

# I. Bilineare und quadratische Formen

In diesem Kapitel wird die grundlegende Theorie der symmetrischen Bilinearformen und quadratischen Formen über beliebigen kommutativen Ringen in geometrischer Sprechweise entwickelt. Naturgemäß benötigen Resultate wie der Wittsche Kürzungssatz oder die Erzeugung orthogonaler Gruppen durch Spiegelungen weitere Voraussetzungen insbesondere an den Grundring: dieser muß ein Körper oder ein lokaler Ring sein. Ist die Charakteristik ungleich 2 (oder besitzt allgemeiner  $1 + 1 = 2$  im Grundring ein Inverses  $\frac{1}{2}$ ), so entsprechen sich symmetrische Bilinearformen und quadratische Formen umkehrbar eindeutig. Andererseits gibt es in Charakteristik 2 Situationen, wo sich quadratische Formen besser verhalten als symmetrische Bilinearformen, so daß eine sorgfältige Unterscheidung angebracht erscheint.

Alle in dieser Vorlesung vorkommenden Ringe sollen ein Einselement 1 haben, alle Ringhomomorphismen Eins in Eins überführen, und für  $A$ -Moduln  $E$  gelte stets  $1 \cdot x = x$  für alle  $x \in E$ . In diesem ersten Kapitel sind zudem alle Ringe kommutativ.

## 1 Symmetrische Bilinearformen

Im folgenden ist  $A$  ein kommutativer Ring,  $E$  ein  $A$ -Modul und  $b : E \times E \rightarrow A$  eine symmetrische Bilinearform auf  $E$ , also  $b(x, y)$  linear in  $x$  (bzw.  $y$ ) bei festem  $y$  (bzw.  $x$ ) und  $b(x, y) = b(y, x)$ .

### (1.1) Definition

- a) Zwei Elemente  $x$  und  $y$  von  $E$  stehen *senkrecht aufeinander* oder sind *orthogonal* (bezüglich  $b$ ), falls  $b(x, y) = 0$  ist.
- b) Für eine Teilmenge  $F$  von  $E$  nennen wir  $F^\perp = \{y \in E \mid b(F, y) = 0\}$  den zu  $F$  *orthogonalen Untermodul*.
- c)  $E$  heißt *orthogonale Summe* der Untermoduln  $E_1, \dots, E_n$ , in Formeln

$$E = E_1 \perp \dots \perp E_n = \perp_{i=1}^n E_i,$$

wenn  $E$  direkte Summe der  $E_i$  ist und  $b(E_i, E_j) = 0$  für  $i \neq j$ .

Für einen  $A$ -Modul  $E$  bezeichne  $E^* = \text{Hom}(E, A)$  den dualen Modul der Linearformen auf  $E$ . Für den Wert einer Linearform  $u$  an der Stelle  $x$  schreiben wir auch  $u(x) = \langle x, u \rangle$ .

Wenn  $E = F \perp F'$  ist, so gilt offensichtlich  $F' \subseteq F^\perp$ . Umgekehrt fragen wir uns bei gegebenem Untermodul  $F$ , wann  $E = F \perp F^\perp$  ist. Hierzu führen wir den folgenden Modulhomomorphismus  $b_F$  ein:

$$(1.2) \quad b_F : E \rightarrow F^*, \quad \langle x, b_F(y) \rangle = b(x, y), \quad x \in F, \quad y \in E.$$

Man beachte, daß  $F^\perp$  genau der Kern von  $b_F$  ist. Unmittelbar aus der Definition von  $b_F$  ergibt sich folgendes Kriterium.

(1.3) Für einen Untermodul  $F$  von  $E$  gilt  $E = F \perp F^\perp$  genau dann, wenn  $b_F$  eine Bijektion von  $F$  auf  $b_F(E)$  induziert, wenn also  $b_F(E) = b_F(F)$  und  $F \cap F^\perp = \{0\}$  ist.

In der Tat drücken die angegebenen Bedingungen aus, daß es bei gegebenem  $y \in E$  genau ein  $z \in F$  mit  $b_F(z) = b_F(y)$ , d.h. mit  $y - z \in F^\perp$  gibt.

Im Fall, daß  $F = Ae$  frei mit einem erzeugenden Element  $e$  ist, hat man eine einfache geometrische Deutung des vorangegangenen Satzes. Der Ansatz  $y - ae \in F^\perp$  führt zu  $b(y, e) - ab(e, e) = 0$ , und das ist nach  $a$  auflösbar, wenn  $b_F$  bijektiv,  $b(e, e)$  also invertierbar ist. Die Komponente von  $y$  in  $Ae$ :

$$(1.4) \quad \text{pr}_e(y) = \frac{b(y, e)}{b(e, e)}e$$

bedeutet geometrisch die orthogonale Projektion von  $y$  auf die Gerade  $Ae$ .

(1.5) **Definition** Ein Modul mit symmetrischer Bilinearform  $(E, b)$  (oder auch einfach  $E$  oder  $b$ ) heißt *nicht ausgeartet*, falls  $b_E$  injektiv ist, wenn also  $E^\perp = \{0\}$  ist;  $(E, b)$  heißt *regulär*, falls  $b_E$  bijektiv und  $E$  endlich erzeugt projektiv ist.

Dabei heißt ein endlich erzeugter Modul projektiv, wenn er direkter Summand in einem endlich erzeugten freien Modul ist. Im weiteren Verlauf werden wir es fast ausschließlich mit freien Moduln zu tun haben.

Wenn  $(E, b)$  ein Modul mit symmetrischer Bilinearform ist und  $F \subseteq E$  ein Untermodul, so verstehen wir  $F$  mit der Einschränkung  $b|_{F \times F}$  von  $b$  und können so z.B. davon sprechen, daß  $F$  regulär oder nicht ausgeartet sei. Die zur Einschränkung gehörige Abbildung  $b_F : F \rightarrow F^*$  ist gleich der Einschränkung der obigen Abbildung  $b_F : E \rightarrow F^*$ . Hierdurch ist gerechtfertigt, daß in unserer Bezeichnung  $b_F$  der Definitionsbereich  $E$  der Form  $b$  nicht vorkommt. Wenn speziell  $F$  regulär bezüglich  $b$  ist, so gilt in der Inklusionskette  $b_F(F) \subseteq b_F(E) \subseteq F^*$  notwendig überall Gleichheit, und aus (1.3) folgt

(1.6) **Satz** Jeder reguläre Untermodul eines Moduls mit symmetrischer Bilinearform spaltet als orthogonaler Summand ab.

Als nächstes betrachten wir das Verhalten der Eigenschaften ‘nicht ausgeartet’ und ‘regulär’ bei orthogonalen Summen. Man hat eine kanonische Iso-

morphie  $E^* = \bigoplus_{i=1}^n E_i^*$  für jede direkte Summe  $E = \bigoplus_{i=1}^n E_i$  von  $A$ -Moduln. Die Orthogonalität einer solchen direkten Summe bezüglich einer symmetrischen Bilinearform  $b$  drückt sich durch die Gleichung  $b_{E_i}|_{E_j} = 0$  für  $i \neq j$  aus. Also ist  $b_E : E \rightarrow E^*$  genau dann injektiv (surjektiv), wenn alle  $b_{E_i} : E_i \rightarrow E_i^*$  es sind. Weiter gehört wie eben  $b_{E_i}|_{E_i}$  zur Einschränkung der Bilinearform auf  $E_i$ . Wir haben folgenden Satz bewiesen.

**(1.7) Satz** *Eine orthogonale Summe von Moduln mit Bilinearform ist genau dann nicht ausgeartet bzw. regulär, wenn dieses für jeden Summanden gilt.*

Wir kommen schließlich zur Beschreibung von Bilinearformen auf freien Moduln und ihrer Eigenschaften durch Matrizen. Die Transponierte einer Matrix  $T$  bezeichnen wir mit  $T^t$ . Speziell wird für einen Zeilenvektor  $\mathbf{x} = (x_1, \dots, x_n)$  mit  $\mathbf{x}^t$  der zugehörige Spaltenvektor bezeichnet. Für  $e_1, \dots, e_n \in E$  betrachte die symmetrische Matrix  $B = (b(e_i, e_j))_{i,j=1,\dots,n}$ . Wenn  $x = \sum x_i e_i$  und  $y = \sum y_j e_j$ , dabei  $x_i, y_j \in A$ , zwei Linearkombinationen der  $e_i$  sind, so gilt

$$(1.8) \quad b(x, y) = \mathbf{x} B \mathbf{y}^t.$$

Wenn alle Vektoren eines weiteren Systems  $e'_j$ ,  $j = 1, \dots, m$  sich linear aus den  $e_i$  kombinieren lassen,  $e'_j = \sum t_{ji} e_i$ , so gilt für die entsprechende Matrix  $B' = (b(e'_i, e'_j))$  und die Übergangsmatrix  $T = (t_{ji})$  die Formel

$$(1.9) \quad B' = T B T^t.$$

Wir bezeichnen mit  $d(e_1, \dots, e_n)$  die Determinante der obigen Matrix  $B$ . Ist speziell  $m = n$ , also  $T$  eine quadratische Matrix, so ergibt sich

$$(1.10) \quad d(e'_1, \dots, e'_n) = d(e_1, \dots, e_n) \det(T)^2.$$

Zerfällt das System  $\{e_1, \dots, e_n\}$  in zwei zueinander orthogonale Teilsysteme  $\{e_1, \dots, e_m\}$  und  $\{e_{m+1}, \dots, e_n\}$ , also  $b(e_i, e_j) = 0$  für  $i \leq m < j$ , so hat man

$$(1.11) \quad d(e_1, \dots, e_n) = d(e_1, \dots, e_m) d(e_{m+1}, \dots, e_n).$$

**(1.12)** Ist  $d(e_1, \dots, e_n)$  kein Nullteiler, so sind  $e_1, \dots, e_n$  linear unabhängig.

Denn aus  $\sum_i a_i e_i = 0$  folgt  $\sum_i a_i b(e_i, e_j) = 0$  für  $j = 1, \dots, n$ , also weiter  $a_i d(e_1, \dots, e_n) = 0$ .

