Frobenius-Schur-Indikatoren in Charakteristik 2

von
SEBASTIAN STIGLER

DIPLOMARBEIT

in Mathematik

vorgelegt der
Fakultät für Mathematik, Informatik und Naturwissenschaften der
Rheinisch-Westfälische Technische Hochschule Aachen
März 2007

Angefertigt am
Lehrstuhl D für Mathematik
bei
Professor Dr. G. Hiß

Inhaltsverzeichnis

Notation

Kapitel 1

$b(x,y)$ 1
symmetrische Bilinearform.

$F^{\perp}$ 2
der zu F orthogonale Untermodul (von $E \supseteq F$).

$\operatorname{rad} E$ 2
das Radikal von E.

E^* 2
der zu E duale Modul.

b_F 2
der durch die Bilinearform b induzierte Homomorphismus von E nach F^*.

(E,b) 2
ein Modul E mit symmetrischer Bilinearform.

$\mathbf{x} = (x_1,\ldots,x_n)$ 3
der Koordinatenvektor von $x = \sum x_i e_i$ bezüglich der Basis $\underline{e} = (e_1,\ldots,e_n)$.

T^t 3
die zur Matrix T transponierte Matrix.

${}_{\underline{e}}b_{\underline{e}}$ 3
die Gram-Matrix von b bezüglich der Basis $\underline{e}$.

Vorwort

> Philosophieren, sagt er, heißt, eine schlechte Begründung dafür finden, woran man instinktiv glaubt. Als ob der Mensch an irgend etwas instinktiv glaubte![1]
>
> *(Aldous Huxley, Schöne neue Welt)*

In dieser Arbeit wollen wir uns mit dem folgenden Problem beschäftigen: Gegeben sei eine endlich erzeugte Gruppe G, ein endlicher Körper F der Charakteristik zwei und ein als F-Vektorraum endlich dimensionaler FG-Modul V. Die Frage, die uns interessiert ist: trägt V eine G-invariante reguläre quadratische Form (vgl. (1.72))?

Im ersten Kapitel erarbeiten wir die hierfür notwendigen theoretische Grundlagen. Hierbei orientieren wir uns an der Vorlesung **Quadratische Formen** von Prof. Nebe [Neb06] und dem Buch **Quadratische Formen** von Martin Kneser [Kne02], da bei diesen Quellen nicht, wie bei den meisten Quellen, der Charakteristik zwei Fall a priori ausgeschlossen wird.

Im zweiten Kapitel beschreiben wir zwei von Jon Thackray entwickelte Algorithmen, die zum einen testen, ob ein gegebener FG-Modul eine G-invariante reguläre quadratische Form trägt oder nicht, und zum anderen, falls der Modul eine solche quadratische Form trägt, zu welchem der zwei Isometrietypen der Modul gehört.

Im letzten Kapitel führen wir zunächst die Technik der Kondensation ein und untersuchen anschließend, ob wir mit Hilfe dieser Technik bei sehr großen Moduln (im Bezug auf die Dimension) entscheiden können, ob der Modul eine G-invariante reguläre quadratische Form trägt oder nicht.

Dieses Kapitel, und damit auch diese Arbeit, abschließend wollen wir noch eine gänzlich anderen Ansatz erwähnen. Hierbei wird die Untermodulstruktur eines Moduls mit G-invarianter regulärer quadratische Form benutzt um zu entscheiden ob ein Kompositionsfaktor eines bestimmten Faktormoduls eine G-invariante reguläre quadratische Form trägt oder nicht.

[1] Anm. des Autors: Glücklicherweise betreiben wir hier Mathematik.

Schließlich enthält diese Arbeit noch drei weiter erwähnenswerte Abschnitte: Ein Notationsverzeichnis, in welchem jedes Symbol und jede Schreibweise, die in dieser Arbeit verwendet wird aufgeführt wird mit einer kurzen Erklärung und der Erwähnung der ersten Seite, auf der diese benutzt wird. Ein Stichwortverzeichnis in dem jeder definierte Begriff aufgeführt wird. Und schlussendlich ein Liste aller mit den Algorithmen des zweiten Kapitels getesteter Moduln.

Kapitel 1

Theoretische Grundlagen

> Dies hier ist ein erstes Kapitel,
> welches verhindern soll, daß
> vorliegendes Werkchen mit
> einem zweiten Kapitel beginne.
>
> *(Franz Werfel, Stern der Ungeborenen)*

In diesem Kapitel werden wir uns mit einigen Grundlagen der Theorie der bilinearen und quadratischen Formen über beliebigen kommutativen Ringen (immer mit 1) beschäftigen. Neben den wesentlichen Definitionen und Schreibweisen werden wir, dabei weitestgehend dem ersten Kapitel von [Kne02] und der auf diesem Buch aufbauenden Vorlesung Quadratischen Formen von Prof. Nebe [Neb06] folgend, den Wittschen Fortsetzungssatz (vgl. (1.41)) über einem beliebigen Körper beweisen. Dieser soll auch gleichzeitig einen Abschluss für die allgemeinen Grundlagen der Theorie bilden.

Mit einem Blick auf das Kapitel 2 werden wir die endlich-dimensionalen (halb-)regulären quadratischen Räume über endlichen Körpern klassifizieren. Die Klassifikation liefert zugleich auch schon die Beweisidee für die Korrektheit des Algorithmus zur Berechnung des Witt-Index in (2.11) für gewisse quadratische FG-Moduln.

Schlussendlich werden wir mit dem Lemma von Fong (vgl. [HB82, Seite 108, Theorem 8.13] und (1.71)) und einigen darauf aufbauenden Sätzen dieses Kapitel beschließen.

§ 1.1. Symmetrische Bilinearformen

In diesem Abschnitt ist A ein kommutativer Ring, E ein A-Modul und $b : E \times E \to A$ eine **symmetrische Bilinearform**.

(1.1) Definition:

(a) Wir nennen die Elemente x und y aus E ***senkrecht zueinander*** *oder* ***orthogonal*** *(bezüglich*

der Bilinearform 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****. Wir nennen* $\operatorname{rad} E := E^\perp$ *das* ***Radikal*** *von b.*

(c) *E heißt* ***orthogonale Summe*** *der Untermoduln $E_1, \ldots, E_n$, in Zeichen*

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

wenn E direkte Summe der Untermoduln $E_1, \ldots, E_n$ ist und $b(E_i, E_j) = 0$ für $i \neq j$.

(d) *Für einen A-Modul E bezeichnet $E^* = \operatorname{Hom}_A(E, A)$ den* ***dualen Modul****.* ■

Der nun folgende Satz gibt uns Auskunft darüber, wann ein Teilmodul F von E ein **orthogonales Komplement** in E besitzt. Das heißt, wann $E = F \perp F^\perp$ gilt.

(1.2) Satz:
Sei F ein Teilmodul von E. Dann gilt für den Modulhomomorphismus

$$b_F : E \to F^* ; y \mapsto (F \to A; x \mapsto b(x,y)) :$$

(a) *Der Kern von b_F ist $F^\perp$.*

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

Beweis: (a) Mit Definition (1.1)(b) ist dies sofort klar.

(b) Ist $E = F \perp F^\perp$ so gilt $b_F(E) = b_F(F \perp F^\perp) \overset{(a)}{=} b_F(F)$. Weiter haben F und $F^\perp$ nach Definition der orthogonalen Summe trivialen Schnitt.
Induziert umgekehrt b_F eine Bijektion von F auf $b_F(E)$, so gibt es zu jedem $y \in E$ genau ein $x \in F$ mit $b_F(y) = b_F(x)$. Dann ist $y - x \in \operatorname{Kern} b_F = F^\perp$. Folglich ist $E = F \perp F^\perp$. ■

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

Um die Begriffe aus (1.3) auch auf einen Teilmodul F von (E,b) anwenden zu können, trägt F, falls nichts anderes gesagt wird, stets die Bilinearform $b|_{F\times F}$.
Da die zur Einschränkung gehörende Abbildung $b_F : F \to F^*$ gleich der Einschränkung der obigen Abbildung $b_F : E \to F^*$ auf F ist, ist nun auch im Nachhinein klar, wieso auf die Nennung des Definitionsbereichs E von b bei der Bezeichnung der Abbildung b_F verzichtet wurde.

(1.4) Satz:
Jeder reguläre Untermodul F eines Moduls E mit symmetrischer Bilinearform spaltet als orthogonaler Summand ab.

Beweis: Für jeden Teilmodul F von E gilt folgende Inklusionskette

$$b_F(F) \subseteq b_F(E) \subseteq F^*.$$

Da F regulär ist, gilt in der obigen Kette an jeder Stelle die Gleichheit. Mit dem Kriterium aus (1.2)(b) folgt die Behauptung. ■

Als nächstes interessiert uns, wie sich die Eigenschaften „nicht ausgeartet“ und „regulär“ bezüglich orthogonaler Summen verhalten.

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

Beweis: Ist $E = \bigoplus_{i=1}^n E_i$ so haben wir den kanonischen Isomorphismus $E^* \simeq \bigoplus_{i=1}^n E_i^*$. Ist diese Summe auch noch orthogonal bezüglich b, so haben wir $b_{E_i}|_{E_j} = 0$ für $i \neq j$. Also ist $b_E : E \to E^*$ genau dann injektiv (surjektiv), wenn alle $b_{E_i} : E_i \to E_i^*$ es sind. ■

Schließlich wollen wir Bilinearformen auf freien Moduln durch Matrizen beschreiben. Dabei werden wir, in Anlehnung an das Computeralgebrasystem GAP [GAP05], die Koordinatenvektoren in freien Moduln als Zeilenvektoren schreiben. Dabei gilt: Ist $\underline{e} = (e_1, \ldots, e_n)$ eine Basis des Moduls und $x = \sum x_i e_i$ ein Element des Moduls ($x_i \in A$), so schreiben wir $\mathbf{x} = (x_1, \ldots, x_n)$ für den Koordinatenvektor (zur Basis $\underline{e}$).

(1.6) Definition & Bemerkung:
Sei (E, b) ein endlich erzeugter (e.e.) freier Modul mit Bilinearform und $\underline{e} = (e_1, \ldots, e_n)$ eine Basis von E. Dann heißt die Matrix

$$_{\underline{e}}b_{\underline{e}} = (b(e_i, e_j))_{1 \leqslant i,j \leqslant n}$$

*die **Gram-Matrix** von b bzw. von (E, b) bezüglich der Basis $\underline{e}$. Sind $x = \sum x_i e_i$ und $y = \sum y_i e_i$ Linearkombinationen der e_i mit $x_i, y_i \in A$ so gilt*

$$b(x, y) = \mathbf{x}\,{}_{\underline{e}}b_{\underline{e}}\,\mathbf{y}^t.$$

Ist $\underline{e'} = \left(e'_1, \ldots, e'_n\right)$ eine weitere Basis von E und gilt $e'_j = \sum t_{ji} e_i$, so gilt für die entsprechende Matrix ${}_{\underline{e'}}b_{\underline{e'}}$ und die Basiswechselmatrix $T = (t_{ij})$ der folgende Zusammenhang:

$${}_{\underline{e'}}b_{\underline{e'}} = T\,{}_{\underline{e}}b_{\underline{e}}\,T^t$$

*Mit $d(e_1, \ldots, e_n)$ bezeichnen wir die **Determinante** von ${}_{\underline{e}}b_{\underline{e}}$. Aus dem Determinantenmultiplikationssatz ergibt sich (mit den Bezeichnungen wie oben)*

$$d(e'_1, \ldots, e'_n) = d(e_1, \ldots, e_n) \det(T)^2. \tag{1.6.1}$$

Das heißt, die Determinante der Gram-Matrix ändert sich bei Basiswechsel um ein Quadrat der Einheitengruppe $A^\times$ von A. Ihre Klasse modulo $A^{\times 2}$ nennen wir daher die Determinante von (E, b) und schreiben dafür $d(e_1, \ldots, e_n)A^{\times 2} = \det(E, b) = \det E$. ■

Um der Tatsache Rechnung zu tragen, dass wir uns zwar die Einträge der Gram-Matrix interessieren, nicht aber für die dafür konkret gewählte Basis, führen wir die folgende Schreibweise ein.

(1.7) Definition:
Einen freien Modul mit Gram-Matrix ${}_{\underline{e}}b_{\underline{e}} = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}$ *bezeichnen wir mit* $\left\langle \begin{matrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{matrix} \right\rangle$, *speziell für eine Diagonalmatrix mit Diagonaleinträgen* $b_1, \ldots, b_n$ *schreiben wir* $\langle b_1, \ldots, b_n \rangle$. ■

Schließlich wollen wir die Gram-Matrix ${}_{\underline{e}}b_{\underline{e}}$ als Abbildungsmatrix der linearen Abbildung $b_E : E \to E^*$ auffassen. Dafür benötigen wir eine geeignete Basis von E^*.

(1.8) Definition:
Hat der Modul E *die Basis* $\underline{e} = (e_1, \ldots, e_n)$, *so ist die* ***duale Basis*** $\underline{e^*} = \left(e_1^*, \ldots, e_n^*\right)$ *von* E^* *definiert durch*

$$e_j^*(e_i) = \delta_{i,j} = \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{sonst.} \end{cases}$$

■

Definieren wir die Koeffizienten b'_{kj} durch $b_E(e_j) = \sum_k b'_{kj} e_k^*$, so gilt:

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

Somit ist die Gram-Matrix tatsächlich die Abbildungsmatrix zur Abbildung $b_E : E \to E^*$ bezüglich der Basen $e_1, \ldots, e_n$ und $e_1^*, \ldots, e_n^*$.

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

Beweis (vgl. [OR74, Kapitel V, §6 Satz 5 und Satz 6']): Sei im Folgenden G die Gram-Matrix von b bezüglich der Basis $e_1, \ldots, e_n$ und G' die zu G adjungierte Matrix, i.e.

$$GG' = G'G = \det(G) E_n. \tag{1.9.1}$$

Ist G invertierbar, so folgt aus dem Determinantenmultiplikationssatz, dass auch $\det(G)$ invertierbar ist. Ist umgekehrt $\det(G)$ invertierbar, so definieren wir $H := \det(G)^{-1} G'$ und es gilt wegen (1.9.1) die Identität $HG = GH = E_n$; also ist $H = G^{-1}$.

Die Aussage, dass b_E genau dann injektiv ist, wenn $d(e_1, \ldots, e_n)$ kein Nullteiler ist, ist nicht ganz so einfach zu zeigen.

Wir zeigen zunächst, dass die Determinante von G den Kern von G annulliert: Für $z \in \operatorname{Kern} G$ gilt

$$z \det(G) \overset{(1.9.1)}{=} zGG' = 0G' = 0.$$

Ist also $\det(G)$ kein Nullteiler, so muss der Kern von G Null sein. Mithin ist b_E injektiv, i.e. b nicht ausgeartet.

Sei umgekehrt $\det(G)$ ein Nullteiler und $x \in A \setminus \{0\}$ so gewählt, dass $x\det(G) = 0$ ist. Sei $1 \leqslant r \leqslant n$ minimal mit der Eigenschaft, dass für jede $r \times r$ Untermatrix U von G gilt: $x\det(U) = 0$.

Ist $r = 1$, so annulliert x jeden Eintrag in G, also ist beispielsweise $(x, \ldots, x)$ im Kern von b_E.

Ist $r \geqslant 2$, so gibt es eine $(r-1) \times (r-1)$ Untermatrix V von G mit $x\det(V) \neq 0$. Sei o.B.d.A. (evtl. umnummerieren) V von der Form

$$V = \begin{pmatrix} g_{22} & \cdots & g_{2r} \\ \vdots & & \vdots \\ g_{r2} & \cdots & g_{rr} \end{pmatrix},$$

wobei die g_{ij} die Einträge von G sind. Wir ergänzen nun die Matrix V durch Hinzufügen einer beliebigen (Teil-) Spalte von G auf folgende Art zu einer $r \times r$ Matrix:

$$V'_{(k)} = \left(\begin{array}{c|ccc} g_{1k} & g_{12} & \cdots & g_{1r} \\ \hline g_{2k} & & & \\ \vdots & & V & \\ g_{rk} & & & \end{array}\right)$$

Diese Matrix hat nun entweder zwei gleiche Spalte oder ist, bis auf Permutation der Spalten, eine Untermatrix von G und nach der Wahl von r gilt $x\det(V'_{(k)}) = 0$.

Wir berechnen nun die Determinante d_k der Matrizen $V'_{(k)}$ indem wir nach der eben eingefügten, ersten Spalte entwickeln. Es ist also $d_k = \det(V'_{(k)}) = \sum_{i=1}^{r} g_{ik}c_i$ für gewisse $c_i \in A$, die nicht von k abhängen. Nach der Konstruktion von $V'_{(k)}$ ist $c_1 = \det(V)$; mithin ist $xc_1 \neq 0$. Da aber stets $xd_k = 0$ ist, haben wir mit $\sum_{i=1}^{r}(xc_i)g_{ik} = 0$ für $1 \leqslant k \leqslant n$ eine nichttriviale Linearkombination der Null aus Zeilen von G erhalten. Somit ist auch in diesem Fall der Kern von b_E nicht trivial. ■

Mit einer Induktion über den Rang erhält man aus diesem Satz eine Diagonalisierung für gewisse freie Moduln.

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

$$E \simeq \left\langle d_1, \frac{d_2}{d_1}, \ldots, \frac{d_n}{d_{n-1}} \right\rangle.$$

Beweis: Nach (1.4) ist

$$\sum_{i=1}^{j} Ae_i = \sum_{i=1}^{j-1} Ae_i \perp \langle c_j \rangle \text{ mit einem } c_j \in A.$$

Somit ist die Gram-Matrix der rechten Seite der Gleichung von der Form $\left(\begin{array}{ccc|c} b_{1\,1} & \cdots & b_{1\,j-1} & \\ \vdots & & \vdots & 0 \\ b_{j-1\,1} & \cdots & b_{j-1\,j-1} & \\ \hline & 0 & & c_j \end{array}\right)$

und es gilt $d_j = d_{j-1}c_j$. ■

(1.11) Definition:
*Sei (E,b) regulär und $\underline{e} = (e_1,\ldots,e_n)$ eine Basis von E. Sei $e_i^{\#} \in E$, mit $e_i^{\#} := b_E^{-1}(e_i^*)$ (d.h. $b(e_j,e_i^{\#}) = \delta_{ji}$). Die Basis $\underline{e^{\#}} = \left(e_1^{\#},\ldots,e_n^{\#}\right)$ heißt die **zu $\underline{e}$ duale Basis von** E.*
Es gilt $e_i = \sum_{j=1}^{n} b(e_i,e_j)e_j^{\#}$, also ist ${}_{\underline{e}}b_{\underline{e}}$ die Basiswechselmatrix von $\underline{e^{\#}}$ nach $\underline{e}$. ■

(1.12) Folgerung:
Sei E regulär und F ein freier Teilmodul mit A-Basis $(e_1,\ldots,e_m)$, die sich zu einer Basis von E ergänzen lässt. Dann gilt $F^{\perp\perp} = F$

Beweis: Es ist $F = \bigoplus_{i=1}^{m} Ae_i$ und $E = \bigoplus_{i=1}^{n} Ae_n$. Der Modul E ist regulär mit Basis $\underline{e} = (e_1,\ldots,e_n)$ und der dazu dualen Basis $\underline{e^{\#}} = \left(e_1^{\#},\ldots,e_n^{\#}\right)$. Damit gilt $F^{\perp} = Ae_{m+1}^{\#} \oplus \cdots \oplus Ae_n^{\#}$ und schließlich $F^{\perp\perp} = Ae_1 \oplus \cdots \oplus Ae_m = F$. ■

Im Allgemeinen gilt allerdings nur $F^{\perp\perp} \supsetneq F$, wie das folgende Beispiel zeigt.

(1.13) Beispiel:
Sei $A = \mathbb{Z}$ und $E = Ae_1$ mit $b(e_1,e_1) = 1$. Für den Teilmodul wählen wir $F = \mathbb{Z}2e_1$. Dann ist $F^{\perp} = \{ae_1 \in E \mid 0 = b(ae_1,2e_1) = 2a\} = \{0\}$. Somit ist $F^{\perp\perp} = \{0\}^{\perp} = E \neq F$ ■

Ist nun A ein Körper, so erhalten wir die folgenden, verschärften Aussagen.

(1.14) Satz:
Ein endlich-dimensionaler Vektorraum über einem Körper ist genau dann regulär, wenn er nicht ausgeartet ist. Für jeden Unterraum F eines regulären Vektorraums E gilt

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

■

(1.15) Satz:
Ist A ein Körper und E endlich-dimensional, so gibt es eine Zerlegung $E = E_1 \perp \ldots \perp E_r \perp F$ in reguläre Teilräume E_i der Dimension 1 oder 2 und einen Raum F mit $b(F,F) = 0$. Der Raum 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 $e_1,\ldots,e_r$ von $E_1,\ldots,E_r$ durch Hinzunahme einer Basis von F zu einer Basis von E aus paarweise orthogonalen Vektoren ergänzen.

Beweis: Wir machen eine Induktion nach der Dimension von E, beginnend mit $E = \{0\}$.

Ist $b(E,E) = 0$, so sind wir mit $r = 0$ und $F = E$ fertig. Anderenfalls haben wir zwei Fälle zu unterscheiden:

(a) Es gibt einen Vektor $e \in E$ mit $b(e,e) \neq 0$. Dann können wir Ae nach (1.4) abspalten und auf $Ae^\perp$ die Induktionsvoraussetzung anwenden.
(b) Es ist $b(e,e) = 0$ für alle $e \in E$ aber es gibt zwei Vektoren $e, f \in E$ mit $b(e,f) \neq 0$. Dann ist $d(e,f) = -b(e,f)^2 \neq 0$, und wir können $Ae + Af$ nach (1.4) und (1.9) abspalten. Der Fall (b) kann wegen $2b(e,f) = b(e+f, e+f) - b(e,e) - b(f,f)$ nicht vorkommen, wenn $2 \neq 0$ in A gilt. ■

Zum Abschluss dieses Abschnitts wollen wir noch eine Reihe von Beispielen betrachten, wobei in den ersten Dreien Begriffe wie Determinante, Gram-Matrix und orthogonale Summe behandelt werden, wohingegen die letzten drei Beispiele uns im Laufe dieser Arbeit noch öfter begegnen werden.

(1.16) Beispiel:
Wir betrachten die folgenden drei Serien von freien $\mathbb{Z}$-Moduln mit symmetrischer Bilinearform und bezeichnen diese, der Literatur folgend, mit I_n, A_n und D_n. Dabei deutet der Index n den Rang des Moduls an.

(a) Sei $I_n = \mathbb{Z}^n$ mit dem Standardskalarprodukt $b(\mathbf{x},\mathbf{y}) = \sum_{i=1}^n x_i y_i$, wobei $\mathbf{x} = (x_1,\dots,x_n)$, $\mathbf{y} = (y_1,\dots,y_n)$ und $x_i, y_i \in \mathbb{Z}$. Wir betrachten die Gram-Matrix von I_n bezüglich der Standardbasis $\mathbf{e}_1,\dots,\mathbf{e}_n$. Die Determinante von I_n ist somit 1 und folglich ist I_n regulär. Weiter ist I_n als orthogonale Summe in $I_n = \perp_{i=1}^n \mathbb{Z}\mathbf{e}_i$ zerlegbar, mit $\mathbb{Z}\mathbf{e}_i \simeq I_1$.
(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 beispielsweise 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

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

Es ist $\det A_n = n+1$. Die Determinante erhält man durch Entwicklung nach der ersten Zeile und anschließender Induktion. Nach dem Kriterium aus (1.9) ist A_n nur für $n = 0$ regulär; für $n \geqslant 1$ ist A_n lediglich nicht ausgeartet.
(c) Sei $D_n = \{\sum x_i\mathbf{e}_i \in I_n \mid \sum x_i \equiv_2 0\}$. Wir wählen, im Gegensatz zu [Kne02], die Basis $\underline{e'} = (\mathbf{e}_1 - \mathbf{e}_2, \mathbf{e}_2 - \mathbf{e}_3, \dots, \mathbf{e}_{n-1} - \mathbf{e}_n, 2\mathbf{e}_n)$, da diese Basis auch für $n = 1$ noch stimmt[1]. Die Basiswechselmatrix von der Standardbasis $\underline{e}$ zur Basis $\underline{e'}$ sei mit T bezeichnet; sie hat Determinante 2. Wir wollen Nachrechnen, dass $\underline{e'}$ auch wirklich eine Basis von D_n ist. Sei dazu

[1] In [Kne02] wird hierfür die Basis $(\mathbf{e}_1 - \mathbf{e}_2, \mathbf{e}_2 - \mathbf{e}_3, \dots, \mathbf{e}_{n-1} - \mathbf{e}_n, \mathbf{e}_{n-1} + \mathbf{e}_n)$ verwendet. Ist nun aber $n = 1$, so fällt diese Basis zu $(\mathbf{e}_1)$ zusammen. Dies ist aber keine Basis von D_1!

$\sum_{i=1}^{n} x_i \mathbf{e}_i \in D_n$ *gegeben (d.h.* $\sum x_i \equiv_2 0$*). Es gilt*

$$\sum_{i=1}^{n} x_i \mathbf{e}_i = \sum_{i=1}^{n} x_i (\mathbf{e}_i - \mathbf{e}_n) + \underbrace{\left(\sum_{i=1}^{n} x_i \right)}_{\equiv_2 0} \mathbf{e}_n,$$

und $\mathbf{e}_i - \mathbf{e}_n$ *ist darstellbar als* $\sum_{j=i}^{n} \mathbf{e}_j - \mathbf{e}_{j+1}$*. Damit ist* $\underline{e'}$ *als Basis von* D_n *nachgewiesen. Die Gram-Matrix bezüglich der Basis* $\underline{e'}$ *ergibt sich nach (1.6) durch:*

$${}_{\underline{e'}}b_{\underline{e'}} = T\,{}_{\underline{e}}b_{\underline{e}}T^t = TE_nT^t = \begin{pmatrix} 2 & -1 & & & & \\ -1 & 2 & -1 & & & \\ & \ddots & \ddots & \ddots & & \\ & & -1 & 2 & -1 & \\ & & & -1 & 2 & -2 \\ & & & & -2 & 4 \end{pmatrix}$$

Die Determinante von ${}_{\underline{e}}b_{\underline{e}}$ *ist somit gleich* $\det(TT^t) = \det(T)^2 = 4$*. Also ist* D_n *für alle* n *nicht ausgeartet jedoch nicht regulär.*

Bei den nächsten drei Beispielen sei der Grundring stets der Körper $\mathbb{F}_2$ *und der Modul* $E \simeq \mathbb{F}_2^6 (= \mathbb{F}_2^{1\times 6})$*. Es werden lediglich drei verschiedene Bilinearformen darauf betrachtet. Im Moment mag dies etwas willkürlich erscheinen, jedoch wird sich im Lauf der Arbeit herausstellen, dass diese drei Formen höchst verschiedene Eigenschaften haben. Diese wollen wir mit den Algorithmen im zweiten Kapitel bestimmen.*
Als Basis sei stets die Standardbasis $\underline{e} = (e_1, \ldots, e_6)$ *des Raums* $\mathbb{F}_2^6$ *zugrunde gelegt. Zur besseren Lesbarkeit werden Nullen als Punkt geschrieben.*

(d) *Wir betrachten die Bilinearform* b_1 *die durch ihre Gram-Matrix gegeben ist:*

$$\begin{pmatrix} . & 1 & 1 & 1 & . & . \\ 1 & . & 1 & 1 & . & . \\ 1 & 1 & . & 1 & 1 & . \\ 1 & 1 & 1 & . & . & . \\ . & . & 1 & . & . & 1 \\ . & . & . & . & 1 & . \end{pmatrix}.$$

Ihre Determinante ist 1, also ist (E, b_1) *regulär.*

(e) *Als nächstes betrachten wir die Bilinearform* b_2 *mit Gram-Matrix*

$$\begin{pmatrix} . & 1 & . & . & 1 & . \\ 1 & . & 1 & 1 & 1 & . \\ . & 1 & . & . & . & 1 \\ . & 1 & . & . & . & . \\ 1 & 1 & . & . & . & . \\ . & . & 1 & . & . & . \end{pmatrix}.$$

Die Determinante ist ebenfalls 1, also ist auch (E, b_2) *regulär.*

(f) *Schließlich haben wir noch b_3 mit Gram-Matrix*

$$\begin{pmatrix} . & 1 & . & . & 1 & 1 \\ 1 & . & 1 & 1 & 1 & . \\ . & 1 & . & . & . & 1 \\ . & 1 & . & . & . & . \\ 1 & 1 & . & . & . & . \\ 1 & . & 1 & . & . & . \end{pmatrix}.$$

Und auch diese Matrix hat Determinante 1, was bedeutet, dass auch (E, b_3) regulär ist.

Ohne zu viel vorweg zu nehmen wird sich in den nächsten Paragraphen herausstellen, dass es kein Zufall ist, dass sich alle drei Räume als regulär herausgestellt haben. Wir werden sehen, dass auf den einzelnen Räumen Gruppen operieren, welche die Bilinearformen invariant lassen. Weiter werden auf den ersten beiden Räumen sogar unter dieser Operation invariante quadratische Formen existieren, welche unterschiedliche Orthogonalitätstypen haben. Zudem wird sich ergeben, dass der dritte Raum keine solche quadratische Form trägt. ■

Die abschließenden Worte des Beispiels führen uns auch sogleich zum folgenden Paragraphen.

§ 1.2. Quadratische Formen

Es gelten die selben Voraussetzungen wie im Abschnitt § 1.1.

(1.17) Definition:

(a) *Eine Abbildung $q : E \to A$ heißt **quadratische Form**, wenn die folgenden zwei Bedingungen erfüllt sind:*
   (i) *$q(ax) = a^2 q(x)$ für alle $a \in A$ und $x \in E$.*
   (ii) *Es existiert eine symmetrische Bilinearform $b_q : E \times E \to A$, die $b_q(x, y) = q(x + y) - q(x) - q(y)$ für alle $x, y \in E$ erfüllt.*

   *Wir nennen einen Modul E mit quadratischer Form q kurz einen **quadratischen Modul**, in Zeichen (E, q).*

(b) *Die Abbildung $\varphi : (E, q) \to (E', q')$ heißt **Isometrie**, wenn φ ein injektiver Modulmorphismus ist, für den $q'(\varphi(x)) = q(x)$ für alle $x \in E$ gilt.*

(c) *Zwei quadratische Moduln (E, q) und (E', q') heißen **isometrisch**, falls es eine bijektive Isometrie zwischen ihnen gibt. Wir schreiben $(E, q) \simeq (E', q')$ oder kurz $E \simeq E'$ dafür.*

(d) *Sind (E, q) und (E', q') quadratische Moduln, so heißt $(E, q) \perp (E', q')$ die orthogonale Summe falls gilt: $(E, q) \perp (E', q') = (E \oplus E', q \perp q')$ mit $q \perp q'(x + x') = q(x) + q'(x')$ für $x \in E$ und $x' \in E'$.* ■

(1.18) Bemerkung:

Aus der definierenden Gleichung in (1.17)(a)(ii) erhält man für $x = y$ die Gleichung

$$2q(x) = b_q(x, x). \tag{1.18.1}$$

Hieran können wir sehen, dass die Begriffe „quadratische Form“ und „symmetrische Bilinearform“ im Falle $2 \in A^*$ übereinstimmen (da gemäß (1.18.1) jeder symmetrischen Bilinearform auf E eineindeutig eine quadratische Form zugeordnet ist). Ist 2 kein Nullteiler in A, so kann man immer noch bei gegebener symmetrischer Bilinearform b eine quadratische Form q mit $b_q = b$ definieren, falls $b(x,x) \in 2A$ für alle $x \in E$ gilt. Ist aber 2 ein Nullteiler in A, so ist der Begriff der quadratischen Form „stärker“[2] als der der symmetrischen Bilinearform. ■

(1.19) Folgerung:

(a) Isr a eine (nicht notwendig symmetrische) Bilinearform, so wird durch

$$q(x) := a(x,x)$$

eine quadratische Form definiert. Die zugehörige symmetrische Bilinearform ist gemäß (1.17)(a)(ii) durch

$$b_q(x,y) := a(x,y) + a(y,x)$$

gegeben.

(b) Für einen endlich erzeugten freien Modul können wir umgekehrt zu gegebener quadratischer Form q ein solches a finden.

Beweis: (a) Klar.

(b) Aus (1.17)(a) und (1.18.1) erhalten wir durch Induktion

$$q(\sum_i x_i e_i) = \sum_i q(e_i) x_i^2 + \sum_{i<j} b_q(e_i, e_j) x_i x_j$$

falls $e_1, \ldots, e_n$ eine Basis von E ist. Wir erhalten a indem wir $a(\sum x_i e_i, \sum y_j e_j) = \sum\limits_{i \leqslant j} a_{ij} x_i y_j$ mit $a_{ii} = q(e_i)$ und $a_{ij} = b_q(e_i, e_j)$ für $i < j$ setzen. ■

Die Aussage in (1.19)(b) veranlasst uns zu folgender Kurzschreibweise (vgl. (1.7)).

(1.20) Definition:

Ist E ein freier quadratischer Modul mit Basis $(e_1, \ldots, e_n)$ und a wie im Beweis zu (1.19)(b), so schreiben wir für E abkürzend

$$E = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & a_{22} & & \\ & & \ddots & \\ & & & a_{nn} \end{bmatrix}$$

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

$$E = \left\langle \begin{matrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{matrix} \right\rangle .$$

■

[2] Vgl. z.B. (1.21)(b)

(1.21) Definition:

(a) *Ein quadratischer A-Modul (E,q) heißt genau dann* ***regulär*** *(bzw.* ***nicht ausgeartet*** *), wenn (E,b_q) regulär (bzw. nicht ausgeartet) ist.*

(b) *Ein Teilmodul $F \leqslant E$ heißt* ***singulär****, falls $q(F) = \{0\}$ ist. Dies ist, falls 2 ein Nullteiler ist, eine stärkere Forderung als $F \subseteq F^\perp$ (d.h. $b_q(F,F) = \{0\}$).*

(c) *Ein Element $x \in E$ heißt* ***singulär****, falls $q(x) = 0$ ist.* ■

(1.22) Beispiel:

(a) *Sei 2 kein Nullteiler in A. Wir schreiben $E = [1] = \langle 2 \rangle$ für den Modul $E = A$ mit $q(x) = x^2$. Ist $2 \notin A^*$, so ist (E,q) nicht regulär.*

(b) *Sei A wieder ein beliebiger Ring. Ist $E = Ae_1 \oplus Ae_2$ mit $q(x_1e_1 + x_2e_2) = x_1x_2$, so heißt dieser Modul* ***hyperbolische Ebene*** *und es gilt $E = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} = \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right\rangle =: \mathbb{H} = \mathbb{H}(A)$. Da die Determinante dieses Moduls in der Einheitengruppe eines jeden Rings liegt, ist $\mathbb{H}(A)$ für jeden Ring A regulär.* ■

Wir wollen den Zusatz in (1.22)(a) noch etwas verallgemeinern.

(1.23) Satz:
Sei $E = \bigoplus_{i=1}^n Ae_i$ ein freier quadratischer Modul von ungeradem Rang n und sei $2 \notin A^*$. Dann ist (E,q) nicht regulär.

Beweis: Wegen (1.21)(a) ist (E,q) genau dann regulär, wenn (E,b_q) regulär ist. Dies wiederum ist genau dann der Fall, wenn $\det({}_e b_{qe}) \in A^*$ ist. Die Determinante berechnet sich wie folgt

$$\det({}_e b_{qe}) = \det \begin{pmatrix} 2a_1 & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b_{n-1,n} \\ b_{n,1} & \cdots & b_{n,n-1} & 2a_n \end{pmatrix}.$$

Sei abkürzend $(G_{ij}) := {}_e b_{qe}$, $a_i := q(e_i)$ und $b_{ij} := b_q(e_i,e_j)$ für $i \neq j$. Nach der Leibnitzformel gilt für die Determinante:

$$\det G = \sum_{\pi \in \mathfrak{S}_n} \operatorname{sgn}(\pi) \prod_{i=1}^n G_{i,\pi(i)}.$$

Unser Ziel wird sein zu zeigen, dass die Determinante in $2A$ liegt. Hierfür zerlegen wir die symmetrische Gruppe auf geschickte Weise in zwei disjunkte Teilmengen, über die wir dann separat summieren werden.

Sei $I = \left\{\pi \in \mathfrak{S}_n \mid \pi = \pi^{-1}\right\}$ die Menge der selbstinversen Permutationen und $N = \{\pi \in \mathfrak{S}_n \mid \pi \neq \pi^{-1}\right\}$ die Menge der nicht selbstinversen Permutationen. Wir zerlegen N weiter in zwei disjunkte und gleichgroße Mengen X und Y mit der Bedingung: für alle $\pi \in X$ ist $\pi^{-1} \in Y$ und für alle $\sigma \in Y$ ist $\sigma^{-1} \in X$.

Da n ungerade ist, hat jede Permutation π aus I wegen $\pi^2 = 1$ wenigstens einen Fixpunkt, das heißt, dass in der Summe $\sum_{\pi\in I} \operatorname{sgn}(\pi) \prod_{i=1}^{n} G_{i,\pi(i)}$ in jedem Summanden ein Element der Hauptdiagonale von G als Faktor auftaucht. Diese Summe liegt also in $2A$.

Da G symmetrisch ist, gilt für $\pi \in X$:

$$\prod_{i=1}^{n} G_{i,\pi(i)} = \prod_{i=1}^{n} G_{\pi(i),i} = \prod_{l=1}^{n} G_{l,\pi^{-1}(l)}.$$

Damit kommt in $\sum_{\pi\in N} \operatorname{sgn}(\pi) \prod_{i=1}^{n} G_{i,\pi(i)}$ jeder Summand zwei mal vor.

Zusammenfassend erhalten wir $\det G \in 2A$. ■

Der Beweis des vorherigen lässt sich auch wie folgt umschreiben: Ist n ungerade, so gibt es ein Polynom $P_n(x_i, y_{ij}) \in \mathbb{Z}[x_i, y_{ij} | 1 \leqslant i \neq j \leqslant n]$, so dass $2P_n(a_i, b_{ij}) = \det G$ ist.

Die Einführung des Polynoms P_n mag etwas artifiziell wirken, ist aber ein wichtiges Hilfsmittel für die nächste Definition. Damit wir das Polynom P_n genauer angeben können benötigen wir noch drei Kurzschreibweisen:
Ist $\pi \in \mathfrak{S}_n$ so bezeichnet $\operatorname{Fix}(\pi) := \{i \in \{1,\dots,n\} \mid \pi(i) = i\}$ die Menge der Fixpunkte von π und $\operatorname{Mov}(\pi) := \{1,\dots,n\} \setminus \operatorname{Fix}(\pi)$ die Menge der von π bewegten Punkte. Mit $\operatorname{mfix}(\pi)$ ist der kleinste Fixpunkt von π gemeint (so es denn überhaupt einen gibt).

