\lambda f)(x) = f(x)\lambda^*$ für $\lambda \in K,\ x \in A$ und $f \in \mathrm{Hom}(A, K)$. Die Abbildung $A \to \mathrm{Hom}(A, K)$, $a \mapsto f_a$, wobei $f_a(x) = xa$ für alle $x \in A$ sei, ist dann linkslinear nach (2). Sie ist injektiv, da A regulär ist, und daher aus Dimensionsgründen auch surjektiv. Es sei $e \in E$ und $g : A \to K, x \mapsto xe$. Dann gibt es ein $a \in A$ so, daß $g = f_a$, also gilt für jedes $x \in A$

$$xe = g(x) = f_a(x) = xa, \quad \text{also} \quad x(e - a) = 0.$$

Es folgt $e - a \in A^{\perp}$, und wir haben eine Zerlegung $E = A + A^{\perp}$ gefunden. Da A regulär ist, folgt die Behauptung. □

Man nennt die in 5.1 definierte orthogonale Summe häufig auch *innere* orthogonale Summe, da es sich hier um die Summe von Teilräumen handelt.

Es seien nun zwei metrische Vektorräume E_1 und E_2 vorgegeben. Das Skalarprodukt auf E_i, $i = 1, 2$, bezeichnen wir dann mit f_i, und wir schreiben dann auch (E_i, f_i) anstelle von E_i. Für $f_i : E_i \times E_i \to K$ gelten dann die Regeln

$$(2) \qquad f_i(\lambda x, y) = \lambda f_i(x, y), \;\; f_i(x + y, z) = f_i(x, z) + f_i(y, z), \;\; \overline{f_i(x, y)} = f_i(y, x).$$

5.3 Definition. Seien (E_1, f_1) und (E_2, f_2) zwei metrische Vektorräume. Dann ist die *orthogonale Summe* $(E_1, f_1) \perp (E_2, f_2) =: (E, f)$ folgendermaßen definiert: Es ist $E = E_1 \oplus E_2$ und $f : E \times E \to K, \; \big((x_1, x_2), (y_1, y_2)\big) \mapsto f_1(x_1, y_1) + f_2(x_2, y_2)$.

Man überzeuge sich, daß auch f die Regeln (2) erfüllt. Es ist $E = E_1 \perp E_2$ im Sinne von Definition 5.1, da $f\big((x_1, 0), (0, y_2)\big) = 0$ ist für alle $x_1 \in E_1, \; y_2 \in E_2$.

5.4 Definition Eine linkslineare Abbildung $\varphi : E_1 \to E_2$ heißt *metrisch*, falls

$$f_2(\varphi x, \varphi y) = f_1(x, y)$$

für alle $x, y \in E_1$ gilt. Ist φ bijektiv, so heißt φ ein *Isomorphismus*.

Ist $\varphi : E_1 \to E_2$ eine metrische Abbildung und ist E_1 regulär, so ist φ injektiv, denn andernfalls gäbe es ein $x \in E_1$ mit $\varphi(x) = 0$ und ein $y \in E_1$ mit $f_1(x, y) \neq 0$, aber $f_2(\varphi x, \varphi y) = 0$.

Wir erhalten nun den Kürzungssatz von Witt für metrische Räume als Korollar zum Satz von Witt. Dabei benutzen wir auch das Zeichen $A \simeq B$, wenn A und B isomorph sind.

Kürzungssatz. *Die vorkommenden Räume seien regulär und gerade. Wenn*

$$(E_1, f_1) \perp (E_2, f_2) \simeq (E_1', f_1') \perp (E_2', f_2') \quad \textit{und} \quad (E_1, f_1) \simeq (E_1', f_1')$$

gilt, so gilt auch $(E_2, f_2) \simeq (E_2', f_2')$.

Beweis. Es sei $(E, f) := (E_1, f_1) \perp (E_2, f_2)$ und $(E', f') := (E_1', f_1') \perp (E_2', f_2')$, also $E = E_1 \perp E_2$ und $E' = E_1' \perp E_2'$. Nach Voraussetzung gibt es Isomorphien

$$\varphi : E \to E' \quad \text{und} \quad \varphi_1 : E_1 \to E_1'.$$

Wir betrachten die metrische Abbildung $\varphi^{-1} \circ \varphi_1 : E_1 \to E$ und setzen $A = E_1$ und $B = (\varphi^{-1} \circ \varphi_1)E_1$. Dann hat $\varphi^{-1} \circ \varphi_1 : A \to B$ nach dem Satz von Witt eine Fortsetzung zu einem $\sigma \in \mathrm{Aut}E$, und $\varphi \circ \sigma : E \to E'$ ist dann ein Isomorphismus, der φ_1 fortsetzt. Es ist $E_1^{\perp} = E_2$, da $E_2 \subseteq E_1^{\perp}$ gilt und daher nach Lemma 5.2 aus Dimensionsgründen die Gleichheit folgt. Analog ist $E_1'^{\perp} = E_2'$. Es folgt nun, daß $\varphi \circ \sigma$ ein Isomorphismus ist, der E_2 auf E_2' abbildet. □