**(1.13)** Ist  $E$  ein freier Modul mit Basis  $e_1, \dots, e_n$ , so heißt die obige Matrix  $B$  die *Gramsche Matrix* oder *Gram-Matrix*<sup>1</sup> von  $b$  oder  $(E, b)$  bezüglich der Basis  $e_1, \dots, e_n$ . Ihre Determinante  $d(e_1, \dots, e_n)$  ändert sich bei Basiswechsel um ein Quadrat aus der multiplikativen Gruppe  $A^\times$  der Einheiten von  $A$ . Ihre

<sup>1</sup> Nach J.P. Gram, 1850–1916

Klasse modulo  $A^{\times 2}$  nennen wir daher die *Determinante* von  $(E, b)$ , oder kurz von  $E$ , und schreiben dafür  $d(e_1, \dots, e_n)A^{\times 2} = \det(E, b) = \det E$ .

**(1.14)** Einen freien Modul mit Gram-Matrix  $B = (b_{ij})$  bezeichnen wir mit  $\langle b_{ij} \rangle$ , speziell für eine Diagonalmatrix mit Diagonalelementen  $b_1, \dots, b_n$  auch mit  $\langle b_1, \dots, b_n \rangle$ .

Sei  $e_1^*, \dots, e_n^*$  die durch

$$\langle e_i, e_j^* \rangle = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \quad \text{für}$$

beschriebene duale Basis von  $E^*$ . Definieren wir Koeffizienten  $b'_{kj}$  durch  $b_E(e_j) = \sum_k b'_{kj} e_k^*$ , so gilt:

$$b_{ij} = b(e_i, e_j) = \langle e_i, b_E(e_j) \rangle = \sum_k b'_{kj} \langle e_i, e_k^* \rangle = b'_{ij},$$

d. h. die Gram-Matrix  $B$  ist die Matrix der linearen Abbildung  $b_E : E \rightarrow E^*$  bezüglich der Basen  $e_1, \dots, e_n$  und  $e_1^*, \dots, e_n^*$ .

Aus bekannten Sätzen der linearen Algebra<sup>2</sup> folgt, daß  $b_E : E \rightarrow E^*$  genau dann injektiv (bijektiv) ist, wenn  $d(e_1, \dots, e_n)$  kein Nullteiler (invertierbar) ist. Dieses beweist den folgenden Satz.

**(1.15) Satz** *Eine symmetrische Bilinearform  $b$  auf einem freien Modul mit Basis  $e_1, \dots, e_n$  ist genau dann nicht ausgeartet (bzw. regulär), wenn  $d(e_1, \dots, e_n)$  kein Nullteiler (bzw. invertierbar) ist.*

Aus diesem Satz erhält man per Induktion über den Rang  $n$  die folgende, im Grunde schon auf C.G.J. Jacobi<sup>3</sup> (1804-1851) zurückgehende Diagonalisierung für gewisse freie Moduln.

**(1.16)** Es sei  $E$  ein freier Modul mit Basis  $e_1, \dots, e_n$  derart, daß alle Elemente  $d_i := d(e_1, \dots, e_i)$ ,  $i = 1, \dots, n$  Einheiten in  $A$  sind. Dann gilt

$$E \cong \langle d_1, \frac{d_2}{d_1}, \frac{d_3}{d_2}, \dots, \frac{d_n}{d_{n-1}} \rangle.$$

**Beweis:** Nach (1.6) ist

$$\sum_{i=1}^j A e_i = \sum_{i=1}^{j-1} A e_i \perp \langle c_j \rangle$$

<sup>2</sup> Wegen der für die Injektivität benötigten Aussage, daß ein lineares homogenes Gleichungssystem, dessen Determinante Nullteiler ist, eine nichttriviale Lösung hat, vgl. man z.B. N. Bourbaki, Algebra, Chap. III, §8, prop. 14, oder Oeljeklaus/Remmert, Lineare Algebra I, Kap. V, Satz 6.

<sup>3</sup> Gesammelte Werke, vol. 3, p. 590

und  $d_j = d_{j-1}c_j$  nach (1.11).

Als Anwendung ergibt sich das bekannte Positivitätskriterium für reelle quadratische Formen.

**(1.17)** Sei  $(E, b)$  regulär und  $e_1, \dots, e_n$  eine Basis von  $E$ . Definiere  $e_i^\#$  durch  $e_i^* = b_E(e_i^\#)$ . Die Basis  $e_1^\#, \dots, e_n^\#$  heißt die zu  $e_1, \dots, e_n$  bezüglich  $b$  *duale Basis*. Die definierenden Gleichungen

$$b(e_i, e_j^\#) = \delta_{ij}$$

und die Symmetrie von  $b$  zeigen, daß die Rollen der  $e_i$  und der  $e_i^\#$  in der Tat symmetrisch sind, also die  $e_i^\#$  die duale Basis zu den  $e_i$  bilden.

Ist  $F$  der von  $e_1, \dots, e_m$  erzeugte Untermodul, so hat  $F^\perp$  ersichtlich die Basis  $e_{m+1}^\#, \dots, e_n^\#$ . Für Untermoduln  $F$  mit einer Basis, die sich zu einer Basis von  $E$  ergänzen läßt, gilt folglich  $F^{\perp\perp} = F$ . Für Vektorräume über einem Körper ist das natürlich stets der Fall. Im allgemeinen gilt dagegen nur

$$(1.18) \quad F^{\perp\perp} \supseteq F,$$

wie man z.B. daran sieht, daß  $(aE)^{\perp\perp} = E$  ist, falls  $a$  kein Nullteiler ist.

Wir setzen nun voraus, daß der Grundring ein Körper ist und notieren einige Spezialisierungen bzw. Verschärfungen bisheriger Resultate.

**(1.19) Satz** *Ein endlichdimensionaler Vektorraum über einem Körper ist genau dann regulär, wenn er nicht ausgeartet ist. Für jeden Unterraum  $F$  eines regulären Vektorraums  $E$  gilt*

$$\dim F + \dim F^\perp = \dim E \quad \text{und} \quad F^{\perp\perp} = F.$$

Die zweite Aussage ist ein Spezialfall der üblichen Dimensionsformel für lineare Abbildungen, denn  $b_F$  ist surjektiv und hat  $F^\perp$  als Kern.

**(1.20) Satz** *Ist  $A$  ein Körper und  $E$  endlich-dimensional, so gibt es eine Zerlegung  $E = E_1 \perp \dots \perp E_r \perp F$  in reguläre Teilräume  $E_i$  der Dimension 1 oder 2 und einen Raum  $F$  mit  $b(F, F) = 0$ .  $E$  ist genau dann regulär, wenn  $F = \{0\}$  ist. Ist die Charakteristik von  $A$  nicht 2, so braucht man nur Räume  $E_i$  der Dimension 1 und kann Erzeugende  $e_1, \dots, e_r$  von  $E_1, \dots, E_r$  durch Hinzunahme einer Basis von  $F$  zu einer Basis von  $E$  aus paarweise orthogonalen Vektoren ergänzen.*

**Beweis:** Durch Induktion nach der Dimension von  $E$  mit Induktionsanfang  $E = \{0\}$ . Ist  $b(E, E) = 0$ , so sind wir mit  $r = 0$ ,  $F = E$  fertig. Anderenfalls bestehen zwei Möglichkeiten:

- a) Es gibt einen Vektor  $e \in E$  mit  $b(e, e) \neq 0$ . Dann kann man  $Ae$  nach (1.15) abspalten und auf  $Ae^\perp$  die Induktionsannahme anwenden.

- b) Es ist  $b(e, e) = 0$  für alle  $e \in E$  aber es gibt zwei Vektoren  $e$  und  $f$  in  $E$  mit  $b(e, f) \neq 0$ . Dann ist  $d(e, f) = -b(e, f)^2 \neq 0$ , und man kann  $Ae + Af$  nach (1.6) und (1.15) abspalten. Der Fall b) kann wegen  $2b(e, f) = b(e + f) - b(e) - b(f)$  nicht vorkommen, wenn  $2 \neq 0$  ist.

**(1.21) Beispiele.** Wir legen den Ring  $\mathbb{Z}$  der ganzen rationalen Zahlen zugrunde und definieren drei Serien von freien Moduln mit symmetrischer Bilinearform, die wir, der Literatur folgend, mit  $I_n, A_n, D_n$  bezeichnen. Dabei ist der Index  $n$  gleich dem Rang des Moduln.