(1.24) Definition & Bemerkung:
Sei E ein freier quadratischer Modul mit Basis $(e_1,\dots,e_n)$ von ungeradem Rang. Mit der Notation und Argumentation aus dem Beweis von (1.23) gilt:

$$\begin{aligned} P_n(x_i, y_{ij}) \;=\; & \sum_{\pi\in X} \operatorname{sgn}(\pi) \prod_{i\in \operatorname{Fix}(\pi)} 2x_i \prod_{i\in \operatorname{Mov}(\pi)} y_{i,\pi(i)} + \\ & \sum_{\pi\in I} \operatorname{sgn}(\pi)\, x_{\operatorname{mfix}(\pi)} \prod_{\substack{i\in \operatorname{Fix}(\pi)\\ i\neq \operatorname{mfix}(\pi)}} 2x_i \prod_{i\in \operatorname{Mov}(\pi)} y_{i,\pi(i)} \end{aligned}$$

Damit definieren wir nun:

(a) *Die **Halbdeterminante** $d'(e_1,\dots,e_n)$ von E wird mittels des Polynoms P_n wie folgt definiert*

$$d'(e_1,\dots,e_n) := P_n(q(e_i), b_q(e_i,e_j)).$$

(b) *Mit den Bezeichnungen aus (1.6) gilt, entsprechend der Formel (1.6.1),*

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

(c) *E heißt **halbregulär**, wenn $d'(e_1,\dots,e_n)$ invertierbar ist.*

Beweis: (b) Ist 2 kein Nullteiler, so folgt die Gleichung aus (1.6.1). Nun fassen wir die Größen $a_i = q(e_i), b_{ij} = b_q(e_i, e_j)$ und t_{ij}, wobei $(t_{ij}) = T$ wie in (1.6) definiert ist, als Unbestimmte über $\mathbb{Z}$ auf. Somit können wir die Gleichung als Identität im Polynomring $\mathbb{Z}[a_i, b_{ij}, t_{ij}]$ ansehen. Diese Identität bleibt erhalten, wenn wir für die Unbestimmten Werte aus einem Ring einsetzen. ■

(1.25) Bemerkung:
Die Halbdeterminante ist im Allgemeinen nicht multiplikativ. Ist $(E, q) = \perp_{i=1}^{n} (Ae_i, q_i)$ *mit ungeradem n, so ist*

$$\prod_{i=1}^{n} d'(e_i) = \prod_{i=1}^{n} q(e_i) \quad \text{aber} \quad d'(e_1, \ldots, e_n) = 2^{n-1} \prod_{i=1}^{n} q(e_i).$$

Es gilt aber für einen quadratischen Modul der Form $E = \bigoplus_{i=1}^{n} Ae_i$ *mit ungeradem n und der orthogonalen Zerlegung* $(E, q) = (E_1, q_1) \perp (E_2, q_2)$, *wobei* $E_1 = \bigoplus_{i=1}^{2m} Ae_i$ *und* $E_2 = \bigoplus_{i=2m+1}^{n} Ae_i$ *ist, der folgende Zusammenhang*

$$d'(e_1, \ldots, e_n) = d(e_1, \ldots, e_{2m}) d'(e_{2m+1}, \ldots, e_n). \tag{1.25.1}$$

(Achtung, hier ist wirklich die Determinante von E_1 *gemeint; vgl. (1.6).)*

Beweis: Ist 2 kein Nullteiler, so folgt die Gleichung (1.25.1) aus der entsprechenden Gleichung für die Berechnung der Determinante von Blockdiagonalmatrizen. Mit der Argumentation aus dem Beweis von (1.24)(b) folgt nun auch die Gleichheit falls 2 ein Nullteiler ist. ■

Nun wollen wir die Zerlegung $E = E_1 \perp \ldots \perp E_r \perp F$ aus (1.15) für quadratische Vektorräume noch ein wenig verfeinern.

(1.26) Satz:
Ist A ein Körper und (E, q) *ein endlich-dimensionaler quadratischer Vektorraum, so gibt es Teilräume* $E_1, \ldots, E_r, F_1, \ldots, F_s, G \leqslant E$ *derart, dass*

$$E = E_1 \perp \ldots \perp E_r \perp F_1 \perp \ldots \perp F_s \perp G \tag{1.26.1}$$

gilt. Dabei sind die E_i *zweidimensional und regulär, die* F_j *sind eindimensional und halbregulär und* $q(G) = \{0\}$.

Ist $\operatorname{char} A \neq 2$ *so kann* $r = 0$ *gewählt werden und* (E, q) *ist genau dann regulär, wenn* $G = \{0\}$ *ist.*

Ist $\operatorname{char} A = 2$ *so kann* $s \leqslant \left[A : A^2\right]$ *gewählt werden, wobei* $A^2 = \left\{a^2 \mid a \in A\right\}$ *Teilkörper von A ist und* $\left[A : A^2\right]$ *den Grad der Körpererweiterung bezeichnet. Es gilt:* (E, q) *ist genau dann regulär, wenn* $s = 0$ *und* $G = \{0\}$ *ist. Zudem gilt:* (E, q) *ist genau dann halbregulär, wenn* $s = 1$ *und* $G = \{0\}$ *ist.*

Beweis: Ist $\operatorname{char} A \neq 2$ so folgt die Behauptung sofort aus (1.15).

Ist $\operatorname{char} A = 2$, so liefert Satz (1.15) schon mal die Zerlegung $(E, b_q) = E_1 \perp \ldots \perp E_r \perp F$ mit E_i regulär mit $\dim(E_i) = 1$ oder 2 und $b_q(F,F) = 0$. Wegen Satz (1.23) ist $\dim(E_i) = 2$. Nach der Bemerkung in Definition (1.21)(b) ist $b_q(F,F) = 0$ in Charakteristik 2 aber noch nicht der Weisheit letzter Schluss. Deshalb zerlegen wir F noch weiter.

Für alle $x, y \in F$ gilt $0 \overset{F \subseteq F^\perp}{=} b_q(x,y) \overset{(1.17)(a)(ii)}{=} q(x+y) - q(x) - q(y)$. Die quadratische Form ist also ein Gruppenhomomorphismus von $(F,+)$ nach $(A,+)$. Wegen $q(ax) = a^2 q(x)$ für $a \in A$ und $x \in F$ ist $G := \{x \in F \mid q(x) = 0\}$ ein A-Teilraum von F. Weiter ist $q(F)$ ein A^2-Teilraum von A und es gilt $s := \dim_{A^2}(q(F)) \leqslant \dim_{A^2}(A) = \left[A : A^2\right]$. Ist die A^2-Dimension von A endlich, so folgt sofort, dass auch s endlich ist. Ist hingegen $\left[A : A^2\right] = \infty$ so können wir daraus nicht sofort schließen, dass s endlich ist. In diesem Fall argumentieren wir wie folgt: Wir werden zeigen, dass jede A^2-Basis von $q(F)$ durch Urbildnahme zu einer A-Basis von F/G von gleicher Kardinalität wird. Weiter ist, da E endlich-dimensional (über A) ist, auch F/G als A-Vektorraum endlich-dimensional. Somit muss eine jede A^2-Basis von $q(F)$, als Bild einer endlichen Teilmenge, auch endlich sein.

Sei $(z_1, \ldots, z_s)$ eine A^2-Basis von $q(F)$. Wir wählen zu jedem z_i ein Urbild x_i unter q, i.e. $q(x_i) = z_i$. Ist $f \in F$, so gilt $q(f) = \sum_{i=1}^s c_i^2 q(x_i)$ mit $c_i \in A$. Da q Gruppenhomomorphismus ist, erhalten wir $q(f - \sum_{i=1}^s c_i x_i) = 0$, also ist $f - \sum_{i=1}^s c_i x_i \in G$ und $F = \langle x_1, \ldots, x_s, G\rangle_A$. Bleibt noch zu zeigen, dass $(x_1 + G, \ldots, x_s + G)$ in F/G linear unabhängig sind: Sei dazu $\sum_{i=1}^s c_i x_i \in G$, $c_i \in A$. Wenden wir q an, so ergibt sich $q(\sum_{i=1}^s c_i x_i) = \sum_{i=1}^s c_i^2 q(x_i) = \sum_{i=1}^s c_i^2 z_i = 0$. Da die z_i ein A^2-Basis von $q(F)$ bilden, sind die $c_i^2 = 0$. Somit haben wir $F = \bigoplus_{i=1}^s Ax_i \oplus G$ und da $F \subseteq F^\perp$ ist, ist die direkte Summe eine orthogonale. Setzten wir $F_i := Ax_i$ so erhalten wir insgesamt $E = E_1 \perp \ldots \perp E_r \perp F_1 \perp \ldots \perp F_s \perp G$.

■

(1.27) Beispiel:
Sei $A = \mathbb{F}_2(X)$ und $E = A \oplus A \oplus A$ mit der quadratischen Form $q((y_1,y_2,y_3)) = y_1^2 + y_2^2 X + y_3^2 X^2$, i.e. $(E,q) = \left[1, X, X^2\right]$. Sei weiterhin $\underline{e}$ die Standardbasis von E. Die Halbdeterminante $d'(\underline{e})$ ist gleich $4X^3 = 0$ (vgl. (1.25)), also ist (E,q) nach (1.24)(c) nicht halbregulär.
Die Bilinearform $b_q(x,y)$ ist gleich Null für alle $x, y \in E$. Wir erhalten $G = \left\{(y_1,y_2,y_3) \in E \mid y_1^2 + y_2^2 X + y_3^2 X^2 = 0\right\} = \langle (X,0,1)\rangle_A$. Nach (1.26) lässt sich die Anzahl der halbregulären Summanden von E zu $s = \dim_{A^2}(q(E)) \overset{(1.26.1)}{=} \dim(E) - \dim(G) = 2$ berechnen. Wir wählen $f_1 = (1,0,0)$ und $f_2 = (0,1,0)$, da $q(f_i) \neq 0$ (i=1,2) ist und erhalten $E = Af_1 \perp Af_2 \perp G$. ■

Als nächstes führen wir ein paar Sprechweisen ein.

(1.28) Definition:

*(a) Ein Untermodul F eines A-Moduls E heißt **primitiv** (in E), wenn er ein direkter Summand von E ist, i.e. es gibt einen Teilmodul G von E mit $E = F \oplus G$.*

*(b) Trägt E eine symmetrische Bilinearform b, so heißt F **scharf primitiv** (bezüglich b), wenn F endlich erzeugter freier A-Modul und $b_F(E) = F^*$ ist.* ■

(1.29) Bemerkung:

Sei (E,q) ein quadratischer A-Modul und F ein Teilmodul. Dann gilt:

(a) Ein regulärer Untermodul F ist stets scharf primitiv.

(b) Ein scharf primitiver Untermodul F ist immer auch primitiv.

(c) Ist E regulär und F primitiv, endlich erzeugt und frei, so ist F scharf primitiv.

(d) Ist A ein Hauptidealbereich (HIB) und E regulär, so sind die folgenden Aussagen äquivalent:

- *Der Teilmodul F ist primitiv.*
- *Der Teilmodul F ist scharf primitiv.*

Beweis: Wir schreiben für die zu q gehörende Bilinearform b_q kurz b.

(a) Nach Definition (1.3) ist F endlich erzeugt frei und es gilt $b_F(F) = F^*$, also ist erst recht $b_F(E) = F^*$.

(b) Sei $(f_1,\dots,f_m)$ ein Basis von F. Da $b_F(E) = F^*$ ist, gibt es $e_1,\dots,e_m \in E$ mit $b_F(e_i) = f_i^*$, wobei $(f_1^*,\dots,f_m^*)$ die zu $(f_1,\dots,f_m)$ duale Basis von F^* ist. Setze $G := \langle e_1,\dots,e_m\rangle^\perp$. Ist $\sum_{i=1}^m a_i f_i \in F \cap G$ so gilt $0 = b(\sum_{i=1}^m a_i f_i, e_j) = a_j$ für alle j; also ist $F \cap G = \{0\}$. Ist $e \in E$ und definieren wir $a_i = b(e,e_i)$, so gilt $e - \sum_{i=1}^m a_i f_i \in G$. Damit ist $E = F \oplus G$ und F primitiv.

(c) Da F primitiv ist, ist $E = F \oplus G$. Da E regulär ist gilt $b_E(E) = E^*$. Daraus folgt, wegen $E^* = F^* \oplus G^*$, dass $b_F(E) = F^*$ ist, da $E^* \to F^* \oplus G^*$, $\varphi \mapsto (\varphi|_F + \varphi|_G)$ ein Isomorphismus ist.

(d) Nach dem Hauptsatz über e.e. Moduln über HIB ist, da E e.e. frei ist, auch F, als direkter Summand, frei. Damit folgt die Behauptung aus (b) und (c). ■

(1.30) Definition:

*Für einen A-Modul G definieren wir $\mathbb{H}(G) := (G \oplus G^*, q_{\mathbb{H}(G)})$ mit $q_{\mathbb{H}(G)}(x + x^*) = x^*(x)$ für alle $x \in G$ und $x^* \in G^* (= \mathrm{Hom}_A(G,A))$ und nennen $\mathbb{H}(G)$ den zu G gehörenden **hyperbolischen Modul**. Die zugehörige Bilinearform ist durch $b_{q_{\mathbb{H}(G)}}(x + x^*, y + y^*) = x^*(y) + y^*(x)$ gegeben. Ist $G = \bigoplus_{i=1}^n Ae_i$ frei mit Basis $\underline{e}$, so ist $\underline{f} = (\underline{e}, \underline{e^*})$ Basis von $G \oplus G^*$ und ${}_{\underline{f}}b_{q_{\mathbb{H}(G)}\underline{f}} = \begin{pmatrix} 0 & E_n \\ E_n & 0 \end{pmatrix}$. Der zu G gehörende hyperbolische Modul $\mathbb{H}(G)$ ist stets regulär.* ■

Dem aufmerksamen Leser wird an dieser Stelle nicht entgangen sein, dass in der Definition des hyperbolischen Moduls nicht berücksichtigt wurde, dass G möglicherweise schon eine quadratische Form trägt und sich dieser Umstand doch auch in der Form $q_{\mathbb{H}(G)}$ widerspiegeln sollte. Der nun folgende Satz wird unter anderem zeigen (wenn auch nur für den Fall, dass G frei ist, da dies der Fall ist, der uns im folgenden hauptsächlich interessiert), dass der zu G gehörende hyperbolische Modul vollkommen unabhängig von der quadratischen Form auf G ist.

Doch zuvor wollen wir noch eine kleine Bemerkung über Isometrien machen.

(1.31) Bemerkung:
Sei (E,q) ein freier quadratischer Modul mit Basis $\underline{e} = (e_1,\dots,e_n)$. Sei (F,q') ein weiterer quadratischer Modul und $\varphi : (E,q) \to (F,q')$ ein Modulmonomorphismus. Dann ist φ genau dann eine Isometrie, wenn $q'(\varphi(e_i)) = q(e_i)$ für $i = 1,\dots,n$ und $b_{q'}(\varphi(e_i),\varphi(e_j)) = b_q(e_i,e_j)$ für $i < j$ ist.

Beweis: Folgt sofort aus (1.17)(a)(ii) und (1.17)(b). ■

(1.32) Satz:
Ist (E,q) ein freier quadratischer Modul, so gibt es eine Isometrie (Achtung! nur injektiv, nicht surjektiv; vgl. (1.17)(b)) $\varphi : (E,q) \to \mathbb{H}(E)$, so dass $\varphi(E)^\perp \simeq (E,-q)$ ist. Wenn (E,q) regulär ist, so ist $\mathbb{H}(E) = \varphi(E) \perp \varphi(E)^\perp \simeq (E,q) \perp (E,-q)$.

Beweis: Sei $\underline{e} = (e_1,\dots,e_n)$ eine Basis von $(E,q) = \begin{bmatrix} a_1 & & b_{ij} \\ & \ddots & \\ & & a_n \end{bmatrix}$, so dass $q(e_i) = a_i$ und $b_q(e_i,e_j) = b_{ij}$ ist. Wir definieren Elemente f_i^* im Dualraum E^* von E wie folgt:

$$f_i^* = \sum_{j=1}^{i-1} b_{ij}e_j^* + a_i e_i^* \in E^*.$$

Der Modulmonomorphismus φ sein nun durch

$$\varphi : E \to \mathbb{H}(E) = E \oplus E^* ; e_i \mapsto e_i + f_i^*$$

definiert. Wir rechnen leicht nach, dass $q_{\mathbb{H}(E)}(\varphi(e_i)) = f_i^*(e_i) = a_i = q(e_i)$ und $b_{q_{\mathbb{H}(E)}}(\varphi(e_i),\varphi(e_j)) = f_i^*(e_j) + f_j^*(e_i) = b_{ij} = b(e_i,e_j)$ ist. Somit ist φ nach (1.31) eine Isometrie.

Als nächstes wenden wir uns dem Teilmodul $\varphi(E)^\perp$ zu. Wir definieren $g_j = e_j + (-\sum_{i=j+1}^n b_{ij}e_i^* - a_j e_j^*)$ und behaupten, dass g_j in $\varphi(E)^\perp$ für $j = 1,\dots,n$ liegt. Wir rechnen

$$b_{q_{\mathbb{H}(E)}}(g_j,\varphi(e_i)) = f_i^*(e_j) - (\sum_{l=j+1}^{n} b_{lj}e_l^* + a_j e_j^*)(e_i) = \begin{cases} a_i - a_i = 0 & \text{falls } i = j, \\ b_{ij} - b_{ij} = 0 & \text{falls } i > j, \\ 0 - 0 = 0 & \text{falls } i < j. \end{cases}$$

Nach Definition der g_j ist $q_{\mathbb{H}(E)}(g_j) = -a_j$ und $b_{q_{\mathbb{H}(E)}}(g_i,g_j) = -b_{ij}$ für $i \neq j$. Weiter sehen wir, dass die $(g_1,\dots,g_n)$ linear unabhängig sind und deshalb ist $\varphi(E)^\perp = \langle g_1,\dots,g_n\rangle_A \simeq (E,-q)$. ■

(1.33) Satz:
Jeder scharf primitive singuläre Untermodul F von E ist in einem zum hyperbolischen Modul $\mathbb{H}(F)$ 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 $b_q(f_i,g_j) = \delta_{ij}$ und $q(\sum Ag_i) = \{0\}$ ist.

Beweis: Seien $e_1, \ldots, e_m \in E$ mit $b_q(e_i, f_j) = \delta_{ij}$ (vgl. (1.28)(b)). Damit ist $\langle f_1, \ldots, f_m, e_1, \ldots, e_m \rangle_A \simeq \begin{bmatrix} 0 & E_n \\ * & \end{bmatrix}$. Unser Ziel ist es, die Elemente e_i so abzuändern, dass wir Elemente $g_1, \ldots, g_m$ erhalten, so dass $H = \langle f_1, \ldots, f_m, g_1, \ldots, g_m \rangle_A \simeq \begin{bmatrix} 0 & E_n \\ 0 & \end{bmatrix}$ ist. Dafür setzen wir $g_1 := e_1 - q(e_1)f_1$ und erhalten $b_q(g_1, f_i) = b_q(e_1, f_i)$ für alle i, da F singulär ist. Weiter ist auch g_1 singulär, da $q(g_1) = q(e_1) + q(e_1)^2 q(f_1) - b_q(e_1, q(e_1)f_1) = q(e_1) + 0 - q(e_1) = 0$ ist. Als nächstes setzen wir $g_2 := e_2 - b_q(g_1, e_2)f_1 - q(e_2)f_2$ und allgemein $g_j := e_j - \sum_{i=1}^{j-1} b_q(g_i, e_j)f_i - q(e_j)f_j$ und erhalten $b_q(g_i, g_j) = 0$ für $i \neq j$ und $q(g_j) = 0$. ■

Prinzipiell sind wir jetzt in der Lage, die (halb)regulären quadratischen Räume über endlichen Körpern zu klassifizieren. Da uns aber auch interessiert (bzw. interessieren wird), wie die entsprechenden orthogonalen Gruppen dazu aussehen, werden wir uns zuvor noch den folgenden Paragraphen ansehen.

§ 1.3. Die orthogonale Gruppe und der Satz von Witt

Es gelten die selben Voraussetzungen wie im Abschnitt § 1.1.

(1.34) Definition:
Sei (E, q) ein quadratischer A-Modul. Dann heißt

$$O(E, q) := \{\varphi : E \to E \mid \varphi \text{ ist } A\text{-Modulautomorphismus und } q(\varphi(e)) = q(e) \text{ für alle } e \in E\}$$

*die **orthogonale Gruppe** von (E, q).* ■

Als erstes wollen wir uns eine wichtige Klasse von orthogonalen Abbildungen ansehen, nämlich die Spiegelungen.

(1.35) Beispiel:
*Sei (E, q) ein quadratischer Modul, $e \in E$ mit $q(e) \in A^*$. Dann heißt $s_e : E \to E ; x \mapsto x - \frac{b_q(x,e)}{q(e)} e$ die **Spiegelung** entlang e (oder an $\langle e \rangle^\perp$). Wir rechnen leicht nach, dass die folgenden Eigenschaften gelten.*

(a) $s_e(e) = -e$ und $s_e(x) = x$ falls $x \in \langle e \rangle^\perp$ ist (i.e. $b_q(x, e) = 0$ ist).
(b) $s_e^2 = id$.

(c) $s_e \in O(E,q)$. *Für* $x \in E$ *gilt nämlich:*

$$\begin{aligned} q(s_e(x)) &= q(x - \frac{b_q(x,e)}{q(e)}e) \\ &= q(x) + q(\frac{b_q(x,e)}{q(e)}e) - b_q(x, \frac{b_q(x,e)}{q(e)}e) \\ &= q(x) + \frac{b_q(x,e)^2}{q(e)^2}q(e) - \frac{b_q(x,e)}{q(e)}b_q(x,e) \\ &= q(x). \end{aligned}$$

Hieraus ersehen wir sofort, dass s_e *die Bedingungen für eine orthogonale Abbildung erfüllt.*

(d) Für $g \in O(E,q)$ *und* $x \in E$ *so gilt*

$$\begin{aligned} gs_eg^{-1}(x) &= g(g^{-1}(x) - \frac{b_q(g^{-1}(x),e)}{q(e)}e) \\ &= x - \frac{b_q(g^{-1}(x),e)}{q(e)}g(e) \\ &= x - \frac{b_q(x,g(e))}{q(e)}g(e) \\ &= s_{g(e)}(x). \end{aligned}$$

(e) Die Rechnung aus (d) zeigt, dass

$$S(E,q) = \langle s_e \mid e \in E,\ q(e) \in A^* \rangle \leqslant O(E,q)$$

ein Normalteiler, der ***Spiegelungsnormalteiler****, in* $O(E,q)$ *ist.*

(f) Ist $2 \in A^*$ *und* $q(e) \in A^*$, *so ist* $E = Ae \perp (Ae)^\perp$ *und* $s_e = -id_{Ae} \perp id_{(Ae)^\perp}$. ■

Nun wollen wir uns mit dem Fortsetzungssatz von Witt beschäftigen. Zunächst werden wir den Spezialfall, dass die Charakteristik von A ungleich 2 ist, behandeln. Später wird er dann auf beliebige Körper verallgemeinert.

(1.36) Satz (Fortsetzungssatz von Witt):
Sei A *ein Körper der Charakteristik ungleich* 2, E *ein quadratischer Raum über* A, F_1 *und* F_2 *Unterräume wobei* F_1 *regulär sein soll (vgl. (1.40)) und* $\varphi : F_1 \to F_2$ *eine Isometrie. Dann gibt es ein* $\Phi \in O(E,q)$ *derart, dass* $\Phi|_{F_1} = \varphi$ *ist.*

Beweis: Wir führen eine Induktion nach der Dimension von F_1 durch.
Sei $\dim F_1 = 1$, $F_1 = Af_1$ und $f_2 := \varphi(f_1)$. Da F_1 regulär ist, ist $q(f_1) = q(f_2) \neq 0$. 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 zwei Fälle zu unterscheiden:

1. Fall $q(f_1 - f_2) \neq 0$. Daher existiert die Spiegelung an $e := f_1 - f_2$. Wir rechnen nach, dass

$$\begin{aligned} s_e(f_1) &= f_1 - \frac{b_q(f_1, f_1 - f_2)}{q(f_1 - f_2)} e \\ &= f_1 - \frac{b_q(f_1, f_1) - b_q(f_1, f_2)}{q(f_1) + q(f_2) - b_q(f_1, f_2)} e \\ &\overset{b_q(f_1,f_1)=2q(f_1)}{=} f_1 - e = f_2 \end{aligned}$$

gilt. Folglich erfüllt s_e bereits die Bedingung $s_e|_{F_1} = \varphi$.

2. Fall $q(f_1 + f_2) \neq 0$. Somit haben wir die Spiegelung an $e := f_1 + f_2$ zur Verfügung. Analog zum ersten Fall rechnen wir nach, dass $s_e(f_1) = -f_2$ und $s_{f_2}(-f_2) = f_2$ ist. Ergo ist $s_{f_2} \circ s_e$ die gesuchte Fortsetzung.

Sei nun $\dim F_1 = m > 1$, $F_1 = Ae_1 \perp \ldots \perp Ae_m$ (vgl. (1.26)). Nach Induktionsvoraussetzung gibt es ein $\Psi \in O(E,q)$ mit $\Psi(e_i) = \varphi(e_i)$ für $1 \leqslant i \leqslant m-1$. Die Isometrie $\Psi^{-1} \circ \varphi$ lässt $e_1, \ldots, e_{m-1}$ fest und überführt den dazu orthogonalen Vektor e_m in einen ebenfalls zu $e_1, \ldots, e_{m-1}$ orthogonalen Vektor f_m über. Dem Induktionsanfang zufolge gibt es ein $\Gamma \in O(E,q)$, mit $\Gamma(e_m) = f_m$ welches $e_1, \ldots, e_{m-1}$ fest lässt. (Γ ist von der Form $\Gamma = s_{e_m - f_m}$ oder $\Gamma = s_{f_m} \circ s_{e_m + f_m}$.) In beiden Fällen leistet $\Phi := \Psi \circ \Gamma$ das Gewünschte. ■

(1.37) Folgerung:
Ist (E,q) ein regulärer quadratischer Raum über einem Körper A der Charakteristik ungleich 2, so lässt sich jedes Element aus $O(E,q)$ als Produkt von höchstens $2 \dim E$ Spiegelungen schreiben. Somit gilt $S(E,q) = O(E,q)$.

Beweis: Nach Satz (1.26) ist $(E,q) \simeq (E_1, q_1) \perp \ldots \perp (E_n, q_n)$, wobei $n = \dim E$ und $\dim E_i = 1$ für $1 \leqslant i \leqslant n$. Wir wenden nun Satz (1.36) mit $F_1 = F_2 = E$ auf E an. Dem Beweis dieses Satzes folgend können wir jede Isometrie in ein Produkt von höchstens $2n$ Spiegelungen zerlegen. ■

Äquivalent zum Satz (1.36) ist der sogenannte Wittsche Kürzungssatz.

(1.38) Satz (Kürzungssatz von Witt):
Sei A ein Körper der Charakteristik $\neq 2$, F, G_1, G_2 quadratische Räume über A und F regulär. Gilt $F \perp G_1 \simeq F \perp G_2$ so ist bereits $G_1 \simeq G_2$.

Beweis: Sei $\psi : F \perp G_1 \to F \perp G_2$ eine bijektive Isometrie und $\varphi := \psi|_F$. Wir definieren $E := F \perp G_2$ und fassen φ als eine Isometrie von F nach E auf. Nach dem Fortsetzungssatz (1.36) gibt es ein $g \in O(E,q)$ mit $g|_F = \varphi$. Es gilt

$$E = F \perp G_2 = \psi(F \perp G_1) = \psi(F) \perp \psi(G_1) = \varphi(F) \perp \psi(G_1).$$

Da F regulär ist, ist auch $\varphi(F)$ regulär und wir haben

$$\psi(G_1) = \varphi(F)^\perp = g(F)^\perp = g(F^\perp) = g(G_2).$$

Das heißt $g^{-1} \circ \psi : G_1 \to G_2$ ist die gesuchte bijektive Isometrie. ■

Um die **Äquivalenz** von (1.36) und (1.38) zu beweisen, müssen wir noch zeigen, wie aus (1.38) der Satz (1.36) folgt.
Gelte also (1.38) und die Situation von (1.36) liege vor. Sei o.B.d.A. $F_1 \simeq F_2$ (falls nicht, so setzt man $F_2 := \varphi(F_1)$); dann ist

$$E = F_1 \perp F_1^\perp = F_2 \perp F_2^\perp \simeq F_1 \perp F_2^\perp.$$

Nach (1.38) gibt es eine bijektive Isometrie $\varphi' : F_1^\perp \to F_2^\perp$ und $\Phi := \varphi \perp \varphi'$ ist eine Fortsetzung von φ.

(1.39) Beispiel:
Satz (1.38) ist für bilineare Räume im Fall $\operatorname{char} A = 2$ *falsch: Sei* $A = \mathbb{F}_2$, $E = A \oplus A \oplus A$ *und* $b(x,y) = x_1y_1 + x_2y_2 + x_3y_3$. *Weiter seien* $F_1 := \langle (1 \;\; 0 \;\; 0) \rangle_A$, $F_2 := \langle (1 \;\; 1 \;\; 1) \rangle_A$. *Es ist leicht zu sehen, dass* $(F_1, b) \simeq (F_2, b)$ *ist. Da die* F_i *regulär sind* ($\det(F_i) = 1$) *ist* $E = F_1 \perp F_1^\perp = F_2 \perp F_2^\perp$. *Es ist aber* $F_1^\perp = \langle (0 \;\; 1 \;\; 0), (0 \;\; 0 \;\; 1) \rangle_A = \left\langle \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right\rangle$ *und* $F_2^\perp = \langle (1 \;\; 1 \;\; 0), (0 \;\; 1 \;\; 1) \rangle_A = \left\langle \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right\rangle$, *also ist* $b(x,x) = 0$ *für alle* $x \in F_2^\perp$, *i.e.* $F_1^\perp \neq F_2^\perp$. ■

(1.40) Beispiel:
Auch auf die Regularität von F_1 *in (1.36) darf nicht (völlig, vgl. (1.41)) verzichtet werden. Sei* $(E,q) = [1,-1,0]$, A *ein beliebiger Körper der Charakteristik* $\neq 2$, $F_1 := \langle e_1 + e_2 \rangle_A$, $F_2 := \langle e_3 \rangle$. *Die Abbildung* $\varphi : F_1 \to F_2$; $e_1 + e_2 \mapsto e_3$ *ist wegen* $q(e_1 + e_2) = q(e_3) = 0$ *sicherlich eine Isometrie, nur liegt* e_3 *im Radikal von* E *und* $e_1 + e_2$ *nicht (z.B. ist* $b_q(e_1, e_1 + e_2) = 2 \neq 0$*). Somit lässt sich die Abbildung nicht zu einem Element aus* $O(E,q)$ *fortsetzen.* ■

Wie schon zu Beginn dieses Kapitels angedeutet, wollen wir den Satz (1.36) noch auf den Fall, dass der Körper Charakteristik 2 hat, verallgemeinern. Hierzu werden wir zunächst den Satz formulieren und ihn anschließend mit der Hilfe dreier Lemmata beweisen. Hierbei werden wir uns nur noch auf [Neb06] berufen, da die Ausführungen in [Kne02] für unsere Zwecke unnötig allgemein formuliert sind.

(1.41) Satz (Satz von Witt):
Sei (E,q) *ein quadratischer Vektorraum über dem Körper* A ($\operatorname{char} A$ *beliebig). Seien* F_1, $F_2 \leqslant E$ *scharf primitiv (i.e.* $b_{F_i}(E) = F_i^*$, F_i *endlichdimensional für* $i = 1,2$*) und* $\varphi : F_1 \to F_2$ *eine bijektive Isometrie. Dann gibt es ein* $g \in O(E,q)$ *mit* $g|_{F_1} = \varphi$. ■

(1.42) Lemma:
Sei E *ein endlichdimensionaler Vektorraum über einem Körper* A *mit mehr als zwei Elementen (i.e.* $|A| \geqslant 3$*). Seien weiter* H_1, $H_2 \leqslant E$ *zwei Hyperebenen (i.e.* $\operatorname{codim} H_i = 1$*) in* E. *Dann gilt*

$$\langle E \setminus (H_1 \cup H_2) \rangle_A = E.$$

Beweis: Ist E eindimensional, so ist klar, dass $\langle E \setminus \{0\}\rangle_A = E$ ist. Sei also $\dim E \geqslant 2$. Sei ohne Einschränkung $H_1 \neq H_2$ (sonst wähle für H_2 eine Basis und ersetze einen dieser Vektoren durch einen, der nicht in H_1 ist). Wir wählen eine Basis $\underline{e'} = \{e_3, \dots, e_n\}$ von $H_1 \cap H_2$ und ergänzen diese einmal um e_1 zu einer Basis von H_1 und einmal um e_2 zu einer Basis von H_2. Da H_1 und H_2 verschieden sind, ist $\{e_1, e_2\}$ linear unabhängig und $\underline{e} := \underline{e'} \cup \{e_1, e_2\}$ ist eine Basis von E. Nun gilt es, diese Basis von E so abzuwandeln, dass nur Vektoren aus $E \setminus (H_1 \cup H_2)$ darin vorkommen. Dazu bemerken wir, dass nach Konstruktion $H_1 \cup H_2 = \left\{\sum a_i e_i \mid a_1 a_2 = 0,\ e_i \in \underline{e},\ a_i \in A\right\}$ gilt. Dies bedeutet, dass jeder Vektor in $E \setminus (H_1 \cup H_2)$ sowohl e_1 als auch e_2 in seiner Zerlegung in $\underline{e}$ enthalten muss. Da A nach Voraussetzung mindestens drei Elemente hat, ist die Matrix $\begin{pmatrix} 1 & 1 \\ 1 & a \end{pmatrix}$ mit $a \in A \setminus \{0, 1\}$invertierbar. Nun haben wir alles, was wir zur Konstruktion einer Basis mit Vektoren aus $E \setminus (H_1 \cup H_2)$ benötigen, zusammen, und erhalten, dass

$$\{e_1 + e_2, e_1 + ae_2, e_1 + e_2 + e_3, \dots, e_1 + e_2 + e_n\} \subseteq E \setminus (H_1 \cup H_2)$$

eine Basis von E ist. ■

Im Folgenden sei mit b stets b_q gemeint.

(1.43) Lemma:
Sei (E, q) ein quadratischer Vektorraum über A und seien $F, G, H \leqslant E$ mit

$$b_F(H) = F^*, \tag{1.43.1}$$
$$b_G(H) = G^*, \tag{1.43.2}$$

$\varphi : F \to G$ eine bijektive Isometrie mit

$$\varphi(x) - x \in H \tag{1.43.3}$$

für alle $x \in F$. Weiter gelte entweder

$$A \neq \mathbb{F}_2 \text{ und } q(H) \neq \{0\} \tag{1.43.4}$$
oder
$$A = \mathbb{F}_2 \text{ und } q(H^\perp) \neq \{0\}. \tag{1.43.5}$$

Dann gibt es $l \in \mathbb{N}$, $h_1, \dots, h_l \in H$, $q(h_i) \neq 0$ für $i = 1, \dots, l$ so, dass

$$\varphi = s_{h_1} \dots s_{h_l}|_F$$

ist.

Wir bemerken, dass stets $s_h \in O(E, q)$ für alle $h \in H$ mit $q(h) \neq 0$ gilt. Insbesondere ist stets $s_h(x) - x \in H$ weshalb die Voraussetzung (1.43.3) notwendig ist.

Beweis: Wir zeigen die Aussage durch Induktion über $r := \dim F = \dim G$.

$r = 1$: Sei $F = \langle f \rangle$, $g := \varphi(f)$. Dann ist $G = \langle g \rangle$ und wegen (1.43.3) gibt es ein $h \in H$ mit $g = f + h$. Es ist $q(g) = q(f)$, also gilt einerseits

$$\begin{aligned} q(h) &= q(g-f) = q(g) + q(f) - b(g,f) = 2q(f) - b(g,f) \\ &= b(f,f) - b(g,f) = b(f-g,f) = -b(h,f) \end{aligned}$$

und andererseits

$$\begin{aligned} q(h) &= q(g-f) = q(g) + q(f) - b(g,f) = 2q(g) - b(g,f) \\ &= b(g,g) - b(g,f) = b(g,g-f) = b(h,g). \end{aligned}$$

Nun haben wir zwei Fälle zu unterscheiden

(i) Ist $q(h) \neq 0$, so ist $s_h(f) = f - \frac{b(h,f)}{q(h)}h = f + h = g$ und s_h setzt φ fort.