Es sei $\delta K = 0$, also K kommutativ und $\mathrm{Char} K \neq 2$. Dann ist eine quadratische Form $q : E \to K$ eindeutig durch ihr zugehöriges Skalarprodukt $f(x,y)$ bestimmt. Wir nennen dann auch q *regulär*, falls E regulär ist, und wir sagen, daß zwei quadratische Formen $q_1 : E_1 \to K$ und $q_2 : E_2 \to K$ *isomorph* sind, wenn es eine bijektive lineare Abbildung $\varphi : E_1 \to E_2$ gibt mit $q_2(\varphi x) = q_1(x)$ für alle $x \in E_1$. Aus (4) folgt dann, daß φ eine metrische Abbildung im Sinne von Definition 5.4 ist. Die *orthogonale Summe* $q_1 \perp q_2$ wird definiert als Abbildung $q_1 \perp q_2 : E_1 \oplus E_2 \to K$, $(x,y) \mapsto q_1(x) + q_2(y)$.

Kürzungssatz für quadratische Formen. *Seien q_1, q_2 und q reguläre quadratische Formen. Ist $q \perp q_1 \simeq q \perp q_2$, so ist $q_1 \simeq q_2$.*

6. Der Wittring

In diesem Abschnitt ist $\delta K = 0$, also K kommutativ und Char $K \neq 2$. Es sei E ein endlich dimensionaler Vektorraum der Dimension n über K und $q : E \to K$ eine quadratische Form mit Bilinearform $f(x,y) := \frac{1}{2}\big(q(x+y) - q(x) - q(y)\big)$. Es gilt dann $f(x,x) = q(x)$. Die *Dimension von q* definieren wir als die Dimension von E über K. Ferner benutzen wir die Definitionen am Ende von Abschnitt 5.

Beschreibung von q bezüglich einer Basis:

Sei $e_1, \dots e_n$ eine Basis von E. Dann gilt für jedes $x \in E$

$$q(x) = \sum e_{ik} \lambda_i \lambda_k$$

mit $e_{ik} = f(e_i, e_k)$; dabei sind λ_i die Koordinaten von x bezüglich der Basis $e_1, \dots, e_n$. Die Matrix $M = (e_{ik})$ heißt die *zu q gehörige Matrix bezüglich der Basis* $e_1, \dots, e_n$.

Ist q regulär, so ist $\det M \neq 0$, denn dann ist die lineare Abbildung $E \to \mathrm{Hom}(E,K)$, $e \mapsto f_e$ mit $f_e(x) = xe$ für alle $x \in E$, bijektiv. Man sieht dann, daß (e_{ik}) gerade die Matrix dieses Vektorraumisomorphismus ist bezüglich der Basis $\{e_i\}$ von E und der zu $\{e_i\}$ gehörigen Dualbasis von $\mathrm{Hom}(E,K)$ und also invertierbar ist.

Verhalten bei Basistransformation

Es seien $e_1, \dots, e_n$ und $e'_1, \dots, e'_n$ Basen von E und $S = (s_{ik})$ die Übergangsmatrix d.h. $e'_i = \sum_l s_{li} e_l$. Dann gilt für die zugehörigen Matrizen M, M' bezüglich $\{e_i\}$, $\{e'_i\}$:

$$M' = S^t \, M \, S,$$

wobei S^t die zu S transponierte Matrix bezeichnet, denn für das Element an der Stelle (i,k) in der Matrix M' gilt $f(e'_i, e'_k) = f\big(\sum_l s_{li}\, e_l, \sum_j s_{jk}\, e_j\big) = \sum_{l,j} s_{li}\, f(e_l, e_j)\, s_{jk}$.

Zwei $(n \times n)$–Matrizen M und M' heißen *kongruent*, wenn es eine invertierbare Matrix S gibt derart, daß $M' = S^t \, M \, S$ gilt.