- a) Sei  $I_n = \mathbb{Z}^n$  mit dem Standardskalarprodukt  $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n x_i y_i$ , wobei  $\mathbf{x} = (x_1, \dots, x_n)$ ,  $\mathbf{y} = (y_1, \dots, y_n)$ ,  $x_i, y_j \in \mathbb{Z}$ . Eine Basis bilden die Vektoren  $\mathbf{e}_1, \dots, \mathbf{e}_n$  mit  $\mathbf{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$ . Die Gram-Matrix bezüglich dieser Basis ist die Einheitsmatrix. Die Determinante von  $I_n$  ist eins,  $I_n$  ist regulär.  $I_n$  ist zerlegbar als orthogonale Summe  $I_n = \perp_{i=1}^n \mathbb{Z} \mathbf{e}_i$  mit  $\mathbb{Z} \mathbf{e}_i \cong I_1$ .
- b) Sei  $A_n = \{\sum x_i \mathbf{e}_i \in I_{n+1} \mid \sum x_i = 0\}$ . Eine Basis von  $A_n$  bilden z.B. die Elemente  $\mathbf{e}_1 - \mathbf{e}_2, \mathbf{e}_2 - \mathbf{e}_3, \dots, \mathbf{e}_n - \mathbf{e}_{n+1}$ . Die zugehörige Gram-Matrix ist

$$\begin{pmatrix} 2 & -1 & & & \\ -1 & 2 & -1 & & \\ & -1 & 2 & & \\ & & & \ddots & \\ 0 & & & & 2 & -1 \\ & & & & -1 & 2 \end{pmatrix} \quad \det A_n = n + 1$$

Die Determinante berechnet man aus der angegebenen Gram-Matrix durch Entwicklung nach der ersten Zeile und Induktion.

- c) Sei  $D_n = \{\sum x_i \mathbf{e}_i \in I_n \mid \sum x_i \in 2\mathbb{Z}\}$ . Eine Basis von  $D_n$  bilden z.B. die Elemente  $\mathbf{e}_1 - \mathbf{e}_2, \mathbf{e}_2 - \mathbf{e}_3, \dots, \mathbf{e}_{n-1} - \mathbf{e}_n, \mathbf{e}_{n-1} + \mathbf{e}_n$ . Die zugehörige Gram-Matrix ist

$$\begin{pmatrix} 2 & -1 & & & \\ -1 & 2 & -1 & & \\ & -1 & 2 & & \\ & & & \ddots & \\ 0 & & & & 2 & -1 & -1 \\ & & & & -1 & 2 & 0 \\ & & & & -1 & 0 & 2 \end{pmatrix}$$

Die Determinante berechnet man ähnlich wie bei  $A_n$ .

## 2 Quadratische Formen

### (2.1) Definition

a) Eine *quadratische Form* auf einem  $A$ -Modul  $E$  ist eine Abbildung  $q : E \rightarrow A$  mit den Eigenschaften

$$\begin{aligned} q(ax) &= a^2 q(x) \quad \text{für } a \in A, x \in E, \\ q(x+y) &= q(x) + q(y) + b(x, y) \end{aligned}$$

mit einer symmetrischen Bilinearform  $b$ . Ein solches Paar  $(E, q)$  (oder auch einfach  $E$ ) heißt *quadratischer  $A$ -Modul*.

b) Eine *isometrische Abbildung* oder kurz *Isometrie* zwischen zwei quadratischen Moduln  $(E, q)$  und  $(E', q')$  ist ein injektiver Modulhomomorphismus  $f : E \rightarrow E'$  mit  $q'(f(x)) = q(x)$  für alle  $x \in E$ .

c) Zwei quadratische Moduln  $(E, q)$  und  $(E', q')$  heißen *isometrisch*, in Zeichen  $(E, q) \cong (E', q')$  oder kurz  $E \cong E'$ , wenn eine bijektive Isometrie zwischen ihnen existiert.

Mit  $a = 2$ ,  $x = y$  erhält man

$$(2.2) \quad 2q(x) = b(x, x)$$

Das zeigt, daß  $q$  durch  $b$  bis auf einen Summanden bestimmt ist, der von 2 annulliert wird. Insbesondere ist  $q$  durch  $b$  eindeutig bestimmt, wenn 2 kein Nullteiler ist. Darüber hinaus kann man in diesem Fall zu gegebener symmetrischer Bilinearform  $b$  durch (2.2) eine quadratische Form  $q$  definieren, falls alle Werte  $b(x, x)$  in  $2A$  liegen. Ist 2 sogar invertierbar, so kann man natürlich einfach  $q(x) = \frac{1}{2}b(x, x)$  schreiben. Im allgemeinen kann man immerhin noch versuchen, eine (nicht notwendig symmetrische) Bilinearform  $a$  zu finden, so daß

$$(2.3) \quad q(x) = a(x, x)$$

wird. Für beliebiges  $a$  wird durch (2.3) eine quadratische Form definiert, deren zugehörige symmetrische Bilinearform

$$(2.4) \quad b(x, y) = a(x, y) + a(y, x)$$

ist. Zu einer gegebenen quadratischen Form auf einem freien Modul kann man stets ein solches  $a$  finden. Man hat nur aus (2.1) und (2.2) durch Induktion die Formel

$$(2.5) \quad q\left(\sum_i x_i e_i\right) = \sum_i q(e_i) x_i^2 + \sum_{i < j} b(e_i, e_j) x_i x_j$$

abzuleiten und dann, wenn  $e_1, \dots, e_n$  eine Basis ist,  $a(\sum x_i e_i, \sum y_j e_j) = \sum_{i \leq j} a_{ij} x_i y_j$  zu setzen mit  $a_{ii} = q(e_i)$  und  $a_{ij} = b(e_i, e_j)$  für  $i < j$  (oder

allgemeiner  $a_{ij} + a_{ji} = b_{ij}$  für  $i \neq j$  für eine i.a. nicht-symmetrische Matrix  $(a_{ij})$ .

Einen solchen freien Modul  $E$  bezeichnen wir abkürzend mit

$$(2.6) \quad \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \end{bmatrix}$$

bzw.  $E = [a_1, a_2, \dots, a_n]$ , wenn  $q(\sum_i x_i e_i) = \sum_i a_i x_i^2$  ist, oder, falls 2 nicht Nullteiler und  $b_{ij} = b(e_i, e_j) = b_{ji}$  ist, auch mit

$$(2.7) \quad E = \left\langle \begin{matrix} b_{11} \dots b_{1n} \\ \dots \dots \dots \\ b_{n1} \dots b_{nn} \end{matrix} \right\rangle$$

So schreiben wir z.B.  $E = [1] = \langle 2 \rangle$  für den Modul  $E = A$  mit  $q(x) = x^2$  und  $H = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \left\langle \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \right\rangle$  für die sogenannte hyperbolische Ebene  $H = A^2$  mit  $q(x_1, x_2) = x_1 x_2$ .

Die Darstellung (2.3) hat man auch noch für projektive Moduln  $E$ . Ist nämlich  $E \oplus F$  frei, so setze man  $q$  auf  $E \oplus F$  fort durch  $q(x+y) = q(x)$  für  $x \in E$ ,  $y \in F$ , schreibe die Fortsetzung in der Form (2.3) und schränke dann alles auf  $E$  ein.

Die in §1 für symmetrische Bilinearformen eingeführten Bezeichnungen können wir natürlich auch auf die einer quadratischen Form zugehörige Bilinearform anwenden. So sprechen wir z.B. von nicht ausgearteten oder regulären quadratischen Moduln, oder von einem Modul  $E = \perp E_i$  als orthogonaler Summe von Untermoduln  $E_i$ . Das bedeutet insbesondere, wenn wir die Einschränkung von  $q$  auf  $E_i$  mit  $q_i$  bezeichnen,

$$(2.8) \quad q(\sum x_i) = \sum q_i(x_i) \quad \text{für} \quad x_i \in E_i.$$

Sind umgekehrt quadratische Moduln  $(E_i, q_i)$  gegeben, so kann man auf der direkten Summe  $E$  der Moduln  $E_i$  durch (2.8) eine quadratische Form  $q$  definieren. Auch in dieser Situation schreiben wir  $E = \perp E_i$ . Der  $n$ -dimensionale euklidische Raum  $\mathbb{R}^n$  mit dem gewöhnlichen Skalarprodukt  $\sum x_i y_i$  als Bilinearform und  $\frac{1}{2} \sum x_i^2$  als quadratischer Form wäre demnach mit  $\perp_{i=1}^n \langle 1 \rangle$  zu bezeichnen.