(ii) Ist $q(h) = 0$, so ist auch $b(g,h) = b(f,h) = 0$. Wir setzen $H_1 := \{x \in H \mid b(f,x) = 0\} \leqslant H$ und $H_2 := \{x \in H \mid b(g,x) = 0\} \leqslant H$. Wegen (1.43.1) und (1.43.2) ist $\dim(H/H_i) = 1$ für $i = 1,2$. Die Idee ist nun eine Spiegelung s_e mit $e \in H$ zu suchen, so dass sich $s_e(f)$ mit einer weiteren Spiegelung (s_d für ein $d \in H$) in g überführen lässt. Das Element d definieren wir durch $g = s_e(f) + d$. Dies bedeutet, dass

$$d = g - s_e(f) = g - f + \frac{b(f,e)}{q(e)}e = h + \frac{b(f,e)}{q(e)}e$$

ist. Damit ist $d \in H$. Auf die obige Gleichung q angewandt ergibt

$$\begin{aligned} q(d) &= q(h) + q(\frac{b(f,e)}{q(e)}e) + b(h, \frac{b(f,e)}{q(e)}e) \\ &= 0 + \frac{b(f,e)^2}{q(e)^2}q(e) + \frac{b(f,e)}{q(e)}b(g-f,e) = \frac{b(f,e)b(g,e)}{q(e)} \end{aligned}$$

d.h. $q(d) \neq 0$ falls $b(f,e) \neq 0 \neq b(g,e)$ ist. Wir müssen also e in $H \setminus (H_1 \cup H_2)$ mit $q(e) \neq 0$ suchen. Hierfür müssen wir zeigen, dass ein solches Element überhaupt existiert, i.e. wir müssen zeigen, dass $q(H \setminus (H_1 \cup H_2)) \neq \{0\}$ ist. Wurde dies gezeigt, so können wir den ersten Fall mit $s_e(f)$ statt f anwenden.
Annahme: $q(H \setminus (H_1 \cup H_2)) = \{0\}$. Dann gilt für alle $x \in H_1 \cap H_2$, $y \in H \setminus (H_1 \cup H_2)$ und $a \in A$: $ax + y \in H \setminus (H_1 \cup H_2)$ und damit

$$0 = q(ax+y) = a^2 q(x) + ab(x,y) + q(y). \tag{1.43.6}$$

Wir unterscheiden auch hier zwei Fälle:

– $|A| \geqslant 3$: Sei $a \in A \setminus \{0,1\}$. Dann hat die Matrix $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ a^2 & a & 1 \end{pmatrix}$ Rang 3 und wegen (1.43.6) gilt

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ a^2 & a & 1 \end{pmatrix} \begin{pmatrix} q(x) \\ b(x,y) \\ q(y) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

und wir erhalten

$$q(x) = b(x,y) = q(y) = 0 \tag{1.43.7}$$

für alle $x \in H_1 \cap H_2$, $y \in H \setminus (H_1 \cup H_2)$. Insbesondere gilt dies für $x = h \in H_1 \cap H_2$, d.h. $b(h, H \setminus (H_1 \cup H_2)) = \{0\}$. Da $H \setminus (H_1 \cup H_2)$ im Falle $|A| \geqslant 3$ nach (1.42) ganz H erzeugt, gilt $b(h,H) = \{0\}$, also ist $h \in H^\perp$.
Wir haben $g = f + h$ und für $x \in H$ mit $b(f,x) = 0$ (also $x \in H_1$)gilt

$$b(g,x) = b(f+h,x) = b(f,x) + b(h,x) \overset{h \in H^\perp}{=} 0.$$

Damit ist x auch in H_2, also ist $H_1 = H_2$. Wegen (1.43.7) ist $q(x) = 0$ für alle $x \in H_1 = H_1 \cap H_2$ und $q(y) = 0$ für alle $y \in H \setminus (H_1 \cup H_2) = H \setminus H_1$. Deshalb ist auch $q(z) = 0$ für alle $z \in H$ und dies widerspricht der Voraussetzung (1.43.4).

- $|A| = 2$: Hier haben wir $q(H^\perp) \neq \{0\}$ nach (1.43.5). Sei $H_i' := H_i \cap H^\perp$ $(i = 1,2)$. Dann ist $H_1' = H_2'$ (da $b(h,x) = 0$ für alle $x \in H^\perp$). Wegen (1.43.6) gilt für alle $x \in H_1 \cap H_2$, $y \in H^\perp \setminus \left(H_1' \cup H_2'\right)$: $q(x) = q(y) = 0$. Wegen $H_1' = H_2' \subseteq H_1 \cap H_2$ gilt $q(H^\perp \setminus H_1') = \{0\}$ und $q(H_1') = \{0\}$. Das ist aber ein Widerspruch zu (1.43.5).

Es ist also $q(H \setminus (H_1 \cup H_2)) \neq \{0\}$ und somit ist der Fall $r = 1$ gezeigt.

$r-1 \rightsquigarrow r$: Sei $\dim G = \dim F = r > 1$. Ist $|A| \neq 2$, so wählen wir $h_0 \in H$ mit $q(h_0) \neq 0$ (existiert wegen (1.43.4)), anderenfalls können wir $h_0 \in H$ beliebig wählen. Setzte $D := F^\perp \cap H$; dann ist wegen (1.43.1) $H\big/D \simeq F^*$ (als A-Moduln). Wir wählen $h_r \in H \setminus D$ mit $h_0 \in \langle h_r \rangle_A \oplus D$ und ergänzen $h_r + D$ zu einer Basis $(h_r + D, h_{r-1} + D, \ldots, h_1 + D)$ von $H\big/D$. Sei $(f_1, \ldots, f_r)$ die zu $(h_1, \ldots, h_r)$ duale Basis von F (existiert wegen (1.43.1)), i.e. $b(f_i, h_j) = \delta_{ij}$. Nach der Induktionsvoraussetzung gibt es ein $\sigma \in O(E,q)$ mit $\sigma(f_i) = \varphi(f_i)$ für $i = 1, \ldots, r-1$ so, dass σ ein Produkt von Spiegelungen entlang Elementen aus H ist. Insbesondere gilt $\sigma(H) = H$. Setzen wir $\tilde{\varphi} := \sigma^{-1} \circ \varphi : F \to \sigma^{-1}(G) =: G_1$, so erfüllt diese Abbildung: $\tilde{\varphi}(f_i) = \sigma^{-1}(\varphi(f_i)) = f_i$ für $i = 1, \ldots, r-1$. Also ist $G_1 = \sigma^{-1}(\varphi(F)) = \langle f_1, \ldots, f_{r-1}, \tilde{g}_r \rangle_A$ mit $\tilde{g}_r := \tilde{\varphi}(f_r)$. Setzte $\tilde{F} := \langle f_r \rangle_A$, $\tilde{G} := \langle \tilde{g}_r \rangle_A$ und fasse $\tilde{\varphi}$ als Isometrie von $\tilde{F}$ nach $\tilde{G}$ auf. Schließlich setzen wir $\tilde{H} := H \cap \langle f_1, \ldots, f_{r-1} \rangle_A^\perp = \langle h_r \rangle_A \oplus D$ und wenden den Fall $r = 1$ auf $(\tilde{F}, \tilde{G}, \tilde{H}, \tilde{\varphi})$ an. Um dies tun zu können, müssen wir verifizieren, dass dieses Quadrupel die Voraussetzungen (1.43.1)-(1.43.5) erfüllt:

- Nach der Wahl von h_r ist $b_{\tilde{F}}(\tilde{H}) = \langle b_{\tilde{F}}(h_r) \rangle_A = \tilde{F}^*$.

- $b_{\tilde{G}}(\tilde{H}) = \tilde{G}^*$, da $b_{G_1}(H) = G_1^*$. Wegen $f_1, \ldots, f_{r-1}, \tilde{g}_r \in G_1$ gibt es also ein $h \in H$ mit $b(h, f_i) = 0$ für $i = 1, \ldots, r-1$ und $b(h, \tilde{g}_r) = 1$. Damit ist $h \in \tilde{H}$ und $\langle b_{\tilde{G}}(h) \rangle = \tilde{G}^*$.

- $\tilde{h} := \tilde{\varphi}(f_r) - f_r \in \tilde{H}$, da $\varphi(f_r) - f_r \in H$ und $\tilde{\varphi}(f_r) - \sigma^{-1}(f_r) = \sigma^{-1}(\varphi(f_r) - f_r) \in H$ ist. Weiter ist σ Produkt von Spiegelungen entlang Elementen aus H, also ist

$\sigma^{-1}(x) - x \in H$ für alle $x \in E$. Da $\sigma^{-1}(\varphi(f_r)) - \varphi(f_r)$ und $\varphi(f_r) - f_r$ in H liegen, ist auch $\sigma^{-1}(\varphi(f_r)) - f_r \in H$. Es gilt für alle $1 \leqslant i \leqslant r-1$:

$$b(\tilde{h}, f_i) = b(\tilde{\varphi}(f_r), f_i) - b(f_r, f_i) = b(\tilde{\varphi}(f_r), \tilde{\varphi}(f_i)) - b(f_r, f_i) = 0.$$

Somit ist $\tilde{h} \in H \cap \langle f_1, \ldots, f_{r-1}\rangle_A^\perp = \tilde{H}$.

– Ist $|A| \neq 2$ so gilt (1.43.4), da h_0 in $\tilde{H}(= \langle h_r\rangle_A \oplus D)$ liegt. Die Bedingung (1.43.5) gilt im Falle $|A| = 2$ wegen $H^\perp \subseteq \tilde{H}^\perp$.

Die Voraussetzungen gelten, also wenden wir den Fall $r = 1$ an und erhalten:
Es gibt ein $\tilde{\sigma} \in O(E,q)$ mit $\tilde{\sigma}(f_r) = \tilde{\varphi}(f_r)$. Weiter ist $\tilde{\sigma}$ Produkt von Spiegelungen an $\tilde{H}$ und somit gilt $\tilde{\sigma}(f_i) = f_i$ für alle $i = 1, \ldots, r-1$ und $\sigma \circ \tilde{\sigma}$ setzt φ fort. ■

Als nächstes werden wir zeigen, dass die Voraussetzungen (1.43.4) bzw. (1.43.5) überflüssig sind und die Aussage aus (1.43) auch ohne sie gilt. Da allerdings nichts umsonst ist, müssen wir uns den Verzicht dieser Voraussetzungen damit erkaufen, dass die Fortsetzung nicht mehr als Produkt von Spiegelungen darstellbar ist.

(1.44) Lemma:
Sei (E,q) ein quadratischer Vektorraum über A und seien $F, G, H \leqslant E$ mit $b_F(H) = F^*$, $b_G(H) = G^*$. Weiter sei $\varphi : F \to G$ eine bijektive Isometrie mit $\varphi(x) - x \in H$ für alle $x \in F$. Dann gibt es $\sigma \in O(E,q)$ mit $\sigma|_F = \varphi$.

Beweis: Wir wollen das Lemma (1.43) anwenden und müssen daher dafür sorgen, dass neben (1.43.1) - (1.43.3) auch die Bedingung (1.43.4) bzw. (1.43.5) gilt. Hierfür sei $\langle e, f\rangle_A = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$ die hyperbolische Ebene über A. Wir betrachten $(E', q') := (E,q) \perp \langle e, f\rangle_A$, $F' := F \perp \langle e\rangle_A$, $G' := G \perp \langle e\rangle_A$, $H' := H \perp \langle e + f\rangle_A$ und $\varphi' := \varphi \perp \mathrm{id}_{\langle e\rangle_A}$. Dann gilt für $(E', F', G', H', \varphi')$ (1.43.1) - (1.43.3). Zudem gilt $q'(H') \neq \{0\}$ wegen $q'(e+f) = 1$ und sogar $q'(H'^\perp) \neq \{0\}$, falls $\mathrm{char}\, A = 2$, da dann $e + f \in H'^\perp$ ist. Nach (1.43) gibt es nun ein $\sigma' \in O(E', q')$ mit $\sigma'|_{F'} = \varphi'$, wobei σ' Produkt von Spiegelungen entlang Elementen in H' ist. Wegen $b(e-f, H') = \{0\}$ ist $\sigma'(e-f) = e - f$. Außerdem ist $\sigma'(e) = \varphi'(e) = e$, $\langle e - f, e\rangle_A = \langle e, f\rangle_A$, woraus $\sigma'|_{\langle e,f\rangle_A} = \mathrm{id}|_{\langle e,f\rangle_A}$ folgt. Weiterhin folgt $\sigma'(\langle e, f\rangle_A^\perp) = \langle e, f\rangle_A^\perp = E$. Somit liefert $\sigma := \sigma'|_E \in O(E,q)$ eine Fortsetzung von φ. ■

Nun sind wir soweit, die Lemmata zum Beweis von (1.41) zusammenzusetzen.

Beweis (von Satz (1.41)): Wir wenden (1.44) mit $H := E$, $F := F_1$ und $G := F_2$ an. ■

Schließlich wollen wir, analog zum Satz (1.36), aus (1.41) einige Folgerungen ziehen.

(1.45) Folgerung (vgl. (1.37)):
Ist E ein regulärer oder halbregulärer endlich-dimensionaler quadratischer Raum über einem Körper A, so lässt sich jeder Automorphismus $\sigma \in O(E)$ als Produkt von Spiegelungen schreiben, außer wenn A der Primkörper $\mathbb{F}_2$ der Charakteristik 2 und $E = E_1 \perp E_2$ mit $E_1 \simeq E_2 \simeq \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ ist.

Beweis: Für Körper der Charakteristik $\neq 2$ wurde dies bereits in (1.37) gezeigt. Für Körper ungleich $\mathbb{F}_2$ können wir dem Beweis von (1.37) folgen und dabei Satz (1.41) zusammen mit dem Beweis von (1.43) benutzen, da die Bedingung (1.43.3) in diesem Fall wegen $H = E$ stets gilt.

Bevor wir uns dem vollständigen Beweis zuwenden, wollen wir zunächst zeigen, dass es in dem oben genannten Ausnahmefall tatsächlich eine Isometrie gibt, die sich nicht als Produkt von Spiegelungen schreiben lässt:
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 E_2 liegt, jede Spiegelung s_e also E_1 und E_2 jeweils in sich selbst überführen, während es natürlich Automorphismen gibt, die E_1 und E_2 vertauschen.

Um die Folgerung auch im Fall $A = \mathbb{F}_2$ zu zeigen, wollen wir zunächst annehmen, dass $\dim E > 4$ und E regulär ist. Gibt es einen Vektor $e \in E$ mit $q(e) \neq 0$, der unter σ fix bleibt, so erhalten wir die Behauptung indem wir E als direkte (nicht notwendig orthogonale) Summe $E = Ae \oplus F$ schreiben und (1.43) auf $\varphi = \sigma|_F$, $G = \varphi(F)$ und $H = e^\perp$ anwenden; wegen $e \in H^\perp$ ist nämlich (1.43.5) erfüllt und die Fortsetzung, die wir erhalten, lässt e fest, ist also gerade σ. Im allgemeinen Fall wählen wir einen beliebigen Vektor $e \in E$ mit $q(e) \neq 0$, suchen ein Produkt ψ von Spiegelungen mit $\psi(e) = \sigma(e)$ und wenden die obige Überlegung auf $\psi^{-1} \circ \sigma$ an. Ein solches ψ erhalten wir aus (1.43), angewandt auf $F = Ae$ und $G = A\sigma(e)$. Neben F und G verlangt Lemma (1.43) auch noch einen Unterraum $H \subseteq E$ mit $H \not\subseteq e^\perp$, $H \not\subseteq \sigma(e)^\perp$, $b(e,H) = b(\sigma(e),H) = A$, $\sigma(e) - e \in H$ und $q(H^\perp) \neq 0$. Ein solches H erhalten wie folgt: Wir wählen $H = h^\perp$ mit $q(h) \neq 0$. Damit ist schon mal, wegen $h \in H^\perp$, die letzte Bedingung an H erfüllt. Die anderen Bedingungen übersetzen sich zu $h \in (\sigma(e) - e)^\perp$, $h \neq e$ und $h \neq \sigma(e)$. Nun hat E nach Voraussetzung mindestens die Dimension 6, und somit hat jede Hyperebene wie z.B. $(\sigma(e) - e)^\perp$, wegen (1.33), mindestens zwei Vektoren h mit $q(h) \neq 0$, so dass die übrigen Voraussetzungen auch erfüllt werden können.

Nun wollen wir den Beweis auf alle regulären quadratischen Räume über $\mathbb{F}_2$ ausweiten. Wie wir in (1.60) sehen werden, gibt es insgesamt vier nichtisomorphe reguläre quadratische Räume der Dimension 2 und 4 über $\mathbb{F}_2$. Der Raum $E_4^+(\mathbb{F}_2)$ (vgl. (1.60)) ist, wie wir mit (1.59) sehen können, gerade die oben genannte Ausnahme. Da es keine Isometrie gibt, die in $E_4^-(\mathbb{F}_2)$ die Teilräume $\mathbb{H}$ und $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ miteinander vertauscht, genügt es die zweidimensionalen Räume und deren Isometrien zu betrachten. Ist $\langle x,y\rangle_{\mathbb{F}_2} = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$, so ist die einzige Isometrie die nicht die Identität ist jene, die x und y vertauscht und diese kann durch die Spiegelung an $x+y$ ausgedrückt werden. Ist $\langle x,y\rangle_{\mathbb{F}_2} = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$, so gibt es insgesamt sechs Isometrien: Ist $\sigma \in O_2^-(\mathbb{F}_2)$ (vgl. (1.61)(b)), so ist

$$(\sigma(x),\sigma(y)) \in \{(x,y),(y,x),(x+y,y),(x+y,x),(x,x+y),(y,x+y)\}$$

und jedes σ lässt sich als Produkt von höchstens zwei Spiegelungen entlang x, y oder $x+y$ schreiben.

Sei E nun ein halbregulärer Raum über $\mathbb{F}_2$. Nach (1.26) lässt sich E als orthogonale Summe $F \perp Ay$ mit regulärem F schreiben. Wir wenden (1.43) auf $\psi = \sigma|_F$, $G = \psi(F)$ und $H = E$ an (geht, da $y \in E^\perp$ liegt und unter der quadratischen Form nicht verschwindet) und erhalten ein Produkt φ von Spiegelungen, welches auf F mit σ übereinstimmt. Damit ist $\varphi^{-1} \circ \sigma$ auf F die Identität und führt y in ay mit $a^2 = 1$, also $a = 1$ über. Somit ist $\varphi = \sigma$. ■

(1.46) Folgerung (vgl. (1.38)):
Der Kürzungssatz von Witt gilt auch für Körper der Charakteristik 2: Seien A Körper, F, G_1, G_2 quadratische Räume über A und F regulär. Dann folgt aus $F \perp G_1 \simeq F \perp G_2$, dass bereits $G_1 \simeq G_2$ ist.

Beweis: Wörtlich derselbe wie in (1.38). ■

(1.47) Folgerung:
Seien (E,q) quadratischer A-Vektorraum, F_1, $F_2 \leqslant E$ singuläre, scharf primitive Unterräume der gleichen Dimension. Dann gibt es einen Automorphismus $\sigma \in O(E,q)$ mit $\sigma F_1 = F_2$. ■

Beweis: Da die F_i singulär sind, ist jeder Isomorphismus $\varphi : F_1 \to F_2$ eine Isometrie und als solche nach (1.41) zu einem $\sigma \in O(E,q)$ fortsetzbar. ■

(1.48) Folgerung:
Sind F_1, F_2 zwei maximale singuläre, scharf primitive Unterräume von (E,q), so haben sie die selbe Dimension.

Beweis: Ist etwa $\dim F_2 \leqslant \dim F_1$, so wählen wir $F_1' \subseteq F_1$ mit $\dim F_1' = \dim F_2$. Der Unterraum F_1' ist scharf primitiv in E, also existiert $\sigma \in O(E,q)$ mit $\sigma F_1' = F_2$. Dann ist $\sigma F_1 \supseteq \sigma F_1' = F_2$. Der Unterraum σF_1 ist ebenfalls singulärer scharf primitiver Teilraum und muss, wegen der Maximalität von F_2, bereits gleich F_2 sein. Folglich ist auch die Dimension von F_1 und F_2 gleich. ■

(1.49) Definition:
Sei (E,q) ein endlich-dimensionaler quadratischer A-Vektorraum. Dann heißt die Dimension der maximal singulären, scharf primitiven Unterräume der ***Witt-Index****, in Zeichen* $\operatorname{ind}(E)$*, von E.* ■

(1.50) Beispiel:
Ist $E = \mathbb{H}(G) = (G \oplus G^*,\ q(x + x^*) = x^*(x))$, so ist $\operatorname{ind}(\mathbb{H}(G)) = \dim G$ *und G ist maximal singulärer, scharf primitiver Teilraum.* ■

(1.51) Definition:
(E,q) heißt ***anisotrop*** *wenn für alle $x \in E \setminus \{0\}$ gilt, dass $q(x) \neq 0$ ist.* ■

(1.52) Folgerung:
Ist (E,q) quadratischer A-Vektorraum mit Witt-Index n, so lässt sich (E,q) als

$$(F, q\,|_F) \perp \mathbb{H}(A^n) \tag{1.52.1}$$

schreiben, wobei $\operatorname{ind}(F, q|_F) = 0$ *ist. Diese Zerlegung heißt* ***Witt-Zerlegung*** *und ist bis auf Isometrie eindeutig bestimmt. Ist (E,q) zudem regulär oder halbregulär, so ist $(F, q|_F)$ anisotrop und wird* ***anisotroper Kern*** *genannt.*

Beweis: Sei $G \leqslant (E,q)$ maximal singulärer, scharf primitiver Teilraum. Dann gibt nach (1.33) ein $\mathbb{H}(G) \simeq H \leqslant E$ mit $G \leqslant H$ und H regulär. Somit lässt sich E als $H \perp H^\perp$ schreiben. Der Raum $H^\perp$ enthält, abgesehen von $\{0\}$, keinen scharf primitiv singulären Teilraum, weshalb $\operatorname{ind}(H^\perp) = 0$ ist. Die Folgerungen (1.47) und (1.48) liefern die geforderte Eindeutigkeit. ■

Mit dieser Folgerung wollen wir den allgemein gehaltenen Teil der theoretischen Grundlagen über quadratische Formen abschließen. In den folgenden beiden Paragraphen wollen wir uns auf den Teil der Theorie konzentrieren, der direkte Anwendung in den beiden, im 2. Kapitel vorgestellten, Algorithmen findet.

§ 1.4. Die Klassifikation der (halb-)regulären quadratischen Formen über endlichen Körpern und deren orthogonale Gruppe

Auch in diesem Paragraphen wollen wir uns wieder hauptsächlich auf [Neb06] stützen, da in [Kne02] bei der Klassifikation einige Erkenntnisse aus dem Kapitel über Clifford-Algebren verwendet wurden, welche wir hier nicht vertiefen wollen. Eine etwas weniger ausführliche Klassifikation ist auch in [Asc00, Kapitel 7, Paragraph 20 und 21] zu finden. Was die orthogonalen Gruppen endlicher Körper angeht, lässt sich auch in [Hup67, Kapitel II, Bemerkung 10.16] etwas ausfindig machen.

In diesem Abschnitt sei A stets ein endlicher Körper, genauer sei $A := \mathbb{F}_l$ wobei $l = p^f$ eine Primzahlpotenz ist. Weiter sei (E,q) ein endlich-dimensionaler A-Vektorraum.

(1.53) Satz:
Die Isometrieklassen halbregulärer quadratischer A-Vektorräume der Dimension 1 sind durch die Vertreter von $A^\times/A^{\times 2}$ eindeutig bestimmt.

Beweis: Es sei der quadratische eindimensionale Raum $[a]$ mit $a \in A$ gegeben. Das Bild der quadratischen Form auf $[a]$ ist gleich $a(A^{\times 2}) \cup \{0\}$ und $\det [a] = 2a(A^{\times 2})$, was bedeutet, dass $[a]$ genau dann halbregulär ist, wenn $a \neq 0$ ist. Daraus ergibt sich, dass zwei halbreguläre Räume $[a]$ und $[b]$ genau dann isometrisch sind, wenn a und b die selbe Quadratklasse in $A^\times/A^{\times 2}$ vertreten. Es gilt noch ein Repräsentantensystem der Vertreter der Quadratklassen zu bestimmen.

Es ist $A^\times \simeq C_{l-1}$, woraus man $\left[A^\times : A^{\times 2}\right] = \begin{cases} 2 & \text{falls } p \neq 2, \\ 1 & \text{falls } p = 2 \end{cases}$ erhält. Wir können also für Körper der Charakteristik 2 als Vertreter der einzigen Quadratklasse die 1 wählen und für Körper der Charakteristik ungleich 2 als Vertreter 1 und ε wählen, wenn sich $A^\times$ als $(A^{\times 2}) \dot\cup \varepsilon(A^{\times 2})$ schreiben lässt. ■

(1.54) Satz:
Ist die Dimension von E gleich 2 und E regulär, so ist der Raum eine hyperbolische Ebene oder anisotrop. In beiden Fällen ist $q(E) = A$.

Beweis: (i) Sei (E,q) nicht anisotrop, i.e. es gibt ein $0 \neq x \in E$ mit $q(x) = 0$. Sei F der von x erzeugte Teilraum. Weil E endlich-dimensionaler Vektorraum ist, ist F primitiv. Da E regulär ist, ist F ein scharf primitiver singulärer Teilraum von E (vgl. (1.29)). Nach (1.33) ist F in einem zum hyperbolischen Modul $\mathbb{H}(F)$ isomorphen Teilmodul $H \leqslant E$ enthalten. Da $\dim H = 2$ ist, gilt $E = H$, und somit ist $E \simeq \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$. Der Raum E ist hyperbolisch und enthält somit zwei linear unabhängige Vektoren (u,v) für die $q(u) = q(v) = 0$ und $b_q(u,v) = 1$ gelten; ein solches Paar von Vektoren wird auch **hyperbolisches Paar** genannt. Ist nun $a \in A$ beliebig, so ist

$$q(au+v) = a^2 q(u) + q(v) + a b_q(u,v) = a,$$

also ist $q(E) = A$.

(ii) Sei (E,q) nun anisotrop. Ist $\operatorname{char} A = 2$, so ist klar, dass $q(E) = A$ ist. Sei also $\operatorname{char} A \neq 2$. Nach (1.26) gibt es $e_1, e_2 \in E$ mit $(E,q) = Ae_1 \perp Ae_2 = [t_1, t_2]$, wobei $t_i \in A^\times$ sind (anderenfalls wäre E nicht regulär), es gilt also $q(a_1e_1 + a_2e_2) = a_1^2 t_1 + a_2^2 t_2$. Wir wollen zeigen , das $q(E) = A$ ist. Sei dafür $a \in A$ beliebig. Wir betrachten die Mengen $M_1 := \left\{a_1^2 t_1 \mid a_1 \in A\right\}$ und $M_2 := \left\{a - a_2^2 t_2 \mid a_2 \in A\right\}$. Wir haben nun die Frage, ob $a \in q(E)$ ist äquivalent umgeformt zu: Ist $M_1 \cap M_2 \neq \{0\}$? Ein einfaches Abzählen liefert jetzt: $|M_1| = \left|\left\{a_1^2 t_1 \mid a_1 \in A^\times\right\}\right| + |\{0\}| = \frac{l-1}{2} + 1 = \frac{l+1}{2}$. Völlig analog dazu ist $|M_2| = \frac{l+1}{2}$. Es ist zum einen

$$|M_1 \cup M_2| \leqslant |A| = l.$$

Andererseits ist aber auch

$$|M_1 \cup M_2| = |M_1| + |M_2| - |M_1 \cap M_2| = l + 1 - |M_1 \cap M_2|,$$

woraus sich ergibt, dass $M_1 \cap M_2$ nicht leer ist. Zusammengefasst ist $q(E) = A$. ■

Wir wollen uns nun einmal einen zweidimensionalen regulären anisotropen Raum etwas ausführlicher ansehen.

(1.55) Satz:
*Der Raum $\mathbb{F}_{l^2}$ über dem Körper $\mathbb{F}_l$ mit der quadratischen Form $N : \mathbb{F}_{l^2} \to \mathbb{F}_l$; $x \mapsto x \cdot x^l$, **Normform** genannt, ist regulär anisotrop. Des weiteren nimmt die quadratische Form jeden Wert in $\mathbb{F}_l$ an.*

Beweis: Es ist $E = \mathbb{F}_{l^2} = \mathbb{F}_q \cdot 1 \oplus \mathbb{F}_q \cdot \alpha$, wobei $\mathbb{F}_{l^2} = \mathbb{F}_l[\alpha]$ ist. Da $\operatorname{Gal}\left(\mathbb{F}_{l^2}/\mathbb{F}_l\right) = \left\langle x \mapsto x^l \right\rangle$ ist, gilt für alle $a \in \mathbb{F}_l$: $N(ax) = ax(ax)^l = axax^l = a^2 N(x)$ für alle $x \in \mathbb{F}_{l^2}$. Weiter seit

$b_N : \mathbb{F}_{l^2} \times \mathbb{F}_{l^2} \to \mathbb{F}_l\,;\ (x,y) \mapsto N(x+y) - N(x) - N(y)$. Wir rechnen nach, dass

$$\begin{aligned} b_N(x,y) &= N(x+y) - N(x) - N(y) = (x+y)(x+y)^l - x^{l+1} - y^{l+1} \\ &= xy^l + yx^l \\ &\overset{x^{l^2}=x \forall x \in \mathbb{F}_{l^2}}{=} xy^l + (xy^l)^l \\ &= \mathrm{Spur}_{\mathbb{F}_{l^2}/\mathbb{F}_l}(xy^l) \end{aligned}$$

gilt, also ist b_N eine symmetrische Bilinearform, da die Spur der Körpererweiterung $\mathbb{F}_{l^2}/\mathbb{F}_l$ eine ist. Damit ist N als quadratische Form bestätigt.

Es bleibt noch zu zeigen, dass $(\mathbb{F}_{l^2}, N)$ regulär und anisotrop ist.

Ist $x \in \mathbb{F}_{l^2}$, so folgt aus $N(x) = x^{l+1} = 0$, dass $x = 0$ ist. Wir zeigen, dass $N : \mathbb{F}_{l^2}^\times \simeq C_{l^2-1} \to \mathbb{F}_l^\times \simeq C_{l-1}$ ein surjektiver Gruppenhomomorphismus ist. Es ist $C_{l^2-1} = \langle\beta\rangle$; die Ordnung von β^{l+1} ist $\frac{l^2-1}{l+1} = l-1$, also ist $C_{l-1} = \left\langle N(\beta) = \beta^{l+1} \right\rangle$. Insgesamt ist $(\mathbb{F}_{l^2}, N)$ also anisotrop und N nimmt alle Werte in $\mathbb{F}_l$ an.

Es ist $(b_N)_{\mathbb{F}_{l^2}} : \mathbb{F}_{l^2} \to \mathrm{Hom}_{\mathbb{F}_l}(\mathbb{F}_{l^2}, \mathbb{F}_l)\ ;\ x \mapsto (y \mapsto b_N(x,y) = \mathrm{Spur}_{\mathbb{F}_{l^2}/\mathbb{F}_l}(xy^l))$. Wegen $\dim_{\mathbb{F}_l}(\mathrm{Hom}_{\mathbb{F}_l}(\mathbb{F}_{l^2}, \mathbb{F}_l)) = \dim_{\mathbb{F}_l}(\mathbb{F}_{l^2}) = 2$ genügt es zu zeigen, dass $(b_N)_{\mathbb{F}_{l^2}}$ injektiv ist. Es gilt $\mathrm{Kern}((b_N)_{\mathbb{F}_{l^2}}) = \left\{x \in \mathbb{F}_{l^2} \mid xy^l + yx^l = 0 \text{ für alle } y \in \mathbb{F}_{l^2}\right\}$. Angenommen es gibt ein $0 \neq x \in \mathrm{Kern}((b_N)_{\mathbb{F}_{l^2}})$. Dann ist das Polynom $p_x(Y) := Y^l + x^{l-1}Y \in \mathbb{F}_{l^2}[Y]$ nicht das Nullpolynom. Da x im Kern von $(b_N)_{\mathbb{F}_{l^2}}$ ist, gilt für alle $y \in \mathbb{F}_{l^2}$: $p_x(y) = 0$. Der Grad von p_x ist l, es hat aber l^2 Nullstellen, ein Widerspruch. ■

Der folgende Satz gibt Auskunft darüber, warum wir $(\mathbb{F}_{l^2}, N)$ betrachtet haben.

(1.56) Satz:
Ist (E,q) ein anisotroper regulärer quadratischer $\mathbb{F}_l$-Vektorraum der Dimension 2, so ist

$$(E,q) \simeq (\mathbb{F}_{l^2}, N).$$

Beweis: Wir wählen eine Basis (e_1, e_2) von E mit $q(e_1) = 1$ (geht wegen (1.54)). Somit ist $(E,q) = \begin{bmatrix} 1 & c \\ & a \end{bmatrix}$, also $q(x_1e_1 + x_2e_2) = x_1^2 + cx_1x_2 + ax_2^2$ für alle $x_1, x_2 \in \mathbb{F}_l$. Da (E,q) anisotrop ist, hat das Polynom $f(x) := q(xe_1 + e_2) = x^2 + cx + a \in \mathbb{F}_l[x]$ keine Nullstellen in $\mathbb{F}_l$; $f(x)$ ist also irreduzibel in $\mathbb{F}_l[x]$. Ist $\alpha \in F_{l^2}$ mit $f(\alpha) = 0$, so ist $q(x_1e_1 + x_2e_2) = N(x_1 - x_2\alpha)$ und $e_1 \mapsto 1$, $e_2 \mapsto -\alpha$ die gesuchte Isometrie von $(E,q) \to (\mathbb{F}_{l^2}, N)$. ■

Wir haben nun die Fälle $\dim(E) \leqslant 2$ abgehandelt. Der nachfolgende Satz hilft beim Fall $\dim(E) \geqslant 3$.

(1.57) Satz:
Ein quadratischer A-Vektorraum E, dessen Dimension größer als 2 ist, kann nicht anisotrop sein. Es gibt also ein $0 \neq x \in E$ mit $q(x) = 0$.

Beweis: Nach (1.26) ist $(E,q) = (E_1,q_1) \perp (E_2,q_2) \perp \ldots$ mit $\dim(E_i) = 1$ oder 2 und E_i regulär oder halbregulär.

Ist $\operatorname{char} A \neq 2$, so können die E_i eindimensional gewählt werden und $(E,q) = [a_1,a_2,a_3\ldots]$ (vgl. Definition (1.20)). Ist $a_1a_2a_3 = 0$, so ist bereits $q(e_i) = 0$ für ein $i \in \{1,2,3\}$. Sei also $a_1a_2a_3 \neq 0$. Nach (1.54) gibt es in $E_1 \perp E_2 = [a_1,a_2]$ ein $x = (x_1,x_2) \neq 0$ mit $q(x) = a_1x_1^2 + a_2x_x^2 = -a_3$ und damit ist $q((x_1,x_2,1,0\ldots0)) = 0$.

Ist $\operatorname{char} A = 2$, so ist $\dim E_1 = 1$ und $(E_1, q|_{E_1})$ ist halbregulär oder $\dim E_1 = 2$ und E_1 ist regulär (sonst gibt es trivialerweise ein $0 \neq x \in E$ mit $q(x) = 0$). In beiden Fällen ist $q(E_1) = \mathbb{F}_l$, insbesondere gibt es $0 \neq x_1 \in E_1$ und $0 \neq E_2$ mit $q(x_1) = q(x_2) \neq 0$; dann ist $q(x_1 + x_2) = 0$. ■

(1.58) Folgerung:
Ist (E,q) quadratischer $\mathbb{F}_l$ Vektorraum, so gibt es eine bis auf Isometrie eindeutige Zerlegung

$$(E,q) = (E_1,q_1) \perp (E_2,q_2) \perp (E_3,q_3)$$

wobei $\dim E_1 \leqslant 2$, E_1 regulär oder halbregulär und anisotrop ist (der anisotrope Kern, vgl. (1.52)), E_2 orthogonale Summe von $\begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$ und $q_3(E_3) = \{0\}$ ist.

Beweis: Ist die Dimension von E kleiner oder gleich 2, so ist die Aussage klar. Sei also $\dim(E) \geqslant 3$. Wegen (1.57) gibt es ein $0 \neq x \in E$ mit $q(x) = 0$. Ist $b_q(x,y) = 0$ für alle $y \in E$, so kann man x zu einer Basis $(x,e_1,\ldots,e_{n-1})$ von E ergänzen, so dass $(E,q) = \langle e_1,\ldots,e_{n-1}\rangle_A \perp \langle x\rangle_A$ gilt, und $\langle x\rangle_A$ wird zu E_3 hinzu geschlagen. Gibt es andererseits ein $y \in E$ mit $b_q(x,y) \neq 0$, so ist $\langle x,y\rangle_A$ regulär und isometrisch zu $\mathbb{H}$. Folglich spaltet $\langle x,y\rangle_A$ orthogonal ab. ■

(1.59) Folgerung (vgl. [Asc00, Kapitel 7, (21.2)(3)]):
Die Räume $\perp^{2m}(\mathbb{F}_{l^2},N)$ und $\perp^{2m}\mathbb{H}(\mathbb{F}_l)$ sind isometrisch ($m \in \mathbb{N}$).

Beweis: Sei o.E. $m = 1$. Da $(\mathbb{F}_{l^2},N) \perp (\mathbb{F}_{l^2},N)$ regulär ist, enthält er einen ein- oder zweidimensionalen singulären Teilraum G (nach (1.57) ist G mindestens eindimensional und da $(\mathbb{F}_{l^2},N) \perp (\mathbb{F}_{l^2},N)$ regulär ist, höchstens zweidimensional). Der Fall, dass G eindimensional ist kann nicht auftreten, da sonst $(\mathbb{F}_{l^2},N) \perp (\mathbb{F}_{l^2},N)$ nach (1.58), zusammen mit (1.56), isomorph zu $(\mathbb{F}_{l^2},N) \perp \mathbb{H}$ wäre. Dies aber liefert mit (1.38) bzw. (1.46) den Widerspruch $(\mathbb{F}_{l^2},N) \simeq \mathbb{H}$. Der Raum G ist also zweidimensional. Aus Dimensionsgründen gilt dann $(\mathbb{F}_{l^2},N) \perp (\mathbb{F}_{l^2},N) \simeq \mathbb{H}(G) \simeq \perp^2 \mathbb{H}(\mathbb{F}_l)$. ■

All dies zusammenfassend formulieren wir das nachstehende Korollar.

(1.60) Korollar (Klassifikation der halbregulären und regulären quadratischen A-Vektorräume):
Ist (E,q) regulär und $\dim E = 2n$, so ist

$$(E,q) \simeq \begin{cases} E_{2n}^+(\mathbb{F}_l) := \perp^n \mathbb{H} = \perp^n \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & \\ E_{2n}^-(\mathbb{F}_l) := (\mathbb{F}_{l^2},N) \perp \left(\perp^{n-1}\mathbb{H}\right) = \begin{bmatrix} 1 & c \\ & a \end{bmatrix} \perp \left(\perp^{n-1}\begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}\right), & \end{cases} \quad \text{oder}$$

wobei $x^2 + cx + a \in \mathbb{F}_l[x]$ irreduzibel ist. Da $\mathbb{H}$ einen echten singulären Teilraum hat, $(\mathbb{F}_{l^2}, N)$ jedoch nicht, liefert der Wittsche Kürzungssatz (1.46), dass die beiden Varianten nicht isometrisch sind.

Ist (E,q) halbregulär und $\dim E = 2n+1$, *so ist, im Fall* $\operatorname{char} A = 2$,

$$(E,q) \simeq E_{2n+1}(\mathbb{F}_l) := [1] \perp \left(\perp^n \mathbb{H}\right),$$

und im Fall $\operatorname{char} A \neq 2$,

$$(E,q) \simeq \begin{cases} E_{2n+1}(\mathbb{F}_l) := [1] \perp \left(\perp^n \mathbb{H}\right) & \text{oder} \\ E^{\varepsilon}_{2n+1}(\mathbb{F}_l) := [\varepsilon] \perp \left(\perp^n \mathbb{H}\right). \end{cases}$$

Hierbei ist ε wie in (1.53) gewählt. Auch hier sind die beiden Varianten nicht isometrisch, da sich die Determinanten unterscheiden. ■

Um diesen Paragraphen abzuschließen, wollen wir uns noch die orthogonalen Gruppen dieser Räume ansehen. Obgleich wir im wesentlichen vier verschiedene Räume haben, gibt es doch nur drei Arten von orthogonalen Gruppen.