6.1 Satz. *Zwei quadratische Formen sind genau dann isomorph, wenn die zugehörigen Matrizen kongruent sind (bezüglich beliebiger Basen).*

Beweis. Seien $q : E \to K$ und $q' : E' \to K$ quadratische Formen, M die zu q gehörige Matriz bezüglich einer Basis $e_1, \ldots, e_n$ von E und M' die Matrix von q' bezüglich einer Basis $e'_1, \ldots, e'_n$ von E'. Eine lineare Abbildung $\varphi : E \to E'$ wird beschrieben durch eine Matrix $S = (s_{ik})$ mit $\varphi(e_i) = \sum s_{ki} e'_k$, und φ ist genau dann ein Isomorphismus, wenn S invertierbar ist und wenn

$$x^t\, M\, y = f(x,y) = f'(\varphi x, \varphi y) = x^t\, S^t\, M'\, S\, y$$

für alle $x \in E$ gilt; dabei fassen wir x und y als Spaltenvektoren auf (vgl. die Beschreibung des Skalarproduktes bezüglich einer Basis in §1 und 5.4). □

Aus 6.1 erhält man eine Beschreibung der Automorphismengruppe von E durch Matrizen. Es sei M die zu q gehörige Matrix bezüglich einer Basis von E. Dann ist $\mathrm{Aut}E = \{\varphi : E \xrightarrow{\sim} E \mid q(\varphi x) = q(x) \text{ für alle } x \in E\} \cong \{S \mid \det S \neq 0,\ \ S^t\, M\, S = M\}$. Man nennt diese Gruppe eine *orthogonale Gruppe* und schreibt auch $\mathrm{Aut}q$ dafür.

6.2 Satz. *E ist orthogonale Summe von eindimensionalen Unterräumen; mit anderen Worten: E besitzt eine Basis, die aus paarweise orthogonalen Vektoren besteht (eine "Orthogonalbasis").*

Beweis durch Induktion nach der Dimension von E. Wenn die Bilinearform f identisch Null ist, ist jede Zerlegung von E eine orthogonale Zerlegung. Sei $f \neq 0$. Dann gibt es Vektoren x, $y \in E$ mit $f(x,y) \neq 0$. Es ist $f(x,y) = \frac{1}{2}\big(f(x+y,x+y) - f(x,x) - f(y,y)\big)$, also gibt es einen Vektor $z \in E$ mit $f(z,z) \neq 0$, nämlich x, y oder $x+y$. Der Raum $E_1 = Kz$ ist regulär, und daher gilt $E = E_1 \perp E_1^\perp$ nach 5.2. Wendet man nun die Induktionsvoraussetzung auf $E_1^\perp$ an, so erhält man die gewünschte Zerlegung. □

Bezüglich einer Orthogonalbasis hat die zu q gehörige Matrix Diagonalgestalt. Man schreibt dann auch

$$q = (\alpha_1, \ldots, \alpha_n)$$

und sagt, q sei in *Diagonalform* gegeben.

6.3 Definition. Ein Element $\alpha \in K$ wird *dargestellt von q*, wenn es einen Vektor $x \in E$ gibt mit $q(x) = \alpha$. Die Form q heißt *isotrop*, falls q die Null nichttrivial darstellt, d.h falls es einen Vektor $x \neq 0$ in E gibt mit $q(x) = 0$, andernfalls heißt q *anisotrop*. In dieser Definition braucht nicht vorausgesetzt zu werden, daß Char $K \neq 2$ ist.

Beispiel einer isotropen Form: Es sei $n = 2$, und $q : E \to K$ sei gegeben durch die Matrix $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ bezüglich einer Basis e_1, e_2. Es ist $q(\lambda_1 e_1 + \lambda_2 e_2) = \lambda_1^2 - \lambda_2^2$, also $q(e_1 + e_2) = 0 = q(e_1 - e_2)$. Bezüglich der Basis $e'_1 = \frac{1}{2}(e_1 + e_2)$, $e'_2 = e_1 - e_2$ hat q die Matrix $M' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Als Übergangsmatrix erhält man dann die Matrix $S = \begin{pmatrix} 1/2 & 1 \\ 1/2 & -1 \end{pmatrix}$, und man rechne $M' = S^t\, M\, S$ nach. E wird eine *hyperbolische Ebene* genannt.