Ist 2 nicht invertierbar, so zeigt (2.2), daß auch  $b(x, x)$  für kein  $x$  invertierbar ist. Es gibt also keinen regulären freien quadratischen Modul vom Rang 1. Aber auch ein freier Modul von höherem ungeradem Rang  $n$  kann dann nicht regulär sein. Das sieht man, wenn man die Determinante



$$(2.9) \quad \begin{vmatrix} 2a_1 & b_{12} & \dots & b_{1n} \\ b_{12} & 2a_2 & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{1n} & \dots & \dots & 2a_n \end{vmatrix}$$

ausrechnet. Unter den  $n!$  Summanden kommen zwei Arten vor. Diejenigen, die bei Spiegelung an der Hauptdiagonalen in sich übergehen, enthalten wegen der ungeraden Reihenzahl mindestens einen Faktor  $2a_i$  aus der Hauptdiagonalen; zu jedem anderen kommt aber auch der an der Hauptdiagonalen gespiegelte Summand vor, der wegen der Symmetrie der Matrix den gleichen Beitrag liefert. Die Determinante (2.9) hat also den Wert  $2P_n(a_i, b_{ij})$ , wo  $P_n$  ein Polynom mit ganzrationalen Koeffizienten ist. Hierin kann man für  $a_i, b_{ij}$  Elemente eines beliebigen Ringes einsetzen. Mit

$$(2.10) \quad d'(e_1, \dots, e_n) = P_n(q(e_i), b(e_i, e_j))$$

wird dann

$$(2.11) \quad d(e_1, \dots, e_n) = 2d'(e_1, \dots, e_n).$$

Der Formel (1.10) entspricht bei ungeraden  $n$

$$(2.12) \quad d'(e'_1, \dots, e'_n) = d'(e_1, \dots, e_n) \det(t_{ij})^2 \quad \text{für} \quad e'_i = \sum_{j=1}^n t_{ij} e_j.$$

Das folgt unmittelbar aus (1.10) und (2.11), falls 2 nicht Nullteiler ist, insbesondere dann, wenn die Größen  $a_i = q(e_i)$ ,  $b_{ij} = b(e_i, e_j)$  und  $t_{ij}$  Unbestimmte über  $\mathbb{Z}$  sind. (2.12) ist dann eine Identität, die erhalten bleibt, wenn man für die Unbestimmten Werte aus einem Ring einsetzt.

**(2.13) Definition** Ein freier quadratischer Modul mit Basis  $e_1, \dots, e_n$  ( $n$  ungerade) heißt *halbregulär*, wenn  $d'(e_1, \dots, e_n)$  invertierbar ist.

Die Definition hängt wegen (2.12) nicht von der Wahl der Basis ab. Ist 2 invertierbar, so ist jeder halbreguläre Modul regulär. Hat 2 dagegen kein Inverses, so gibt es keine regulären Moduln von ungeradem Rang  $n$ , wohl aber halbreguläre, z.B. für  $n = 2m + 1$  den Modul

$$\bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \perp [1],$$

wie man z.B. mit Hilfe der (1.11) entsprechenden Formel

$$(2.14) \quad \begin{aligned} d'(e_1, \dots, e_n) &= d(e_1, \dots, e_{2m}) d'(e_{2m+1}, \dots, e_n) \\ &\text{falls } n \text{ ungerade, } b(e_i, e_j) = 0 \text{ für } i \leq 2m < j \end{aligned}$$

feststellt.

Die Zerlegung  $E = E_1 \perp \dots \perp E_r \perp F$  aus (1.20) gilt natürlich auch für quadratische Vektorräume über einem Körper  $A$ . Ist die Charakteristik

$\text{char } A \neq 2$ , so folgt aus  $b(F, F) = 0$  wegen (2.2) auch  $q(F) = 0$ , und es ergibt sich nichts Neues. Für  $\text{char } A = 2$  dagegen haben einerseits alle  $E_i$  die Dimension 2, da es keine regulären eindimensionalen Räume gibt, andererseits folgt nicht mehr  $q(f) = 0$ , sondern nur noch  $q(x+y) = q(x)+q(y)$  für  $x, y \in F$ . Daraus und aus (2.1) entnimmt man, daß  $G = \{x \in F \mid q(x) = 0\}$  ein Unterraum von  $F$  und  $q(F)$  ein Unterraum von  $A$ , aufgefaßt als Vektorraum über dem Unterkörper  $A^2 = \{a^2 \mid a \in A\}$  ist. Ist  $f_1, \dots, f_s$  eine Basis von  $F$  modulo  $G$ ,  $F_i = Af_i$ , so folgt:

**(2.15) Satz** *Ein endlichdimensionaler quadratischer Vektorraum  $E$  über einem Körper  $A$  der Charakteristik 2 läßt sich orthogonal zerlegen als  $E = E_1 \perp \dots \perp E_r \perp F_1 \perp \dots \perp F_s \perp G$  mit  $E_i$  zweidimensional regulär,  $F_j$  eindimensional halbregulär,  $s \leq [A : A^2]$  und  $q(G) = 0$ .  $E$  ist genau dann regulär, wenn  $s = 0$ ,  $G = \{0\}$ , genau dann halbregulär, wenn  $s = 1$ ,  $G = \{0\}$  ist.*

**(2.16)** Ein Element  $x \in E$  bzw. ein Untermodul  $F \subseteq E$  heißt *singulär*, wenn  $q(x) = 0$  bzw.  $q(F) = 0$  ist.

Ist  $A$  ein Körper,  $E$  regulär und  $F \subseteq E$  singulär, so kann man zu einer Basis  $e_1, \dots, e_m$  von  $F$  nach (1.17) Elemente  $e_1^\#, \dots, e_m^\#$  in  $E$  finden mit  $b(e_i, e_j^\#) = \delta_{ij}$ . Wegen  $b(e_i, e_j) = 0$  ist  $d(e_1, \dots, e_m, e_1^\#, \dots, e_m^\#) = (-1)^m \neq 0$  und  $\sum Ae_i + \sum Ae_i^\#$  daher ein regulärer Unterraum der doppelten Dimension, der  $F$  enthält. Diese Konstruktion kann man auch über einem beliebigen Ring  $A$  durchführen, wenn  $F$  ein freier Untermodul mit Basis  $e_1, \dots, e_m$  ist und es  $e_i^\# \in E$  gibt mit  $b_E(e_i^\#) = e_i^*$ . Da uns diese Forderung noch öfter begegnen wird, führen wir dafür einen Namen ein. Es ist vernünftig, dabei wie in (1.5) allgemeiner auch projektive Moduln zu berücksichtigen, obwohl wir in dieser Vorlesung fast ausschließlich freie Moduln betrachten werden.

**(2.17) Definition** Ein Untermodul  $F$  eines  $A$ -Moduls  $E$  heißt *primitiv*, wenn er ein direkter Summand von  $E$  ist; trägt  $E$  eine symmetrische Bilinearform  $b$ , so heißt  $F$  *scharf primitiv* (bezüglich  $b$ ), wenn er endlich erzeugt projektiv und  $b_F(E) = F^*$  ist.

Ein regulärer Untermodul  $F$  ist immer scharf primitiv, da dann schon  $b_F(F) = F^*$  ist. Weiter überlegt man sich leicht, daß jeder scharf primitive Untermodul primitiv ist. Wenn  $E$  regulär und  $F$  primitiv ist, so ist  $F$  scharf primitiv. Denn für  $E = F \oplus G$  kann man jede Linearform auf  $F$  durch 0 auf  $G$  zu einer Linearform auf  $E$  fortsetzen, diese in der Form  $b_E(e)$  schreiben und dann auf  $F$  einschränken.

Wir kehren zu unserem singulären Untermodul  $F$  zurück und setzen  $G = \sum Ae_i^\#$ . Durch  $b$  stehen  $F$  und  $G$  in Dualität, so daß wir  $F$  mit  $G^*$  identifizieren können. Damit wird  $F + G$  isomorph zu einem Modul  $H(G)$ , den wir zu einem beliebigen endlich erzeugten projektiven quadratischen Modul  $G$  folgendermaßen bilden können. Wir konstruieren

$$(2.18) \quad H(G, q) = G \oplus G^*,$$

setzen die quadratische Form  $q$  auf ganz  $H(G)$  fort durch

$$(2.19) \quad q(x + x^*) = q(x) + \langle x, x^* \rangle, \quad x \in G, \quad x^* \in G^*,$$

und erhalten daraus

$$(2.20) \quad b(x + x^*, y + y^*) = b(x, y) + \langle x, y^* \rangle + \langle y, x^* \rangle.$$

$H(G, q)$  ist regulär, da  $b_{H(G, q)}(G^*)$  gerade die sämtlichen Linearformen auf  $H(G, q)$  liefert, die auf  $G^*$  verschwinden, während  $b_{G^*}(G) = G = G^{**}$  ist.

Der quadratische Modul  $H(G, q)$  hängt bis auf Isomorphie in Wirklichkeit gar nicht von  $q$  sondern nur von  $G$  ab. Ist nämlich  $q$  in der Form (2.3) dargestellt, also  $q(x) = \langle x, a_G(x) \rangle$  mit  $a_G : G \rightarrow G^*$ , so ist die Abbildung  $x + x^* \rightarrow x + (a_G(x) + x^*)$  ( $x \in G, x^* \in G^*$ ) ein Isomorphismus von  $H(G, q)$  auf  $H(G, 0)$ .

(2.21) Der eben konstruierte quadratische Modul  $H(G) = H(G, 0)$  heißt hyperbolischer Modul zu  $G$ . Für  $G = A$  erhält man die schon oben eingeführte hyperbolische Ebene  $H(A) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ .

Mit dieser Bezeichnung können wir unsere Überlegungen zusammenfassen.

(2.22) **Satz** Jeder scharf primitive singuläre Untermodul  $F$  von  $E$  ist in einem zum hyperbolischen Modul  $H(F)$  isomorphen Untermodul  $H$  enthalten. Ist  $F$  frei mit Basis  $f_1, \dots, f_m$ , so läßt sich diese durch  $g_1, \dots, g_m$  zu einer Basis von  $H$  ergänzen, für die  $b(f_i, g_j) = \delta_{ij}$ ,  $q(\sum A g_i) = 0$  ist.

Wir wollen noch den zu  $G$  in  $H(G, q)$  orthogonalen Modul bestimmen. Nach (2.20) ist  $y + y^* \in G^\perp$  gleichbedeutend mit  $b(x, y) + \langle x, y^* \rangle = 0$  d.h. mit  $y^* = -b_G(y)$ . Die Abbildung  $y \rightarrow y - b_G(y)$  ist also ein Modulisomorphismus von  $G$  auf  $G^\perp$ , und es gilt  $q(y - b_G(y)) = q(y) - \langle y, b_G(y) \rangle = q(y) - b(y, y) = -q(y)$ .

(2.23) Ist  $E$  ein  $A$ -Modul mit quadratischer Form  $q$  und  $a \in A$ , so sei  ${}^a E$  der quadratische Modul, der als Modul mit  $E$  übereinstimmt, aber die quadratische Form  $aq$  trägt. Fassen wir einen Vektor  $x \in E$  als Element aus  ${}^a E$  auf, so bezeichnen wir ihn mit  ${}^a x$ . Ist  $a$  ein etwas komplizierter Ausdruck, so schreiben wir auch  $\langle a \rangle E$  und  $\langle a \rangle x$ .

(2.24) **Satz** Jeder endlich erzeugte projektive quadratische Modul  $G$  läßt sich in den zugehörigen hyperbolischen Modul  $H(G)$  so einbetten, daß  $G^\perp \cong {}^{-1}G$  wird. Ist speziell  $G$  regulär, so gilt  $G \perp {}^{-1}G \cong G \perp G^\perp = H(G)$ .

### 3 Die orthogonale Gruppe und der Satz von Witt

Die Automorphismengruppe eines quadratischen Moduls  $(E, q)$ , also die Gruppe der bijektiven linearen Abbildungen  $t : E \rightarrow E$  mit  $q(tx) = q(x)$ ,

heißt die orthogonale Gruppe von  $E$  und wird mit  $O(E)$  oder  $O(E, q)$  oder  $O(q)$  bezeichnet. Für das folgende grundlegend ist der *Kürzungssatz von Witt*.

**(3.1) Satz (Witt)** *Sei  $A$  ein Körper der Charakteristik  $\neq 2$ ,  $F, G_1, G_2$  quadratische Räume über  $A$ ,  $F$  regulär und  $F \perp G_1 \cong F \perp G_2$ . Dann ist  $G_1 \cong G_2$ .*

Äquivalent dazu ist die Aussage

**(3.2)** *Sei  $A$  ein Körper der Charakteristik  $\neq 2$ ,  $E$  ein quadratischer Raum über  $A$ ,  $F_1$  und  $F_2$  reguläre Unterräume und  $t: F_1 \rightarrow F_2$  ein Isomorphismus. Dann gibt es einen Automorphismus von  $E$ , der  $t$  fortsetzt, also ein  $u \in O(E)$  mit  $u|_{F_1} = t$ .*

Zunächst der Beweis der Äquivalenz. Gilt (3.1) und liegt die Situation von (3.2) vor, so ist  $E = F_1 \perp F_1^\perp = F_2 \perp F_2^\perp \cong F_1 \perp F_2^\perp$ . Nach (3.1) gibt es einen Isomorphismus  $t': F_1^\perp \rightarrow F_2^\perp$ , und  $u = t \perp t'$  ist eine Fortsetzung von  $t$ . Gilt umgekehrt (3.2) und ist  $t': F \perp G_1 \rightarrow F \perp G_2$  ein Isomorphismus, so ist die Einschränkung  $t$  von  $t'$  auf  $F$  ein Isomorphismus von  $F = F_1$  auf  $t'F = F_2$ , der sich zu einem Automorphismus  $u$  von  $F \perp G_2 = t'(F \perp G_1) = t'F \perp t'G_1$  fortsetzen läßt. Dann ist

$$G_2 \cong u(G_2) = u(F^\perp) = (uF)^\perp = (t'F)^\perp = t'G_1 \cong G_1.$$

In der zweiten Fassung wollen wir den Satz durch Induktion nach  $\dim F_1 = \dim F_2$  beweisen. Dazu benutzen wir spezielle Automorphismen, die Spiegelungen, die wir in quadratischen Moduln über beliebigen Ringen, auch der Charakteristik 2, definieren können. Ist  $e \in E$  und  $q(e)$  in  $A$  invertierbar, so setzen wir

$$s_e(x) = x - b(x, e)q(e)^{-1}e$$

und rechnen leicht nach, daß  $q(s_e x) = q(x)$  und  $s_e^2$  die Identität ist.  $s_e$  ist also ein Automorphismus; er läßt jeden zu  $e$  orthogonalen Vektor fest und führt  $e$  in  $-e$  über. Ist 2 invertierbar, so besteht die orthogonale Zerlegung  $E = Ae \perp Ae^\perp$ , so daß  $s_e$  durch die angegebenen Eigenschaften eindeutig bestimmt ist und geometrisch die Spiegelung an der zu  $e$  orthogonalen Hyperebene bedeutet.

Nun zum Beweis von (3.2) durch Induktion über die Dimension von  $F_i$ . Sei zunächst  $\dim F_i = 1$ ,  $F_i = Af_i$  mit  $f_2 = tf_1$ , also  $q(f_2) = q(f_1) \neq 0$  (da  $F_1$  regulär sein soll). Weil

$$q(f_1 - f_2) + q(f_1 + f_2) = 2q(f_1) + 2q(f_2) = 4q(f_1) \neq 0$$

ist, haben wir wenigstens eine der beiden Spiegelungen  $s_{f_1-f_2}$  oder  $s_{f_1+f_2}$  zur Verfügung. Im ersten Fall berechnet man sofort  $s_{f_1-f_2}(f_1) = f_2$  (wie es sich im Fall eines reellen Skalarproduktes auch anschaulich sofort aus der

Längengleichheit von  $f_1$  und  $f_2$  ergibt). Im zweiten Fall erhält man entsprechend  $s_{f_1+f_2}(f_1) = -f_2$  und weiter  $s_{f_2}(-f_2) = f_2$ .

Im Falle  $\dim F_1 = m > 1$ ,  $F = Ae_1 \perp \dots \perp Ae_m$  gibt es nach Induktionsvoraussetzung ein  $v \in O(E)$  mit  $ve_i = te_i$  für  $i = 1, \dots, m-1$ . Die Isometrie  $v^{-1}t$  läßt  $e_1, \dots, e_{m-1}$  fest und führt den dazu orthogonalen Vektor  $e_m$  in einen ebensolchen  $f_m$  über. Nach dem Induktionsanfang gilt  $we_m = f_m$  mit  $w = s_{e_m-f_m}$  oder  $w = s_{f_m} s_{e_m+f_m}$ .  $w$  läßt  $e_1, \dots, e_{m-1}$  fest, so daß  $u = vw$  das verlangte leistet.

**(3.3)** Der Wittsche Satz ist in mehrfacher Hinsicht verallgemeinert worden: Erstens auf hermitesche Formen anstelle von quadratischen; davon wollen wir hier nicht sprechen. Zweitens auf Körper der Charakteristik 2; das Ergebnis (3.4) wollen wir hier formulieren, den Beweis aber auf den nächsten Paragraphen verschieben, wo wir eine noch allgemeinere Situation betrachten werden.

**(3.4) Satz** *Sei  $E$  ein quadratischer Raum über einem Körper  $A$ ,  $F_1, F_2$  scharf primitive Unterräume von  $E$  und  $t: F_1 \rightarrow F_2$  ein Isomorphismus. Dann läßt sich  $t$  zu einem Automorphismus von  $E$  fortsetzen.*

Man beachte, daß Formulierung und Beweis einheitlich für alle Werte (2 oder  $\neq 2$ ) der Charakteristik gelten, der analoge Satz für symmetrische Bilinearformen in Charakteristik 2 aber falsch ist, wie folgendes Beispiel zeigt:

$A = \mathbb{F}_2$  der Primkörper mit zwei Elementen,  
 $E = A^3$  mit Bilinearform  $b(\mathbf{x}, \mathbf{y}) = x_1y_1 + x_2y_2 + x_3y_3$ ,  
 $F_1 = A(1, 0, 0)$ ,  $F_2 = A(1, 1, 1)$ ,  $F_1^\perp \not\cong F_2^\perp$ ,  
 also ist  $t$  nicht zu einem Automorphismus auf  $E$  fortsetzbar.