(1.61) Definition & Bemerkung:
Seien die Bezeichnungen wie in (1.60). Zunächst bemerken wir, dass $O(E,q) = O(E,aq)$ für $a \in A^\times$ gilt. Weiter ist $(E_{2n+1}(\mathbb{F}_l), q) \simeq (E^{\varepsilon}_{2n+1}(\mathbb{F}_l), \varepsilon^{-1}q)$, was bedeutet, dass es in ungerader Dimension nur eine orthogonale Gruppe gibt. Es ist

(a) $O^+_{2n}(\mathbb{F}_l) := O(E^+_{2n}(\mathbb{F}_l))$,
(b) $O^-_{2n}(\mathbb{F}_l) := O(E^-_{2n}(\mathbb{F}_l))$ *und*
(c) $O_{2n+1}(\mathbb{F}_l) := O(E_{2n+1}(\mathbb{F}_l))$. ■

Als kleiner Ausblick sei hier angemerkt, dass wir uns noch mit den Gruppen $O^+_{2n}(\mathbb{F}_l)$ und $O^-_{2n}(\mathbb{F}_l)$ im 2. Kapitel beschäftigen, da wir dort einen Algorithmus angeben werden, der für einen $2n$-dimensionalen quadratischen $\mathbb{F}_l$-Vektorraum entscheidet, welcher der beiden Typen seine orthogonale Gruppe angehört.

Wir beschließen dieses Kapitel mit der Frage, ob, wenn auf einem Vektorraum eine Gruppe operiert, dieser Raum eine, mit dieser Operation verträgliche, Bilinearform oder sogar eine quadratische Form trägt. Während wir uns im folgenden Abschnitt ausschließlich mit der Frage beschäftigen, unter welchen Umständen eine solche Form existiert, werden wir uns im 2. Kapitel damit beschäftigen, wie man explizit, bei gegebenem Vektorraum mit der Operation, entscheidet ob es eine Form gibt und wenn ja, diese auch konkret berechnet.

§ 1.5. Die Brücke zur Darstellungstheorie

In diesem Abschnitt sei F ein Körper, G eine endliche Gruppe und V ein endlich-dimensionaler F-Vektorraum. Wir folgen in diesem Kapitel im wesentlichen dem Kapitel VII, §8 aus [HB82]. Weiter wird in diesem Paragraphen, gemäß eben genannter Quelle und im Ausblick auf die in [GAP05] implementierten Algorithmen aus Kapitel 2, von rechts operiert.

Zunächst wollen wir an einige Definitionen aus der Darstellungstheorie endlicher Gruppen erinnern.

(1.62) Definition:

(a) *Es sei $\rho : G \to \mathrm{Aut}_F(V)$ ein Gruppenhomomorphismus, also eine* ***Darstellung*** *von G auf V.*

(b) *Der F-Vektorraum V wird vermöge ρ zu einem FG-Modul. Es gilt*

$$vg := v\rho(g) \quad \text{für } v \in V \text{ und } g \in G.$$

(c) *Der zu V duale Modul $V^*(= \mathrm{Hom}_F(V, F))$ wird zum FG-Modul, wenn wir*

$$v(fg) := (vg^{-1})f$$

für alle $v \in V$, $f \in V^*$ und $g \in G$ setzten. ■

Obgleich erst im 2. Kapitel benötigt, bemerken wir hier:

(1.63) Bemerkung:

Ist ρ eine Matrixdarstellung von G auf V, so ist die dazu gehörige ***duale Darstellung*** *ρ^* von G auf V^* durch*

$$\rho^*(g) := \rho(g^{-1})^t \quad \text{für alle } g \in G$$

gegeben. ■

(1.64) Definition (Vgl. [Hup67, Kapitel V, §2] bzw. [HB82, Kapitel VII, §6]):

Für einen Ring R ist das Jacobson Radikal $\mathcal{J}(R)$ als der Schnitt über alle maximalen Rechtsideale von R definiert. ■

(1.65) Lemma:

Seien V und W endlich erzeugte FG-Moduln.

(a) $\mathrm{Hom}_F(V, W)$ *wird vermöge*

$$v(\alpha g) := ((vg^{-1})\alpha)g$$

für alle $v \in V$, $\alpha \in \mathrm{Hom}_F(V, W)$ und $g \in G$ zum FG-Modul. Daraus ergibt sich, dass

$$\mathrm{Hom}_{FG}(V, W) = \{\alpha \mid \alpha \in \mathrm{Hom}_F(V, W), \alpha g = \alpha \text{ für alle } g \in G\}$$

die Menge der Fixpunkte dieser Operation ist.

(b) *Die Abbildung* $\beta : V^* \otimes_F W \to \mathrm{Hom}_F(V, W)$ *die durch*

$$v((f \otimes w)\beta) := (vf)w \quad (v \in V,\ f \in V^*,\ w \in W)$$

definiert ist, ist ein FG-Modulisomorphismus.

Beweis: Direktes Nachrechnen. ■

(1.66) Lemma:
Sind V_1 *und* V_2 *endlich erzeugte FG-Moduln, so bezeichnen wir mit* $\mathcal{B}(V_1, V_2)$ *den F-Vektorraum der F-Bilinearformen auf* $V_1 \times V_2$.

(a) $\mathcal{B}(V_1, V_2)$ *wird zum FG-Modul, wenn wir*

$$(bg)(v_1, v_2) := b(v_1 g^{-1}, v_2 g^{-1})$$

für $v_i \in V_i$ $(i = 1, 2)$, $b \in \mathcal{B}(V_1, V_2)$ *und* $g \in G$ *setzten.*
(b) $V_1^* \otimes_F V_2^*$ *und* $\mathcal{B}(V_1, V_2)$ *sind vermöge der Abbildung* γ, *die durch*

$$((f_1 \otimes f_2)\gamma)(v_1, v_2) = (v_1 f_1)(v_2 f_2) \quad (v_i \in V_i,\ f_i \in V_i^*, I = 1, 2)$$

definiert ist, als FG-Moduln isomorph.

Beweis: Siehe [HB82, Kapitel VII, Lemma 8.9]. ■

(1.67) Lemma:
Seien V_1 *und* V_2 *endlich erzeugte FG-Moduln.*

(a) *Sei* $\alpha \in \mathrm{Hom}_F\left(V_2, V_1^*\right)$ *und* $b \in \mathcal{B}(V_1, V_2)$ *so, dass*

$$b(v_1, v_2) = v_1(v_2\alpha)$$

für alle $v_i \in V_i$ *gilt. Dann ist* α *genau dann ein FG-Homomorphismus, wenn* b ***G-invariant*** *ist, i.e.* $b(v_1 g, v_2 g) = b(v_1, v_2)$ *für alle* $v_i \in V_i$ *und alle* $g \in G$.
(b) *Es ist* $V_2 \simeq V_1^*$ *genau dann, wenn es eine G-invariante reguläre Bilinearform auf* $V_1 \times V_2$ *gibt.*

Beweis: (a) Die Behauptung folgt aus

$$\begin{aligned} b(v_1 g, v_2 g) - b(v_1, v_2) &= (v_1 g)(v_2 g\alpha) - (v_1 g g^{-1})(v_2\alpha) \\ &= (v_1 g)(v_2 g\alpha - v_2\alpha g). \end{aligned}$$

(b) Es ist klar, dass in (a) genau dann α ein Isomorphismus ist, wenn b regulär ist. Die Behauptung folgt nun unmittelbar aus (a). ■

(1.68) Definition:
Eine Bilinearform $b \in \mathcal{B}(V, V)$ *heißt* ***symplektisch****, wenn* $b(v, v) = 0$ *für alle* $v \in V$ *gilt.* ■

(1.69) Satz (Gow):
Sei die Charakteristik von F nicht 2 und $V \neq \{0\}$ ein unzerlegbarer FG-Modul, der selbstdual ist, i.e. $V \simeq V^*$. Dann gilt:

(a) Es gibt eine reguläre symplektische oder symmetrische G-invariante Form auf V.
(b) Wenn V absolut unzerlegbar ist, so können nicht gleichzeitig eine symmetrische und eine symplektische Form auf V existieren.

Beweis: Sei $\mathfrak{R} := \mathrm{Hom}_{FG}(V,V)$ und $\mathfrak{J} := \mathcal{J}(\mathfrak{R})$.

(a) Nach Voraussetzung existiert ein FG-Isomorphismus α von V nach V^*. Sei α^* die dazu duale Abbildung von $V^{**} = V$ nach V^*. Diese ist durch

$$w(v\alpha) = v(w\alpha^*)$$

für alle $v, w \in V$ definiert. Da Dualisieren in der Kategorie der endlich erzeugten FG-Moduln ein exakter Funktor ist, ist auch α^* ein FG-Isomorphismus (vgl. [HB82, Kapitel VII, §8, Lemma 8.3]). Setzten wir $\beta := \alpha^*\alpha^{-1}$, so ist $\beta \in \mathfrak{R}$ und

$$w(v\alpha) = v(w\beta\alpha)$$

für alle $v, w \in V$.
Für $\varepsilon = \pm 1$ seien Bilinearformen b_ε auf V definiert, indem wir

$$b_\varepsilon(v,w) := v(w\alpha) + \varepsilon w(v\alpha)$$

für alle $v, w \in V$ setzen. Nach Lemma (1.67) ist b_ε G-invariant , wobei b_1 symmetrisch und b_{-1} symplektisch ist. Wir nehmen nun an, dass b_1 und b_{-1} beide nicht regulär sind. Da

$$b_\varepsilon(v,w) = v((w + \varepsilon w\beta)\alpha)$$

ist, folgt, dass sowohl $\mathrm{id}_V - \beta$ als auch $\mathrm{id}_V + \beta$ keine Isomorphismen sind. Sie sind deshalb beide Nichteinheiten im lokalen Ring $\mathfrak{R}$ und liegen folglich in $\mathfrak{J}$. Somit liegt auch $2\,\mathrm{id}_V \in \mathfrak{J}$ und, da $\mathrm{char}\, K \neq 2$, liegt sogar id_V selbst im Jacobson Radikal. Dies ist ein Widerspruch zu (1.64). Folglich ist entweder b_1 oder b_{-1} regulär.

(b) Angenommen es existieren reguläre G-invariante Bilinearformen b_1 und b_2 auf V, wobei b_1 symmetrisch und b_2 symplektisch ist. Dann existieren F-Isomorphismen α_1 und α_2 von V nach V^* mit

$$w(v\alpha_1) = b_1(v,w) \quad \text{und} \quad w(v\alpha_2) = b_2(v,w).$$

Wegen (1.67)(a) sind α_1 und α_2 FG-Isomorphismen für die $\alpha_1^* = \alpha_1$ und $\alpha_2^* = -\alpha_2$ gilt. Setzen wir $\beta := \alpha_1\alpha_2^{-1}$ so ist $\beta \in \mathfrak{R}$. Aus $\alpha_1 = \beta\alpha_2$ folgt $\alpha_1^* = \alpha_2^*\beta^*$ und hieraus wiederum $\alpha_1 = -\alpha_2\beta^*$. Deshalb gilt

$$\alpha_1\beta^*\alpha_1^{-1} = \beta\alpha_2\beta^*\alpha_1^{-1} = -\beta\alpha_1\alpha_1^{-1} = -\beta.$$

Da V absolut unzerlegbar ist, ist $\mathfrak{R}/\mathfrak{J} \simeq F$ und $\beta = a\,\mathrm{id}_V + \gamma$ für ein $a \in F$ und ein $\gamma \in \mathfrak{J}$. Es gilt $\beta^* = a\,\mathrm{id}_{V^*} + \gamma^*$ und wegen [HB82, Kapitel VII, §8, Lemma 8.3(b)] ist $\gamma^* \in$

$\mathrm{Hom}_{FG}(V^*, V^*)$. Folglich ist auch $\alpha_1\gamma^*\alpha_1^{-1} \in \mathfrak{R}$. Da γ kein Isomorphismus ist, ist auch γ^* keiner, was $\alpha_1\gamma^*\alpha_1^{-1} \in \mathfrak{J}$ impliziert. Folglich ist

$$-a\,\mathrm{id}_V - \gamma = -\beta = \alpha_1\beta^*\alpha_1^{-1} = a\,\mathrm{id}_V + \alpha_1\gamma^*\alpha_1^{-1},$$

und somit $2a\,\mathrm{id}_V \in \mathfrak{J}$. Da $\mathrm{char}\,K \neq 2$ impliziert dies, dass $a = 0$ ist. Also ist $\beta \in \mathfrak{J}$, β folglich kein Isomorphismus und, wegen $\alpha_1 = \beta\alpha_2$, α_1 ebenfalls nicht, was einen Widerspruch zur Voraussetzung darstellt. ■

(1.70) Satz:
Ist V ein absolut irreduzibler, selbstdualer ($V \simeq V^*$) FG-Modul, so existiert bis auf skalare Vielfache genau eine reguläre G-invariante Bilinearform b auf V. Ist die Charakteristik von F nicht 2, so ist b symmetrisch oder symplektisch.

Beweis: Wir wollen den F-Vektorraum der G-invarianten Bilinearformen mit $\mathcal{B}_0(V)$ bezeichnen. Es gilt $b \in \mathcal{B}_0(V)$ genau dann, wenn

$$b(v_1, v_2) = b(v_1 g, v_2 g) = (bg^{-1})(v_1, v_2)$$

für alle $v_i \in V$ und $g \in G$.

Nach (1.65)(b) und (1.66)(b) haben wir

$$\mathrm{Hom}_F(V, V) \simeq V^* \otimes_F V \simeq V^* \otimes_F V^* \simeq \mathcal{B}(V, V) \text{ als } FG\text{-Moduln}.$$

Wegen (1.65)(a) gilt $\mathrm{Hom}_{FG}(V, V) \simeq \mathcal{B}_0(V)$. Da V absolut irreduzibel ist, ist

$$\dim_F \mathcal{B}_0(V) = \dim_F \mathrm{Hom}_{FG}(V, V) = 1.$$

Die Existenz einer regulären G-invarianten Bilinearform folgt aus (1.67)(b). Ist die Charakteristik von F nicht 2, so folgt aus (1.69)(a), dass diese Bilinearform symmetrisch oder symplektisch ist. ■

(1.71) Satz (Lemma von Fong):
Sei F ein perfekter Körper der Charakteristik 2 und V ein irreduzibler FG-Modul. Ist $V \simeq V^*$ und V kein Modul für die triviale Darstellung von G, so existiert eine reguläre symplektische G-invariante Bilinearform auf V. Insbesondere ist die Dimension von V gerade.

Beweis: Ist die Dimension von V gleich 1, so ist $V = Fv$. Der Isomorphismus $V \simeq V^*$ impliziert $vg = vg^{-1}$ für alle $g \in G$. Da $vg = av$ für ein $a \in F^\times$ ist, folgern wir, dass $a^2 = 1$ sein muss, und, da $\mathrm{char}\,K = 2$ ist, ist $a = 1$. Somit muss die Dimension von V größer als 1 sein.

Nach (1.67)(b) existiert eine reguläre G-invariante Bilinearform f auf V (von der wir aber nicht wissen, ob sie symplektisch ist!). Wir setzen $q(v) := b(v, v)$. Daraus ergibt sich

$$q(v_1 + v_2) = q(v_1) + q(v_2) + [v_1, v_2], \tag{1.71.1}$$

wobei

$$[v_1, v_2] := b(v_1, v_2) + b(v_2, v_1) \tag{1.71.2}$$

ist. Wir unterscheiden zwei Fälle

Fall 1: Die Form $[\cdot, \cdot]$ ist identisch Null, i.e.

$$q(v_1 + v_2) = q(v_1) + q(v_2)$$

für alle $v_1, v_2 \in V$. Wir wählen $v_1, v_2 \in V$ linear unabhängig (geht, da $\dim_F V \geqslant 2$). Falls $q(v_1) \neq 0$, so existiert, da F perfekt ist, ein $a \in F$ mit

$$q(av_1 + v_2) = a^2 q(v_1) + q(v_2) = 0.$$

Deshalb ist die Menge

$$U := \{v \in V \mid q(v) = 0\}$$

ein nicht trivialer G-invarianter Teilraum von V. Da V irreduzibel ist, ist $U = V$ und es gilt

$$0 = q(v) = b(v, v)$$

für alle $v \in V$; b ist also symplektisch.

Fall 2: Ist die Form $[\cdot, \cdot]$ nicht identisch Null, so ist sie wegen (1.71.2) und $\operatorname{char} K = 2$ symplektisch. Sei R das Radikal von $[\cdot, \cdot]$ (i.e. $R = V^\perp$ bezüglich $[\cdot, \cdot]$). Es ist

$$R = \{v \in V \mid [v, w] = 0 \ \forall\, w \in V\}.$$

Da $[\cdot, \cdot]$ nicht identisch Null ist, kann R nicht gleich V sein. Weil R aber G-invariant und V irreduzibel ist, muss $R = \{0\}$ sein, was bedeutet, dass $[\cdot, \cdot]$ regulär ist. ■

(1.72) Definition & Bemerkung:
Sei V ein FG-Modul.

*(a) Eine quadratische Form q auf V heißt **G-invariant**, wenn*

$$q(vg) = q(v)$$

für alle $g \in G$ und $v \in V$ gilt.

(b) Die folgenden Aussagen sind äquivalent:

(i) Die quadratische Form q ist G-invariant.

(ii) Das Bild des Operationshomomorphismus ist in $O(V, q)$; i.e. die Operation eines jeden Gruppenelementes entspricht einer Isometrie. ■

In Anlehnung an Satz (1.70) zeigen wir nun, dass es auf einem irreduziblen selbstdualen FG-Modul auch nicht „allzuviele“ G-invariante quadratische Formen geben kann.

(1.73) Satz:
Sei V ein absolut irreduzibler selbstdualer FG-Modul, der nicht der Modul für die triviale Darstellung von G ist, und $Q_0(V)$ der F-Vektorraum der G-invarianten quadratischen Formen auf V. Es gilt:

(a) Ist die Charakteristik von F nicht 2, so ist $\dim_F Q_0(V) = 1$ (vgl. [HB82, Kapitel VII, §8, Remark 8.15 (a)]).
(b) Ist F ein perfekter Körper der Charakteristik 2, so ist $\dim_F Q_0(V) \leqslant 1$ (vgl. [HB82, Kapitel VII, §8, Exercise 23]).

Beweis: (a) Ist die Charakteristik nicht 2, so stehen die quadratische Form und ihre zugehörige Bilinearform in Bijektion. Nach (1.70) ist $1 = \dim_F \mathcal{B}_0(V) = \dim_F Q_0(V)$.

(b) Seien $q_1, q_2 \in Q_0(V)$ mit gleicher Bilinearform $b \in \mathcal{B}_0(V)$ i.e.

$$q_i(v_1 + v_2) = q_i(v_1) + q_i(v_2) + b(v_1, v_2) \quad \text{für alle} \quad v_1, v_2 \in V,\ i = 1, 2.$$

Zuerst wollen wir zeigen, dass es ein $0 \neq v \in V$ gibt, so dass $q_1(v) = q_2(v)$ ist. Dazu nehmen wir an, dass es ein solches v nicht gibt. Dies bedeutet, dass die quadratische Form $\tilde{q} := q_1 + q_2$ total anisotrop ist, i.e. $\tilde{q}(v) = 0$ impliziert, dass $v = 0$ ist. Weiter ergibt sich aus der Definition, dass die zugehörige Bilinearform von $\tilde{q}$ identisch Null ist. Da nach (1.71) die Dimension von V mindestens 2 ist, gibt es zwei linear unabhängige Vektoren $v, w \in V$ die nicht singulär (bez. $\tilde{q}$) sind. Da F perfekt ist, gibt es ein $a \in F^\times$ mit $a^2\tilde{q}(v) = \tilde{q}(w)$. Daraus folgt, dass

$$\tilde{q}(av + w) = a^2\tilde{q}(v) + q(w) = 0$$

ist, was ein Widerspruch zu „$\tilde{q}$ ist total anisotrop“ ist. Also muss es ein $0 \neq v \in V$ geben mit $q_1(v) = q_2(v)$.
Der von v erzeugte FG-Modul ist ein G-invarianter Teilraum, der v enthält und wegen der Irreduzibilität von V gleich V sein muss. Sei $a = \sum_{g\in G} h_g g \in FG$ mit $h_g \in F$ für alle $g \in G$. Damit gilt

$$\begin{aligned}
\tilde{q}(va) &= q_1(va) + q_2(va) \\
&= \sum_{g\in G} h_g^2 (q_1(vg) + q_2(vg)) \\
&\overset{q_i\ G\text{-invariant}}{=} \sum_{g\in G} h_g^2 (q_1(v) + q_2(v)) \\
&\overset{q_1(v)=q_2(v)}{=} 0.
\end{aligned}$$

Da a beliebig war, sind q_1 und q_2 gleich. Dies bedeutet, dass es, wenn überhaupt, nur eine, bis auf skalare Vielfache eindeutige G-invariante reguläre quadratische Form mit vorgegebener G-invarianter regulärer Bilinearform geben kann. Nach (1.70) ist dann $1 = \dim_F \mathcal{B}_0(V) \geqslant \dim_F Q_0(V)$. ■

Nun interessiert uns natürlich, wann ein absolut irreduzibler selbstdualer FG-Modul über einem perfekten Körper der Charakteristik 2 eine G-invariante quadratische Form trägt. Hierzu benötigen wir ein paar Definitionen und einführende Lemmata.

(1.74) Definition:
Sei F ein Körper der Charakteristik 2 und V ein FG-Modul.

(a) *Die F-lineare Abbildung τ, die durch*

$$(v \otimes w)\tau = w \otimes v$$

definiert ist, ist ein FG-Automorphismus von $V \otimes_F V$.

(b) *Wir setzten*

$$\mathcal{S}(V) := \{t \in V \otimes_F V \mid t\tau = t\},$$

der ***symmetrische Teilmodul*** *von $V \otimes_F V$, und*

$$\mathcal{A}(V) := \{t(\tau - \mathrm{id}_{V\otimes_F V}) \mid t \in V \otimes_F V\},$$

der ***antisymmetrische Teilmodul*** *von $V \otimes_F V$. Da*

$$(\tau - \mathrm{id}_{V\otimes_F V})^2 = \tau^2 - \mathrm{id}_{V\otimes_F V} = 0$$

ist, erhalten wir $\mathcal{A}(V) \subseteq \mathcal{S}(V)$. (Ist die Charakteristik von F nicht 2, so gilt $V \otimes_F V = \mathcal{S}(V) \oplus \mathcal{A}(V)$.) ■

(1.75) Lemma:
Ist F ein perfekter Körper der Charakteristik 2 und V ein endlich erzeugter FG-Modul, so gilt:

(a) $(V \otimes_F V)\big/\mathcal{S}(V) \simeq \mathcal{A}(V)$.

(b) $\mathcal{S}(V)\big/\mathcal{A}(V) \simeq V^{(2)}$, *wobei $V^{(2)}$ der FG-Modul ist, der zu V via des Frobeniusautomorphismus $a \mapsto a^2$ des perfekten Körpers F algebraisch konjugiert ist.*

(c) *Trägt V eine G-invariante symplektische Form b, die nicht identisch Null ist, so existiert ein FG-Epimorphismus δ von $\mathcal{A}(V)$ auf den trivialen FG-Modul F, so dass*

$$(v \otimes w + w \otimes v)\delta = b(v, w)$$

ist.

Beweis: (a) $\tau - \mathrm{id}_{V\otimes_F V}$ ist ein FG-Epimorphismus von $V \otimes_F V$ auf $\mathcal{A}(V)$, dessen Kern $\mathcal{S}(V)$ ist.

(b) Sei $\{v_1, \ldots, v_n\}$ eine F-Basis von V. Dann ist

$$\mathcal{A}(V) = \left\langle v_i \otimes v_j + v_j \otimes v_i \mid i, j = 1, \ldots, n;\ i \neq j \right\rangle_F$$

und

$$\mathcal{S}(V) = \langle v_i \otimes v_i \mid i = 1, \ldots, n\rangle_F \oplus \mathcal{A}(V)$$

als F-Vektorräume. Folglich ist

$$\{v_i \otimes v_i + \mathcal{A}(V) \mid i = 1, \ldots, n\}$$

eine F-Basis von $\mathcal{S}(V)\big/\mathcal{A}(V)$. Ist

$$v_i g = \sum_{j=1}^{n} a_{ij}^g v_j \quad (a_{ij}^g \in F),$$

so gilt

$$\begin{aligned}(v_i \otimes v_i + \mathcal{A}(V))g &= v_i g \otimes v_i g + \mathcal{A}(V)\\ &= \sum_{j,k=1}^{n} a_{ij}^g a_{ik}^g v_j \otimes v_k + \mathcal{A}(V)\\ &= \sum_{j=1}^{n} (a_{ij}^g)^2 v_j \otimes v_j + \mathcal{A}(V).\end{aligned}$$

Diese Rechnung zeigt die Behauptung.

(c) Die Abbildung $\tau - \mathrm{id}_{V\otimes_F V}$ induziert einen FG-Isomorphismus σ von $(V \otimes_F V)\big/\mathcal{S}(V)$ auf $\mathcal{A}(V)$ so, dass

$$(v \otimes w + \mathcal{S}(V))\sigma = v \otimes w + w \otimes v.$$

Die Abbildung $\phi \in \mathrm{Hom}_F(V \otimes_F V, F)$ die durch

$$(v \otimes w)\phi = b(v, w)$$

definiert ist, ist ein FG-Homomorphismus von $V \otimes_F V$ auf den trivialen FG-Modul F, da b G-invariant ist. Da b symplektisch ist, erhalten wir

$$(v \otimes w + w \otimes v)\phi = b(v, w) + b(w, v) = 0$$

und

$$(v \otimes v)\phi = b(v, v) = 0.$$

Damit ist $\mathcal{S}(V) \subseteq \mathrm{Kern}\,\phi$. Folglich gibt es einen FG-Epimorphismus $\overline{\phi}$ von $(V \otimes_F V)\big/\mathcal{S}(V)$ auf F mit

$$(v \otimes w + \mathcal{S}(V))\overline{\phi} = b(v, w).$$

Definieren wir nun δ durch $\delta := \sigma^{-1}\overline{\phi}$, so gilt

$$(v \otimes w + w \otimes v)\delta = (v \otimes w + \mathcal{S}(V))\overline{\phi} = b(v, w).$$

■

(1.76) Lemma:

Sei F ein Körper der Charakteristik 2 und V ein FG-Modul. Sei $\{v_1, \ldots, v_n\}$ eine F-Basis von V und q eine quadratische Form auf V. Wir setzen $q_{ii} := q(v_i)$ und $q_{ij} := b_q(v_i, v_j)$ für $i \neq j$. Wir definieren $\alpha \in \mathrm{Hom}_F(\mathcal{S}(V), F)$ durch

$$\begin{aligned}(v_i \otimes v_i)\alpha &= q_{ii}\\ (v_i \otimes v_j + v_j \otimes v_i)\alpha &= q_{ij} \quad (i \neq j).\end{aligned}$$

Dann ist q genau dann G-invariant, wenn $\alpha \in \mathrm{Hom}_{FG}(\mathcal{S}(V), F)$ ist.

Beweis: Für $v = \sum_{i=1}^{n} x_i v_i$ mit $x_i \in F$, erhalten wir

$$q(v) = \sum_{i \leqslant j} x_i x_j q_{ij}.$$

Nun gilt, dass q genau dann G-invariant ist, wenn

$$q(v_i g) = q(v_i) \quad (i = 1, \ldots, n), \text{ und} \tag{1.76.1}$$
$$b_q(v_i g, v_j g) = b_q(v_i, v_j) \quad (i \neq j) \tag{1.76.2}$$

für alle $g \in G$ ist. Sei

$$v_i g = \sum_{j=1}^{n} a_{ij}^g v_j.$$

Damit ist (1.76.1) äquivalent zu

$$\begin{aligned} q_{ii} = q(v_i) &= q(v_i g) \\ &= \sum_{j=1}^{n} (a_{ij}^g)^2 q_{jj} + \sum_{j<k} a_{ij}^g a_{ik}^g q_{jk} \end{aligned} \tag{1.76.1$'$}$$

und (1.76.2) ist äquivalent zu

$$\begin{aligned} q_{ij} = b_q(v_i, v_j) &= b_q(v_i g, v_j g) \\ &= \sum_{l \neq k} a_{ik}^g a_{jl}^g q_{kl} \quad (i \neq j). \end{aligned} \tag{1.76.2$'$}$$

Andererseits ist α genau dann in $\mathrm{Hom}_{FG}(\mathcal{S}(V), F)$, wenn gilt:

$$\begin{aligned} q_{ii} = q_{ii} g &= (v_i \otimes v_i)\alpha g = (v_i \otimes v_i) g \alpha \\ &= \left(\sum_{j,k} a_{ij}^g a_{ik}^g v_j \otimes v_k \right) \alpha \\ &= \sum_{j=1}^{n} (a_{ij}^g)^2 q_{jj} + \sum_{j<k} a_{ij}^g a_{ik}^g q_{jk}, \end{aligned}$$

und für $i \neq j$

$$\begin{aligned} q_{ij} = q_{ij} g &= (v_i \otimes v_j + v_j \otimes v_i)\alpha g \\ &= (v_i \otimes v_j + v_j \otimes v_i) g \alpha \\ &= \left(\sum_{k,l} a_{ik}^g a_{jl}^g (v_k \otimes v_l + v_l \otimes v_k) \right) \alpha \\ &= \sum_{l \neq k} a_{ik}^g a_{jl}^g q_{kl}. \end{aligned}$$

Aus dieser Rechnung folgt die Behauptung. ■

Der folgende Satz gibt nun Aufschluss darüber, wann eine reguläre G-invariante quadratische Form auf einem irreduziblen nicht-trivialen FG-Modul existiert, wobei F ein perfekter Körper der Charakteristik 2 ist.

(1.77) Satz:
Sei F ein perfekter Körper der Charakteristik 2 und V ein irreduzibler FG-Modul, der nicht isomorph zum trivialen FG-Modul ist. Äquivalent sind:

(a) Es gibt eine reguläre G-invariante quadratische Form auf V.
(b) Es gibt einen FG-Epimorphismus von $\mathcal{S}(V)$ auf den trivialen FG-Modul F.

Beweis: Sei $\{v_1, \ldots, v_n\}$ eine F-Basis von V.

(a)⇒(b): Sei q eine reguläre G-invariante quadratische Form auf V und b_q die zugehörige symplektische Form. Wir setzten

$$q_{ii} := q(v_i) \quad \text{und} \quad q_{ij} := b_q(v_i, v_j)\ (i \neq j).$$

Wir definieren $\alpha \in \mathrm{Hom}_F(\mathcal{S}(V), F)$ durch

$$(v_i \otimes v_i)\alpha := q_{ii} \quad \text{und} \quad (v_i \otimes v_j + v_j \otimes v_i)\alpha := q_{ij}\ (i \neq j).$$

Nach (1.76) ist $\alpha \in \mathrm{Hom}_{FG}(\mathcal{S}(V), F)$; offensichtlich ist $\alpha \neq 0$ und damit ist α surjektiv.

(b)⇒(a): Sei $0 \neq \alpha \in \mathrm{Hom}_{FG}(\mathcal{S}(V), F)$. Wir setzen

$$q_{ii} := (v_i \otimes v_i)\alpha \quad \text{und} \quad q_{ij} := (v_i \otimes v_j + v_j \otimes v_i)\alpha\ (i \neq j).$$

Ebenfalls wegen (1.76) definiert dies eine G-invariante quadratische Form q auf V. Es bleibt zu zeigen, dass q regulär ist.

Lemma (1.75)(b) liefert

$$\mathcal{S}(V)\big/\mathcal{A}(V) \simeq V^{(2)} \neq F.$$

Da V irreduzibel ist, ist auch $V^{(2)}$ irreduzibel. Wegen $\mathcal{A}(V) \nsubseteq \mathrm{Kern}\,\alpha$ gibt es $i \neq j$ mit

$$b_q(v_i, v_j) = q_{ij} = (v_i \otimes v_j + v_j \otimes v_i)\alpha \neq 0.$$

Die G-invariante symplektische Form b_q auf V ist somit nicht die Nullform. Deshalb ist das Radikal dieser Form ein echter FG-Teilmodul von V. Da V irreduzibel ist, muss das Radikal Null sein und folglich ist b_q, und damit auch q, regulär. ■

Nun sind wir soweit, den Frobenius-Schur-Indikator für Körper der Charakteristik 2 zu definieren.

(1.78) Definition (vgl. [JLPW95, Introduction 9 und 10] und [JL01, Kapitel 23]):
Sei F ein perfekter Körper der Charakteristik 2 und V ein absolut irreduzibler FG-Modul. Wir definieren

$$\iota V := \begin{cases} +1, & \text{falls } V \text{ selbstdual ist und eine } G\text{-invariante reguläre quadratische Form trägt,} \\ 0, & \text{falls } V \not\simeq V^* \text{ und} \\ -1, & \text{falls } V \text{ selbstdual ist, aber keine } G\text{-invariante reguläre quadratische Form trägt.} \end{cases}$$

und nennen ιV den ***Frobenius-Schur-Indikator*** *von V.* ■

Dieses Kapitel abschließend, wollen wir uns noch einmal das Beispiel (1.16) (d)-(f) vom Ende des Paragraphen § 1.1 zu Gemüte führen und sehen was uns die bis hierhin entwickelte Theorie über diese Moduln noch sagen kann. Hierfür werden wir uns einiger Darstellungen aus [Wil] bedienen. Die Bezeichnungen der vorkommenden Gruppen sind [JLPW95] bzw. [Wil] entnommen. Des weiteren sind alle vorkommenden Darstellungen absolut irreduzibel und der Körper, da er endlich ist, perfekt. Folglich sind alle Voraussetzungen für Satz (1.71) und für Satz (1.70) erfüllt.

(1.79) Beispiel:
Sei $F = \mathbb{F}_2$ und der Vektorraum $V \simeq \mathbb{F}_2^6 (= \mathbb{F}_2^{1\times 6})$. Als Basis sei stets die Standardbasis $\underline{e} = (e_1, \ldots, e_6)$ des Raums $\mathbb{F}_2^6$ zugrunde gelegt. Zur besseren Lesbarkeit werden Nullen als Punkte geschrieben.

(a) Auf V operiert die Gruppe $G := A_7$, gegeben durch die Darstellung

$$a := \begin{pmatrix} . & 1 & . & . & . & . \\ . & . & . & 1 & . & . \\ . & . & 1 & . & . & . \\ 1 & . & . & . & . & . \\ . & . & . & . & 1 & . \\ . & . & . & . & . & 1 \end{pmatrix} \quad b := \begin{pmatrix} . & . & 1 & . & . & . \\ . & 1 & 1 & . & . & . \\ . & . & . & . & 1 & . \\ . & . & 1 & 1 & . & . \\ . & . & . & . & . & 1 \\ 1 & . & 1 & . & 1 & 1 \end{pmatrix}$$

In (1.16)(d) haben wir gesehen, dass V eine Bilinearform b_1 trägt. Es gilt nun, dass b_1 sogar G-invariant ist. Dies verifizieren wir, indem wir

$$a\, {}_{\underline{e}}b_{1\underline{e}}\, a^t = {}_{\underline{e}}b_{1\underline{e}} = b\, {}_{\underline{e}}b_{1\underline{e}}\, b^t$$

nachrechnen. Sei weiterhin eine quadratische Form q_1 auf V durch die Matrix

$$\tilde{q_1} := \begin{pmatrix} 1 & . & . & . & . & . \\ 1 & 1 & . & . & . & . \\ 1 & 1 & 1 & . & . & . \\ 1 & 1 & 1 & 1 & . & . \\ . & . & 1 & . & 1 & . \\ . & . & . & . & 1 & 1 \end{pmatrix}$$

gegeben, wobei $q_1(v) = \mathbf{v}\tilde{q_1}\mathbf{v}^t$ ist. Es gilt $b_{g_1} = b_1$.
Um zu zeigen, dass q_1 G-invariant ist, genügt es nach Bemerkung (1.72)(b) und (1.31) zu zeigen, dass

$$e_i \cdot a \cdot \tilde{q_1} \cdot (e_i \cdot a)^t = e_i \cdot \tilde{q_1} \cdot e_i^t = e_i \cdot b \cdot \tilde{q_1} \cdot (e_i \cdot b)^t$$

für alle $i = 1, \ldots, 6$ gilt. Nach dieser Bemerkung müssten wir zwar noch die Einträge (i, j) für $1 \leqslant i < j \leqslant 6$ von $\tilde{q_1}$ testen. Da diese Einträge aber von der, schon als G-invariant nachgewiesenen, Bilinearform stammen, können wir uns das hier sparen. Es gilt also, dass der Vektorraum V zusammen mit der quadratischen Form q_1 und der Operation der Gruppe A_7 den Frobenius-Schur-Indikator $\iota(V, q_1, A_7) = +1$ hat.
Weiterhin erhalten wir, unter Benutzung des Algorithmus zur Berechnung des Witt-Index aus dem folgenden Kapitel, dass $\operatorname{ind}(V, q_1) = 3$ *ist.*

(b) Nun operiere auf V die Gruppe $G = U_4(2):2 \simeq O_6^-(\mathbb{F}_2)$. Die zugehörigen Matrizen der Erzeuger a, b dieser Gruppe entnehmen wir [Wil], die dort unter der Bezeichnung `U42d2G1-f2r6B0.m1` *und* `U42d2G1-f2r6B0.m2` *zu finden sind. Wie in Teil (a) rechnen wir nun nach, dass die Bilinearform b_2 aus (1.16)(e) ebenfalls G-invariant ist. Auch hierauf gibt es eine G-invariante quadratische Form q_2 die durch*

$$\tilde{q_2} := \begin{pmatrix} 1 & . & . & . & . & . \\ 1 & 1 & . & . & . & . \\ . & 1 & 1 & . & . & . \\ . & 1 & . & 1 & . & . \\ 1 & 1 & . & . & 1 & . \\ . & . & 1 & . & . & 1 \end{pmatrix}$$

gegeben ist. Folglich ist der Frobenius-Schur-Indikator $\iota(V, q_2, U_4(2):2) = +1$. Wiederum, unter Benutzung des oben genannten Algorithmus, erhalten wir, dass diesmal $\operatorname{ind}(V, q_2) = 2$ *ist (was uns bei der operierenden Gruppe auch nicht verwundern sollte).*

(c) Schließlich lassen wir auf V die symplektische Gruppe $G = S_6(2)$ operieren. Die zugehörigen Matrizen der Erzeuger a, b dieser Gruppe entnehmen wir [Wil], die dort unter der Bezeichnung `S62G1-f2r6B0.m1` *und* `S62G1-f2r6B0.m2` *zu finden sind. Obgleich dieser FG-Modul noch selbstdual ist, i.e. b_3 aus (1.16)(f) ist G-invariant, trägt dieser Modul keine G-invariante quadratische Form mehr. Wie wir dies auf geschickte Weise verifizieren, lernen wir im nächsten Kapitel kennen.* ■

Kapitel 2

Algorithmen

> Er sagt es klar und angenehm,
> was erstens, zweitens und
> drittens käm.
>
> *(Wilhelm Busch, Bilder zur Jobsiade (1872) - Fünftes Kapitel)*

In diesem Kapitel wollen wir uns damit beschäftigen, wie wir für einen gegebenen selbstdualen FG-Modul explizit eine G-invariante Bilinearform bestimmen können. Des weiteren werden wir im Fall, dass $\operatorname{char} F = 2$ ist, algorithmisch testen, ob dieser Modul auch eine G-invariante quadratische Form trägt und, wenn ja, werden wir sie auch bestimmen. Für diese Aufgabe hat Jon Thackray in [Tha02b] einen erstaunlich einfachen Algorithmus beschrieben, der bereits in GAP [GAP05], wenn auch nicht besonders geschickt (vgl. § 2.1.2), implementiert ist.