6.4 SATZ. *Sei q eine 2-dimensionale reguläre quadratische Form auf E. Ist q isotrop, so ist E eine hyperbolische Ebene. Es gibt dann nämlich eine Basis u, v von E mit $q(u) = 0 = q(v)$ und $f(u, v) = 1$.*

Beweis. Nach Voraussetzung gibt es ein $u \in E \setminus 0$ mit $q(u) = 0$. Da q regulär ist, gibt es ein $w \in E$ mit $f(u, w) =: \alpha \neq 0$. Da $f(u, \alpha^{-1} w) = a^{-1} \alpha = 1$ ist, kann man also ohne Einschränkung annehmen, daß $f(u, w) = 1$ gilt. Wir setzen nun $\lambda = -\frac{1}{2} q(w)$ und $v = \lambda u + w$. Dann ist $f(u, v) = f(u, \lambda u + w) = \lambda^2 f(u, u) + f(u, w) = 1$ und also $q(v) = q(\lambda u + w) = q(\lambda u) + q(w) + 2f(\lambda u, w) = q(w) + 2\lambda f(u, w) = 0$. Ist $v = \mu u$, so ist $f(u, v) = \mu f(u, u) = 0$, und man hat einen Widerspruch. Also sind u und v linear unabhängig. □

6.5 SATZ. *Ist q regulär, so läßt sich q schreiben in der Form*

$$q \simeq (1, -1) \perp \ldots \perp (1, -1) \perp q_0$$

mit $r \geq 0$ Summanden $(1, -1)$ und einer anisotropen Form q_0. Die Darstellung ist bis auf Isomorphie eindeutig.

Beweis. Ist q anisotrop, so wähle man $q = q_0$ und $r = 0$. Es sei nun q isotrop, also gibt es einen Vektor $x \neq 0$ mit $q(x) = 0$. Da q regulär ist, gibt es $z \in E$ mit $f(x, z) = \alpha \neq 0$. Wir können dann annehmen, daß $f(x, z) = 1$ ist (durch Multiplikation von z mit α^{-1}). Setzen wir $y = z - \frac{1}{2} f(z, z) x$, so spannen x, y eine hyperbolische Ebene E_1 auf, denn mit Hilfe von (2) rechnet man nach, daß $f(y, y) = 0$ und $f(x, y) = 1$ gilt. Nach 5.2 ist $E = E_1 \perp E_1^{\perp}$, also $q \simeq (1, -1) \perp q'$ mit einer regulären Form q'. Ist q' anisotrop, so sind wir fertig, andernfalls verfahren wir wie eben. Da E endlich dimensional ist, erhalten wir schließlich die gewünschte Zerlegung. Die Eindeutigkeit der Darstellung folgt aus dem Kürzungssatz für quadratische Formen. □

6.6 DEFINITION. Die Form q_0 in 6.5 heißt der *anisotrope Kern* von q; er ist bis auf Isomorphie eindeutig. Die Zahl r heißt der *Wittindex* von q. Wir sagen, daß zwei reguläre quadratische Formen q, q' *ähnlich* sind, im Zeichen $q \sim q'$, wenn ihre anisotropen Kerne isomorph sind.

Die Ähnlichkeitsrelation ist eine Äquivalenzrelation. Mit $\bar{q}$ bezeichnen wir die Ähnlichkeitsklasse von q. Jede Ähnlichkeitsklasse $\bar{q}$ enthält (bis auf Isomorphie) genau eine anisotrope Form, nämlich q_0, und jedes Element in $\bar{q}$ hat die Form $m \times (1, -1) \perp q_0$. Die Klassifikation der quadratischen Formen über K läuft also auf die Bestimmung der Ähnlichkeitsklassen der regulären quadratischen Formen über K hinaus. Die Menge dieser Ähnlichkeitsklassen bezeichnet man mit $W(K)$.

Seien $q_1 : E_1 \to K$ und $q_2 : E_2 \to K$ zwei reguläre quadratische Formen. Die orthogonale Summe $q_1 \perp q_2 : E_1 \oplus E_2 \to K, (x, y) \mapsto q_1(x) + q_2(y)$ und das Tensorprodukt $q_1 \otimes q_2 : E_1 \otimes E_2 \to K$ mit $(q_1 \otimes q_2)(x \otimes y) = q_1(x) q_2(y)$ induzieren dann entsprechende Operationen auf $W(K)$:

$$\bar{q}_1 \perp \bar{q}_2 = \overline{q_1 \perp q_2} \text{ und } \bar{q}_1 \bar{q}_2 = \overline{q_1 \otimes q_2}.$$