Schließlich wollen wir drittens die Forderung, daß  $F_1$  in (3.2) regulär sein soll, abschwächen. Daß man nicht ohne jede Voraussetzung über  $F_1$  und  $F_2$  auskommt, zeigt das Beispiel

$E = Ae_1 \perp Ae_2 \perp Ae_3$   
 $q(e_1) = 1, q(e_2) = -1, q(e_3) = 0$   
 $F_1 = A(e_1 + e_2), F_2 = Ae_3$ .

Hier ist  $q(e_1 + e_2) = q(e_3) = 0$ ,  $e_3$  liegt in  $E^\perp$ ,  $e_1 + e_2$  aber nicht, so daß sich die Abbildung  $t: e_1 + e_2 \rightarrow e_3$  sicher nicht zu einem Automorphismus von  $E$  fortsetzen läßt.

**(3.5) Satz** *Ist  $E$  ein regulärer oder halbregulärer quadratischer Raum über einem Körper  $A$ , so läßt sich jeder Automorphismus  $u \in O(E)$  als Produkt von Spiegelungen schreiben, außer wenn  $A$  der Primkörper  $\mathbb{F}_2$  der Charakteristik 2 und  $E = E_1 \perp E_2$  mit  $E_1 \cong E_2 \cong \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$  ist.*

Der Beweis für Körper der Charakteristik  $\neq 2$  ergibt sich unmittelbar, indem man den Beweis von (3.2) für den Fall  $F_1 = F_2 = E$  durchgeht. Die Aussage

(3.2) ist in diesem Fall zwar trivial, der Beweis liefert aber eine Darstellung von  $u = t$  als Produkt von Spiegelungen.

In dem genannten Ausnahmefall gilt  $q(x) = 1$  für jeden Vektor  $x \neq 0$  aus  $E_1$  oder  $E_2$ . Daraus folgt, daß jeder nichtsinguläre Vektor  $e$  aus  $E = E_1 \perp E_2$  entweder in  $E_1$  oder in  $E_2$  liegt, jede Spiegelung  $s_e$  also  $E_1$  und  $E_2$  jeweils in sich überführt, während es natürlich Automorphismen gibt, die  $E_1$  und  $E_2$  vertauschen.

Wir wollen noch einige Folgerungen aus dem Satz (3.4) ziehen. Dabei sei also  $A$  stets ein Körper,  $E$  ein quadratischer Raum über  $A$ . Unmittelbar folgt

**(3.6)** Sind  $F_1, F_2$  singuläre scharf primitive Unterräume der gleichen Dimension, so gibt es einen Automorphismus  $u \in O(E)$  mit  $uF_1 = F_2$ .

**(3.7)** Sind  $F_1, F_2$  maximale singuläre scharf primitive Unterräume, so ist  $\dim F_1 = \dim F_2$ .

**Beweis:** Ist etwa  $\dim F_2 \leq \dim F_1$ , so wähle man  $F'_1 \subseteq F_1$  mit  $\dim F'_1 = \dim F_2$ .  $F'_1$  ist scharf primitiv in  $E$ , also existiert  $u \in O(E)$  mit  $uF'_1 = F_2$ . Dann ist  $uF_1 \supseteq F_2$ , also  $uF_1 = F_2$  wegen der Maximalität von  $F_2$ , und damit  $\dim F_1 = \dim F_2$ .

**(3.8)** Ist  $A$  ein Körper,  $E$  ein endlich-dimensionaler quadratischer Raum über  $A$ , so heißt die Dimension der maximalen singulären scharf primitiven Unterräume der *Witt-Index* oder einfach *Index*  $\text{ind}(E)$  von  $E$ .

Nach (2.23) kann man einen maximalen singulären scharf primitiven Unterraum in einen hyperbolischen Raum  $H$  vom Rang  $2 \text{ind}(E)$  einbetten und dann nach (1.6)

**(3.9)**  $E = F \perp H$  mit  $\text{ind}(F) = 0$ ,  $H$  hyperbolisch

schreiben. Nach (3.7) und (3.1) ist diese Zerlegung bis auf Isomorphie eindeutig bestimmt; man nennt sie die *Witt-Zerlegung* von  $E$ .

**(3.10)**  $E$  hat genau dann einen zu  $F$  isomorphen scharf primitiven Unterraum, wenn  $\text{ind}(E \perp {}^{-1}F) \geq \dim F$  ist.

**Beweis:** Ist  $t : F \rightarrow tF \subseteq E$  ein Isomorphismus von  $F$  auf einen scharf primitiven Unterraum  $tF$  von  $E$ , und bezeichnen wir mit  ${}^{-1}x$  das  $x \in F$  entsprechende Element aus  ${}^{-1}F$ , so ist  $s : x \rightarrow tx + {}^{-1}x$  eine bijektive lineare Abbildung von  $F$  auf einen Unterraum  $sF$  von  $E \perp {}^{-1}F$ . Wegen  $q(sx) = q(tx) + q({}^{-1}x) = q(x) - q(x) = 0$  ist  $sF$  singulär.  $sF$  ist auch scharf primitiv: Da nämlich  $t : F \rightarrow tF$  und  $s : F \rightarrow sF$  beide bijektiv sind, entsprechen sich die Linearformen  $w$  auf  $tF$  und  $v$  auf  $sF$  mittels  $\langle tx, w \rangle = \langle sx, v \rangle$ . Da  $tF$  scharf primitiv in  $E$  ist, kann man zu  $w$  ein  $z \in E$  finden mit  $\langle tx, w \rangle = b(tx, z)$ . Dann ist aber auch  $\langle sx, v \rangle = \langle tx, w \rangle = b(tx, z) = b(tx + {}^{-1}x, z) = b(sx, z)$ . Außerdem ist  $\dim sF = \dim F$  und damit  $\text{ind}(E \perp {}^{-1}F) \geq \dim F$ .

Enthält umgekehrt  $E \perp {}^{-1}F$  einen hyperbolischen Raum  $H_1$  der Dimension  $2 \dim F$ , so betten wir  ${}^{-1}F$  nach (2.24) in einen hyperbolischen Raum  $H_2$

der Dimension 2  $\dim F$  ein, in dem das orthogonale Komplement  $G$  von  ${}^{-1}F$  scharf primitiv und isomorph zu  $F$  ist. Wir haben dann  $H_1 \subseteq E \perp {}^{-1}F \subseteq E \perp H_2$ . Wegen  $H_1 \cong H_2$  gibt es einen Automorphismus  $u \in O(E \perp H_2)$  mit  $uH_1 = H_2$ . Da  $H_1$  orthogonal zu  $G$  ist, liegt  $uG$  im orthogonalen Komplement  $E$  von  $H_2$  und ist zu  $F$  isomorph. Außerdem ist  $G$  scharf primitiv in  $H_2$  also in  $E \perp H_2$ , demnach  $uG$  scharf primitiv in  $E \perp H_2$ , also wegen  $b(uG, H_2) = 0$  auch in  $E$ .

**(3.11)** Ist  $E = \sum Ae_i$  mit  $q(\sum x_ie_i) = \sum a_{ij}x_ix_j$  regulär und  $F = Af$  mit  $q(f) = a \neq 0$ , so besagt (3.10) gerade, daß  $\sum a_{ij}x_ix_j = a$  genau dann lösbar ist, wenn  $\sum a_{ij}x_ix_j - ax_0^2 = 0$  eine nichttriviale Lösung hat. Der Beweis hierfür ist in der einen Richtung selbstverständlich, in der anderen immer noch einfacher als der für (3.10). Beim Beweis der allgemeineren Aussage sieht man aber deutlich den Zusammenhang mit dem Wittschen Satz.

## 4 Lokale Ringe

In diesem Kapitel wurden bisher außer den für beliebige Ringe  $A$  gültigen Grundtatsachen einige Ergebnisse für den Fall bewiesen, daß  $A$  ein Körper ist. Diese lassen sich meist mit unwesentlich abgeänderten Beweisen auf lokale Ringe übertragen. Um mit möglichst geringen Vorkenntnissen auszukommen, wurde in der Vorlesung darauf verzichtet. Hier soll es nachgeholt werden. Die benötigten einfachen Eigenschaften lokaler Ringe findet man z.B. in N. Bourbaki, *Algèbre commutative*, chap. 2, oder in anderen Büchern über Kommutative Algebra. Die für unsere Bedürfnisse wichtigsten lokalen Ringe – eigentlich die einzigen, die wir wirklich brauchen – sind die diskreten Bewertungsringe, die wir in §15 noch genauer untersuchen werden.

Für das weitere sei also  $A$  ein lokaler Ring, d.h. ein Ring mit einem einzigen maximalen Ideal  $I$ . Der Satz (1.20) überträgt sich in der Form

**(4.1) Satz** *Ist  $E$  endlich erzeugter  $A$ -Modul mit symmetrischer Bilinearform  $b$ , so gibt es eine Zerlegung  $E = E_1 \perp \dots \perp E_r \perp F$  in reguläre Teilmoduln  $E_i$  der Dimension 1 oder 2 und einen Modul  $F$  mit  $b(F, F) \subseteq I$ .  $E$  ist genau dann regulär, wenn  $F = \{0\}$  ist.*

Der Beweis verläuft wie bei (1.20) induktiv; man hat nur zu beachten, daß die Anzahl  $r$  der abgespaltenen eindimensionalen Teile durch die Anzahl der Erzeugenden von  $E$  beschränkt ist.