In den ersten Abschnitten werden wir diesen Algorithmus beschreiben, dessen Korrektheit beweisen, eine neue, in Bezug auf Laufzeit und Speicherplatz optimalere, Implementierung in GAP vorstellen und eine grobe Laufzeit- und Speicherplatzabschätzung vornehmen.

Wie bereits im vorhergehenden Kapitel angedeutet, werden wir einen weiteren Algorithmus, der ebenfalls von Jon Thackray in [Tha02a] beschrieben wurde, vorstellen, der zu einer gegebenen G-invarianten quadratischen Form auf einem FG-Modul den Orthogonalitätstyp bestimmt. Auch hier werden wir die Korrektheit des Algorithmus beweisen sowie eine grobe Laufzeit- und Speicherplatzanalyse liefern.

Dieses Kapitel abschließend werden wir mit Hilfe des ersten Algorithmus zeigen, dass in Beispiel (1.79) (c) keine G-invariante quadratische Form existiert. Auch werden wir exemplarisch den zweiten Algorithmus auf Beispiel (1.79) (a) anwenden um den dort behaupteten Witt-Index zu bestätigen. Der Vollständigkeit halber werden wir im Anhang A eine Liste aller absolut irreduziblen selbstdualen Darstellungen der Charakteristik 2 aus [Wil] nebst deren Indikatoren und Witt-Indizes angegeben, wie sie mit den beiden Algorithmen bestimmt wurden.

Während des gesamten Kapitels sei F ein endlicher Körper mit k Elementen. Des weiteren seien alle FG-Moduln absolut irreduzibel. Wie man dies algorithmisch testen kann, entnimmt man beispielsweise [HEO05, Abschnitt 7.4 und 7.5]. Zur Beschreibung der nun folgenden Algorithmen werden wir einen, an den GAP-Code angelehnten, Pseudocode verwenden. Hierfür ist es notwendig, dass wir eine Datenstruktur für die Speicherung eines FG-Moduls definieren. Doch zunächst wollen wir kurz auflisten, welche Parameter wir für die Beschreibung der Algorithmen benötigen:

Parameter	Bedeutung
c	Speicherplatz für ein Körperelement
d	Dimension des Moduls als F-Vektorraum
k	Anzahl der Elemente des Körpers F
n	Anzahl der Erzeuger des Moduls

(2.1) Definition:
Sei V ein FG-Modul, der als F-Vektorraum d-dimensional ist. Seien weiter $\tilde{g}_1, \ldots, \tilde{g}_n$ Erzeuger von G. Sei eine Basis von V gewählt und die Operation von G auf V bezüglich dieser Basis durch

$$\rho : G \to \mathrm{GL}_d(F)$$

gegeben. Seien $g_1, \ldots, g_n$ die Bilder von $\tilde{g}_1, \ldots, \tilde{g}_n$ unter ρ.

*Die Datenstruktur **GModul** bezüglich V ist nun wie folgt definiert:*

$$\begin{aligned} \mathcal{V} := \mathrm{rec}(\quad & gen \quad := [g_1, \ldots, g_n], \\ & dim \quad := d, \\ & field \quad := k\,). \end{aligned}$$

■

Ab jetzt sei $V = F^d$ und $G = \langle g_1, \ldots, g_n \rangle$.

§ 2.1. G-invariante quadratische Formen algorithmisch bestimmen

§ 2.1.1. Algorithmus und Korrektheit

Bevor wir uns dem eigentlichen Algorithmus zuwenden, benötigen wir einige Hilfsfunktionen.

(2.2) Algorithmus (DUALMODULE):

INPUT: GModul $\mathcal{V}$

```
return rec( gen   := List(V.gen, g -> TransposedMat(g)^-1),
            dim   := V.dim,
            field := V.field );
```

OUTPUT: der dazu duale Modul

Beweis: Die Korrektheit folgt unmittelbar aus Kapitel 1, Bemerkung (1.63). ■

Weiter benötigen wir einen Algorithmus zur Berechnung eines FG-Modulisomorphismus zwischen zwei irreduziblen FG-Moduln. Dieser Algorithmus soll, falls ein solcher Isomorphismus existiert, eine Matrix zurück geben, deren Zeilen eine F-Basis des zweiten Moduls bilden und die Bilder der Standardbasis des ersten Moduls sind. Da dieser Algorithmus einige Zwischenergebnisse aus den Algorithmen für die Tests auf Irreduzibielität benötigt, wollen wir hier auf seine explizite Angabe verzichten und auf das Buch [HEO05] verweisen, in dem er im Abschnitt 7.5.3 beschrieben wird. Es sei hier nur erwähnt, dass der Algorithmus mit MODULEISOMORPHISM($\mathcal{V}$, $\mathcal{W}$) aufgerufen wird und entweder „fail“ oder die Abbildungsmatrix eines FG-Modulisomorphismus vom FG-Modul V in den FG-Modul W zurück gibt.

(2.3) Algorithmus (INVARIANTBILINEARFORM):
Sei V ein absolut irreduzibler FG-Modul.

INPUT: GModul $\mathcal{V}$

```
local V*;
V* := DualModule(V);
return ModuleIsomorphism(V, V*);
```

OUTPUT: `fail`, *falls V nicht selbstdual ist oder*
die Gram-Matrix der G-invarianten Bilinearform auf V (bez. der Standardbasis von V).

Beweis: Die Korrektheit folgt unmittelbar aus der Definition von b_V in Kapitel 1 Satz (1.2). ■

Schließlich brauchen wir noch den Algorithmus BASISINORBIT($\mathcal{V}$), der uns für den irreduziblen Modul V eine Basiswechselmatrix liefert, deren Zeilen in einer G-Bahn von Elementen aus V liegen. Hierfür wird auf den ersten Standardbasisvektor schrittweise ein modifizierter Bahnenalgorithmus angewendet, bei dem in jedem Schritt getestet wird, ob die durch den Algorithmus gelieferten Vektoren bereits eine Basis bilden. Für die genaue Implementierung sei hier auf den

Quelltext in der Datei `lib/meataxe.gi` in [GAP05] verwiesen. Für die Korrektheit dieses Algorithmus müssen wir zeigen, dass jede G-Bahn eines irreduziblen Moduls, die den Nullvektor nicht enthält, eine F-Basis des Moduls beinhaltet. Dazu wählen wir eine maximal linear unabhängige Teilmenge in einer G-Bahn, die den Nullvektor nicht enthält. Das F-Erzeugnis dieser Teilmenge ist, da die Menge in einer G-Bahn liegt, sogar ein FG-Untermodul von V, der wegen der Irreduzibilität von V gleich V ist. Folglich enthält die Bahn, welche den ersten Standardbasisvektor beinhaltet, auch eine F-Basis von V, die diesen Vektor einschließt.

Nun sind wir gewappnet, den Algorithmus zur Berechnung einer G-invarianten quadratischen Form auf einem absolut irreduziblen FG-Modul vollständig zu beschreiben.

(2.4) Algorithmus (InvariantQuadraticForm):
Sei V ein absolut irreduzibler FG-Modul.

INPUT: GModul $\mathcal{V}$

```
1  local iso, bas, invbas, cgen, dim, z, qf, cqf, fix, i, j, x, g;
2  iso := InvariantBilinearForm(V);
3  if iso = fail then return fail; fi;
4  if Characteristic(V.field) <> 2 then return iso/2; fi;
5  bas := BasisInOrbit(V);
6  invbas := bas^-1;
7  cgen := List(V.gen, g -> bas * g * invbas);
8  dim := V.dim;
9  z := Zero(V.field);
10 qf := bas * iso * TransposedMat(bas);
11 for i in [1..dim-1] do
12         for j in [i+1..dim] do
13                 qf[i][j] := z;
14         od;
15 od;
16 for x in V.field do
17         for i in [1..dim] do
18                 qf[i][i] := x;
19         od;
20         fix := true;
21         for g in cgen do
22                 cqf := g * qf * TransposedMat(g);
23                 for j in [1..dim] do
24                         if cqf[j][j] <> x then
25                                 fix := false;
26                                 break;
27                         fi;
28                 od;
29                 if not fix then break; fi;
30         od;
31         if fix then
32                 qf := invbas * qf * TransposedMat(invbas);
33                 for i in [1..dim-1] do
34                         for j in [i+1..dim] do
35                                 qf[j][i] := qf[i][j] + qf[j][i];
```

```
36                                  qf[i][j] := z;
37                              od;
38                          od;
39                          return qf;
40              fi;
41      od;
42      return fail;
```

OUTPUT: `fail`*, falls V keine G-invariante quadratische Form trägt oder eine Matrix, die die G-invariante quadratische Form auf V beschreibt.*

Beweis: Wie wir bereits in Kapitel 1, Bemerkung (1.18) gesehen haben, ist eine quadratische Form über einem Ring, in dem 2 eine Einheit ist, bereits eindeutig durch die zugehörige Bilinearform gegeben. Dies bedeutet, dass, falls V eine G-invariante Bilinearform trägt, dadurch bereits eine G-invariante quadratische Form gegeben ist. Nach Satz (1.73)(a) ist diese Form bis auf skalares Vielfaches eindeutig bestimmt.

Ist die Charakteristik des Grundkörpers gleich 2, so ist zum einen einer gegebenen Bilinearform nicht mehr eindeutig eine quadratische Form zugeordnet und zum anderen muss noch nicht einmal eine G-invariante quadratische Form existieren.

Nun wollen wir annehmen, dass V eine G-invariante Bilinearform b trägt. Nach Folgerung (1.19) wissen wir, dass, wenn V eine G-invariante quadratische Form trägt, diese durch eine untere Dreiecksmatrix A beschrieben werden kann. Dies geschieht, indem man $a_{ii} = q(e_i)$, $a_{ij} = b(e_i, e_j)$ für $i > j$ und $a_{ij} = 0$ für $i < j$ setzt, falls $e_1, \ldots, e_d$ eine F-Basis von V ist. Da V bereits eine G-invariante Bilinearform trägt und diese eindeutig ist (bis auf skalare Vielfache: vgl. (1.70)), sind die Einträge a_{ij} für $i \neq j$ festgesetzt. Dies bedeutet, dass für die quadratische Form nur noch die Diagonale bestimmt werden muss. Um dies auf möglichst geschickte Art und Weise zu tun, wählen wir die Basis $e_1, \ldots, e_d$ so, dass sie in einer G-Bahn liegt. Wenn die Basis so gewählt ist, gibt es $h_2, \ldots, h_d \in G$ mit $e_1 h_i = e_i$ für $i = 2, \ldots, d$ und, wenn es eine G-invariante quadratische Form q auf V gibt, so gilt $q(e_i) = q(e_1 h_i) = q(e_1)$ für alle $i = 2, \ldots, d$. Dies bedeutet, dass alle a_{ii} gleich gewählt werden können.

Der Rest des Algorithmus ist nun recht schnell erklärt. Die Gram-Matrix der Bilinearform aus Zeile 2, die bezüglich der Standardbasis gegeben ist, wird gemäß der Basis, die in einer G-Bahn liegt, in Zeile 10 transformiert. Eben so werden die Matrizen, welche die G-Operation beschreiben, bezüglich dieser neuen Basis transformiert. Anschließend werden von der transformierten Gram-Matrix, die schon aus theoretischen Gründen symplektisch sein muss (vgl. (1.71)), die Einträge über der Hauptdiagonalen gelöscht. Im Anschluss daran werden auf der Hauptdiagonalen alle Körperelemente durchprobiert und jeweils getestet, ob die Einträge auf der Hauptdiagonalen fix bleiben, wenn wir, wie in Zeile 22, $g * qf * g^t$ berechnen. Die Einträge unter der Hauptdiagonalen müssen dabei nicht getestet werden, da diese von einer G-invarianten Bilinearformen kommen. Dass dieser Test genügt, um festzustellen, ob die quadratische Form G-invariant ist, haben wir bereits im Beispiel (1.79)(a) gesehen. Liefert dieser Test nun eine

G-invariante quadratische Form, so können wir die Matrix wieder bezüglich der Standardbasis ausdrücken (Zeile 32). Abschließend betreiben wir noch etwas Kosmetik und wandeln diese Matrix in eine untere Dreiecksmatrix um, welche dieselbe quadratische Form repräsentiert (vgl. Zeilen 33-38 bzw. (1.19) und (1.20)). ■

§ 2.1.2. Computer versus Bleistift und Papier

In diesem Abschnitt wollen wir uns etwas genauer mit der aktuellen[1] Implementierung des Algorithmus (2.4) in GAP [GAP05] beschäftigen. Insbesondere wollen wir untersuchen, wie wir die Implementierung bezüglich Laufzeit und Speicherplatz verbessern können. Doch zunächst wollen wir uns einmal die aktuelle Implementierung ansehen:

```
3497 ##############################################################################
3498 ##
3499 #F  InvariantQuadraticForm ( module ) . . . .
3500 ##
3501 ## Look for an invariant quadratic form of the absolutely irreducible
3502 ## GModule module. Return fail, or the matrix of the form.
3503 SMTX_InvariantQuadraticForm := function ( module )
3504   local iso, bas, cgens, ciso, dim, f, z, x, i, j, qf, g, id, cqf, fix;
3505
3506   if not SMTX.IsMTXModule(module) or
3507                               not SMTX.IsAbsolutelyIrreducible(module) then
3508     Error(
3509  "Argument of InvariantQuadraticForm is not an absolutely irreducible module");
3510   fi;
3511   if IsBound(module.InvariantQuadraticForm) then
3512     return module.InvariantQuadraticForm;
3513   fi;
3514   iso := SMTX.InvariantBilinearForm(module);
3515   if iso = fail then return fail; fi;
3516   if Characteristic(module.field) <> 2 then return iso/2; fi;
3517
3518   #In characteristic two, we change to a basis in orbit.
3519   #This makes the search for an invariant quadratic form quicker.
3520   bas := SMTX.BasisInOrbit(module);
3521   cgens := List (module.generators, x->bas*x*bas^-1 );
3522   ciso := List(bas * iso * TransposedMat(bas),ShallowCopy);
3523   dim := module.dimension;
3524   f := module.field;
3525   z := Zero(f);
3526
3527   #Matrix must be symplectic - perhaps it must be?
3528   for i in [1..dim] do if ciso[i][i] <> z then
3529     Print("Non-symplectic failure!\n");
3530     return fail;
3531   fi; od;
```

[1] CVS Version „Id: meataxe.gi,v 4.64.2.4 2004/02/05 22:08:29 gap Exp“

```
3532
3533      #If there is an invariant quadratic form, then it will be the lower
3534      #left hand part of ciso plus a scalar.
3535      for i in [1..dim-1] do for j in [i+1..dim] do ciso[i][j] := z; od; od;
3536      id := IdentityMat(dim, f);
3537      for x in f do
3538        qf := ciso + x*id;
3539        fix := true;
3540        #Form is preserved if and only if diagonal is.
3541        for g in cgens do
3542          cqf := g * qf * TransposedMat(g);
3543          for j in [1..dim] do if cqf[j][j] <> x then
3544            fix := false;
3545            break;
3546          fi; od;
3547          if not fix then break; fi;
3548        od;
3549        if fix then
3550          qf := bas^-1 * qf * TransposedMat(bas^-1);
3551          #switch to lower triangular equivalent
3552          for i in [1..dim-1] do for j in [i+1..dim] do
3553            qf[j][i] := qf[i][j] + qf[j][i];
3554            qf[i][j] := z;
3555          od; od;
3556          ConvertToMatrixRep(qf,f);
3557          MakeImmutable(qf);
3558          SMTX.SetInvariantQuadraticForm(module, qf);
3559          return qf;
3560        fi;
3561      od;
3562      SMTX.SetInvariantQuadraticForm(module, fail);
3563      return fail;
3564  end;
```

Zuerst einmal fällt auf, dass der Test, ob die Gram-Matrix ciso im Charakteristik 2 Fall symplektisch ist, nicht benötigt wird, da dies nach den Sätzen (1.70) und (1.71) sowieso immer der Fall ist. Folglich können die Zeilen 3527 bis 3531 ersatzlos gestrichen werden.

Als nächstes bemerken wir, dass im Laufe des Algorithmus mehrmals die Inverse der Basiswechselmatrix bas berechnet wird. Dies kostet jedesmal $O(d^3)$ Rechenschritte und $2d^2c$ Einheiten an Speicherplatz, wobei d = module.dimension und c der Platz ist, der für die Speicherung eines Körperelements benötigt wird (vgl. [HEO05, Abschitt 7.2, InvertMatrix(A), Seite 224]). Um dieses Manko zu beseitigen, ersetzen wir die Zeile 3520 durch

```
3520  bas := SMTX.BasisInOrbit(module); invbas := bas^-1;
```

die Zeile 3550 durch

```
3550  qf := invbas * qf * TransposedMat(invbas);
```

und fügen zur Deklaration der Variablen in Zeile 3504 die Variable invbas hinzu.

Schließlich gilt es noch die etwas merkwürdige Überschrift dieses Paragraphen zu rechtfertigen. Es mag in einem Text eine geschickte Schreibweise sein, wenn wir $B = A + xE_n$ dafür schreiben, dass wir bei einer Matrix A, auf deren Hauptdiagonale nur Nullen stehen, diese durch den Skalar x ersetzen wollen. Vom Standpunkt der Komplexitätstheorie her ist dies allerdings viel zu laufzeit- und speicherplatzintensiv. Für die Berechnung in Zeile 3538 benötigen wir zuerst einmal d^2c Speicherplatzeinheiten zur Speicherung der Identitätsmatrix in Zeile 3536. Weiter benötigen wir $2d^2c$ Speicherplatzeinheiten in Zeile 3538 um qf zu bestimmen. Hierfür benötigen wir $2d^2$ Rechenschritte; d^2 Schritte für x*id und d^2 Schritte für ciso + x*id. Es ist besser, auf die Variable ciso vollkommen zu verzichten und die Zeile 3522 durch

```
3522  qf := List(bas * iso * TransposedMat(bas), ShallowCopy);
```

die Zeile 3535 durch

```
3535  for i in [1..dim-1] do for j in [i+1..dim] do qf[i][j] := z; od; od;
```

und die Zeile 3535 durch

```
3538  for i in [1..dim] do qf[i][i] := x; od;
```

zu ersetzen. Weiterhin können wir Zeile 3536 streichen. Hierdurch sparen wir den Speicherplatz für zwei $d \times d$ Matrizen und benötigen nur d Rechenschritte statt $2d^2$.

Nachdem wir alle Änderungen vorgenommen haben, sieht der Quellcode wie folgt aus:

(2.5) Algorithmus (Optimierte GAP Implementierung):

```
1  ##############################################################################
2  ##
3  #F  InvariantQuadraticForm ( module ) . . . .
4  ##
5  ## Look for an invariant quadratic form of the absolutely irreducible
6  ## GModule module. Return fail, or the matrix of the form.
7  SMTX_InvariantQuadraticForm := function ( module )
8    local iso, bas, invbas, cgens, dim, f, z, x, i, j, qf, g, cqf, fix;
9
10   if not SMTX.IsMTXModule(module) or
11                              not SMTX.IsAbsolutelyIrreducible(module) then
12     Error(
13  "Argument of InvariantQuadraticForm is not an absolutely irreducible module");
14   fi;
15   if IsBound(module.InvariantQuadraticForm) then
16     return module.InvariantQuadraticForm;
17   fi;
18   iso := SMTX.InvariantBilinearForm(module);
19   if iso = fail then return fail; fi;
20   if Characteristic(module.field) <> 2 then return iso/2; fi;
21
22   #In characteristic two, we change to a basis in orbit.
23   #This makes the search for an invariant quadratic form quicker.
24   bas := SMTX.BasisInOrbit(module);
```

```
25      invbas := bas^-1;
26      cgens := List (module.generators, x -> bas * x * invbas);
27      qf := List (bas * iso * TransposedMat(bas), ShallowCopy);
28      dim := module.dimension;
29      f := module.field;
30      z := Zero(f);
31
32      #If there is an invariant quadratic form, then it will be the lower
33      #left hand part of ciso plus a scalar.
34      for i in [1..dim-1] do for j in [i+1..dim] do qf[i][j] := z; od; od;
35      for x in f do
36        for i in [1..dim] do qf[i][i] := x; od;
37        fix := true;
38        #Form is preserved if and only if diagonal is.
39        for g in cgens do
40          cqf := g * qf * TransposedMat(g);
41          for j in [1..dim] do if cqf[j][j] <> x then
42            fix := false;
43            break;
44          fi; od;
45          if not fix then break; fi;
46        od;
47        if fix then
48          qf := invbas * qf * TransposedMat(invbas);
49          for i in [1..dim-1] do for j in [i+1..dim] do
50            qf[j][i] := qf[i][j] + qf[j][i];
51            qf[i][j] := z;
52          od; od;
53          ConvertToMatrixRep(qf, f);
54          MakeImmutable(qf);
55          SMTX.SetInvariantQuadraticForm(module, qf);
56          return qf;
57        fi;
58      od;
59      SMTX.SetInvariantQuadraticForm(module, fail);
60      return fail;
61  end;
```

■

§ 2.1.3. Grobe Laufzeit- und Speicherplatzanalyse

Für die Analyse des Algorithmus benutzen wir die in (2.5) angegebene Implementierung. Des weiteren wollen wir annehmen, dass der Modul absolut irreduzibel ist und hierauf bereits getestet wurde. Diese Annahme wollen wir machen, da der Algorithmus zum Testen auf Irreduzibilität an einer Stelle eine zufällige Wahl von Elementen aus dem Gruppenring macht und diese Wahl nur mit einer bestimmten Wahrscheinlichkeit zu einem Element führt, das für den Irreduzibilitätstest geeignet ist.

Wir werden für die Laufzeitanalyse die O-Notation nach Landau (vgl. [Ney04, Abschnitt 1.2.3]) verwenden und diese in Abhängigkeit der Dimension d, der Anzahl k der Elemente im Körper und der Anzahl der Erzeuger n beschreiben. Da wir hier stets Algorithmen mit polynomieller Laufzeit betrachten, können wir die O-Notation wie folgt auffassen: Ist die exakte Laufzeit eines Algorithmus durch ein Polynom f beschrieben, so liegt dieser Algorithmus in der Klasse $O(s)$ wenn s das normierte Monom höchsten Grades von f ist. Gemäß den Rechenregel für die Bestimmung des Grades der Summe oder des Produktes zweier Polynome sind die Rechenregeln für die O-Notation zu verstehen. Wir nehmen an, dass Addition, Subtraktion, Multiplikation und Invertierung von Körperelementen $O(1)$ Rechenschritte benötigen. Auch wollen wir annehmen, dass das allozieren von Speicherplatz für beliebig große Listen, und das Anhängen von Elementen an eine Liste ebenfalls $O(1)$ Schritte erfordern. Wir wollen sogleich noch für die wichtigsten Operationen die Komplexitätsklassen angeben. Hierzu gehören die Multiplikation eines Vektors der Länge d mit einem Skalar ($O(d)$) und die Addition zweier Vektoren ($O(d)$). Weiter sind da noch die Matrix-Vektor-Multiplikation ($O(d^2)$), das Transponieren einer Matrix ($O(d^2)$), die Multiplikation zweier Matrizen ($O(d^3)$), das Invertieren einer Matrix ($O(d^3)$) und das Lösen eines linearen Gleichungssystems mit d Gleichungen und d Unbekannten ($O(d^3)$).

Für die Speicherplatzanalyse werden wir hingegen relativ genau zählen, wieviel Speicher benötigt wird. Dabei werden wir den Speicherplatz für Laufvariablen etc. vernachlässigen und lediglich den Platz für Vektoren und Matrizen berücksichtigen. Hierfür bezeichnen wir mit c den Speicherplatz, der für die Speicherung eines Elements des Körpers, über dem der Modul definiert ist, benötigt wird. Schließlich wollen wir noch die etwas unrealistische, aber vernünftige Annahme machen, dass der Speicherplatz, der mit `Unbind` freigegeben werden soll, auch tatsächlich sofort freigegeben wird und nicht erst dann, wenn der Garbagecollector dies für nötig hält. Ebenso werden wir zum Speicherplatz lediglich das hinzuzählen, was während des Algorithmus neu hinzukommt; der Platz, den die Eingabe benötigt, wird also nicht hinzugezählt, da wir sonst zur Berechnung des Gesamtspeicherplatzes eines, aus Teilalgorithmen zusammengesetzten Algorithmus, nicht einfach addieren können.

Bei den Teilalgorithmen, die im Laufe des Algorithmus (2.5) verwendet werden, wird sowohl der Speicherplatz, der zur Speicherung des Resultats - im folgenden „extern“ genannt - als auch der Speicherplatz, der zur Berechnung des Resultats - „intern“ genannt - gebraucht wird, angegeben.

(2.6) Proposition:
Der Algorithmus DualModule *hat eine Laufzeit von $O(d^3n)$; während der Berechnung wird $(n+2)d^2c$ Einheiten Platz benötigt und die Ausgabe erfordert nd^2c Speicherplatzeinheiten.*

Beweis: Das Transponieren und Invertieren kostet $O(d^3)$ Rechenschritte und muss auf n Matrizen angewandt werden; folglich ist die Laufzeit $O(d^3n)$. Das Transponieren benötigt intern wie extern d^2c Einheiten Platz pro Matrix. Für das Invertieren müssen intern zwei Matrizen gespeichert, aber nur eine ausgegeben werden. Dies bedeutet, dass der Algorithmus den oben angegebenen Speicherplatz benötigt. ■

(2.7) Proposition:
Der Algorithmus ModuleIsomorphism *hat eine Laufzeit von $O(d^3n)$, während der Berechnung*

wird ca. $6d^2c$ Einheiten Platz benötigt und die Ausgabe erfordert d^2c Speicherplatzeinheiten.

Beweis: Direktes Nachrechnen anhand der Beschreibung in [HEO05, Abschnitt 7.5.3] liefert die Laufzeit und die Speicherplatzabschätzung wie behauptet. Es sei hierbei noch erwähnt, dass bei diesem Algorithmus a priori keine genaue Angabe darüber gemacht werden kann, wieviel Speicher tatsächlich während der Berechnung benötigt wird. Dies liegt daran, dass während der Berechnung mit einem zufällig gewählten Element von FG gearbeitet werden muss und dies als Linearkombination von Produkten der Erzeugermatrizen berechnet wird. Für gewöhnlich müssen dabei nicht mehr als sechs Matrixmultiplikationen berechnet werden. ■

(2.8) Proposition:
Der Algorithmus InvariantBilinearForm *hat eine Laufzeit von $O(d^3n)$, während der Berechnung werden ca. $6d^2c$ Einheiten Platz benötigt und die Ausgabe erfordert d^2c Speicherplatzeinheiten.*

Beweis: Folgt unmittelbar aus (2.6) und (2.7). ■

(2.9) Proposition:
Der Algorithmus BasisInOrbit *hat die Laufzeit $O(d^3n)$, benötigt intern $2d^2c + 2dc$ und für die Ausgabe d^2c Speicherplatzeinheiten.*

Beweis: Der Algorithmus besteht im wesentlichen aus zwei Teilen: dem Initialisierungsteil, in welchem die aufwändigste Operation jene ist, die den ersten Standardvektor erzeugt. In der aktuellen[2] Version des Algorithmus benötigt diese Anweisung $O(d^2)$ Schritte; es ist aber möglich, dies auch in $O(d)$ Schritten zu bewerkstelligen indem wir

```
v := ListWithIdenticalEntries( dim, zero ); v[1] := One( F );
```

setzen. Danach gibt es zwei ineinander verschachtelte Schleifen. Eine, die über alle Erzeuger iteriert und eine der Länge d. Innerhalb dieser Schleifen ist die aufwändigste Anweisung eine Matrix-Vektor-Multiplikation, womit dieser Block insgesamt eine Laufzeit von $O(d^3n)$ hat. Nach den Rechenregeln für die O-Notation (vgl. [Ney04, Abschnitt 1.2.3]) ist die Gesamtlaufzeit $O(d^3n)$.

Der benötigte Speicherplatz ergibt sich daraus, dass intern zwei Matrizen und zwei Vektoren gespeichert werden müssen und eine Matrix ausgegeben werden muss. ■

Nun sind wir für die Analyse von Algorithmus (2.5) wohlpräpariert.

(2.10) Satz:
Der Algorithmus InvariantQuadraticForm *hat in Charakteristik zwei, angewandt auf einen, schon auf absolute Irreduzibilität getesteten Modul, die Laufzeit $O(d^3nk)$. Ist die Charakteristik nicht zwei, so hat er die Laufzeit $O(d^3n)$. Unabhängig von der Charakteristik des Grundkörpers benötigt er intern ca. $6d^2c$ und für die Ausgabe d^2c Speicherplatzeinheiten.*

[2] CVS Version „Id: meataxe.gi,v 4.64.2.4 2004/02/05 22:08:29 gap Exp“

Beweis: Zunächst zur Laufzeit: Unter der oben gemachten Annahme sind die Abfragen in den Zeilen 10-17 in $O(1)$ Schritten erledigt. Der Aufruf von InvariantBilinearForm in Zeile 18 benötigt $O(d^3n)$ Schritte. Für den Rest des Algorithmus gehen wir davon aus, dass dieser Aufruf nicht mit `fail` abbricht. Ist die Charakteristik nicht 2, so werden $O(d^2)$ Schritte für die Ausgabe von iso/2 in Zeile 20 benötigt. Ist hingegen die Charakteristik gleich 2, so ist diese Zeile in $O(1)$ Schritten abgearbeitet. Die Anweisungen in den Zeilen 24 und 26 benötigen jeweils $O(d^3n)$ Schritte, die Anweisungen in den Zeilen 25 und 27 brauchen $O(d^3)$ Schritte. Die zwei **for** Schleifen in Zeile 34, welche die obere Hälfte der Gram-Matrix löschen, brauchen $O(d^2)$ Schritte. Die **for** Schleife von Zeile 35 bis Zeile 58 wird maximal k mal wiederholt. Das Setzen der Hauptdiagonalen in Zeile 36 dauert $O(d)$ Schritte. Die **for** Schleife von Zeile 39 bis Zeile 46 iteriert über alle n Erzeuger; hierbei ist die Anweisung in Zeile 40 mit $O(d^3)$ Schritten die Aufwändigste. Die Anweisungen im **if** Block in Zeile 47 bis 57 werden nur einmal ausgeführt und benötigen $O(d^3)$ Schritte. Die Anweisung in Zeile 40 wird $n \cdot k$ mal ausgeführt, was dazu führt, dass der Algorithmus eine Gesamtlaufzeit von $O(d^3nk)$ Schritten hat.

Bezüglich des Speicherplatzes, der während der Berechnung benötigt wird, bemerken wir leicht, dass an keiner Stelle mehr Speicherplatz benötigt wird als bei der Berechnung der Bilinearform. ■

§ 2.2. Algorithmus zur Berechnung des Orthogonalitätstyp der quadratischen Form

Wie wir bereits in Beispiel (1.79)(a) gesehen haben, können wir einen quadratischen FG-Modul V als einen F-Vektorraum auffassen, bei dem wir das Bild der Darstellung nicht nur als Untergruppe der $\mathrm{GL}(V)$ identifizieren können, sondern sogar als Untergruppe der orthogonalen Gruppe $O(V)$. Da in diesem Abschnitt der Körper endlich ist, wissen wir aus Kapitel 1, § 1.4, dass es für quadratische F-Vektorräume gerader Dimension zwei nicht isomorphe Typen von orthogonalen Gruppen gibt. Da die Typen nicht, wie bei der Existenz der quadratischen Form, von der Charakteristik des Grundkörpers abhängen, betrachten wir hier wieder endliche Körper beliebiger Charakteristik. Das Lemma von Fong (1.71) ist der Grund dafür, dass wir uns nicht um Vektorräume ungerader Dimension kümmern müssen. Somit sind in diesem Abschnitt alle Vektorräume von gerader Dimension.

§ 2.2.1. Algorithmus und Korrektheit

Im Gegensatz zum vorherigen Abschnitt wollen wir den hier verwendeten Algorithmus, mit dessen Hilfe wir zu gegebener quadratischer Form den Typ der zugehörigen orthogonalen Gruppe

bestimmen können, in einer etwas freieren Form beschreiben. Danach, während wir die Korrektheit beweisen, wollen wir die konkrete Umsetzung der einzelnen Schritte erörtern und uns Gedanken darüber machen, welche Teile des Algorithmus tatsächlich implementiert werden müssen und welche nur für den geschickteren Beweis der Korrektheit aufgeführt worden sind.

Wie im vorangegangen Paragraphen bezeichnet V den FG-Modul, der diesmal schon eine reguläre G-invariante quadratische Form q mit zugehöriger Bilinearform b trägt. Weiterhin ist $\dim_F V = d$ gerade. Da der Tatsache, dass G auf V operiert schon dadurch Rechnung getragen wird, dass das Bild der Darstellung eine Untergruppe von $O(V)$ ist, können wir uns auf die F-Vektorraumstruktur von V beschränken.

Bevor wir uns dem Algorithmus zuwenden, wollen wir die Idee, die dahinter steht, erläutern. Nach (1.60) ist (V,q) isometrisch zu $E_d^+(F)$ oder zu $E_d^-(F)$ und der Witt-Index von V ist mindestens $\frac{d}{2}-1$. Folglich spalten von V mindestens $\frac{d}{2}-1$ hyperbolische Ebenen ab; also ist

$$(V,q) \simeq E \perp \left(\perp_{i=1}^{\frac{d}{2}-1} \mathbb{H}\right).$$

Laut Satz (1.54), zusammen mit (1.56), gibt es für den zweidimensionalen Raum E nur die Möglichkeit, anisotrop oder hyperbolisch zu sein. Nun könnten wir auf die Idee kommen, schrittweise von V hyperbolische Ebenen abzuspalten. Hierfür wäre es aber notwendig, jeweils das orthogonale Komplement eines zweidimensionalen Raums zu berechnen. Es gibt jedoch eine weniger aufwändige Möglichkeit heraus zu finden, welchen Witt-Index V hat. Nach (1.49) ist der Witt-Index von V die Dimension eines maximal singulären Teilraums. Somit genügt es, einen maximalen singulären Teilraum zu konstruieren und zu prüfen, ob dessen Dimension gleich $\frac{d}{2}-1$ oder $\frac{d}{2}$ ist. Hierbei ist in jedem Schritt jeweils nur das orthogonale Komplement eines einzelnen Vektors zu berechnen. Da die Dimension eines maximal singulären Raums gleich der Anzahl der hyperbolischen Ebenen in der oben angegebenen Zerlegung ist, haben wir dadurch tatsächlich eine Verbesserung gegenüber dem Abspalten der hyperbolischen Ebenen.

***(2.11) Algorithmus* (OrthogonalSign *[Tha02a]*):**
Während des Algorithmus betrachten wir neben V noch die Unterräume U, W und $W^\perp$, so dass $W^\perp = W \oplus U \leqslant V$ gilt wobei U zu Beginn auf V gesetzt wird. Die nun folgende Schleife terminiert, wenn die Dimension von U gleich 2 ist. Zu Beginn der Schleife ist $W = \{0\}$ und folglich U und $W^\perp$ der ganze Raum. Für den Algorithmus speichern wir lediglich eine F-Basis $\left(v_1,\ldots,v_d'\right)$ von U wobei $d' = \dim_F U$ ist. Jeder Schleifendurchlauf besteht aus den nun folgenden Schritten, immer vorausgesetzt, dass $d' \geqslant 3$ ist.

1. *Finde in $\langle v_1,v_2,v_3\rangle_F$ einen Vektor $v \neq 0$ mit $q(v) = 0$. Erweitere W mit v um eine Dimension zu W'.*
2. *Entferne einen der Vektoren v_1, v_2, v_3 von der Basis von U. Hierbei ist zu beachten, dass der gewählte Vektor in der Summe $v = \sum_{i=1}^3 a_i v_i$ ($a_i \in F$) mit einem Koeffizienten ungleich Null vertreten ist. Dies liefert uns einen Teilraum U' von U derart, dass $W^\perp = W' \oplus U'$ ist. Sei $B := \left(v_1',\ldots,v_m'\right)$ mit $m = d'-1$ die so erhaltene Basis von U'.*
3. *Nun berechne $u_i := b(v,v_i')$ für jedes v_i' .*

4. *Wähle ein i, so dass $u_i \neq 0$ ist.*
5. *Für jedes $j \neq i$ subtrahiere $\frac{u_j}{u_i} v'_i$ von v'_j. Fasse diese veränderte Vektoren in B' zusammen.*
6. *Das Erzeugnis von B' nennen wir U''. Dann ist $W'^{\perp} = W' \oplus U''$.*
7. *Es ist $\dim_F U'' = \dim_F U - 2$. Setze $d' := \dim_F U''$, $U := U''$, $W := W'$ und $W^{\perp} := W'^{\perp}$, so erfüllen diese wieder die Eintrittsbedingung für die Schleife. Ist die Dimension von U'' größer als 2, so starte wieder bei Schritt 1.*

Die Schleife endet, wenn die Dimension von U gleich 2 ist. In diesem Fall versuche in U einen isotropen Vektor ungleich Null zu finden. Wurde ein solcher Vektor gefunden, so ist U hyperbolisch und der Orthogonalitätstyp ist „+“. Ist kein isotroper Vektor ungleich Null zu finden, so ist dieser zweidimensionale Raum total anisotrop und der Orthogonalitätstyp ist „−“.

Beweis (Korrektheit): Für einen singulären Teilraum W von V gilt $W \leqslant W^{\perp}$. Folglich starten wir den Algorithmus mit dem singulären Raum $W = 0$, erhalten $W^{\perp} = W \oplus U$ und machen eine Induktion über die Dimension von U.