Mit dieser Addition und Multiplikation wird $W(K)$ ein kommutativer Ring mit Einselement $\overline{(1)}$. Das Nullelement ist die Klasse von $(1, -1)$, und das (additive) Inverse von $q = (\alpha_1, \ldots, \alpha_n)$ wird durch die Form $-q = (-\alpha_1, \ldots, -\alpha_n)$ repräsentiert. Liegen q_1 und q_2 in Diagonalform vor, $q_1 = (a_1, \ldots, a_r)$ und $q_2 = (b_1, \ldots, b_s)$, so ist $q_1 \oplus q_2 = (a_1, \ldots, a_r, b_1, \ldots, b_s)$ und $q_1 \otimes q_2 = (a_1 b_1, a_1 b_2, \ldots, a_1 b_s, \ldots, a_r b_1, \ldots, a_r b_s)$.

Beispiel: Es sei K quadratisch abgeschlossen, d.h. jedes Element $\lambda \in K$ hat die Form μ^2 für ein $\mu \in K$, wie das zum Beispiel für $K = \mathbb{C}$ der Fall ist. Dann ist jede Form isomorph zu einer Diagonalform mit lauter Einsen: $q \simeq (1, 1, \ldots, 1) = m \times 1$ mit $m = \dim q$. Jede Form ist also allein schon durch ihre Dimension bestimmt. Wegen $(1) \simeq (-1)$ folgt $W(K) \cong \mathbb{Z}/2\mathbb{Z}$, wobei ein Isomorphismus durch $\bar{q} \mapsto \dim q \bmod 2$ gegeben ist.

7. Die Sätze von Artin–Springer und Knebusch

Ist L ein Erweiterungskörper eines Körpers K, so kann man jede quadratische Form über K auch als eine quadratische Form über L auffassen, und man hat einen kanonischen Ringhomomorphismus

$$W(K) \to W(L).$$

Dieser Homomorphismus ist im allgemeinen nicht injektiv, z.B. ist die Diagonalform $q = (1,1)$ anisotrop über $\mathbb{R}$, aber isotrop über $\mathbb{C}$, denn es ist $q(\lambda_1, \lambda_2) = \lambda_1^2 + \lambda_2^2$, also $q(x) \neq 0$ für alle $x = (\lambda_1, \lambda_2) \in \mathbb{R}^2$, und läßt man auch Koeffizienten aus $\mathbb{C}$ zu, so ist $q(1, \mathrm{i}) = 0$, also $\bar{q} = 0$ in $W(\mathbb{C})$ nach 6.4. In der berühmten Arbeit [10] aus dem Jahre 1937 äußerte Witt die Vermutung, daß aber bei Grundkörpererweiterung ungeraden Grades $W(K) \to W(L)$ injektiv ist. Bereits 1937 teilte ihm Artin einen Beweis dafür mit, der aber nicht veröffentlicht wurde. Denselben Beweis fand dann unabhängig 1952 Springer [9]. Auch den unten stehenden Satz 2 von Knebusch [3] hatte Witt (in einer etwas abgeschwächten Form) vermutet, und zwar 1968. Später, 1973, fand Witt dann eine gemeinsame Beweisidee für den Satz von Artin–Springer und den Satz von Knebusch. Deren Beweise sind einfach als "additive" und "multiplikative" Variante dieser Idee anzusehen. Hierüber hat Witt 1973 in Barcelona auf Spanisch vorgetragen, was nun (auf Deutsch) in seinen Gesammelten Abhandlungen [12] erscheinen wird und dort auf einer einzigen Seite. Wir setzen voraus, daß $\delta K = 0$ ist, aber die Charakteristik von K beliebig ist.

Bezeichnungen: Es sei $q : E \to K$ eine n-dimensionale quadratische Form $\neq 0$ über einem Körper K, wobei wir die Gleichung (4) (analog zu (4′)) in der Form

$$q(x+y) = q(x) + q(y) + xy \tag{4}$$

schreiben. Die Gleichung (3) $q(\lambda x) = \lambda^2 q(x)$ und die Gleichung (4) gelten auch über dem Quotientenkörper $K(t)$ von $K[t]$, insbesondere können die Komponenten der Vektoren x und y in (3) und (4) auch Polynome aus $K[t]$ sein. Wir betrachten Polynome f, g_i, $h \in K[t]$ und definieren $Q = q(g_1, \ldots, g_n)$.