In den Überlegungen, die zu Satz (2.15) führten, hatten wir die Fälle  $\text{char } A \neq 2$  und  $= 2$  unterschieden. Dem ersten entspricht bei lokalen Ringen der Fall, daß 2 invertierbar, also  $2 \notin I$  ist. Wie damals ergibt sich dann auch hier gegenüber (1.20) nichts Neues. Dagegen läßt sich der Satz (2.15) nicht in naheliegender Weise auf lokale Ringe mit  $2 \in I$  zu übertragen. Um das zu sehen, überlege man sich, daß der Raum  $E = \begin{bmatrix} 1 & a \\ & 0 \end{bmatrix}$  für  $a \in I$  die

Eigenschaften  $b(E, E) \subseteq I$ ,  $q(E) \not\subseteq I$  hat, sich aber nicht als Summe eindimensionaler Untermoduln schreiben läßt, falls  $a$  nicht in  $2A$  liegt. Immerhin hat man noch den

**(4.2) Satz** *Über einem lokalen Ring, in dem 2 nicht invertierbar ist, läßt sich jeder reguläre quadratische Modul als orthogonale Summe zweidimensionaler Untermoduln schreiben, jeder halbreguläre als orthogonale Summe eines regulären und eines eindimensionalen Untermoduls.*

Hauptergebnis des §3 war der Satz von Witt in der Form (3.4), den wir bisher erst für Körper der Charakteristik  $\neq 2$  bewiesen haben. Der folgende Satz füllt diese Lücke und läßt darüber hinaus statt eines Grundkörpers allgemeiner einen lokalen Ring zu.

**(4.3) Satz**  *$E$  sei quadratischer Modul über einem lokalen Ring,  $F, G, H$  Untermoduln;  $F, G$  seien frei von endlichem Rang, und es gelte*

$$b_F(H) = F^*, \quad b_G(H) = G^*. \quad (1)$$

Weiter sei  $t: F \rightarrow G$  ein Isomorphismus mit

$$tx \equiv x \pmod{H} \quad (2)$$

für alle  $x$  aus  $F$ . Dann läßt sich  $t$  zu einem Automorphismus von  $E$  fortsetzen, welcher (2) für alle  $x$  aus  $E$  erfüllt und jeden Vektor aus  $H^\perp$  fest läßt.

Der Spezialfall  $H = E$  dieses Satzes liefert die Folgerung

**(4.4) Folgerung** Sind  $F, G$  scharf primitive freie Untermoduln des quadratischen  $A$ -Moduls  $E$  und  $t: F \rightarrow G$  ein Isomorphismus, so gibt es ein  $u \in O(E)$  mit  $u|_F = t$ .

Damit ist auch der noch ausstehende Beweis für Satz (3.4) erbracht.

Wir wollen die Fortsetzung von  $t$  soweit möglich als Produkt von Spiegelungen  $s_h$  mit  $h \in H$  konstruieren. Dabei bleiben alle Vektoren aus  $H^\perp$  fest, und es gilt (2), so daß wir uns um diese Bedingungen nicht weiter zu kümmern brauchen. Allerdings werden wir zunächst einige zusätzliche Voraussetzungen machen, um die Existenz hinreichend vieler Spiegelungen  $s_h$  sicherzustellen. Dazu sei  $\bar{A} = A/I$  der Restklassenkörper und  $\bar{H} = H/IH$ ; mit  $\bar{x}$  bezeichnen wir die Restklasse mod  $IH$  eines Vektors  $x \in H$ , mit  $\bar{q}$  bzw.  $\bar{b}$  die Werte mod  $I$  von  $q$  bzw.  $b$ . Das orthogonale Komplement  $\bar{C}^\perp$  einer Teilmenge  $\bar{C}$  von  $\bar{H}$  ist innerhalb  $\bar{H}$  bzgl.  $\bar{b}$  zu bilden. Schließlich sei  $\mathbb{F}_2$  der Primkörper mit zwei Elementen.

**(4.5)** Die Fortsetzung von  $t$  kann als Produkt von Spiegelungen  $s_h$  mit  $h \in H$  gewählt werden, falls eine der folgenden Bedingungen erfüllt ist:



$$\bar{A} \not\cong \mathbb{F}_2, \quad \bar{q}(\bar{H}) \neq \{0\}, \quad (3)$$

oder

$$\bar{A} \cong \mathbb{F}_2, \quad \bar{q}(\bar{H}^\perp) \neq \{0\}. \quad (4)$$

Wir setzen zunächst (3) oder (4) voraus und beweisen (4.3) und (4.4) durch Induktion nach dem gemeinsamen Rang  $r$  von  $F$  und  $G$ ; danach führen wir die allgemeine Behauptung (4.3) auf den Spezialfall zurück.

Für  $r = 1$  sei  $F = Af$ ,  $G = Ag$  mit  $g = tf = f + h$ . Ist  $q(h)$  invertierbar, so führt  $s_h$  den Vektor  $f$  in  $g$  über und ist daher die gewünschte Fortsetzung. Anderenfalls haben wir

$$q(h) = -b(f, h) = b(g, h) \in I. \quad (5)$$

Jetzt suchen wir eine Spiegelung  $s_e$  derart, daß sich  $s_e(f)$  durch eine weitere Spiegelung in  $g$  überführen läßt. Wir definieren  $d$  durch  $g = s_e(f) + d$ , also

$$d = b(f, e)q(e)^{-1}e + h$$

$$q(d) = b(f, e)b(g, e)q(e)^{-1} + q(h).$$

Ist außer  $q(e)$  auch  $q(d)$  invertierbar, so gilt  $s_d s_e(f) = g$ , und wir haben in  $s_d s_e$  die gewünschte Fortsetzung von  $t$ . Wegen (5) brauchen wir also einen Vektor  $e \in H$  mit

$$q(e) \notin I, \quad b(f, e) \notin I, \quad b(g, e) \notin I.$$

Wir bezeichnen mit  $\bar{H}_1$  bzw.  $\bar{H}_2$  die Unterräume derjenigen Vektoren  $\bar{x} \in \bar{H}$  für die  $b(f, x) \equiv 0$  bzw.  $b(g, x) \equiv 0 \pmod{I}$  ist. Wegen (1) sind beides Hyperebenen in  $\bar{H}$ . Da man zu jedem Vektor  $\bar{e} \in \bar{H}$  einen Vertreter  $e \in H$  finden kann, haben wir nur zu zeigen, daß  $\bar{q}$  auf dem Komplement  $\bar{H} \setminus (\bar{H}_1 \cup \bar{H}_2)$  nicht identisch verschwindet. Nehmen wir einmal an, das sei doch der Fall. Für beliebige

$$\bar{t} \in \bar{A}, \quad \bar{x} \in \bar{H}_1 \cap \bar{H}_2, \quad \bar{y} \in \bar{H} \setminus (\bar{H}_1 \cup \bar{H}_2)$$

liegt dann  $\bar{t}\bar{x} + \bar{y}$  nicht in  $\bar{H}_1 \cup \bar{H}_2$ , so daß

$$\bar{q}(\bar{t}\bar{x} + \bar{y}) = \bar{t}^2 \bar{q}(\bar{x}) + \bar{t}\bar{b}(\bar{x}, \bar{y}) + \bar{q}(\bar{y}) = 0$$

ist. Hat nun  $\bar{A}$  mindestens drei Elemente, so folgt daraus

$$\bar{q}(\bar{x}) = \bar{b}(\bar{x}, \bar{y}) = \bar{q}(\bar{y}) = 0. \quad (6)$$

Wegen (5) können wir speziell  $\bar{x} = \bar{h}$  setzen und erhalten  $\bar{b}(\bar{h}, \bar{H} \setminus (\bar{H}_1 \cup \bar{H}_2))$ , also, da das Komplement zweier Hyperebenen den ganzen Raum erzeugt, sogar  $\bar{b}(\bar{h}, \bar{H}) = 0$ . Wegen  $g = f + h$  folgt daraus  $\bar{H}_1 = \bar{H}_2$ , und jeder Vektor

aus  $\bar{H}$  liegt entweder in  $\bar{H}_1 \cap \bar{H}_2 = \bar{H}_1$  oder in  $\bar{H} \setminus (\bar{H}_1 \cup \bar{H}_2) = \bar{H} \setminus \bar{H}_1$ . Dann besagt (6) aber  $\bar{q}(\bar{H}) = 0$  im Widerspruch zur Voraussetzung (3).

Ist dagegen  $\bar{A} \cong \mathbb{F}_2$ , so können wir (6) jedenfalls noch dann ableiten, wenn wir zusätzlich verlangen, daß  $\bar{x}, \bar{y}$  in  $\bar{H}^\perp$  liegen. Aus der Definition von  $\bar{H}_1, \bar{H}_2$  folgt aber unmittelbar  $\bar{H}_1 \cap \bar{H}^\perp = \bar{H}_2 \cap \bar{H}^\perp$ , so daß jeder Vektor aus  $\bar{H}^\perp$  entweder in  $\bar{H}_1 \cap \bar{H}_2$  oder in  $\bar{H} \setminus (\bar{H}_1 \cup \bar{H}_2)$  liegt. Aus (6) folgt dann  $\bar{q}(\bar{H}^\perp) = 0$  im Widerspruch zur Voraussetzung (4).