Ein zweidimensionaler regulärer quadratischer Raum über einem endlichen Körper ist entweder eine hyperbolische Ebene oder aber total anisotrop. Eine vollständige Suche nach einem singulären Vektor liefert somit eine eindeutige Antwort auf die Frage nach dem Orthogonalitätstyp.

Sei die Dimension von U also größer als zwei. Der Satz (1.57) liefert im Schritt 1 die Existens eines isotropen Vektors. Schritt 2 ist selbsterklärend. Wir wissen bereits, dass ein isotroper Vektor in einem regulären Raum in einer hyperbolischen Ebene enthalten sein muss. Es muss also einen Vektor unter den übrigen Vektoren $\left(v'_1, \ldots, v'_m\right)$ geben, der nicht senkrecht auf v steht. In Schritt 4 wird ein solcher Vektor v'_i gefunden. Nun wenden wir ein leicht modifiziertes Gram-Schmidt-Verfahren (da das gewöhnliche Gram-Schmidt-Verfahren in Charakteristik 2 nicht funktioniert) an, um die verbliebene Basis so abzuändern, dass sie senkrecht auf v steht. Hierfür müssen wir nachrechnen, dass $b(v, v'_j - \frac{u_j}{u_i} v'_i) = 0$ ist. Wir erhalten

$$\begin{aligned} b(v, v'_j - \frac{u_j}{u_i} v'_i) &= b(v, v'_j) - \frac{u_j}{u_i} b(v, v'_i) \\ &= u_j - \frac{u_j}{u_i} u_i = 0. \end{aligned}$$

Folglich ist $W'^{\perp} = W' \oplus U''$ und W' ist ein singulärer Teilraum von U, dessen Dimension um eins größer als W ist. Da hierbei die Dimension von U'' um zwei kleiner geworden ist, als die von U, terminiert der Algorithmus. ■

(2.12) Definition & Bemerkung:

(a) Ist V ein endlich-dimensionaler F-Vektorraum, so bezeichnen wir mit

$$\mathbb{P}(V) := \{U \mid U \text{ ist eindimensionaler Teilraum von } V\}$$

*den **projektiven Raum über** V.*

(b) Für jedes $X \in \mathbb{P}(V)$ gibt es ein $x \in V$ so, dass $X = xF$ ist. Wir bezeichnen mit $\overline{\mathbb{P}(V)}$ ein Vertretersystem dieser Repräsentanten.

(c) *Ist V ein d-dimensionaler Raum über einem Körper mit k Elementen, so ist* $\left|\mathbb{P}(V)\right| = \frac{k^d-1}{k-1} = \sum_{i=0}^{d-1} k^i$. ■

Ist v ein isotroper Vektor in V, so ist auch jedes F-Vielfache von v isotrop. Folglich müssen im ersten Schritt des Algorithmus (2.11) nicht alle $k^3 - 1$ Vektoren aus $\langle v_1, v_2, v_3\rangle_F$ daraufhin getestet werden, ob sie isotrop sind. Es genügt die $k^2 + k + 1$ Elemente aus $\mathbb{P}(\langle v_1, v_2, v_3\rangle_F)$ auf Isotropie zu testen. Auch bei der Berechnung von $b(v, v'_j)$ im dritten Schritt können wir Rechenzeit sparen, indem wir zunächst $b(v, -) \in V^*$ bestimmen (eine Vektor-Matrix-Multiplikation) und dann $b(v, -)$ auf die Vektoren v'_j anwenden. Schließlich können wir noch das Durchsuchen des zweidimensionalen Raums am Schluss nach einem isotropen Vektor von $k^2 - 1$ Tests auf $k + 1$ Tests verbessern indem wir wieder den Trick mit dem projektiven Raum verwenden.

Für die Laufzeit- und Speicherplatzanalyse im nächsten Unterabschnitt wollen wir uns wieder die Implementierung in GAP ansehen.

(2.13) Algorithmus (GAP Implementierung):

```
3591  SMTX_OrthogonalSign := function(gm)
3592      local   b, q, k, n, W, o, z, lo, lzo, lines, l, w, p,
3593              x, y, r, i;
3594      if IsBound(gm.OrthogonalSign) then
3595          return gm.OrthogonalSign;
3596      fi;
3597      b := MTX.InvariantBilinearForm(gm);
3598      q := MTX.InvariantQuadraticForm(gm);
3599      if q = fail then
3600          return fail;
3601      fi;
3602      n := Length(b);
3603      if n mod 2 = 1 then
3604          return 0;
3605      fi;
3606      k := MTX.Field(gm);
3607     W := IdentityMat(n,k);
3608
3609      #
3610      # Assemble the points of projective 3-space
3611      #
3612      o := One(k);
3613      z := Zero(k);
3614      lo := [o];
3615      lzo := [z,o];
3616      lines := List(Elements(FullRowSpace(k,2)),x -> Concatenation(lo,x));
3617      Append(lines,List(Elements(k), x-> Concatenation(lzo,[x])));
3618      Add(lines,[z,z,o]);
3619
3620      #
3621      # Main loop of Thackray's algorithm, build up a totally isotropic
3622      # subspace and restrict it's perp until the gap between them is just 2 dimensional
3623      #
3624
```

```
3625        while n > 2 do
3626
3627            #
3628            # Find an isotropic vector
3629            #
3630            for l in lines do
3631                w := l*W;
3632                if w*q*w = z then
3633                    break;
3634                fi;
3635            od;
3636            Assert(1,w*b*w = z);
3637            p := PositionNonZero(1);
3638            #
3639            # delete it from W (add it to the subspace)
3640            #
3641            W{[p..n-1]} := W{[p+1..n]};
3642            Unbind(W[n]);
3643            n := n-1;
3644            #
3645            # find a vector with which it has non-zero inner product
3646            #
3647            x := w*b;
3648            p := PositionProperty(W, row -> x*row <> z);
3649            Assert(1, p <> fail);
3650            #
3651            # use it to find the perp of the enlarged subspace
3652            #
3653            y := W[p];
3654            r := x*y;
3655            for i in [p+1..n] do
3656                AddRowVector(W[i], y, - x*W[i]/r);
3657                W[i-1] := W[i];
3658            od;
3659            Unbind(W[n]);
3660            n := n-1;
3661            #
3662            # Now n has gone down by 2 and W is still the "gap" between the
3663            # subspace and its perp
3664            #
3665        od;
3666
3667        #
3668        # Now we need to see if the span of W contains an isotropic vector
3669        #
3670        if W[2]*q*W[2] = z then
3671            SMTX.SetOrthogonalSign(gm,1);
3672            return 1;
3673        else
3674            for x in k do
3675                w := W[1]+x*W[2];
3676                if w*q*w = z then
3677                    SMTX.SetOrthogonalSign(gm,1);
3678                    return 1;
```

```
3679                fi;
3680            od;
3681            SMTX.SetOrthogonalSign(gm,-1);
3682            return -1;
3683        fi;
3684    end;
```

■

Da sich die Implementierung doch ein wenig von der Beschreibung in (2.11) unterscheidet, wollen wir hier noch einmal kurz aufzeigen was in den einzelnen Schritten passiert. Leider werden hier einige Variablen anders als in (2.11) verwendet. Zuerst bemerken wir, dass in (2.13) lediglich eine Basis von U gespeichert wird. Hierbei ist zu beachten, dass der Raum U aus (2.11) hier mit W bezeichnet wird und dessen Dimension nicht mit d' sondern mit n. Schritt 1 wird in den Zeilen 3625 – 3635 beschrieben. Der zweite Schritt wird in den Zeilen 3636 – 3643 abgearbeitet. Die Schritte 3-6 werden in den Zeilen 3647 – 3660 abgehandelt. Der Schritt 7 wird on the fly währen der Abarbeitung der Schleife in den Zeilen 3625 – 3665 ausgeführt. Die Räume W, $W^{\perp}$ werden in der Implementierung nicht benötigt, da sie in die Beschreibung in (2.11) nur aufgenommen worden sind, damit wir die Korrektheit leichter beweisen können.

§ 2.2.2. Grobe Laufzeit- und Speicherplatzanalyse

(2.14) Satz:
Der Algorithmus (2.13) hat eine Laufzeit von $O(d^4k^2)$, während der Berechnung werden $(d^2+d+3(k^2+k+1))c$ Platzeinheiten benötigt und die Ausgabe erfordert eine Speicherplatzeinheit.

Beweis: Wir nehmen an, dass die quadratische Form nebst der zugehörigen Bilinearform bereits berechnet und gespeichert ist. Folglich kosten die Anweisungen in Zeile 3597 und 3598 weder Zeit noch zusätzlichen Speicherplatz. Es beansprucht lediglich die Matrix in Zeile 3607 einen Speicherplatz von cd^2 Einheiten, die k^2+k+1 Elemente des dreidimensionalen projektiven Raums jeweils $3c$ Speicherplatzeinheiten und dc Einheiten für die Speicherung eines Zeilenvektors in Zeile 3631 bzw. 3675.

Das Erzeugen der Einheitsmatrix in Zeile 3607 fällt mit $O(d^2)$ Schritten nicht ins Gewicht. Die **while** Schleife 3625-3665 wird genau $\frac{d}{2}-1$ mal durchlaufen. Dabei verringert sich die Anzahl der Elemente in der Basis jeweils um zwei. Die Anzahl der Elemente der Basis innerhalb der Schleife wollen wir mit $\tilde{d}$ bezeichnen (hierbei wollen wir nur im Hinterkopf behalten, dass $\tilde{d}$ durch d nach oben begrenzt ist). Für die Berechnung des projektiven Raums, der von den ersten drei Zeilen von W erzeugt wird, benötigt man in der Schleife 3630-3635 $O(d^3k^2)$ Schritte; $O(d^3)$ Schritte für die Berechnung von w*q*w und das Ganze k^2+k+1 mal. Die Kalkulation in

Zeile 3647 braucht $O(d^2)$ Schritte und die Rechnung in der darauf folgenden Zeile $O(d\tilde{d})$. Die Durchführung des Gram-Schmidt-Verfahrens in Zeile 3655 bis 3658 dauert $O(d^2\tilde{d})$ Schritte.

Schließlich gilt es noch, die $k+1$ Elemente des zweidimensionalen projektiven Raums über den verbliebenen zwei Elementen der Basis nach einem isotropen Vektor zu durchsuchen. Hierfür brauchen wir $O(d^3k)$ Schritte.

Nach den Rechenregeln für die O-Notation erhalten wir eine Gesamtlaufzeit von $O(d^4k^2)$. ■

§ 2.3. Die Anwendung der Algorithmen

An dieser Stelle wollen wir die offen gebliebenen Fragen aus Beispiel (1.79) beantworten. Zuerst werden wir uns den Teil (c) dieses Beispiels ansehen und zeigen, dass dieser Modul tatsächlich keine G-invariante quadratische Form hat, wobei $G = S_6(2)$ ist.

Wir wissen bereits, dass V selbstdual ist, und die G-invariante Bilinearform b_3 aus Beispiel (1.16)(f) trägt. Dem Algorithmus (2.4) folgend, verifizieren wir, dass die Standardbasis $(e_1, \ldots, e_6)$ des $\mathbb{F}_2^6$ in einer G-Bahn liegt. Seien hierfür die Erzeuger von G wie in (1.79)(c) mit mit a und b bezeichnet. Damit rechnen wir leicht nach, dass $(e_1, \ldots, e_6) = \left(e_1,\ e_1a,\ e_1b,\ e_1b^2,\ e_1b^3,\ e_1b^4\right)$ gilt. Folglich muss eine G-invariante quadratische Form entweder durch $q_1 := \begin{pmatrix} . & . & . & . & . & . \\ 1 & . & . & . & . & . \\ . & 1 & . & . & . & . \\ . & 1 & . & . & . & . \\ 1 & 1 & . & . & . & . \\ 1 & . & 1 & . & . & . \end{pmatrix}$ oder $q_2 := \begin{pmatrix} 1 & . & . & . & . & . \\ 1 & 1 & . & . & . & . \\ . & 1 & 1 & . & . & . \\ . & 1 & . & 1 & . & . \\ 1 & 1 & . & . & 1 & . \\ 1 & . & 1 & . & . & 1 \end{pmatrix}$ beschrieben sein. In beiden Fällen bleibt aber die Diagonale von bq_ib^t $(i = 1, 2)$ nicht konstant ($(bq_1b^t)_{22} = 1$ und $(bq_2b^t)_{66} = 0$). Somit trägt dieser FG-Modul tatsächlich keine G-invariante quadratische Form.

Als nächstes wollen wir exemplarisch an Beispiel (1.79)(a) den Algorithmus (2.11) anwenden, um den Witt-Index zu bestimmen. Hierfür sind die Bezeichnungen wie im Algorithmus gewählt und die Zeilen der folgenden Matrizen erzeugen die jeweiligen Räume. Wir beginnen mit der Standardbasis von V. Die Summe der ersten drei Vektoren dieser Basis ist singulär. Somit lassen wir für U' den ersten Basisvektor weg. Der vierte Basisvektor steht nicht senkrecht auf v. Somit erhalten wir

$$W' = \begin{pmatrix} 1 & 1 & 1 & . & . & . \end{pmatrix} \quad U'' = \begin{pmatrix} . & 1 & . & . & . & . \\ . & . & 1 & . & . & . \\ . & . & . & 1 & 1 & . \\ . & . & . & . & . & 1 \end{pmatrix}.$$

Da die Dimension von U'' größer als zwei ist, setzen wir $U := U''$ und $W := W'$. Die Summe des ersten und dritten Vektors der Basis von U ist wieder singulär. Für U' können wir somit den ersten Vektor weglassen. Der erste Vektor der Basis von U' ist nicht orthogonal zu v. Nach Anwendung des modifizierten Gram-Schmidt-Verfahrens erhalten wir

$$W' = \begin{pmatrix} 1 & 1 & 1 & . & . & . \\ . & 1 & . & 1 & 1 & . \end{pmatrix} \quad U'' = \begin{pmatrix} . & . & 1 & 1 & 1 & . \\ . & . & 1 & . & . & 1 \end{pmatrix}.$$

Schließlich ist auch noch der zweite Basisvektor von U'' singulär. Da wir mit

$$W = \begin{pmatrix} 1 & 1 & 1 & . & . & . \\ . & 1 & . & 1 & 1 & . \\ . & . & 1 & . & . & 1 \end{pmatrix}$$

einen singulären Teilraum von maximaler Dimension gefunden haben, ist der Witt-Index gleich drei und somit ist der Orthogonalitätstyp „+“.

Einen Gesamtüberblick über alle absolut irreduziblen Darstellungen der Charakteristik 2, die in [Wil] aufgelistet und über [Bre04] in GAP abrufbar sind, gibt der Anhang A. Dort gibt es auch am Anfang eine kleine Übersicht darüber, wieviele davon selbstdual und quadratisch sind. Ferner wird noch aufgelistet, welchen Orthogonalitätstyp die quadratischen Darstellungen haben.

Kapitel 3

Der FG-Modul ist für die Algorithmen nicht geeignet - was nun?

> Es ist nicht schwer, zu komponieren, aber es ist fabelhaft schwer, die überflüssigen Noten unter den Tisch fallen zu lassen.
>
> *(Johannes Brahms)*

In diesem Kapitel wollen wir untersuchen, ob und wenn ja wie wir den Frobenius-Schur-Indikator berechnen können oder wenigstens entscheiden können ob ein FG-Modul selbstdual ist oder nicht, wenn dieser Modul für die Algorithmen aus Kapitel 2 ungeeignet ist. Hierfür wollen wir zwei Methoden diskutieren.

Zum einen wollen wir einfache FG-Moduln betrachten, die so groß sind, dass wir die Algorithmen aus Platzgründen nicht anwenden können. Um dieses Problem zu lösen wollen wir uns der Technik der Kondensation bedienen:

Die Kondensation hat sich, seit ihrer Entwicklung Anfang der 1980er Jahre durch Richard Parker und Jon Thackray sowie unabhängig von diesen durch James A. Green, zu einem der wichtigsten Werkzeuge der algorithmischen Darstellungstheorie gemausert. So ist es nicht weiter verwunderlich, dass wir uns hier die Frage stellen, ob wir mit Hilfe der Kondensation entscheiden können ob ein gegebener einfacher FG-Modul selbstdual ist und wenn ja, ob dieser auch eine G-invariante quadratische Form trägt.

Doch bevor wir uns dieser Frage zuwenden, wollen wir zunächst einmal klären, was überhaupt Kondensation ist und wie sie funktioniert; dies geschieht in den ersten zwei Abschnitten. Hierfür werden wir uns der Sprache der Kategorientheorie bedienen: Da wir diese nicht in Gänze neu entwickeln wollen, verweisen wir für die Grundlagen dieser Theorie auf die ersten Kapitel von [Kün06] beziehungsweise auf das Buch [AF74]. Für die Beschreibung der Kondensation werden wir uns weitestgehend an den Arbeiten von Klaus Lux [Lux97] und Felix Noeske [Noe05] orientieren.

Schließlich werden wir uns der Frage zuwenden, wie (und ob) wir diese Technik mit den Algorithmen aus dem vorherigen Kapitel zusammen einsetzen können um zu entscheiden, ob ein einfacher FG-Modul selbstdual ist oder ob er sogar eine G-invariante quadratische Form trägt.

Zum anderen wollen wir uns die Untermodulstruktur eines größeren Moduls zu Nutze machen, der eine G-invariante reguläre quadratische Form trägt, und bei dem der zu testende Modul als Kompositionsfaktor eines gewissen Faktormoduls vorkommt.

§ 3.1. Grundbegriffe aus der Kategorientheorie

In diesem Paragraphen ist F stets ein beliebiger Körper und A und B sind F-Algebren. Wir setzen des weiteren voraus, dass der Leser mit den Begriffen Kategorie, Funktor und natürliche Äquivalenz von Funktoren vertraut ist.

(3.1) Definition:
Ist C eine Kategorie, so bezeichnen wir mit $\mathfrak{Ob}\, C$ die Klasse der Objekte von C und mit $\mathfrak{Mor}\, C$ die Klasse der Morphismen von C.

Für uns sind in diesem Kapitel vor allem die Modulkategorien von Bedeutung, weshalb wir für diese besondere Kurzschreibweisen einführen wollen. Wir bezeichnen mit

$$ {}_A\mathfrak{mod}, \quad \mathfrak{mod}_B \quad \text{bzw.} \quad {}_A\mathfrak{mod}_B $$

die Kategorien der endlich erzeugten A-Links-, B-Rechts- bzw. $A-B$-Bimoduln. ■

§ 3.1.1. Äquivalenz von Kategoriern und Morita-Äquivalenz

(3.2) Definition:
(a) Die Kategorien C und $\mathcal{D}$ heißen äquivalent, falls kovariante Funktoren $C \xrightarrow{\mathcal{F}} \mathcal{D}$ und $C \xleftarrow{\mathcal{G}} \mathcal{D}$ existieren, so dass $\mathcal{F} \circ \mathcal{G} \simeq \mathrm{id}_{\mathcal{D}}$ und $\mathcal{G} \circ \mathcal{F} \simeq \mathrm{id}_C$ sind. In diesem Zusammenhang nennt man F bzw. G auch Äquivalenzen.
(b) Sind speziell die Kategorien $\mathfrak{mod}_A$ und $\mathfrak{mod}_B$ äquivalent, so heißen die F-Algebren A und B ***Morita-äquivalent****.* ■

In der folgenden Proposition wollen wir einige Eigenschaften aufsammeln, die bei Moritaäquivalenten Algebren durch die Äquivalenz auf den Modulkategorien erhalten bleiben.

(3.3) Proposition:
Es seien A und B Morita-äquivalent vermöge des Funktors $\mathfrak{mod}_A \xrightarrow{\mathcal{F}} \mathfrak{mod}_B$ und es seien $U, V, W \in \mathfrak{Ob}\, \mathfrak{mod}_A$.

(i) *Die Sequenz*

$$0 \longrightarrow U \xrightarrow{\iota} V \xrightarrow{\pi} W \longrightarrow 0$$

ist genau dann (split-) kurzexakt in $\mathfrak{mod}_A$*, wenn die Sequenz*

$$0 \longrightarrow \mathcal{F}(U) \xrightarrow{\mathcal{F}(\iota)} \mathcal{F}(V) \xrightarrow{\mathcal{F}(\pi)} \mathcal{F}(W) \longrightarrow 0$$

(split-) kurzexakt in $\mathfrak{mod}_B$ *ist.*

(ii) *Der Untermodulverband von* V *ist isomorph zum Untermodulverband von* $\mathcal{F}(V)$.

(iii) V *ist genau dann projektiv, wenn es* $\mathcal{F}(V)$ *ist.*

(iv) V *ist genau dann einfach, wenn es* $\mathcal{F}(V)$ *ist.*

(v) V *ist genau dann unzerlegbar, wenn es* $\mathcal{F}(V)$ *ist.*

(vi) *Die Zentren* $\mathrm{Z}(A)$ *und* $\mathrm{Z}(B)$ *sind isomorphe Ringe.*

Beweis: Siehe [AF74, Abschnitt §21] oder [Noe05, Kapitel II, Proposition (1.2) und (1.3)] ■

(3.4) Korollar:
Sind A *und* B *Morita-äquivalent, so stehen die Isomorphieklassen einfacher* A*- und* B*-Moduln in Bijektion.*

Beweis: Folgt sofort aus (3.3)(iv). ■

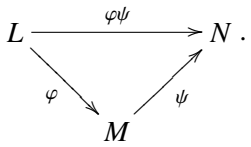
§ 3.1.2. Hom- und ⊗-Funktoren

In diesem Unterabschnitt wollen wir den ko- und kontravarianten Hom-Funktor, sowie die beiden kovarianten ⊗-Funktoren definieren und ein paar Eigenschaften aufführen die für den Unterabschnitt § 3.1.3 und den Paragraphen § 3.2 hilfreich sind. Wir halten uns dabei im Wesentlichen an die Ausführungen in [Hen96, 1.2.1].

(3.5) Bemerkung:
Für Morphismen in den Modulkategorien benutzen wir die Rechtsschreibweise. Das bedeutet, für Morphismen $L \xrightarrow{\varphi} M$, $M \xrightarrow{\psi} N$ *in einer (beliebigen) Modulkategorie und* $l \in L$ *schreiben wir*

$$l\varphi$$

für das Bild von l *unter* φ*. Weiter schreiben wir für die Komposition von* φ *und* ψ*:*



■

Im Folgenden seien $M \in \mathfrak{Ob}\,{}_B\mathfrak{mod}_A$, $N \in \mathfrak{Ob}\,{}_A\mathfrak{mod}_B$ und V trage die jeweils durch den Index angedeutete A-Modulstruktur. Weiter seien $m \in M$, $n \in N$, $v \in V$ und $b_1, b_2, b \in B$.

(3.6) Bemerkung:

Die Menge $\mathrm{Hom}_A(M, V_A)$ *ist eine abelsche Gruppe. Auf ihr lässt sich eine B-Rechtsmodulstruktur definieren:*

$$m(\varphi \cdot b) := bm\varphi.$$

Wir verifizieren hier kurz, dass diese Setzung wirklich eine Operation definiert. Hierfür rechnen wir:

$$m(\varphi \cdot b_1) \cdot b_2 = b_2 m\varphi \cdot b_1 = b_1 b_2 m\varphi = m\varphi \cdot (b_1 b_2). \tag{3.6.1}$$

Analog können wir auf den abelschen Gruppen $\mathrm{Hom}_A(V_A, M)$, $\mathrm{Hom}_A(N, {}_AV)$ *und* $\mathrm{Hom}_A({}_AV, N)$ *eine B-Modulstruktur definieren. Ob es sich dabei um eine Links- oder Rechtsmodulstruktur handelt muss man ähnlich zu (3.6.1) nachrechnen.*

Die abelsche Gruppe $V_A \otimes_A N$ wird zu einem B-Rechtsmodul durch:

$$(v \otimes n) \cdot b = v \otimes nb.$$

Entsprechend wir die abelsche Gruppe $M \otimes_A {}_AV$ zu einem B-Linksmodul.

Seien $V, W \in \mathfrak{Ob}\,\mathfrak{mod}_A$ und $\alpha \in \mathrm{Hom}_A(V, W)$. Mit den obigen Modulstrukturen definieren wir folgende B-Homomorphismen:

$$\begin{aligned} \alpha_* &:= \mathrm{Hom}_A(M, \alpha) : \mathrm{Hom}_A(M, V) \to \mathrm{Hom}_A(M, W) \;;\; \varphi \mapsto \varphi\alpha \\ \alpha^* &:= \mathrm{Hom}_A(\alpha, N) : \mathrm{Hom}_A(W, N) \to \mathrm{Hom}_A(V, N) \;;\; \varphi \mapsto \alpha\varphi, \end{aligned}$$

und

$$\begin{aligned} \alpha_* &:= \alpha \otimes N : V \otimes_A N \to W \otimes_A N \,;\, v \otimes n \mapsto v\alpha \otimes n \\ \alpha^* &:= M \otimes \alpha : M \otimes_A V \to M \otimes_A W \,;\, m \otimes v \mapsto m \otimes (v\alpha). \end{aligned}$$

Analog definieren wir die Abbildungen, falls V und W jeweils A-Linksmoduln sind. ■

(3.7) Definition:

Mit den Setzungen aus (3.6) definieren wir die folgenden Funktoren:

$\mathfrak{mod}_A \xrightarrow{\mathrm{Hom}_A(M,=)} \mathfrak{mod}_B$ *ist der kovariante* Hom*-Funktor.*

$\mathfrak{mod}_A \xrightarrow{-\otimes_A N} \mathfrak{mod}_B$ *ist der (in der ersten Variable) kovariante $\otimes$-Funktor.*

$\mathfrak{mod}_A \xrightarrow{\mathrm{Hom}_A(-,N)} {}_B\mathfrak{mod}$ *ist der kontravariante* Hom*-Funktor.*

$\mathfrak{mod}_A \xrightarrow{M\otimes_A =} {}_B\mathfrak{mod}$ *ist der (in der zweiten Variable) kovariante $\otimes$-Funktor.* ■

Wann ein Funktor linksexakt, rechtsexakt oder exakt ist entnehmen wir [Hen96, 1.2.1, Definition 1.11].

(3.8) Satz:

Die Hom*-Funktoren sind linksexakt, die $\otimes$-Funktoren sind rechtsexakt.*

Beweis: Vergleiche [CR90, Seite 21, Proposition (2.8) und Seite 26, Proposition (2.20)]. ■

§ 3.1.3. Duale und kontragrediente Moduln

Auch in diesem Unterabschnitt orientieren wir uns an [Hen96, 1.2.2]. Es gilt immer noch, dass F ein Körper und A und B endlich-dimensionale F-Algebren sind. Weiter ist G eine endliche Gruppe.

(3.9) Definition:

(a) *Der kontravariante Funktor* $\mathrm{Hom}_F(-,F) : \mathfrak{mod}_F \to {}_F\mathfrak{mod}$ *lässt sich durch die in Bemerkung (3.6) definierte A-Operation zu einem kontravarianten Funktor* $\mathcal{D}$ *von* $\mathfrak{mod}_A \to {}_A\mathfrak{mod}$ *fortsetzen:* $\mathcal{D}(V_A) = \mathrm{Hom}_F(V_A, F)$, $\mathcal{D}(\alpha) = \alpha^*$. *Dieser Funktor heißt* ***Funktor des Dualisierens****, der Modul* $V^* := \mathcal{D}(V)$ *heißt der zu* V ***duale Modul****.*

(b) *Sei* $\sigma : B \to A$ *ein* F*-Algebrenantihomomorphismus. Ordnen wir jedem* A*-Linksmodul* M *den* B*-Rechtsmodul* M *mit der Operation* $m \cdot b := \sigma(b) \cdot m$ *zu und lassen die Morphismen invariant, so definiert dies einen kovarianten Funktor* $\Sigma : {}_A\mathfrak{mod} \to \mathfrak{mod}_B$.
Sei $\sigma : B \to A$ *ein* F*-Algebrenhomomorphismus. Ordnen wir jedem* A*-Rechtsmodul* M *den* B*-Rechtsmodul* M *mit der Operation* $m \cdot b := m \cdot \sigma(b)$ *zu und lassen die Morphismen invariant, so definiert dies einen kovarianten Funktor* $\mathfrak{mod}_A \to \mathfrak{mod}_B$ *den wir ebenfalls mit* Σ *bezeichnen.*
Analog sind die beiden verbliebenen Fälle definiert. ■

(3.10) Satz:

Die kontravarianten Funktoren $\mathcal{D} \circ \Sigma$ *und* $\Sigma \circ \mathcal{D}$ *sind gleich.*

Beweis: Siehe [Jan95] Seite 33, Satz (1.56). ■

(3.11) Definition & Bemerkung:

(a) *Sei* $A = B = FG$, $g \in G$ *und sei* σ *die lineare Fortsetzung von* $g \mapsto g^{-1}$ *auf* FG. *Dann ist* σ *ein Algebrenantihomomorphismus. Der kontravariante Funktor* $\mathcal{K} := \Sigma \circ \mathcal{D} : \mathfrak{mod}_{FG} \to \mathfrak{mod}_{FG}$ *heißt* ***Kontragredienzfunktor****. Ist* V *ein* FG*-Modul, so heißt* $\mathcal{K}(V) =: V^*$ *der zu* V ***kontragrediente Modul*** *(vgl. (1.62)(c)).*

(b) *Ist* V *ein* FG*-Modul, so ist mit* V^* *stets der kontragrediente Modul gemeint, auch wenn dieser häufig als dualer Modul bezeichnet wird.* ■

(3.12) Korollar:

Die Funktoren $\mathcal{D} : \mathfrak{mod}_A \to {}_A\mathfrak{mod}$ *und* $\mathcal{K} : \mathfrak{mod}_{FG} \to \mathfrak{mod}_{FG}$ *sind linksexakt.*

Beweis: Folgt direkt aus Satz (3.8). ■

(3.13) Definition:

Sei V *ein* A*-Modul. Die Summe aller einfachen Teilmoduln von* V *heißt der* ***Sockel*** *von* V, *geschrieben* $\mathrm{Soc}(V)$ *oder auch* $\mathrm{Soc}_A(V)$, *wenn wir die Algebra, bezüglich der* V *definiert ist, angeben wollen. Sei* N *der kleinste Teilmodul, so dass der Faktormodul* V/N *halbeinfach ist. Dann bezeichnen wir* V/N *als* ***Kopf*** *des Moduls* V *und* $\mathrm{Rad}(V) := N$ *als* ***Radikal*** *von* V. ■

(3.14) Bemerkung:

Der Modul $\mathrm{Rad}(V)$ *ist als Schnitt aller maximalen Untermoduln von* V *eindeutig bestimmt.* ■

(3.15) Satz:
Seien V und W jeweils FG-Moduln. Es gelten die folgenden FG-Modulisomorphismen:

(a) $V \simeq (V^*)^*$.
(b) $(V \oplus W)^* \simeq V^* \oplus W^*$.
(c) $(V \otimes_F W)^* \simeq V^* \otimes_F W^*$.

Beweis: Vergleiche [Alp93], Seite 39. ■

(3.16) Korollar:
Sei V ein FG-Modul.

(a) Ist W ein FG-Untermodul von V, so hat V^* einen Untermodul, der natürlich isomorph zu $\left(V/W\right)^*$ ist.
(b) Ist V einfach, so auch V^*.
(c) $\mathrm{Soc}(V^*) \simeq \left(V/\mathrm{Rad}(V)\right)^*$.
(d) $V^*/\mathrm{Rad}(V^*) \simeq \mathrm{Soc}(V)^*$.

Beweis: Vergleiche [Alp93], Seite 40. ■

§ 3.2. Einführung in die Technik der Kondensation

In diesem Abschnitt wollen wir die theoretischen Grundlagen der Kondensation legen. Für die praktische Umsetzung sei beispielsweise auf den Artikel [Ryb90] verwiesen, in dem anhand des n-fachen äußeren Produkts beschrieben wird, wie diese Technik angewendet werden muss.

Idealerweise liefert Kondensation eine Morita-Äquivalenz einer F-Algebra A und einer Teilmenge von A, die eine F-Algebra mit nicht notwendig der selben 1 bildet, wobei die F-Dimension des kondensierten A-Moduls deutlich kleiner ist als die F-Dimension des Ursprünglichen A-Moduls. Wir werden beschreiben, wann dies der Fall ist, und was wir noch tun können, wenn die Kondensation keine Morita-Äquivalenz liefert.

Wir orientieren uns in diesem Abschnitt wieder an den Arbeiten [Noe05] und [Hen96]. Des weiteren sei F ein Körper, A eine endlich-dimensionale F-Algebra, $e \in A$ ein Idempotent, G eine endliche Gruppe und es seien alle A-Moduln endlich erzeugt.

§ 3.2.1. Der Kondensier- und Entkondensierfunktor

(3.17) Definition & Bemerkung:

(a) *Die durch die zueinander orthogonalen Idempotente e und $1-e$ induzierte Zerlegung der Algebra A in eine direkte Summe von F-Vektorräumen:*

$$A = eAe \oplus eA(1-e) \oplus (1-e)Ae \oplus (1-e)A(1-e)$$

heißt ***Pierce-Zerlegung****. Der Summand eAe der Pierce-Zerlegung ist selbst wieder eine Algebra mit Einselement e.*

(b) *Die endlich-dimensionale F-Algebra eAe heißt* ***Hecke Algebra*** *zu e oder auch die* ***zu*** *e* ***gehörende kondensierte Algebra****.*

(c) *Ebenso induziert das Idempotent e die Zerlegung eines beliebigen A-Moduls V in eine direkte Summe von F-Vektorräumen $V = Ve \oplus V(1-e)$. Offensichtlich ist Ve ein eAe-Modul.* ■

Die Überlegung von (3.17)(c) wollen wir nun formalisieren.

(3.18) Definition:

Seien $V, W \in \mathfrak{mod}_A$ und $\alpha \in \mathrm{Hom}_A(V, W)$. Wir definieren den zu e gehörenden ***Kondensationsfunktor*** $\mathrm{cond}^A_{eAe}(-) : \mathfrak{mod}_A \to \mathfrak{mod}_{eAe}$ *durch:*

$$\begin{aligned} \mathrm{cond}^A_{eAe}(-) : V &\mapsto Ve, \\ \alpha &\mapsto \alpha|_{Ve}. \end{aligned}$$

Der aus V resultierende eAe-Modul Ve wird als ***kondensierter Modul*** *bezeichnet. Völlig analog definieren wir den Kondensationsfunktor für Linksmoduln, wobei wir auch diesen Funktor mit $\mathrm{cond}^A_{eAe}(-)$ bezeichnen.* ■

Nun wollen wir uns den Kondensationsfunktor etwas genauer ansehen und einige seiner Eigenschaften untersuchen. Als erstes werden wir zeigen, dass der Funktor exakt ist:

(3.19) Lemma:

Die eAe-Moduln $\mathrm{Hom}_A(eA, V)$ und Ve sind isomorph via der Abbildung $\tau_V : \varphi \mapsto e\varphi$. Die eAe-Moduln Ve und $V \otimes_A Ae$ sind isomorph via der Abbildung $\tau'_V : ve \mapsto v \otimes e$

Beweis: Siehe [Hen96, Lemma 2.11]. ■

(3.20) Satz:

Die kovarianten Funktoren $\mathrm{Hom}_A(eA, -)$, $- \otimes_A Ae$ und $\mathrm{cond}^A_{eAe}(-)$ sind natürlich äquivalente Funktoren von der Kategorie $\mathfrak{mod}_A$ in die Kategorie $\mathfrak{mod}_{eAe}$.

Beweis: Seien $V, W \in \mathfrak{mod}_A$ und $\alpha \in \mathrm{Hom}_A(V, W)$. Mit den Isomorphismen τ_V und τ_W aus (3.19) erhalten wir:

Das Diagramm

$$\begin{array}{ccc} \mathrm{Hom}_A(eA, V) & \xrightarrow{\tau_V} & Ve \\ \downarrow{\scriptstyle \alpha_*} & & \downarrow{\scriptstyle \alpha|_{Ve}} \\ \mathrm{Hom}_A(eA, W) & \xrightarrow{\tau_W} & We \end{array}$$

kommutiert wegen $\varphi(\tau_V\alpha|_{Ve}) = \varphi\tau_V\alpha|_{Ve} = e\varphi\alpha|_{Ve} = e\varphi\alpha = e(\varphi\alpha) = \varphi\alpha\tau_W = \varphi\alpha_*\tau_W = \varphi(\alpha_*\tau_W)$. Folglich realisieren die durch die Objekte von $\mathfrak{mod}_A$ indizierten Isomorphismen τ eine natürliche Äquivalenz der Funktoren $\mathrm{Hom}_A(eA, -)$ und $\mathrm{cond}^A_{eAe}(-)$.
Das Diagramm

$$\begin{array}{ccc} Ve & \xrightarrow{\tau'_V} & V \otimes_A Ae \\ \downarrow{\scriptstyle \alpha|_{Ve}} & & \downarrow{\scriptstyle \alpha_*} \\ We & \xrightarrow{\tau'_W} & W \otimes_A Ae \end{array}$$

kommutiert wegen $(ve)(\tau'_V\alpha_*) = (ve)\tau'_V\alpha_* = (v \otimes e)\alpha_* = v\alpha \otimes e = (v\alpha e)\tau'_W = (ve)\alpha\tau'_W = (ve)(\alpha|_{Ve}\tau'_W)$. Somit realisieren die durch die Objekte von $\mathfrak{mod}_A$ indizierten Isomorphismen τ' eine natürliche Äquivalenz der Funktoren $\mathrm{cond}^A_{eAe}(-)$ und $- \otimes_A Ae$. ■

(3.21) Korollar:
Der Funktor $\mathrm{cond}^A_{eAe}(-)$ *ist exakt.*

Beweis: Da der Kondensationsfunktor sowohl zu einem Tensorproduktfunktor als auch zu einem Homfunktor natürlich äquivalent ist, ist dieser Funktor nach (3.8) exakt. ■

Als nächstes wollen wir untersuchen, wie sich das Dualisieren mit dem Kondensieren verträgt:

(3.22) Lemma:
Sei V ein A-Rechtsmodul und V^* der dazu duale Modul. Es gilt der folgende eAe-Linksmodulisomorphismus $\delta_V : e(V^*) \to (Ve)^* ; \lambda \mapsto \lambda|_{Ve}$

Beweis: Siehe [Jan95, Seite 32, Lemma (1.53)]. ■

(3.23) Satz:
Die kontravarianten Funktoren $\mathrm{cond}^A_{eAe} \circ \mathcal{D}$ *und* $\mathcal{D} \circ \mathrm{cond}^A_{eAe}$ *von* $\mathfrak{mod}_A$ *nach* ${}_{eAe}\mathfrak{mod}$ *sind natürlich äquivalent. Die Äquivalenz wird von den Isomorphismen δ aus Lemma (3.22) realisiert.*

Beweis: Siehe [Jan95, Seite 33, Lemma (1.54)]. ■

Sei $\sigma : B \to A$ ein F-Algebren(anti)homomorphismus und $f \in B$ ein Idempotent. Dann ist, falls $\sigma(f) \neq 0$ ist, $\sigma(f) = e \in A$ ein Idempotent und $\sigma(fBf) \subseteq eAe$. Sei Σ der durch σ definierte Funktor (vgl. Definition (3.9)(b)).