Es sei $|f| = \mathrm{Grad} f$ und N die Norm von L über K. Ferner sei $D(q)$ die Menge der von q dargestellten Elemente von $K^* = K \setminus 0$, also $D(q) = \{\alpha \in K^* \mid \alpha = q(x)$ für ein $x \in E\}$, und entsprechend sei $D(q_L) = (\mathrm{bild}(q_L) \setminus 0) \subseteq L^*$. Es bezeichne $D(q)^m$

die Menge aller Produkte von m Faktoren aus $D(q)$. Es sei ggT die Abkürzung für "größter gemeinsamer Teiler".

Wir sagen, daß q *regulär* ist, falls die zugehörige Bilinearform $(x, y) \mapsto xy$ nicht ausgeartet ist. Bei Char$K = 2$ kann es vorkommen, daß eine anisotrope Form nicht regulär ist, sonst aber nicht.

Beispiel 1: Es sei q regulär und isotrop. Dann ist $D(q) = K^*$, wie man folgendermaßen einsieht. Es sei $x \neq 0$ in E und $q(x) = 0$. Da q regulär ist, gibt es ein $y \in E$ mit $xy \neq 0$. Man kann dann y so wählen, daß $xy = 1$ gilt, und (4) ergibt dann $q(\mu x + y) = q(y) + \mu$ für jedes $\mu \in K$, da $q(\mu x) = \mu^2 q(x) = 0$ gilt. Für $\alpha \in K^*$ setze man nun $\mu = \alpha - q(y)$ und erhält $q(\mu x + y) = \alpha$. Es folgt $D(q) = K^*$, und insbesondere ist $D(q)$ eine Gruppe. Da dann $1 \in D(q)$ ist, folgt $D(q) = D(q)^m$ für alle $m > 0$.

Beispiel 2: Ist $\alpha \in K^*$ und $\alpha = \beta^2$ für ein $\beta \in K^*$, so ist $\alpha \in D(q)^2$, denn sei $c \in D(q)$ beliebig, $c = q(x)$ mit einem $x \in E$. Dann folgt $\alpha = \beta^2 = \beta^2 c^{-2} cc = \beta^2 c^{-2} q(x) q(x) = q(\beta c^{-1} x) q(x)$ nach (3). Insbesondere ist $1 \in D(q)^2$, also $D(q)^m \subseteq D(q)^{m+2k}$ für jedes $k \geq 0$.

7.1 SATZ. *Ist $\alpha \in D(q)$, so ist $q \perp (-\alpha)$ isotrop. Umgekehrt gilt: Ist q anisotrop oder regulär und ist $q \perp (-\alpha)$ isotrop für $\alpha \in K^*$, so ist $\alpha \in D(q)$.*

Beweis. Die eindimensionale Form $q' := (-\alpha)$ ist gegeben als Abbildung $q' : E_1 \to K$ eines eindimensionalen K- Vektorraumes $E_1 = Ky$ nach K so, daß $q'(\lambda y) = -\alpha\lambda^2$ gilt für alle $\lambda \in K$.

Sei $\alpha \in D(q)$. Dann gibt es einen Vektor $x \in E$ mit $q(x) = \alpha$, also $0 = q(x) - \alpha = (q \perp (-\alpha))(x, y)$, und es ist $(x, y) \neq 0$ in $E \oplus E_1$.

Sei $q \perp (-\alpha)$ isotrop. Ist q anisotrop, so gibt es ein $x \in E$ und ein $\lambda \in K^*$ mit $q(x) - \alpha\lambda^2 = 0$, und es folgt $\alpha = \lambda^{-2} q(x) = q(\lambda^{-1} x)$ und also $\alpha \in D(q)$. Ist q isotrop und regulär, so ist $\alpha \in D(q)$ nach Beispiel 1. □

LEMMA 1 [12]. *Sei q anisotrop. Für jeden Teiler f von Q mit* $\mathrm{ggT}(f, g_1, \ldots, g_n) = 1$ *ist $|f|$ gerade.*

Beweis durch Induktion über $|f|$. Ist $|f| = 0$, so ist $|f|$ gerade. Sei nun $|f| > 0$.

Ohne Einschränkung können wir annehmen, daß $|g_i| < |f|$ gilt, denn andernfalls ist $g_i = r_i f + g_i'$ mit $|g_i'| < |f|$, und wir können g_i durch g_i' ersetzen, denn aus (3) und (4) folgt, daß f auch ein Teiler von $q(g_1', \ldots, g_n')$ ist. Dabei können wir annehmen, daß nicht alle $g_i' = 0$ sind, denn andernfalls folgt aus der Voraussetzung $\mathrm{ggT}(f, g_1, \ldots, g_n) = 1$, daß f konstant ist und also $|f| = 0$ gerade ist.