Nun sei  $r > 1$  und  $f_1, \dots, f_r$  eine Basis von  $F$ . Nach Voraussetzung (1) gibt es Vektoren  $h_1, \dots, h_r$  in  $H$  mit  $b(f_i, h_j) = \delta_{ij}$ .  $H$  ist dann direkte Summe von  $\sum_{i=1}^r Ah_i$  und  $F^\perp \cap H = D$ , und die  $h_i$  bilden eine Basis von  $H$  modulo  $D$ . Wir

wenden die Induktionsannahme auf  $\sum_{i=1}^{r-1} Af_i$  anstelle von  $F$  an und bekommen

ein Produkt von Spiegelungen  $s_h$ , das auf  $\sum_{i=1}^{r-1} Af_i$  mit  $t$  übereinstimmt. Indem wir  $t$  von links mit dem inversen Produkt multiplizieren, reduzieren wir unsere Aufgabe auf den Spezialfall, daß  $tf_i = f_i$  ist für  $i = 1, \dots, r-1$ . Für diese  $i$  und  $x \in F$  ist dann aber

$$b(tx - x, f_i) = b(tx, tf_i) - b(x, f_i) = 0,$$

also

$$tx \equiv x \pmod{Ah_r + D}.$$

Wenn wir den Induktionsanfang auf  $Af_r$  statt  $F$  und  $Ah_r + D$  statt  $H$  anwenden können, so sind wir fertig, da bei dem so erhaltenen Automorphismus  $u$  von  $E$  die zu  $Ah_r + D$  orthogonalen Vektoren  $f_1, \dots, f_r$  fest bleiben.

Wir müssen die (1) bis (4) entsprechenden Voraussetzungen für  $Af_r$  und  $Ah_r + D$  anstelle von  $F$  und  $H$  prüfen. (1) bleibt offenbar erhalten, und für (2) haben wir es eben gesehen. Wir zeigen nun, daß bei geeigneter Wahl der Basis  $f_1, \dots, f_r$  auch (3) bzw. (4) für  $Ah_r + D$  anstelle von  $H$  gilt. Nach Voraussetzung gibt es jedenfalls einen Vektor  $\bar{h}$  mit  $\bar{q}(\bar{h}) \neq 0$  in  $\bar{H}$  bzw.  $\bar{H}^\perp$ . Wir wählen  $\bar{h}_r \in \bar{H} \setminus \bar{D}$  so, daß  $\bar{h}$  in  $\overline{A\bar{h}_r + \bar{D}}$  liegt, und ergänzen  $\bar{h}_r$  zu einer Basis  $\bar{h}_1, \dots, \bar{h}_r$  von  $\bar{H} \bmod \bar{D}$ . Repräsentanten  $h_1, \dots, h_r$  der  $\bar{h}_i$  in  $H$  bilden eine Basis von  $H \bmod D$ , und die duale Basis  $f_1, \dots, f_r$  von  $F$  hat dann alle gewünschten Eigenschaften.

Zum Abschluß haben wir noch zu zeigen, daß der Satz auch ohne die Bedingungen (3), (4) gilt. In diesem Fall betrachten wir eine hyperbolische Ebene  $Ae + Af$  mit  $q(xe + yf) = xy$  und bilden die orthogonale Summe  $E' = E \perp (Ae + Af)$ . Wegen  $q(e + f) = 1$  können wir den schon bewiesenen Teil des Satzes auf  $E', F' = F \perp Ae, G' = G \perp Ae, H' = H \perp A(e + f), t' = t \perp \text{id}_{Ae}$  anstelle von  $E, F, G, H, t$  anwenden. Wir erhalten eine Fortsetzung  $u'$  von  $t'$  die außer  $e$  wegen  $b(H', e - f) = 0$  auch  $e - f$  fest läßt. Also

läßt sich  $u' = u \perp \text{id}_{Ae+Af}$  schreiben, und  $u$  ist die gewünschte Fortsetzung von  $t$ .

**(4.6) Satz** *Ist  $E$  ein regulärer quadratischer Modul über einem lokalen Ring  $A$  und ist nicht gleichzeitig der Restklassenkörper  $\bar{A} \cong \mathbb{F}_2$  und  $\dim E \leq 4$ , so läßt sich jeder Automorphismus  $u \in O(E)$  als Produkt von Spiegelungen schreiben.*

Ist  $\bar{A} \not\cong \mathbb{F}_2$ , so folgt dies unmittelbar aus (4.5) mit  $F = G = H = E$ . Im Fall  $\bar{A} \cong \mathbb{F}_2$  kann man etwa folgendermaßen vorgehen. Gibt es einen Vektor  $e \in E$  mit  $q(e) \notin I$ , der unter  $u$  fest bleibt, so erhält man die Behauptung, indem man  $E$  als direkte (nicht notwendig orthogonale) Summe  $E = Ae + F$  schreibt und (4.5) auf  $t = u|_F$ ,  $G = tF$ ,  $H = e^\perp$  anwendet; wegen  $\bar{e} \in \bar{H}^\perp$  ist nämlich (4) erfüllt, und die Fortsetzung, die man erhält, läßt  $e \in H^\perp$  fest, ist also gerade  $u$ . Im allgemeinen Fall wähle man irgendeinen Vektor  $e \in E$  mit  $q(e) \notin I$ , suche ein Produkt  $v$  von Spiegelungen mit  $ve = ue$  und wende die obige Überlegung auf  $v^{-1}u$  an. Ein solches  $v$  bekommt man wiederum aus (4.4), angewandt auf  $F = Ae$ ,  $G = Aue$ , sobald man einen Untermodul  $H \subseteq E$  hat mit  $\bar{H} \not\subseteq \bar{e}^\perp$ ,  $\bar{H} \not\subseteq (\overline{ue})^\perp$ ,  $b(e, H) = b(ue, H) = A$ ,  $ue - e \in H$  und  $\bar{q}(\bar{H}^\perp) \neq \{0\}$ . Wählt man  $H = h^\perp + IE$  mit  $q(h) \notin I$ , so ist wegen  $\bar{h} \in \bar{H}^\perp$  die letzte Bedingung erfüllt, und die anderen lauten  $\bar{h} \in (\overline{ue - e})^\perp$ ,  $\bar{h} \neq \bar{e}$ ,  $\bar{h} \neq \overline{ue}$ . Nun hat  $\bar{E}$  nach Voraussetzung mindestens die Dimension 6, und man überlegt sich leicht, daß dann jede Hyperebene wie z.B.  $(\overline{ue - e})^\perp$  mehr als zwei Vektoren  $\bar{h}$  mit  $\bar{q}(\bar{h}) \neq 0$  enthält, so daß diese Bedingungen erfüllt werden können.

Um jetzt auch den Satz (3.5) vollständig zu beweisen, hat man noch die regulären Räume der Dimension 2 und 4 über  $\mathbb{F}_2$  und die halbregulären zu behandeln. Von der ersten Sorte gibt es, wie wir in Kapitel IV sehen werden, nur vier nicht isomorphe. Man kann diese einzeln durchdiskutieren oder, eleganter, die obigen allgemeinen Überlegungen noch etwas weiterführen, und sieht so, daß es nur den in (3.5) angegebenen Ausnahmefall gibt. Einen halbregulären Raum  $E$  über einem Körper der Charakteristik 2 schreibt man nach (2.15) als orthogonale Summe  $E = F \perp Ae$  mit regulärem  $F$  und wendet (4.4) auf  $t = u|_F$ ,  $G = tF$ ,  $H = E$  an. Man erhält ein Produkt  $v$  von Spiegelungen, welches auf  $F$  mit  $u$  übereinstimmt. Dann ist  $v^{-1}u$  auf  $F$  die Identität und führt  $e$  in  $ae$  mit  $a^2 = 1$ , also  $a = 1$  über, und daraus folgt  $u = v$ .

Die weiteren in §3 enthaltenen Folgerungen aus dem Wittschen Satz sind so formuliert, daß sie sich samt ihren Beweisen ohne wesentliche Änderungen auf lokale Ringe übertragen lassen.

## Anmerkungen zu Kapitel I

Die systematische Verwendung der geometrischen Sprache und geometrischer Argumente zur Untersuchung quadratischer Formen, deren auch wir uns befleißigen, geht auf E. Witt zurück. Der Satz (3.1) findet sich in seiner Habilitationsschrift [W]. Das Analogon für Körper der Charakteristik 2 steht in C. Arf [A]. Über die in §3 erwähnten Verallgemeinerungen findet man Angaben z.B. bei J. Dieudonné [D], W. Scharlau [Sch], für lokale Ringe in M. Knebusch, *Isometrien über semilokalen Ringen*, Math. Z. **108** (1969), 255–268, M. Kneser, *Witts Satz für quadratische Formen über lokalen Ringen*, Nachr. Akad. Wiss. Göttingen, Math. Phys. Klasse, Heft 9, 1972. Unseren Beweis des Satzes (4.3) haben wir im wesentlichen der letztgenannten Arbeit entnommen.

Quadratische Formen

Kneser, M.

2002, VIII, 164 S. 2 Abb., Softcover

ISBN: 978-3-540-64650-1