(3.24) Satz:
Ist σ ein Homomorphismus, so sind die Funktoren $\mathrm{cond}^B_{fBf} \circ \Sigma$ und $\Sigma \circ \mathrm{cond}^A_{eAe}$ von $\mathfrak{mod}_A$ nach ${}_{fBf}\mathfrak{mod}$ gleich. Ist σ ein Antihomomorphismus, so sind die Funktoren $\mathrm{cond}^B_{fBf} \circ \Sigma$ und $\Sigma \circ \mathrm{cond}^A_{eAe}$ von $\mathfrak{mod}_A$ nach $\mathfrak{mod}_{fBf}$ gleich.
Ist $A = B = FG$ und gilt $\sigma(e) = e$, so sind die Funktoren $\mathrm{cond}^A_{eAe} \circ \mathcal{K}$ und $\mathcal{K} \circ \mathrm{cond}^A_{eAe}$ äquivalent.

Beweis: Für die erste Behauptung vergleiche [Jan95, Seite 34, Lemma (1.57)]. Die zweite Behauptung folgt mit Satz (3.10) aus der ersten. ■

Nachdem wir nun einige Eigenschaften des Kondensationsfunktors auf Ebene der Kategorientheorie angesehen haben, wollen wir sehen was dies für die Moduln bedeutet, auf die dieser angewandt wird.

(3.25) Lemma:
Sei V ein A-Modul, W ein A-Untermodul von V und X ein eAe-Untermodul von Ve. Dann gilt:

(a) We ist ein eAe-Untermodul von Ve, der Modul $\left(V/W\right)e$ ist als eAe-Modul isomorph zum Faktormodul Ve/We.
(b) Es existiert ein A-Untermodul W von V mit $X = We$.
(c) Ist V einfach, so ist Ve ein einfacher eAe-Modul oder $Ve = \{0\}$.

Beweis: (a) Diese Behauptung folgt aus Korollar (3.21).
(b) Vgl. [Ryb90, Lemma 3]. Sei W der A-Teilmodul von V, der durch die Vektoren von XA gegeben ist. Wir beachten dass e auf Ve (und somit auch auf X) wie die Identität operiert. Wir erhalten zum einen: $X = Xe \leqslant XAe = We$. Und zum anderen: $X \geqslant XeAe = We$. Damit ist $X = We$.
(c) Es sei $0 \neq v \in Ve$. Dann erhalten wir $veAe = vAe = Ve$, da V einfach ist. Damit ist auch Ve einfach. ■

Damit erhalten wir den folgenden Satz:

(3.26) Satz:
Sei V ein A-Modul mit Kompositionsreihe $\{0\} = V_0 < V_1 < \ldots < V_n = V$. Dann existiert eine Folge von Zahlen $0 \leqslant i_0 < i_1 < \ldots < i_m \leqslant n$ so, dass $\{0\} = V_{i_0}e < V_{i_1}e < \ldots < V_{i_m}e = Ve$ eine Kompositionsreihe des Moduls Ve ist.
Ist umgekehrt $\{0\} = W_0 < W_1 < \ldots < W_n = Ve$ eine Kompositionsreihe des Moduls Ve, so existiert eine Kompositionsreihe von V der Form $\{0\} = V_{01} < V_{02} < \ldots < V_{0r_0} < V_{11} < \ldots < V_{mr_m} = V$, wobei die Moduln $V_{ir_i}e$ gleich dem Modul W_i sind, $1 \leqslant i \leqslant m$. ■

(3.27) Korollar:
Sei $\{S_1, \ldots, S_n\}$ ein Repräsentantensystem einfacher A-Moduln. Dann ist $\{S_ie \mid S_ie \neq \{0\}\}$ ein Repräsentantensystem einfacher eAe-Moduln. Insbesondere gilt: Sind S und S' zwei einfache, nicht isomorphe A-Moduln, dann ist $Se = S'e = \{0\}$ oder $Se \neq S'e$.

Beweis: Siehe [Hen96, Korollar 2.19]. ■

Bis jetzt haben wir uns mit der Möglichkeit beschäftigt, dass wir aus einem A-Modul einen eAe-Modul machen. Nun wollen wir uns mit einem Funktor auseinander setzen, der aus einem eAe-Modul einen A-Modul macht.

(3.28) Definition:
Wir wollen den Tensorfunktor $- \otimes_{eAe} eA : \mathrm{mod}_{eAe} \to \mathrm{mod}_A$ *als* ***Entkondensationsfunktor*** *bezeichnen und ihn als* $\mathrm{uncond}^A_{eAe}(-)$ *schreiben.* ■

Die folgende Bemerkung zeigt uns, dass diese Definition vernünftig ist:

(3.29) Bemerkung:
Ist A eine F-Algebra und e ein Idempotent, dann ist $eA \otimes_A Ae \simeq eAe$ als $eAe - eAe$-Bimodul. Folglich ist $(- \otimes_A Ae) \circ (- \otimes_{eAe} eA) = \mathrm{cond}^A_{eAe} \circ \mathrm{uncond}^A_{eAe}$ *natürlich äquivalent zum Identitätsfunktor* $\mathrm{id}_{\mathrm{mod}_{eAe}}$. ■

Diese Bemerkung lässt uns auf die Idee kommen, dass möglicherweise auch $\mathrm{uncond}^A_{eAe} \circ \mathrm{cond}^A_{eAe}$ natürlich äquivalent zum Identiätsfunktor $\mathrm{id}_{\mathrm{mod}_A}$ ist. Dies würde bedeuten, dass die Funktoren cond^A_{eAe} und uncond^A_{eAe} eine Morita-Äquivalenz zwischen A und eAe induzieren. Im nachfolgenden Unterabschnitt wollen wir die Voraussetzungen diskutieren, die eine solche Morita-Äquivalenz garantieren.

§ 3.2.2. Treue und nicht treue Idempotente

Wie im vorangegangenen Unterabschnitt angedeutet, wollen wir hier Bedingungen an das Idempotent e stellen, so dass der Kondensationsfunktor eine Morita-Äquivalenz ist.

(3.30) Satz:
Es sei $e \in A$ ein Idempotent und $e_1A, \ldots, e_rA$ Repräsentanten der Isomorphieklassen der projektiv unzerlegbaren Moduln von A. Weiter seien $S_1, \ldots, S_r$ Repräsentanten der Isomorphieklassen einfacher A-Moduln, sodass $e_iA/\mathrm{Rad}(e_iA) \simeq S_i$ *ist. Dann sind die folgenden Aussagen äquivalent:*

(a) Die Funktoren $\mathrm{cond}^A_{eAe}(-)$ *und* $\mathrm{uncond}^A_{eAe}(-)$ *induzieren eine Morita-Äquivalenz zwischen den Algebren A und eAe.*
(b) Es ist $AeA = A$.
(c) Für alle $1 \leqslant i \leqslant r$ ist der A-Modul e_iA ein direkter Summand von eA.
(d) Es ist $S_ie \neq \{0\}$ für alle $1 \leqslant i \leqslant r$.

Beweis: Siehe [Noe05, Kapitel II, Satz (2.3)]. ■

(3.31) Definition:
Es sei A eine F-Algebra und $e \in A$ ein Idempotent. Erfüllt e eine der Bedingungen von (3.30), so nennen wir e ein ***treues Idempotent*** *von A.* ■

(3.32) Korollar:
Es sei e ein treues Idempotent von A und V ein A-Modul. Dann ist $\mathrm{uncond}^A_{eAe}(Ve) = Ve \otimes_{eAe} eA$ isomorph zu $V = VeA$ als A-Modul.

Beweis: Da e treu ist, ist der Funktor $\mathcal{F} := \mathrm{uncond}^A_{eAe} \circ \mathrm{cond}^A_{eAe}$ natürlich äquivalent zum Identitätsfunktor $\mathrm{id}_{\mathtt{mod}_A}$. Da V somit isomorph zu $\mathcal{F}(V)$ ist, können wir unmittelbar folgern, dass V auch isomorph zu $\mathrm{uncond}^A_{eAe}(Ve) = Ve \otimes_{eAe} eA$ ist. Aus der Treue von e folgt mit Satz (3.30)(b) weiter, dass $V = VA = VAeA = VeA$ ist. ■

Als nächstes wollen wir uns fragen, was passiert, wenn wir einen einfachen eAe-Modul entkondensieren, falls e nicht treu ist. Wir beginnen mit einer Definition.

(3.33) Definition:
Für einen A-Modul V bezeichnen wir mit $V_{(e)}$ die Summe aller Untermoduln von V, die von e annulliert werden, d.h. $V_{(e)}$ ist der größte A-Untermodul von V, der in $V(1-e)$ liegt. ■

(3.34) Proposition:
Es sei W ein einfacher eAe-Modul. Dann ist $\mathrm{uncond}^A_{eAe}(W)_{(e)}$ der eindeutige maximale Untermodul von $\mathrm{uncond}^A_{eAe}(W)$ und der Faktormodul $\mathrm{uncond}^A_{eAe}(W)\Big/\mathrm{uncond}^A_{eAe}(W)_{(e)}$ ein einfacher A-Modul. Insbesondere ist jeder einfache eAe-Modul der kondensierte eines einfachen A-Moduls.

Beweis: Es stehe V für $\mathrm{uncond}^A_{eAe}(W)$. Der Modul $V_{(e)}$ ist ein echter Untermodul von V, denn es ist $\left(V\Big/V_{(e)}\right)e \simeq W$ nach (3.25)(a) und (3.29), und W ist nicht der Nullmodul. Es sei $V' \lneqq V$ ein echter Untermodul. Ist $V'e \neq 0$, so ist $V'e = Ve$, da $V'e \leqslant Ve \simeq W$ und W einfach ist. Folglich erhalten wir $V' \supseteq V'eA = VeA = W \otimes_{eAe} eA$, was ein Widerspruch zur Wahl von V' ist. Also ist $V'e = 0$ und damit liegt V' in $V_{(e)}$. Damit ist gezeigt, dass der Untermodul $V_{(e)}$ der eindeutig maximale Untermodul von V ist. Setzen wir $U := V\Big/V_{(e)}$, so erhalten wir mit U einen einfachen A-Modul mit $Ue = W$. ■

Die nun folgende Proposition liefert uns: Faktorisieren wir nach erfolgter Entkondensation eines einfachen eAe-Moduls den maximalen Untermodul heraus, so erhalten wir den ursprünglichen Modul.

(3.35) Proposition:
Es sei V ein einfacher A-Modul mit $Ve \neq 0$. Dann ist $\mathrm{uncond}^A_{eAe}(Ve)\Big/\mathrm{uncond}^A_{eAe}(Ve)_{(e)}$ isomorph zu V.

Beweis: Wir definieren einen A-Modulhomomorphismus $\varphi : Ve \otimes_{eAe} eA \to V$ über $ve \otimes a \mapsto vea$ für alle $v \in V$ und $a \in A$. Das Bild von φ ist $VeA = V$, da nach Voraussetzung $Ve \neq 0$ und V einfach ist. Folglich ist der Kern von φ ein maximaler Untermodul von $\mathrm{uncond}^A_{eAe}(Ve)$. Da dieser nach Proposition (3.34) eindeutig ist, ist $\mathrm{Kern}\,\varphi = \mathrm{uncond}^A_{eAe}(Ve)_{(e)}$, woraus die Behauptung folgt. ■

(3.36) Korollar:
Sind V und V' zwei einfache A-Moduln, die nicht zum Nullmodul kondensieren, so ist $Ve \simeq V'e$ genau dann, wenn $V \simeq V'$.

Beweis: Dies folgt aus den beiden vorangegangenen Propositionen. ■

§ 3.2.3. Einige praktische Überlegungen

In diesem Unterabschnitt wollen wir unsere Überlegungen für eine beliebige e.e. F-Algebra A auf die F-Algebra FG anwenden, wobei F ein endlicher Körper und G eine endliche Gruppe ist. Wir wollen diskutieren, wie wir an das Idempotent kommen, mit dem wir kondensieren wollen. Außerdem wollen wir darauf hinweisen, wie wir an ein F-Algebren-Erzeugendensystem von $eFGe$ kommen.

(3.37) Definition & Bemerkung:
Sei K eine Untergruppe von G, deren Ordnung nicht von der Charakteristik der Körpers F geteilt wird. Dann wird durch

$$e := e_K := |K|^{-1} \sum_{k \in K} k$$

ein Idempotent von FG definiert. In diesem Zusammenhang nennen wir K ***Kondensationsuntergruppe****.* ■

(3.38) Korollar:
Sei α ein Gruppenisomorphismus von G und sei K eine Kondensationsuntergruppe von G mit $K^\alpha = K$. Sei $\sigma : FG \to FG$ die lineare Fortsetzung von α. Dann vertauscht der Funktor Σ (vgl. (3.9)(b)) mit dem Funktor cond^A_{eAe}.

Beweis: Da $\alpha(K) = K$ ist, ist $\sigma(e) = e$. Mit Satz (3.24) folgt nun die Behauptung. ■

Als nächstes geben wir ein nützliches Kriterium an, um ein durch die Kondensationsuntergruppe definiertes Idempotent auf Treue zu testen. Die Definition eines Brauercharakters, der Menge der irreduziblen Brauercharaktere der Gruppe G über dem Körper F, kurz $\mathrm{IBr}_F(G)$, eines Zerfällungskörpers, der Restriktion eines Brauercharakters auf eine Untergruppe und des Standardskalarprodukts auf $\mathrm{IBr}_F(G)$ entnimmt man seinem Lieblingswerk zur Charaktertheorie - beispielsweise [CR90].

(3.39) Proposition:
Sei K eine Kondensationsuntergruppe von G, e_K das durch K definierte Idempotent, F ein Zerfällungskörper für FK und V ein einfacher FG-Modul, der den Brauercharakter φ bewirkt. Sei $[\![\cdot,\cdot]\!]_K$ das Standardskalarprodukt auf $\mathrm{IBr}_F(K)$. Dann gilt

$$\dim_F Ve_K = [\![1_K, \varphi\downarrow_K]\!]_K.$$

Beweis: Siehe [Noe05, Kapitel III, Proposition (1.2)]. ■

(3.40) Korollar:
Es sei $e \in FG$ ein Idempotent wie in (3.37). Die Funktoren $\mathrm{cond}_{eFGe}^{FG}$ und $\mathrm{uncond}_{eFGe}^{FG}$ induzieren genau dann eine Morita-Äquivalenz zwischen den Algebren FG und e_KFGe_K, wenn für alle Brauercharaktere $\varphi \in \mathrm{IBr}_F(G)$ das Skalarprodukt $[\![1_K, \varphi\downarrow_K]\!]_K$ nicht Null ist.

Beweis: Aus Satz (3.30) wissen wir, dass die Kondensier- und Entkondensierfunktoren genau dann eine Morita-Äquivalenz zwischen den Algebren induzieren, wenn alle einfachen FG-Moduln nicht zum Nullmodul kondensieren. Ein FG-Modul, der nicht der Nullmodul ist, hat eine F-Dimension ungleich Null. Somit liefert Proposition (3.39) die Behauptung. ■

(3.41) Lemma:
Es ist $Ve = \mathrm{Fix}_K(V)$ der Fixraum von V unter der Operation von K.

Beweis: Siehe [Hen96, Lemma 2.31]. ■

Als nächstes wollen wir auf das sogenannte **Erzeugnisproblem** der Algebra $eFGe$ hinweisen.

(3.42) Proposition:
*Sei $\{g_1, \ldots, g_k\}$ ein Erzeugendensystem der Gruppe G und $e \in FG$ ein Idempotent. Dann heißt das F-Algebrenerzeugnis $\mathcal{C} := F\langle eg_1e, \ldots, eg_ke\rangle$ **Kondensationsalgebra**.* ■

(3.43) Bemerkung (Erzeugnisproblem):
Die Kondensationsalgebra $\mathcal{C}$ ist im Allgemeinen lediglich eine echte Teilalgebra der kondensierten Algebra $eFGe$. ■

Mit diesem Problem können wir nun auf verschiedene Arten umgehen. Beispielsweise hat Christoph Jansen das Problem in [Jan95, Abschnitt 1.3.5] dadurch gelöst (oder besser gesagt umgangen), indem er zeigte, wie nachgerechet werden kann dass ein $\mathcal{C}$-Modul auch ein $eFGe$-Modul ist.

Einen anderen Zugang wählte Markus Wiegelmann in [Wie94], wo er ein Kriterium dafür angab, wann für eine Teilmenge $X \subseteq G$ gilt, dass $F\langle exe \mid \forall x \in X\rangle$ gleich $eFGe$ ist.

Einen ähnlichen Zugang wählte auch Felix Noeske in seiner Dissertation [Noe05], in der er eine Konstruktion beschreibt, die eine Teilmenge $X \subseteq G$ liefert, so dass $F\langle exe \mid \forall x \in X\rangle$ gleich $eFGe$ ist.

§ 3.3. Anwendbarkeit der Kondensation auf unsere Probleme

In diesem Paragraphen wollen wir untersuchen, ob der Frobenius-Schur-Indikator eines einfachen FG-Moduls bereits mittels des kondensierten Moduls bestimmt werden kann. Hierfür müssen wir dieses Problem in die folgenden Teilprobleme zerlegen:

1. Können wir aus der Selbstdualität des kondensierten Moduls auf die Selbstdualität des ursprünglichen Moduls schließen?

2. Können wir aus der Tatsache, dass der kondensierte Modul eine mit der „Operation von $eFGe$ verträgliche“ reguläre quadratische Form trägt schließen, dass auch der ursprüngliche Modul eine G-invariante reguläre quadratische Form trägt?

In diesem Abschnitt gilt: F ist ein endlicher Körper der Charakteristik $p > 0$ und G eine Gruppe, deren Ordnung durch p und durch wenigstens eine weitere Primzahl teilbar ist (anderenfalls macht die Benutzung der Kondensation wenig Sinn). Weiter sei $e \in FG$ Idempotent, das unter der Abbildung $\sigma : FG \to FG ; \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g g^{-1}$ invariant bleibt; d.h $\sigma(e) = e$. Schließlich sei V ein einfacher FG-Rechtsmodul, der nicht zu Null kondensiert. Weiterhin sei F groß genug, d.h. die durch den Modul V gegeben Darstellung von G soll absolut irreduzibel sein.

An dieser Stelle wollen wir noch einmal daran erinnern, dass wir mit dem FG-Modul V^* stets den kontragrdienten Modul $\mathcal{K}(V)$ meinen, obwohl wir vom dualen Modul sprechen. Da nach Voraussetzung $\sigma(e) = e$ ist, werden wir ebenso mit $\mathrm{cond}_{eFGe}^{FG}(V)^*$ stets den kontragredienten Modul $\mathcal{K} \circ \mathrm{cond}_{eFGe}^{FG}(V)$ bezeichnen.

(3.44) Satz:
Ist das Idempotent e treu, so gilt: Der einfache FG-Modul V ist genau dann selbstdual (beachte (3.11)(b)), wenn der $eFGe$-Modul $\mathrm{cond}_{eFGe}^{FG}(V)$ isomorph zu $\mathrm{cond}_{eFGe}^{FG}(V)^*$ ist.

Beweis: Da e treu ist, bilden die Funktoren $\mathrm{cond}_{eFGe}^{FG}$ und $\mathrm{uncond}_{eFGe}^{FG}$ eine Morita-Äquivalenz zwischen FG und $eFGe$. Eine Äquivalenz von Kategorien bildet Isomorphismen auf Isomorphismen ab. Aus (3.24) folgt die Behauptung. ■

(3.45) Satz:
Ist das Idempotent nicht treu, so gilt: Der einfache FG-Modul V ist genau dann selbstdual (beachte (3.11)(b)), wenn der $eFGe$-Modul $\mathrm{cond}_{eFGe}^{FG}(V)$ isomorph zu $\mathrm{cond}_{eFGe}^{FG}(V)^*$ ist.

Beweis: Seien $\delta : V \to V^*$ und $\delta' : Ve \to \mathcal{K}(Ve)$ die jeweiligen Isomorphismen.
$\underline{\Rightarrow}$: Da $\mathrm{cond}_{eFGe}^{FG}$ exakt ist (vgl. Korollar (3.21)), ist

$$\mathrm{cond}_{eFGe}^{FG}(\ 0 = \mathrm{Kern}\,\delta \longrightarrow V \xrightarrow{\delta} V^* \longrightarrow \mathrm{Kokern}\,\delta = 0\ ) =$$
$$(\ 0 = \mathrm{Kern}\,\mathrm{cond}_{eFGe}^{FG}(\delta) \longrightarrow \mathrm{cond}_{eFGe}^{FG} V \xrightarrow{\mathrm{cond}_{eFGe}^{FG}(\delta)} \mathrm{cond}_{eFGe}^{FG}(\mathcal{K}(V)) \longrightarrow \mathrm{Kokern}\,\mathrm{cond}_{eFGe}^{FG}(\delta) = 0\ )$$

kurzexakt. Folglich ist $\mathrm{cond}_{eFGe}^{FG}(\delta)$ ein Isomorphismus, und da $\mathrm{cond}_{eFGe}^{FG} \circ \mathcal{D} \simeq \mathcal{D} \circ \mathrm{cond}_{eFGe}^{FG}$ (vgl. Satz (3.23)) bzw. $\mathrm{cond}_{eFGe}^{FG} \circ \mathcal{K} \simeq \mathcal{K} \circ \mathrm{cond}_{eFGe}^{FG}$ (vgl. Satz (3.24)) gilt folgt die Behauptung.

$\underline{\Leftarrow:}$ Da $\mathrm{uncond}_{eFGe}^{FG}$ rechtsexakt ist, ist $\mathrm{uncond}_{eFGe}^{FG}(Ve) \xrightarrow{\mathrm{uncond}_{eFGe}^{FG}(\delta')} \mathrm{uncond}_{eFGe}^{FG}(\mathcal{K}(Ve))$ surjektiv. Die kanonische Abbildung

$\mathrm{uncond}_{eFGe}^{FG}(\mathcal{K}(Ve)) \xrightarrow{\varphi} \mathrm{uncond}_{eFGe}^{FG}(\mathcal{K}(Ve)) \Big/ \mathrm{uncond}_{eFGe}^{FG}(\mathcal{K}(Ve))_{(e)}$ ist ebenfalls surjektiv. Außerdem gilt nach (3.35), dass $\mathrm{uncond}_{eFGe}^{FG}(\mathcal{K}(Ve)) \Big/ \mathrm{uncond}_{eFGe}^{FG}(\mathcal{K}(Ve))_{(e)} \simeq \mathcal{K}(V)$ ist. Folglich ist

$$\mathrm{uncond}_{eFGe}^{FG}(Ve) \xrightarrow{\mathrm{uncond}_{eFGe}^{FG}(\delta')\varphi} \mathcal{K}(V) \tag{3.45.1}$$

ebenfalls surjektiv. Der Kern dieser Abbildung ist, wegen (3.34) in $\mathrm{uncond}_{eFGe}^{FG}(Ve)_{(e)}$ enthalten. Die Abbildung (3.45.1) faktorisiert über ihrem Kern, und da $\mathcal{K}(V)$ einfach ist, ist auch $\mathrm{uncond}_{eFGe}^{FG}(Ve) \Big/ \mathrm{Kern}\, \mathrm{uncond}_{eFGe}^{FG}(\delta')\varphi$ einfach. Hieraus folgt, dass der Kern von $\mathrm{uncond}_{eFGe}^{FG}(\delta')\varphi$ ein maximaler Teilmodul von $\mathrm{uncond}_{eFGe}^{FG}(Ve)$, also nach (3.34) gleich $\mathrm{uncond}_{eFGe}^{FG}(Ve)_{(e)}$. Damit ist $\mathrm{uncond}_{eFGe}^{FG}(Ve) \Big/ \mathrm{Kern}\, \mathrm{uncond}_{eFGe}^{FG}(\delta')\varphi$ nach (3.35) isomorph zu V. Also ist $V \simeq \mathcal{K}(V)$. ■

Nun stellt sich die Frage, ob wir die Aussagen der Sätze (3.44) und (3.45) algorithmisch verifizieren können? Die Antwort lautet: Ja, aber nicht direkt mit den Algorithmen (2.2) und (2.3). Wohl aber können wir die Ideen der Algorithmen verwenden: Sei $X \subseteq G$ eine möglichst kleine Menge, für die $eFGe = F\langle ege \mid g \in X\rangle$ ist. Ist Ve als F-Vektorraum d'-dimensional, so sei $\rho : eFGe \to F^{d'\times d'}$ die zu Ve gehörige Matrixdarstellung von $eFGe$. Wegen $\mathcal{K}(Ve) = \mathcal{K}(V)e$ (vgl. (3.24)) beschreiben die Elemente $\rho(eg^{-1}e)^t$ mit $g \in X$ die Matrixdarstellung zu $\mathcal{K}(Ve)$. Wir benutzen also die Mengen $\{\rho(ege) \mid g \in X\}$ und $\left\{\rho(eg^{-1}e)^t \mid g \in X\right\}$ als Eingabe für den Algorithmus ModuleIsomorphism. Dieser liefert entweder eine Isomorphismus zwischen Ve und $\mathcal{K}(Ve)$ oder `fail`.

Die zweite Frage vom Anfang des Paragraphen lässt sich leider nicht so einfach beantworten. Zwar schränkt eine G-invariante reguläre quadratische Form auf V auf Ve ein, nur lässt sich der Begriff „G-invariant“ nicht ohne weiteres für den $eFGe$-Modul Ve übersetzen. Auch wenn wir eine vernünftige Übersetzung gefunden hätten, könnten wir nur aus dem Fehlen einer entsprechenden quadratischen Form auf Ve auf das Fehlen einer G-invarianten regulären quadratischen Form auf V schließen.

§ 3.4. Vorgehen bei nicht einfachen FG-Moduln

In diesem Abschnitt wollen wir eine weitere Methode untersuchen, mit der wir den Frobenius-Schur-Indikator eines einfachen FG-Moduls bestimmen können, ohne, wie es im Algorithmus

(2.4) getan wird, die quadratische Form explizit zu berechnen. Vielmehr werden wir größere Moduln betrachten, die selbst eine G-invariante quadratische Form tragen und die den einfachen Modul, für den wir uns interessieren, als Kompositionsfaktor haben. Wir stützen uns dabei auf die Arbeiten [GW95] und [GW97]. Im Folgenden sei F ein perfekter Körper der Charakteristik 2 und W ein FG-Modul mit einer G-invarianten quadratischen Form q nebst zugehöriger Bilinearform b. In Anlehnung an Satz (1.26) wollen wir die nächste Definition formulieren:

(3.46) Definition:

Das ***singuläre Radikal*** *von W bezüglich q ist wie folgt definiert:*

$$\operatorname{rad}_0 W := \{w \in \operatorname{rad} W \mid q(w) = 0\}.$$

Vergleiche die Definition (1.1) (b) für das Radikal von W. ■

(3.47) Bemerkung:

Sei F ein perfekter Körper der Charakteristik 2 und W ein FG-Modul mit G-invarianter quadratischer Form. Dann gilt entweder $\operatorname{rad} W = \operatorname{rad}_0 W$ oder $\operatorname{rad} W / \operatorname{rad}_0 W$ ist der triviale Modul.

Beweis: Da F perfekt ist und $\operatorname{char} F = 2$, gilt $F = F^2 (= \{f^2 \mid f \in F\})$. Mit Satz (1.26) folgt die Behauptung. ■

Wir führen die folgende Sprechweise ein:

(3.48) Definition & Bemerkung:

(a) *Sei W ein halbregulärer oder regulärer FG-Modul mit G-invarianter quadratischer Form q. Dann nennen wir W einen FG-Modul von quadratischem Typ.*

(b) *Ist F ein perfekter Körper der Charakteristik 2, so ist W genau dann halbregulär oder regulär wenn $\operatorname{rad}_0 W = 0$ ist.* ■

Beweis: Ad (b): Folgt sofort aus Bemerkung (3.47) und der Definition der Begriffe halbregulär und regulär. ■

Wir formulieren zunächst ein Lemma um kleinere FG-Moduln von quadratischem Typ aus größeren zu konstruieren. Der elementare Beweis hierzu wird ausgelassen.

(3.49) Lemma:

Sei W ein FG-Modul von quadratischem Typ. Sei U ein FG-Teilmodul von W mit $\operatorname{rad}_0 U = U$. Dann ist $U^\perp / U$ ebenfalls ein FG-Modul von quadratischem Typ. ■

Wir geben nun eine hinreichende Bedingung dafür an, dass ein einfacher selbstdualer Modul von quadratischem Typ ist.

(3.50) Lemma:

Sei W ein FG-Modul von quadratischem Typ und sei V ein einfacher selbstdualer FG-Modul, der als Kompositionsfaktor von W in ungerader Vielfachheit vorkommt. Wir nehmen weiter an, dass der triviale FG-Modul nicht als Kompositionsfaktor von W vorkommt. Dann ist V von quadratischem Typ.

Beweis: Wir machen eine Induktion nach der Dimension von W und nehmen an, dass W nicht einfach ist. Sei U ein einfacher FG-Teilmodul von W. Da U einfach ist, ist entweder $\operatorname{rad} U = 0$ oder $\operatorname{rad} U = U$. Wir nehmen zunächst an, das $\operatorname{rad} U = 0$ ist. Dann haben wir die orthogonale Zerlegung $W = U \perp U^\perp$ und U und $U^\perp$ sind FG-Teilmoduln von W von quadratischem Typ. Die Behauptung folgt in diesem Fall per Induktion. Wir wenden uns nun dem Fall $\operatorname{rad} U = U$ zu. Aus Bemerkung (3.47) wissen wir, dass $\operatorname{rad}_0 U$ ein FG-Teilmodul von Codimension höchstens 1 in $\operatorname{rad} U$ ist. Somit ist $\operatorname{rad}_0 U = U$ oder $\dim U = 1$, da U einfach ist. Ein eindimensionaler FG-Teilmodul jedoch, der eine G-invariante quadratische Form trägt, die nicht Null ist, ist trivial. Nach unserer Annahme ist also $\operatorname{rad}_0 U = U$ und Lemma (3.49) zeigt, dass $U^\perp/U$ ein FG-Modul von quadratischem Typ ist. Weiter ist $W/U^\perp$ als FG-Modul isomorph zu U^*. Wir sehen, dass wenn r die Vielfachheit von V als Kompositionsfaktor in W ist, dass V in der Vielfachheit r oder $r-2$ als Kompositionsfaktor in $U^\perp/U$ vorkommt. Da $r-2$ ungerade ist, folgt die Behauptung nun per Induktion. ■

Als nächstes wollen wir ein Kriterium formulieren, das sicherstellt, dass ein einfacher selbstdualer Modul nicht von quadratischem Typ ist.

(3.51) Satz:
Sei V ein nicht-trivialer einfacher selbstdualer FG-Modul und sei W ein FG-Modul von quadratischem Typ. Wir wollen weiter annehmen, dass der Sockel S von W der eindimensionale triviale FG-Modul ist und $W/S \simeq V$. Zudem soll $\operatorname{rad}_0 S = 0$ sein. Dann ist V nicht von quadratischem Typ.

Beweis: Sei q die reguläre G-invariante quadratische Form auf W und b die zugehörige Bilinearform. Wir nehmen an, dass es auf V eine reguläre G-invariante quadratische Form Q mit Bilinearform B gibt und werden diese Annahme zum Widerspruch führen. Es ist klar, dass $S = \operatorname{rad} W$ ist, da $W/S \simeq V$, V selbstdual und S eindimensional. Deshalb induziert b eine reguläre G-invariante alternierende Bilinearform $\bar{b}$ auf V. Sei $E = \operatorname{End}_{FG}(V)$. Nach dem Lemma von Schur [CR90, Lemma (3.17)] ist E ein Schiefkörper von endlichem Grad über F. Da $\bar{b}$ und B zwei G-invariante Bilinearformen auf V sind gibt es nach (1.71) ein $\alpha \in E$, so dass $\bar{b}(u,v) = B(u\alpha, v)$ für alle $u, v \in V$ ist. Sei nun σ ein Endomorphismus auf V und sei $\sigma^\dagger$ der, bezüglich B, adjungierte Endomorphismus. Somit gilt:

$$B(u\alpha, v) = \bar{b}(u,v) = \bar{b}(v,u) = B(v\alpha, u) = B(v, u\alpha^\dagger) = b(u\alpha^\dagger, v),$$

weshalb $\alpha^\dagger = \alpha$ ist. Wenn wir $\hat{F} = F(\alpha)$ setzen, so ist $\hat{F}$ ein kommutativer Teilkörper von E der elementweise von † fest gelassen wird. Da F perfekt ist, und $\hat{F}$ endlichen Grad über F hat, ist $\hat{F}$ ebenfalls perfekt. Somit ist $\alpha = \gamma^2 = \gamma\gamma^\dagger$ für ein $\gamma \in \hat{F}$. Also gilt:

$$\bar{b}(u,v) = B(u\gamma\gamma^\dagger, v) = B(u\gamma, v\gamma)$$

für alle $u, v \in V$.

Jetzt definieren wir eine neue reguläre G-invariante quadratische Form p auf V durch $p(v) = Q(v\gamma)$ für alle $v \in V$. Dann gilt:

$$\begin{aligned} p(u+v) = & \quad Q(u\gamma, v\gamma) = Q(u\gamma) + Q(v\gamma) + B(u\gamma, v\gamma) \\ = & \quad p(u) + p(v) + \bar{b}(u,v) \end{aligned}$$

für alle $u, v \in V$; also ist die zu p gehörige Bilinearform gleich $\bar{b}$. Schließlich liften wir p zu einer quadratischen Form P auf W, so dass $S = \mathrm{rad}_0 W$ ist. Ebenso ist klar, dass P eine G-invariant quadratische Form ist und dass die zugehörige Bilinearform gleich b ist. Da q ebenfalls G-invariant ist und b als zugehörige Bilinearform besitzt folgt, dass $q + P = f^2$ ist, wobei f eine G-invariante Linearform ungleich Null auf W ist. Nun ist aber der Kern von f ein KG-Teilmodul von W ist, der ein Komplement zu S ist und dies liefert einen Widerspruch, da S der Sockel von W ist. Folglich ist V nicht von quadratischem Typ. ■

Spätestens an dieser Stelle müssen wir uns fragen: Hilft uns das wirklich weiter, oder verlagern wir hier das Problem nicht nur von einem Modul auf den anderen? Die Antwort ist simpel: Ja, dies hilft uns tatsächlich weiter, da es Moduln gibt, auf denen es eine recht nahe liegende G-invariante reguläre quadratische Form gibt, nämlich Permutationsmoduln.

Im Folgenden sei G eine Gruppe, die auf der Menge Ω mit $|\Omega| = n$ transitiv operiert. Sei weiterhin V der zugehörige Permutationsmodul über F und $v_1, \ldots, v_n$ eine F-Basis von V.

(3.52) Definition:
Sei V wie oben, so definiert

$$q\left(\sum_{i=1}^{n} \lambda_i v_i\right) = \sum_{k=1}^{n} \sum_{j<k} \lambda_j \lambda_k$$

eine G-invariante quadratische Form auf V. Die zugehörige Bilinearform ist durch

$$b(v_i, v_j) = \delta_{ij} + 1$$

gegeben. ■

Entwickeln wir die Gram-Matrix von b bezüglich der Basis $v_1, \ldots, v_n$ nach der ersten Zeile mit anschließender Induktion, so erhalten wir, dass q für gerades n regulär ist, und dass die Gram-Matrix Rang $n-1$ für ungerades n hat. Ist S der eindimensionale Teilraum von V, der von dem Element $u = v_1 + \ldots + v_n$ erzeugt wird, dann ist S der Teilraum der G-Fixpunkte von V. Wenn n ungerade ist, hat S den FG-Modul $T = \left\{\sum_{i=1}^{n} \lambda_i v_i \mid \sum_{i=1}^{n} \lambda_i = 0\right\}$ als Komplement, der von quadratischem Typ ist. Ist nun n gerade, so hat $S^\perp$ Codimension 1 in V und $V/S^\perp$ ist der triviale FG-Modul. Wir nennen $H = S^\perp/S$ das **Herz** des Permutationsmoduls V.

(3.53) Satz:
Wir nutzen die eben gemachten Notation und nehmen an, dass $n \geqslant 4$ und gerade ist. Weiter sei jeder Kompositionsfaktor W_i des Herzes H von V nichttrivial, selbstdual und trete in Vielfachheit

1 auf. Dann gilt: Ist $n \equiv_4 0$ so ist jedes W_i von quadatischem Typ. Ist hingegen $n \equiv_4 2$ und G operiert entweder primitiv auf Ω oder G enthält keinen Normalteiler vom Index 2, so ist wenigstens einer der W_i nicht von quadratischem Typ.

Beweis: Da b auf H eine reguläre Bilinearform induziert und jeder Kompositionsfaktor von H selbstdual ist und in Vielfachheit 1 vorkommt, folgt, dass H halbeinfach ist, also $H \simeq W_1 \oplus \ldots \oplus W_r$ für ein $r \in \mathbb{N}$. Aus der Definition der quadratischen Form q ergibt sich:

$$q(u) = q(v_1 + \ldots + v_n) \equiv_2 \frac{n(n-1)}{2}.$$

Daraus erhalten wir: $q(u) = 0$ falls $n \equiv_4 0$ und $q(u) = 1$ falls $n \equiv_4 2$. Folglich ist, falls $n \equiv_4 0$ ist, das Herz von V ebenfalls von quadratischem Typ und somit auch jedes W_i. Nun wollen wir annehmen, dass $n \equiv_4 2$ ist. Seien mit U_i die Urbilder der W_i in $S^\perp$ für $1 \leqslant i \leqslant r$ bezeichnet. Wir wollen zeigen, dass es einen Index j gibt, so dass S der Sockel von U_j ist. Wir nehmen an, dass dies nicht der Fall ist. Dann ist jedes U_i die direkte Summe aus S und einem einfachen Untermodul von $S^\perp$, der zu W_i isomorph ist. Wir wollen diesen Teilmodul ebenfalls mit W_i bezeichnen. Es ist nun einfach einzusehen, dass wir folgende direkte Summenzerlegung von V in FG-Teilmoduln haben:

$$V = W_1 \oplus \ldots \oplus W_r \oplus X$$

wobei X eine nichtspaltende Erweiterung von S durch den trivialen Modul ist. (Der Modul X ist eine nichtspaltende Erweiterung, da S der Teilraum der G-Fixpunkte von V ist.) Sei N der Kern der Operation von G auf X. Es ist klar, dass $[G : N]$ eine Zweierpotenz größer als 1 ist. Wir erhalten einen Widerspruch, falls G keinen Normalteiler von Index 2 hat. Operiert G andererseits primitiv auf Ω, so operiert N transitiv auf Ω und S ist der Teilraum der N-Fixpunkte in V. Dies widerspricht aber der Tatsache, dass N auf X trivial operiert. Somit können wir schließen, dass S der Sockel eines U_j ist. Schließlich induziert q eine reguläre quadratische Form auf jedem U_i. Mit Satz (3.51) folgt schlussendlich, dass W_j nicht von quadratischem Typ ist. ■

Diese Arbeit abschließend wollen wir noch zwei Bemerkungen zu Satz (3.53) aus [GW97] zitieren.