Wir zeigen nun, daß Q geraden Grad hat. Es sei m das Maximum der Grade der Polynome g_i. Wir setzen $g_i^* = \alpha_i t^m$, wobei α_i der Koeffizient von t^m in g_i ist, also ist $\alpha_i = 0$ möglich, aber nicht für alle i. Es ist dann $g_i = g_i^* + \tilde{g}_i$, wobei $|\tilde{g}_i| < m$ ist. Setzen wir $x = (g_1^*, \ldots, g_n^*)$ und $y = (\tilde{g}_1, \ldots, \tilde{g}_n)$, so ist nach (4) ist $Q = q(x + y) = q(x) + q(y) + xy$, wobei $q(y)$ und xy kleineren Grad als $q(x)$ haben, denn da q anisotrop ist, ist $q(x) = t^{2m} q(\alpha_1, \ldots, \alpha_n) \neq 0$ und $|Q| = 2m$ gerade.

Da f nach Voraussetzung ein Teiler von Q ist, ist $Q = hf$ mit einem Polynom h, für das $|h| < |f|$ gilt, da $m < |f|$ ist. Sei $\mathrm{ggT}(h, g_1, \ldots, g_n) =: \tau$. Dann wird Q von

τ^2 geteilt nach (3). Da aber nun f nicht von τ geteilt wird (wegen der Voraussetzung $\mathrm{ggT}(f, g_1, \dots, g_n) = 1$), ist τ^2 ein Teiler von h. Es folgt $Q = \tau^2\, h' f$ mit einem Polynom h', das $\mathrm{ggT}(h', g_1, \dots, g_n) = 1$ und $|h'| < |f|$ erfüllt. Nach Induktionsvoraussetzung ist dann $|h'|$ gerade, und es folgt, daß mit Q und h' auch f geraden Grad hat. ◻

LEMMA 2 [12]. *Sei q anisotrop. Für jeden normierten Teiler f von $1 + tQ$ ist $f(0) \in D(q)^{|f|}$.*

Beweis durch Induktion über $|f|$. Ist $|f| = 0$, so ist $f = 1$, da f normiert ist, also $f(0) = 1 \in D(q)^0$ mit der Konvention, daß ein Produkt aus 0 Faktoren 1 ist. Sei $|f| > 0$ und ohne Einschränkung wie oben $|g_i| < |f|$. Es ist $1 + tQ = cfh$ mit $c \in K^*$ und $h \in K[t]$ normiert. Analog wie im Beweis von Lemma 1 gibt es einen Vektor $(\alpha_1, \dots, \alpha_n) \neq 0$ in E so, daß nach (4) gilt $cfh = 1 + tQ = 1 + t^{2m+1} q(\alpha_1, \dots, \alpha_n) + t\tilde{g}$ mit $|\tilde{g}| < 2m$. Durch Koeffizientenvergleich folgt nun $c = q(\alpha_1, \dots, \alpha_n) \in D(q)$ und $|h| < |f|$. Mit c ist auch c^{-1} in $D(q)$, denn $c = q(a)$ impliziert $q(c^{-1}a) = c^{-2}c = c^{-1}$. Für $t = 0$ folgt $1 = cf(0)h(0)$, also $f(0) = c^{-1}h(0)^{-1}$. Wenden wir die Induktionsvoraussetzung auf h an, so folgt $f(0) \in D(q)\, D(q)^{|h|} = D(q)^{|h|+1}$. Es ist $|f| - (|h| + 1)$ gerade, da tQ ungeraden Grad hat und $1 + tQ = cfh$ ist. Nach Beispiel 2 oben ist $D(q)^{|h|+1} \subseteq D(q)^{|f|}$. ◻

SATZ 1 [9]. *Eine anisotrope Form $q : E \to K$ bleibt anisotrop bei jeder Körpererweiterung L/K ungeraden Grades.*

Beweis. Es genügt, dies für eine einfache Erweiterung $L = K(\alpha)$ zu zeigen. Sei f das Minimalpolynom von α über K. Dann kann jedes Element aus L geschrieben werden als $g(\alpha)$, wobei $g \in K[t]$ ein Polynom vom Grad $< |f|$ ist. Ist q_L isotrop, so gibt es also Polynome $g_1, \dots, g_n \in K[t]$ mit $|g_i| < |f|$ und $Q = q_L(g_1, \dots, g_n) \equiv 0 \bmod f$, d.h. f teilt Q. Nach Lemma 1 ist nun $(L : K) = |f|$ gerade. ◻

SATZ 2 [3]. *Sei $q : E \to K$ eine reguläre quadratische Form und L eine Körpererweiterung von K vom Grad $m < \infty$. Dann ist $\mathrm{N}(D(q_L)) \subseteq D(q)^m$.*

Beweis. Ist q isotrop, so ist die Behauptung trivial nach Beispiel 1. Sei nun q anisotrop. Wir führen den Beweis durch Induktion nach m. Für $\alpha \in D(q_L)$ haben wir zu zeigen, daß $\mathrm{N}(\alpha) \in D(q)^m$ gilt.

1. Fall: Es ist $\alpha \in K$. Dann ist $\mathrm{N}(\alpha) = \alpha^m$. Angenommen, es gilt $\alpha^m \notin D(q)^m$. Dann ist m nach Beispiel 2 ungerade, $\alpha \notin D(q)$ und daher $(-\alpha) \perp q$ anisotrop nach 7.1. Nach Satz 1 ist dann auch $(-\alpha) \perp q_L$ anisotrop im Widerspruch dazu, daß $\alpha \in D(q_L)$ liegt.

2. Fall: Es ist $\alpha \notin K$ und $L = K(\alpha)$. Es sei f das Minimalpolynom von $-\alpha$ über K, also $\mathrm{N}(\alpha) = \mathrm{f}(0)$. Analog wie im Beweis von Lemma 2 zeigt man, daß mit α auch α^{-1} in $D(q_L)$ liegt und also $\alpha^{-1} = q_L(g_1(-\alpha), \dots, g_n(-\alpha))$ mit $g_i \in K[t]$ gilt. Es folgt $1 = \alpha q_L(g_1(-\alpha), \dots, g_n(-\alpha)) = \alpha Q(-\alpha)$, also $0 \equiv 1 + tQ \bmod f$. Daher ist f ein Teiler von $1 + tQ$, und nach Lemma 2 folgt $\mathrm{N}(\alpha) \in D(q)^m$.

3. Fall: Es ist $\alpha \notin K$ und $K(\alpha)$ echt in L enthalten. Es gilt $\mathrm{N}_{L/K} = \mathrm{N}_{K(\alpha)/K} \circ \mathrm{N}_{L/K(\alpha)}$ und $\mathrm{N}_{L/K(\alpha)}(\alpha) \in D(q_{K(\alpha)})^r$ mit $r = (L : K(\alpha))$ trivialerweise, wenn $q_{K(\alpha)}$ isotrop ist, und sonst nach dem 1. Fall angewandt auf $K(\alpha)$, da $\alpha \in K(\alpha)$ gilt. Es folgt nun $\alpha \in D(q)^m$ nach Induktionsvoraussetzung und da die Norm multiplikativ ist. ◻

LITERATUR

1. *J. Dieudonné:* La Géométrie des Groupes Classiques. Springer–Verlag 1955.
2. *A. J. Hahn und O. T. O'Meara:* The Classical Groups and K–Theory. Springer–Verlag 1989.
3. *M. Knebusch:* Ein Satz über die Werte von quadratischen Formen über Körpern über Körpern. Invent. Math. 12, (1971), 300-303.
4. *M. A. Knus:* Quadratic and Hermitian Forms over Rings. Springer–Verlag 1991.
5. *T. Y. Lam:* The algebraic theory of quadratic forms. Benjamin 1973.
6. *H. Lenz:* Grundlagen der Elementarmathematik. VEB Deutscher Verlag der Wissenschaften, 1. Auflage, 1961.
7. *F. Lorenz:* Quadratische Formen über Körpern. Lecture Notes in Math. vol. 130. Springer–Verlag 1970.
8. *W. Scharlau:* Quadratic and Hermitian forms. Springer–Verlag 1985.
9. *T. A. Springer:* Sur les formes quadratiques d'indice zéro. C.R. Acad. Sci. 234, (1952), 1517-1519.
10. *E. Witt:* Quadratische Formen über beliebigen Körpern. J. Reine Angew. Math. 176, (1937,) 31–44.
11. *E. Witt und H. Lenz:* Euklidische Kongruenzsätze in metrischen Vektorräumen. Unveröffentlicht 1957. Erscheint in: Ernst Witt, Gesammelte Abhandlungen, Collected Papers. Springer-Verlag.
12. *E. Witt:* Über die Sätze von Artin-Springer und Knebusch. Unveröffentlicht 1973. Erscheint in: Ernst Witt, Gesammelte Abhandlungen, Collected Papers. Springer-Verlag.