Zum einen wollen wir zeigen, dass die Folgerung aus Satz (3.53) im Falle, dass $n \equiv_4 2$ ist und G nicht primitiv operiert und eine Untergruppe vom Index 2 besitzt, nicht korrekt sein muss. Ein Beispiel hierfür liefert das Kranzprodukt $\mathfrak{S}_3 \wr \mathfrak{S}_2$, das auf sechs Punkten operiert. Das Herz H des zugehörigen Permutationsmoduls ist einfach und von Dimension 4 über $\mathbb{F}_2$. Zudem ist H von quadratischem Typ, ein Fakt, der beweist, dass die orthogonale Gruppe $O_4^+(\mathbb{F}_2)$ isomorph zu $\mathfrak{S}_3 \wr \mathfrak{S}_2$ ist.
Zum anderen wollen wir annehmen, dass S der Sockel von V ist. Dann gilt, falls $n \equiv_4 2$ ist, dass keiner der einfachen Moduln W_i von quadratischem Typ ist. Wenn wir dem Beweis des Satzes (3.53) folgen, so ist S der Sockel von jedem U_i und wir folgern wie oben, das keiner der W_i von quadratischem Typ ist. Hierbei muss keine weitere Annahme an die Operation der Gruppe oder deren Struktur gemacht werden. In der oben zitierten Arbeit werden im zweiten Abschnitt Beispiele dieser Situationen beschrieben.

Anhang A

Eine Übersicht der getesteten Darstellungen, deren Indikator und Witt-Index

Im ATLAS of Finite Group Representations [Wil] in der Version 2, der über das Gap-Inteface [Bre04] erreichbar ist, sind 803 Darstellungen über Körpern der Charakteristik 2 enthalten. Von diesen sind 744 absolut irreduzibel. Davon wiederum sind 526 selbstdual. Es tragen 432 eine G-invariante quadratische Form.Von diesen sind 285 vom Orthogonalitätstyp „+“ und 147 vom Typ „−“.

In der nun folgenden Tabelle steht in der Spalte „Dim“ die Dimension der jeweiligen Darstellung. In der Spalte „F“ steht die Ordnung des Körpers, über welchem die Darstellung gegeben ist. In Spalte „FSI“ wird der Frobenius-Schur-Indikator notiert. Dabei steht ein „$\circ$“ dafür, dass die Darstellung nicht selbstdual ist. Es steht dort ein „+“, wenn die Darstellung eine G-invariante quadratische Form trägt und ein „−“, wenn die Darstellung zwar selbstdual ist, aber keine G-invariante quadratische Form trägt. In der Spalte „Typ“ schließlich steht ein „+“, wenn der Wittindex der quadratische Form Dimension / 2 ist und ein „−“, wenn der Wittindex Dimension / 2 − 1 ist.

In der Tabelle werden nur die absolut irreduziblen Darstellungen aufgeführt.

Gruppe	Dim	F	FSI	Typ
A_5	2a	4	−	
A_5	2b	4	−	
A_5	4a	2	+	−
$A_5:2$	4a	2	−	
$A_5:2$	4b	2	+	−
A_6	4a	2	−	
A_6	4b	2	−	
A_6	8a	4	+	+
A_6	8b	4	+	+
$3.A_6$	3a	4	∘	
$3.A_6$	3b	4	∘	
$3.A_6$	9a	4	∘	
A_7	4a	2	∘	
A_7	4b	2	∘	
A_7	6	2	+	+
A_7	14	2	+	−
A_7	20	2	−	
A_8	4a	2	∘	
A_8	4b	2	∘	
A_8	6	2	+	+
A_8	14	2	+	−
A_8	20a	2	∘	
A_8	20b	2	∘	
A_8	64	2	+	+
$A_8:2$	6	2	+	+
$A_8:2$	8	2	+	+
$A_8:2$	14	2	+	−
$A_8:2$	40	2	+	+
$A_8:2$	64	2	+	+
A_9	8a	2	+	+
A_9	8b	2	+	+
A_9	8c	2	+	+
A_9	20a	2	∘	
A_9	20b	2	∘	
A_9	26	2	+	−
A_9	48	2	+	+
A_9	78	2	+	−
A_9	160	2	+	+
A_{10}	8	2	−	
A_{10}	16	2	+	+
A_{10}	26	2	+	−
A_{10}	48	2	+	+

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
A_{10}	64a	2	+	+
A_{10}	64b	2	+	+
A_{10}	160	2	+	+
A_{10}	198	2	+	+
A_{10}	200	2	+	+
A_{10}	384a	4	+	+
A_{11}	10	2	+	−
A_{11}	16a	4	∘	
A_{11}	16b	4	∘	
A_{11}	44	2	+	−
A_{11}	100	2	+	+
A_{11}	144	2	+	+
A_{11}	164	2	−	
A_{11}	186	2	+	−
A_{11}	198	2	+	+
A_{11}	416	2	+	+
A_{11}	584a	4	+	+
A_{11}	848	2	+	+
$A_{11}:2$	32	2	+	+
A_{12}	10	2	+	−
A_{12}	16a	4	∘	
A_{12}	16b	4	∘	
A_{12}	44	2	+	−
A_{12}	100	2	+	+
A_{13}	32a	4	+	+
A_{13}	32b	4	+	+
A_{14}	12	2	−	
A_{14}	64a	2	−	
A_{14}	64b	2	+	+
$A_{14}:2$	12	2	−	
$A_{14}:2$	64a	2	−	
$A_{14}:2$	64b	2	+	+
$U_3(3)$	6	2	−	
$U_3(3)$	14	2	+	−
$U_3(3)$	32a	2	∘	
$U_3(3)$	32b	2	∘	
$U_3(3):2$	6	2	−	
$U_3(3):2$	14	2	+	−
$U_3(3):2$	64	2	+	+
$U_3(4)$	3a	16	∘	
$U_3(4)$	3b	16	∘	
$U_3(4)$	3c	16	∘	
$U_3(4)$	3d	16	∘	

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$U_3(4)$	8a	4	+	−
$U_3(4)$	8b	4	+	−
$U_3(4)$	9a	16	∘	
$U_3(4)$	9b	16	∘	
$U_3(4)$	9c	16	∘	
$U_3(4)$	9d	16	∘	
$U_3(4)$	24a	16	∘	
$U_3(4)$	24b	16	∘	
$U_3(4)$	24c	16	∘	
$U_3(4)$	24d	16	∘	
$U_3(4)$	64	2	+	+
$U_3(4):4$	12	2	+	−
$U_3(4):4$	16	2	+	−
$U_3(4):4$	36	2	+	−
$U_3(4):4$	64	2	+	+
$U_3(4):4$	96	2	+	+
$U_3(5):2$	20	2	−	
$U_3(5):2$	28	2	+	−
$U_3(5):2$	56	2	+	+
$U_3(5):2$	104	2	−	
$U_3(5):2$	288	2	+	+
$U_3(7)$	42	2	−	
$U_3(7)$	258	2	+	+
$U_3(7)$	344	2	+	−
$U_3(8):6$	24	2	+	+
$U_3(8):6$	54a	2	+	−
$U_3(8):6$	54b	2	+	−
$U_3(8):6$	192	2	+	+
$U_3(8):6$	432	2	+	+
$U_3(8):6$	512	2	+	+
$3.U_3(8)$	3a	64	∘	
$U_3(11)$	110	2	−	
$U_3(11)$	370a	2	+	−
$U_3(11)$	370b	2	+	−
$U_3(11)$	370c	2	+	−
$U_3(11):2$	110	2	−	
$U_4(2)$	4a	4	∘	
$U_4(2):2$	6	2	+	−
$U_4(2):2$	8	2	+	+
$U_4(2):2$	14	2	+	−
$U_4(2):2$	40	2	+	+
$U_4(2):2$	64	2	+	+
$U_5(2)$	5a	4	∘	

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$U_5(2)$	5b	4	∘	
$U_5(2)$	10a	4	∘	
$U_5(2)$	10b	4	∘	
$U_5(2)$	24	2	+	−
$U_5(2)$	74	2	−	
$U_5(2):2$	10	2	+	−
$U_5(2):2$	20	2	+	+
$U_5(2):2$	24	2	+	−
$U_5(2):2$	74	2	−	
$U_5(2):2$	80a	2	+	+
$U_5(2):2$	80b	2	+	+
$U_5(2):2$	320	2	+	+
$U_5(2):2$	560	2	+	+
$U_5(2):2$	1024	2	+	+
$U_6(2)$	20	2	+	+
$U_6(2)$	34	2	−	
$U_6(2)$	70a	4	∘	
$U_6(2)$	70b	4	∘	
$U_6(2)$	154	2	−	
$U_6(2)$	400	2	+	+
$U_6(2)$	896a	4	∘	
$3.U_6(2)$	6a	4	∘	
$3.U_6(2)$	15a	4	∘	
$3.U_6(2)$	84a	4	∘	
$3.U_6(2)$	90a	4	∘	
$3.U_6(2)$	204a	4	∘	
$3.U_6(2)$	384a	4	∘	
$3.U_6(2)$	720a	4	∘	
$3.U_6(2)$	924a	4	∘	
$U_6(2):2$	20	2	+	+
$U_6(2):2$	34	2	−	
$U_6(2):2$	140	2	+	+
$U_6(2):2$	154	2	−	
$U_6(2):2$	400	2	+	+
$U_6(2):S_3$	20	2	+	+
$U_6(2):S_3$	34	2	−	
$U_6(2):S_3$	140a0	2	+	+
$U_6(2):S_3$	140a1	2	+	+
$U_6(2):S_3$	140a2	2	+	+
$U_6(2):S_3$	154	2	−	
$U_6(2):S_3$	400	2	+	+
$U_7(2)$	7a	4	∘	
$U_7(2)$	7b	4	∘	

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$O_7(3)$	78	2	+	−
$O_7(3)$	90	2	+	+
$O_7(3)$	104	2	+	+
$O_7(3)$	260a	2	+	+
$O_7(3)$	260b	2	∘	
$3.O_7(3)$	27a	4	∘	
$O_7(3):2$	78	2	+	−
$3.O_7(3):2$	54	2	+	−
$O_8^-(2)$	8	2	+	−
$O_8^-(2)$	8b	4	+	+
$O_8^-(2)$	8c	4	+	+
$O_8^-(2)$	26	2	+	−
$O_8^-(2)$	48	2	+	+
$O_8^-(2)$	48b	4	+	+
$O_8^-(2)$	48c	4	+	+
$O_8^-(2):2$	8	2	+	−
$O_8^+(3)$	298	2	+	+
$O_{10}^+(2)$	10	2	+	+
$O_{10}^+(2)$	16a	2	∘	
$O_{10}^+(2)$	16b	2	∘	
$O_{10}^+(2)$	44	2	+	−
$O_{10}^+(2)$	100	2	+	+
$O_{10}^+(2)$	144a	2	∘	
$O_{10}^+(2)$	144b	2	∘	
$O_{10}^+(2)$	164	2	−	
$O_{10}^+(2)$	320	2	+	+
$O_{10}^+(2)$	416a	2	∘	
$O_{10}^+(2)$	416b	2	∘	
$O_{10}^+(2)$	670	2	+	+
$O_{10}^+(2):2$	10	2	+	+
$O_{10}^+(2):2$	32	2	+	+
$O_{10}^+(2):2$	44	2	+	−
$O_{10}^+(2):2$	100	2	+	+
$O_{10}^+(2):2$	164	2	−	
$O_{10}^+(2):2$	288	2	+	+
$O_{10}^+(2):2$	320	2	+	+
$O_{10}^+(2):2$	670	2	+	+
$O_{10}^+(2):2$	832	2	+	+
$O_{10}^-(2)$	10	2	+	−
$O_{10}^-(2)$	16a	4	∘	
$O_{10}^-(2)$	16b	4	∘	
$O_{10}^-(2)$	44	2	+	−
$O_{10}^-(2)$	100	2	+	+

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$O_{10}^-(2)$	164	2	−	
$O_{10}^-(2)$	670	2	+	+
$O_{10}^-(2):2$	10	2	+	−
$O_{10}^-(2):2$	32	2	+	+
$O_{10}^-(2):2$	44	2	+	−
$O_{10}^-(2):2$	100	2	+	+
$O_{10}^-(2):2$	164	2	−	
$O_{10}^-(2):2$	670	2	+	+
$S_4(4)$	4c	4	−	
$S_4(4):2$	8a	2	−	
$S_4(4):4$	16	2	−	
$S_4(5)$	12a	4	−	
$S_4(5):2$	24	2	−	
$S_4(5):2$	40	2	+	+
$S_4(5):2$	64	2	−	
$S_4(5):2$	104a	2	+	+
$S_4(5):2$	104b	2	+	+
$S_6(2)$	6	2	−	
$S_6(2)$	8	2	+	+
$S_6(2)$	14	2	+	−
$S_6(2)$	48	2	+	+
$S_6(2)$	64	2	+	+
$S_6(2)$	112	2	+	+
$S_6(2)$	512	2	+	+
$S_6(3)$	13a	4	∘	
$S_6(3)$	78	2	+	−
$S_6(3):2$	26	2	+	−
$S_8(2)$	8	2	−	
$S_8(2)$	16	2	+	+
$S_8(2)$	26	2	+	−
$S_8(2)$	48	2	+	+
$S_{10}(2)$	10	2	−	
$S_{10}(2)$	32	2	+	+
$S_{10}(2)$	44	2	+	−
$S_{10}(2)$	100	2	+	+
$S_{10}(2)$	164	2	−	
$G_2(3)$	14	2	+	−
$G_2(3)$	64a	4	∘	
$G_2(3)$	64	4	∘	
$G_2(3)$	78	2	+	−
$G_2(3)$	90a	2	+	+
$G_2(3)$	90b	2	+	−
$G_2(3)$	90c	2	+	−

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$G_2(3)$	378	2	+	−
$3.G_2(3)$	27	4	∘	
$G_2(3):2$	14	2	+	−
$3.G_2(3):2$	54	2	+	−
$G_2(4)$	6a	4	−	
$G_2(4)$	6b	4	−	
$G_2(4)$	14a	4	+	+
$G_2(4)$	14b	4	+	+
$G_2(4)$	36	2	+	−
$G_2(4)$	64a	4	+	+
$G_2(4)$	64b	4	+	+
$G_2(4)$	84a	4	+	+
$G_2(4)$	84b	4	+	+
$G_2(4)$	196	2	+	−
$G_2(4)$	384a	4	+	+
$G_2(4)$	896a	4	+	+
$G_2(4):2$	12	2	−	
$G_2(4):2$	28	2	+	+
$G_2(4):2$	36	2	+	−
$G_2(4):2$	128	2	+	+
$G_2(4):2$	168	2	+	+
$G_2(4):2$	196	2	+	−
$G_2(4):2$	768	2	+	+
$G_2(5)$	124	2	+	−
$F_4(2)$	26a	2	+	−
$F_4(2):2$	52	2	+	+
$E_6(2)$	27a	2	∘	
$E_6(2)$	27b	2	∘	
$E_6(2)$	27a	2	∘	
$E_6(2)$	27b	2	∘	
$E_6(2)$	78	2	+	−
$E_6(2)$	78	2	+	−
$E_6(4)$	78	4	+	+
$3.E_6(4)$	27	4	∘	
$3.E_6(4):2$	54	4	+	+
$E_7(2)$	56	2	+	+
$E_7(2)$	132	2	−	
$E_7(4)$	56a	4	+	+
$E_7(4)$	132a	4	−	
$E_8(2)$	248	2	+	+
$E_8(2)$	248	2	+	+
$Sz(8)$	4a	8	−	
$Sz(8)$	16a	8	+	+

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$Sz(8)$	64	2	+	+
$Sz(8):3$	12	2	−	
$Sz(8):3$	48	2	+	+
$Sz(8):3$	64	2	+	+
$Sz(32)$	4a	32	−	
$Sz(32):5$	20	2	−	
$R(27)$	702	2	−	
$R(27):3$	702	2	−	
$R(27):3$	741	4	∘	
${}^2F_4(2)'$	26	2	+	−
${}^2F_4(2)'$	246	2	+	+
${}^2F_4(2)'$	2048a	4	+	+
${}^2F_4(2)':2$	26	2	+	−
${}^2F_4(2)':2$	246	2	+	+
${}^3D_4(2)$	8a	8	+	+
${}^3D_4(2)$	26	2	+	−
${}^3D_4(2):3$	24	2	+	+
${}^3D_4(2):3$	26	2	+	−
${}^3D_4(2):3$	144	2	+	+
${}^3D_4(2):3$	246a	2	+	+
${}^3D_4(2):3$	480	2	+	+
${}^3D_4(3)$	218	2	+	−
${}^2E_6(2)$	78	2	+	−
$3.{}^2E_6(2)$	27	4	∘	
${}^2E_6(2):2$	78	2	+	−
$3.{}^2E_6(2):2$	54	2	+	−
${}^2E_6(2):3$	78	2	+	−
$3.{}^2E_6(2):2$	27	4	∘	
${}^2E_6(2):S_3$	78	2	+	−
$3.{}^2E_6(2):S_3$	54	2	+	−
$L_2(8)$	2a	8	−	
$L_2(8)$	2b	8	−	
$L_2(8)$	2c	8	−	
$L_2(8)$	4a	8	+	+
$L_2(8)$	4b	8	+	+
$L_2(8)$	4c	8	+	+
$L_2(8)$	8	2	+	+
$L_2(8):3$	6	2	−	
$L_2(8):3$	8	2	+	+
$L_2(8):3$	12	2	+	+
$L_2(11)$	5a	4	∘	
$L_2(11)$	5b	4	∘	
$L_2(11)$	10	2	+	−

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$L_2(11)$	12a	4	+	−
$L_2(11)$	12b	4	+	−
$L_2(11):2$	10a	2	+	−
$L_2(11):2$	10b	2	+	−
$L_2(11):2$	12a	4	+	−
$L_2(11):2$	12b	4	+	−
$L_2(13)$	6a	4	−	
$L_2(13)$	6b	4	−	
$L_2(13)$	12a	8	+	−
$L_2(13)$	12b	8	+	−
$L_2(13)$	12c	8	+	−
$L_2(13)$	14	2	+	+
$L_2(13):2$	12a	2	−	
$L_2(13):2$	14	2	+	+
$L_2(16)$	2a	16	−	
$L_2(16):2$	4a	4	−	
$L_2(16):4$	8a	2	−	
$L_2(16):4$	8b	2	+	−
$L_2(16):4$	16a	2	+	+
$L_2(16):4$	16b	2	+	+
$L_2(16):4$	32	2	+	+
$L_2(17)$	8a	2	−	
$L_2(17)$	8b	2	−	
$L_2(17)$	16a	2	+	+
$L_2(17)$	16b	8	+	+
$L_2(17)$	16c	8	+	+
$L_2(17)$	16d	8	+	+
$L_2(19)$	9a	4	∘	
$L_2(19)$	9b	4	∘	
$L_2(19)$	18a	4	+	+
$L_2(19)$	18b	4	+	+
$L_2(19)$	20a	2	+	+
$L_2(19)$	20b	8	+	+
$L_2(19)$	20c	8	+	+
$L_2(19)$	20d	8	+	+
$L_2(23)$	11a	2	∘	
$L_2(23)$	11b	2	∘	
$L_2(23)$	22	2	+	+
$L_2(23)$	24a	32	+	−
$L_2(23)$	24b	32	+	−
$L_2(23)$	24c	32	+	−
$L_2(23)$	24d	32	+	−
$L_2(23)$	24e	32	+	−

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$L_2(23):2$	22a	2	+	+
$L_2(27)$	13a	4	∘	
$L_2(27)$	13b	4	∘	
$L_2(29)$	14a	4	−	
$L_2(29)$	14b	4	−	
$L_2(31)$	15a	2	∘	
$L_2(31)$	15b	2	∘	
$L_2(31)$	32d	16	+	+
$L_2(31)$	32e	16	+	+
$L_2(31)$	32f	16	+	+
$L_2(31)$	32g	16	+	+
$L_2(31)$	32	2	+	−
$L_2(31)$	32b	4	+	−
$L_2(31)$	32c	4	+	−
$L_2(31):2$	30	2	+	+
$L_2(32)$	2a	32	−	
$L_2(32):5$	10	2	−	
$L_2(32):5$	20a	2	+	+
$L_2(32):5$	20b	2	+	+
$L_2(32):5$	32	2	+	+
$L_2(32):5$	40a	2	+	+
$L_2(32):5$	40b	2	+	+
$L_2(32):5$	80	2	+	+
$L_3(2)$	3a	2	∘	
$L_3(2)$	3b	2	∘	
$L_3(2)$	8	2	+	−
$L_3(3)$	12	2	+	−
$L_3(3)$	16a	16	∘	
$L_3(3)$	26	2	+	−
$L_3(3):2$	12	2	+	−
$L_3(3):2$	26	2	+	−
$L_3(3):2$	32a	4	+	+
$L_3(3):2$	32b	4	+	+
$L_3(4)$	8a	4	+	+
$L_3(4)$	8b	4	+	+
$L_3(4)$	9a	2	∘	
$L_3(4)$	9b	2	∘	
$L_3(4)$	64	2	+	+
$3.L_3(4)$	3a	4	∘	
$3.L_3(4)$	3b	4	∘	
$3.L_3(4)$	9a	4	∘	
$3.L_3(4)$	24a	4	∘	
$3.L_3(4)$	24b	4	∘	

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$L_3(4):2_1$	16a	2	+	+
$L_3(4):2_1$	18a	2	+	+
$L_3(4):2_1$	64a	2	+	+
$3.L_3(4):2_1$	6a	4	∘	
$3.L_3(4):2_1$	9a	4	∘	
$3.L_3(4):2_1$	48a	4	∘	
$L_3(7)$	152a	2	+	−
$L_3(7):2$	56	2	+	+
$L_3(7):2$	152	2	+	−
$L_3(7):2$	342	2	+	+
$L_3(8)$	3	8	∘	
$L_3(8)$	8	8	+	−
$L_3(8)$	9a	8	∘	
$L_3(8)$	9b	8	∘	
$L_3(8)$	24a	8	∘	
$L_3(8)$	24b	8	∘	
$L_3(8)$	27	2	∘	
$L_3(8)$	27	8	∘	
$L_3(8)$	64	8	+	+
$L_3(8)$	72a	8	∘	
$L_3(8)$	72b	8	∘	
$L_3(8)$	192	8	∘	
$L_3(8)$	512	2	+	+
$L_3(8):2$	6	8	+	+
$L_3(8):2$	8	8	+	−
$L_3(8):2$	18a	8	+	+
$L_3(8):2$	18b	8	+	+
$L_3(8):2$	48a	8	+	+
$L_3(8):2$	48b	8	+	+
$L_3(8):2$	54	2	+	+
$L_3(8):2$	54	8	+	+
$L_3(8):2$	64	8	+	+
$L_3(8):2$	144a	8	+	+
$L_3(8):2$	144b	8	+	+
$L_3(8):2$	384	8	+	+
$L_3(8):2$	512	2	+	+
$L_3(8):3$	9	2	∘	
$L_3(8):3$	24	2	+	−
$L_3(8):3$	27a	2	∘	
$L_3(8):3$	27b	2	∘	
$L_3(8):3$	27c	2	∘	
$L_3(8):3$	72a	2	∘	
$L_3(8):3$	72b	2	∘	

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$L_3(8):3$	81	2	∘	
$L_3(8):3$	192	2	+	+
$L_3(8):3$	216a	2	∘	
$L_3(8):3$	216b	2	∘	
$L_3(8):3$	512	2	+	+
$L_3(8):3$	576	2	∘	
$L_3(8):6$	18	2	+	+
$L_3(8):6$	24	2	+	−
$L_3(8):6$	54a	2	+	+
$L_3(8):6$	54b	2	+	+
$L_3(8):6$	54c	2	+	+
$L_3(8):6$	144a	2	+	+
$L_3(8):6$	144b	2	+	+
$L_3(8):6$	162	2	+	+
$L_3(8):6$	192	2	+	+
$L_3(8):6$	432a	2	+	+
$L_3(8):6$	432b	2	+	+
$L_3(8):6$	512	2	+	+
$L_3(8):6$	1152	2	+	+
$L_3(11)$	132	2	+	−
$L_5(2)$	5a	2	∘	
$L_5(2)$	5b	2	∘	
$L_5(2)$	10a	2	∘	
$L_5(2)$	10b	2	∘	
$L_5(2)$	24	2	+	−
$L_5(2):2$	10	2	+	+
$L_5(2):2$	20	2	+	+
$L_5(2):2$	24	2	+	−
$L_6(2)$	6a	2	∘	
$L_6(2)$	6b	2	∘	
$L_6(2)$	15a	2	∘	
$L_6(2)$	15b	2	∘	
$L_6(2)$	20	2	+	+
$L_6(2)$	34	2	−	
$L_6(2)$	70a	2	∘	
$L_6(2)$	84a	2	∘	
$L_6(2)$	90a	2	∘	
$L_6(2)$	154	2	−	
$L_6(2)$	204a	2	∘	
$L_6(2)$	384a	2	∘	
$L_6(2)$	400	2	+	+
$L_6(2)$	720a	2	∘	
$L_6(2)$	896a	2	∘	

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$L_6(2)$	924a	2	∘	
$L_6(2):2$	12	2	+	+
$L_6(2):2$	20	2	+	+
$L_6(2):2$	30	2	+	+
$L_6(2):2$	34	2	−	
$L_6(2):2$	140	2	+	+
$L_6(2):2$	154	2	−	
$L_6(2):2$	168	2	+	+
$L_6(2):2$	180	2	+	+
$L_6(2):2$	400	2	+	+
$L_6(2):2$	408	2	+	+
$L_6(2):2$	768	2	+	+
$L_7(2)$	7a	2	∘	
$L_7(2)$	7b	2	∘	
$L_7(2)$	21a	2	∘	
$L_7(2)$	21b	2	∘	
$L_7(2)$	35a	2	∘	
$L_7(2)$	35b	2	∘	
$L_7(2)$	48	2	+	+
$L_7(2)$	112a	2	∘	
$L_7(2)$	112b	2	∘	
$L_7(2)$	133a	2	∘	
$L_7(2)$	133b	2	∘	
$L_7(2)$	175a	2	∘	
$L_7(2)$	175b	2	∘	
$L_7(2)$	224a	2	∘	
$L_7(2)$	224b	2	∘	
$L_7(2)$	392a	2	+	−
$L_7(2)$	448a	2	∘	
$L_7(2)$	448b	2	∘	
$L_7(2)$	469a	2	∘	
$L_7(2)$	469b	2	∘	
$L_7(2)$	707a	2	∘	
$L_7(2)$	707b	2	∘	
$L_7(2)$	736a	2	+	+
$L_7(2):2$	14	2	+	+
$L_7(2):2$	42	2	+	+
$L_7(2):2$	48	2	+	+
$L_7(2):2$	70	2	+	+
$L_7(2):2$	224	2	+	+
$L_7(2):2$	266	2	+	+
$L_7(2):2$	350	2	+	+
$L_7(2):2$	392	2	+	−

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$L_7(2):2$	448	2	+	+
$L_7(2):2$	736	2	+	+
$L_7(2):2$	896	2	+	+
$L_7(2):2$	938	2	+	+
$5^3.L_3(5)$	620	2	+	−
M_{11}	10	2	+	−
M_{11}	16a	4	∘	
M_{11}	16b	4	∘	
M_{11}	44	2	+	−
M_{12}	10	2	+	−
M_{12}	16a	4	∘	
M_{12}	16b	4	∘	
M_{12}	44	2	+	−
M_{12}	144	2	+	+
$M_{12}.2$	10	2	+	−
$M_{12}.2$	32	2	+	+
$M_{12}.2$	44	2	+	−
$M_{12}.2$	144	2	+	+
M_{22}	10a	2	∘	
M_{22}	10b	2	∘	
M_{22}	34	2	−	
M_{22}	70a	4	∘	
M_{22}	70b	4	∘	
M_{22}	98	2	−	
$3.M_{22}$	6a	4	∘	
$3.M_{22}$	15a	4	∘	
$3.M_{22}$	45a	4	∘	
$3.M_{22}$	45b	4	∘	
$3.M_{22}$	84a	4	∘	
$3.M_{22}$	384a	4	∘	
$M_{22}.2$	10a	2	∘	
$M_{22}.2$	10b	2	∘	
$M_{22}.2$	34	2	−	
$M_{22}.2$	98	2	−	
$M_{22}.2$	140	2	+	+
$3.M_{22}.2$	12	2	+	+
M_{23}	11a	2	∘	
M_{23}	11b	2	∘	
M_{23}	44a	2	∘	
M_{23}	44b	2	∘	
M_{23}	120	2	+	−
M_{23}	220a	2	∘	
M_{23}	220b	2	∘	

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
M_{23}	252	2	−	
M_{23}	896a	4	∘	
M_{23}	896b	4	∘	
M_{24}	11a	2	∘	
M_{24}	11b	2	∘	
M_{24}	44a	2	∘	
M_{24}	44b	2	∘	
M_{24}	120	2	+	−
M_{24}	220a	2	∘	
M_{24}	220b	2	∘	
M_{24}	252	2	−	
M_{24}	320a	2	∘	
M_{24}	320b	2	∘	
M_{24}	1242	2	+	+
M_{24}	1792	2	+	+
HS	20	2	−	
HS	56	2	+	+
HS	132	2	−	
HS	518	2	+	+
HS	896a	4	∘	
HS	896b	4	∘	
HS	1000	2	+	+
$HS:2$	20	2	−	
$HS:2$	56	2	+	+
$HS:2$	132	2	−	
$HS:2$	518	2	+	+
$HS:2$	1000	2	+	+
$HS:2$	1408	2	+	+
$HS:2$	1792	2	+	+
McL	22	2	+	+
McL	230	2	+	−
McL	748a	2	∘	
McL	748b	2	∘	
McL	896a	4	∘	
McL	896b	4	∘	
$3.McL$	126a	4	∘	
$3.McL$	396d	4	∘	
$McL:2$	22	2	+	+
$McL:2$	230a	2	+	−
$McL:2$	1496a	2	+	+
$3.McL:2$	252a	4	∘	
Co_3	22	2	−	
Co_3	230	2	+	−

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
Co_3	896a	4	∘	
Co_2	22	2	+	+
Co_2	230	2	+	−
Co_2	748a	2	∘	
Co_2	748b	2	∘	
Co_1	24	2	+	+
Co_1	274	2	+	−
J_2	6a	4	−	
J_2	14a	4	+	+
J_2	36	2	+	−
J_2	64a	4	+	+
J_2	84	2	+	−
J_2	160	2	+	+
$J_2:2$	12	2	−	
$J_2:2$	28	2	+	+
$J_2:2$	36	2	+	−
$J_2:2$	84	2	+	−
$J_2:2$	128	2	+	+
$J_2:2$	160	2	+	+
Suz	110a	4	+	+
Suz	142	2	+	−
Suz	572a	4	∘	
Suz	572b	4	∘	
Suz	638	2	+	−
$3.Suz$	12a	4	∘	
$3.Suz$	66a	4	∘	
$3.Suz$	429a	4	∘	
$3.Suz$	825a	4	∘	
$3.Suz$	825b	4	∘	
$3.Suz:2$	24	2	+	+
Fi_{22}	78	2	+	−
Fi_{22}	350	2	+	+
Fi_{22}	572	2	+	+
$3.Fi_{22}$	27a	4	∘	
$Fi_{22}:2$	78	2	+	−
$Fi_{22}:2$	350	2	+	+
$Fi_{22}:2$	572	2	+	+
$Fi_{22}:2$	1352	2	+	+
$3.Fi_{22}:2$	54	2	+	−
Fi_{23}	782	2	+	−
Fi_{23}	1494	2	+	+
Fi'_{24}	3774	2	+	+
$3.Fi'_{24}$	783	4	∘	

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$3.Fi'_{24}:2$	1566	2	+	−
He	51	2	∘	
He	101	2	∘	
He	246	2	+	+
He	680	2	+	−
$He:2$	102	2	+	+
$He:2$	202	2	+	+
$He:2$	492	2	+	+
$He:2$	680	2	+	−
HN	132a	4	−	
HN	132b	4	−	
HN	760	2	+	+
HN	2650a	4	∘	
$HN:2$	264	2	−	
Th	248	2	+	+
B	4370	2	+	−
$3.Fi_{24}$	1566	2	+	−
J_1	20	2	+	+
J_1	56a	4	−	
J_1	56b	4	−	
J_1	56c	4	+	+
J_1	56d	4	+	+
J_1	76a	2	−	
J_1	76b	2	+	−
J_1	120a	8	+	+
J_1	120b	8	+	+
J_1	120c	8	+	+
$3.O'N$	153	4	∘	
$3.O'N:2$	306	2	+	−
Ly	2480	4	∘	
J_3	78b	4	+	+
J_3	80	2	+	+
J_3	84a	4	∘	
J_3	244	2	+	−
J_3	322a	4	−	
J_3	966	2	+	−
$3.J_3$	9a	4	∘	
$3.J_3$	18a	4	∘	
$3.J_3$	18b	4	∘	
$3.J_3$	126a	4	∘	
$3.J_3$	153a	4	∘	
$3.J_3$	153b	4	∘	
$3.J_3$	324a	4	∘	

Fortsetzung der Tabelle auf der nächsten Seite

Fortsetzung der Tabelle

Gruppe	Dim	F	FSI	Typ
$3.J_3$	720a	4	∘	
$3.J_3$	1008a	4	∘	
$J_3:2$	80a	2	+	+
$J_3:2$	156a	2	+	+
$J_3:2$	168a	2	+	+
$J_3:2$	244a	2	+	−
$J_3:2$	644a	2	−	
$J_3:2$	966a	2	+	−
$3.J_3:2$	18	2	+	−
J_4	112	2	+	+
J_4	1220a	2	∘	
Ru	28	2	+	−
Ru	376	2	−	
Ru	1246	2	+	+

Literaturverzeichnis

[AF74] Frank W. Anderson und Kent R. Fuller. Rings and Categories of Modules. Springer-Verlag, 1974.

[Alp93] J. L. Alperin. Local representation theory. Cambridge Univerty Press, 1993.

[Asc00] M. Aschbacher. Finite Group Theory. Cambridge University Press, 2000.

[Bre04] Thomas Breuer. Manual for the GAP 4 Package AtlasRep, Version 1.2. Lehrstuhl D für Mathematik, RWTH Aachen, 2004.

[CR90] Charles W. Curtis und Irving Reiner. Methods of Representation Theory, Vol. I. Wiley, 1990.

[GAP05] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.4, 2005. (`http://www.gap-system.org`).

[GW95] Roderick Gow und Wolfgang Willems. Methods to decide if simple self-dual modules over fields of characteristic 2 are of quadratic type. Journal of Algebra, 175:1067–1081, 1995.

[GW97] Rod Gow und Wolfgang Willems. On the quadratic type of some simple self-dual modules over fields of characteristic two. Journal of Algebra, 195:634–649, 1997.

[HB82] B. Huppert und N. Blackburn. Finite Groups II. Springer-Verlag, 1982.

[Hen96] Anne Henke. Zur Berechnung der 7-modularen Charaktertafel der sporadischen Gruppe von O'Nan. Universität Heidelberg, 1996. Diplomarbeit.

[HEO05] Derek Holt, Bettina Eick und Eamonn O'Brien. Handbook of Computational Group Theory. CRC Press, 2005.

[Hup67] B. Huppert. Endliche Gruppen I. Springer-Verlag, 1967.

[Jan95] Christoph Jansen. Ein Atlas 3-modularer Charaktertafeln. M+M Wissenschaftsverlag, 1995.

[JL01] Gordon James und Martin Liebeck. Representations and Characters of Groups. Cambridge University Press, 2001.

[JLPW95] C. Jansen, K. Lux, R Parker und R. Wilson. An Atlas of Brauer Characters. Oxford University Press, 1995.

[Kün06] Matthias Künzer. (Co)homologie von Gruppen. RWTH Aachen, Lehrstuhl D für Mathematik, 2006. (http://www.math.rwth-aachen.de/~Matthias.Kuenzer/cohomologie/).

[Kne02] Martin Kneser. Quadratische Formen. Springer-Verlag, 2002.

[Lux97] Klaus Lux. Algorithmic Methodes in Modular Representation Theory. RWTH Aachen, 1997. Habitilationsschrift.

[Neb06] Gabriele Nebe. Quadratische Formen. Vorlesung, RWTH Aachen, 2005 / 2006.

[Ney04] H. Ney. Algorithmen und Datenstrukturen. RWTH Aachen, Lehrstuhl für Informatik VI, 2004. (http://www-i6.informatik.rwth-aachen.de/web/Teaching/LectureNotes/).

[Noe05] Felix Noeske. Morita-Äquivalenzen in der algorithmischen Darstellungstheorie. RWTH Aachen, 2005. Dissertation.

[OR74] Oeljeklaus und Remmert. Lineare Algebra I. Springer-Verlag, 1974.

[Ryb90] A. J. E. Ryba. Computer condensation of modular representations. J. Symb. Comput., 9(5/6):591–600, 1990.

[Tha02a] Jon Thackray. Computing orthogonal group signs. In Nikolauskonferenz 2002, Lehrstuhl D für Mathematik, RWTH Aachen, 2002.

[Tha02b] Jon Thackray. Some new results from computational modular representation theory. Unpubliziert, Juni 2002.

[Wie94] M. Wiegelmann. Fixpunktkondensation von Tensorproduktmoduln. Aachen, 1994. Diplomarbeit.

[Wil] Robert A. Wilson. ATLAS of Finite Group Representations. (http://web.mat.bham.ac.uk/atlas/v2.0).

Stichwortverzeichnis

Die ***fett***gedruckte Seitenzahl verweist auf die Definition des Begriffs.

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig und nur unter Benutzung der angegebenen Hilfsmittel angefertigt habe.