

DEPARTEMENT FÜR MATHEMATIK
EIDGENÖSSISCHE TECHNISCHE HOCHSCHULE ZÜRICH

EINE VERALLGEMEINERUNG DER
KOMPOSITION VON
QUADRATISCHEN FORMEN

Diplomarbeit
von
Roland Lötscher
(rolandlo@gmail.com)

WS 2005/06

Ausgeführt unter der Leitung von

Prof. Dr. Max-Albert Knus
Mathematik-Departement
ETH Zürich

Inhaltsverzeichnis

Einleitung	2
1 Grundbegriffe	5
1.1 Azumaya-Algebren	5
1.2 Involutionen	9
1.3 Quadratische und hermitesche Räume	10
1.4 Quadratische und hermitesche Kompositionen	14
1.5 Die Clifford-Algebra	15
2 Kompositionen über kommutativen Ringen	18
2.1 Charakterisierung von hermiteschen Kompositionen	18
2.2 Minimale Kompositionen	19
2.3 Zusammenhang von symmetrischer und quadratischer Komposition	24
2.4 Spur von Kompositionen	27
3 Komposition von quadratischen Paaren	29
3.1 Quadratische Paare	29
3.2 Clifford-Algebra von quadratischen Paaren	31
3.3 Verallgemeinerung des Kompositionsproblems	33
3.4 Minimale Kompositionen	35
3.5 Kompositionspaare	45
3.6 Beispiele von Kompositionen	47
Literaturverzeichnis	50

Einleitung

Wir untersuchen in der vorliegenden Arbeit Kompositionen von quadratischen Formen und eine Verallgemeinerung solcher Kompositionen. Das ursprüngliche Kompositionsproblem geht auf den deutschen Mathematiker Adolf Hurwitz (1859-1919) zurück und lässt sich wie folgt formuliert werden: Für welche Werte von s und n existiert eine Formel

$$(x_1^2 + \cdots + x_s^2) \cdot (y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2,$$

wobei z_1, \dots, z_n Bilinearformen in den Variablen $x_1, \dots, x_s; y_1, \dots, y_n$ und Koeffizienten in einem Körper F sind. Die Aufgabe wurde von A. Hurwitz in der Arbeit [Hur98] für den Körper $F = \mathbb{C}$ der komplexen Zahlen gelöst. Später hat J. Radon in [Rad22] die Aufgabe für reelle Koeffizienten gelöst. Seine Formulierung der Antwort besagt, dass solche (reellen) Bilinearformen dann und nur dann existieren, wenn $s \leq \rho(n)$ ist für eine Funktion $\rho: \mathbb{N} \rightarrow \mathbb{N}$, welche seitdem Radon-Hurwitz-Funktion genannt wird und wie folgt gegeben ist: Sei $n = n_0 \cdot 2^{4a+b}$ für n_0 ungerade und $0 \leq b < 4$. Dann ist $\rho(n) = 8a + 2^b$. In dieser Antwort ist als einfache Folgerung enthalten, dass solche Bilinearformen für $n = s$ nur dann existieren, wenn $n = 1, 2, 4$ oder 8 ist.

Hurwitz und Radon arbeiteten mit Systemen von orthogonalen Matrizen. B. Eckmann hat schliesslich in [Eck43] einen Beweis gegeben, der auf grundlegenden Sätzen der Darstellungstheorie endlicher Gruppen basiert. Er betrachtete die Gruppe G , welche durch Erzeugende $a_1, \dots, a_{p-1}, \varepsilon$ und Relationen $\varepsilon^2 = 1, a_k^2 = \varepsilon, \varepsilon a_k = a_k \varepsilon, a_k a_l = \varepsilon a_l a_k$ für $k, l = 1, \dots, p-1; k \neq l$ gegeben ist. Eine Kompositionsformel der obigen Form (mit komplexen Koeffizienten) ist dann äquivalent zu einer Darstellung von G durch orthogonale $n \times n$ -Matrizen, bei welcher ε durch die Matrix $-E$ dargestellt wird.

Später wurde das Kompositionsproblem von verschiedenen Autoren verallgemeinert. Den Körper der reellen oder komplexen Zahlen hat man durch einen beliebigen Körper F und die Summe von Quadraten durch eine beliebige (reguläre) quadratische Formen ersetzt. Eine Komposition von zwei

quadratischen Räumen (V, q) und (W, p) über F wird dann als bilineare Abbildung $\phi: V \times W \rightarrow W$ mit der Eigenschaft

$$p(\phi(v, w)) = q(v)p(w) \text{ für alle } v \in V, w \in W$$

definiert. In den Siebzigerjahren konnte D. Shapiro beweisen, dass es für beliebige Körper von $\text{char } F \neq 2$ genau dann zwei quadratische Räume (V, q) und (E, p) mit $\dim V = s$, $\dim E = n$ und eine Komposition $\phi: V \times W \rightarrow W$ gibt, falls $s \leq \rho(n)$. Auch untersuchte er die quadratischen Formen, welche eine Komposition erlauben. Shapiros Ergebnisse und vieles mehr über Kompositionen von quadratischen Formen kann in seinem Buch [Sha00] nachgelesen werden. Er verwendet für die Untersuchung folgende Beobachtung: Ist $\phi: V \times W \rightarrow W$ eine Komposition zweier quadratischer Räume (V, q) und (W, p) , so ist der Endomorphismus $\phi_v \in \text{End}_F(W)$ gegeben durch $\phi_v(w) = \phi(v, w)$ eine Ähnlichkeitsabbildung mit Faktor $q(v)$. Die Abbildung

$$V \rightarrow \text{Sim}(W, p), v \mapsto \phi_v$$

bettet V als linearen Teilraum in den Raum der Ähnlichkeitsabbildungen von (W, p) ein. Umgekehrt liefert ein linearer Teilraum $S \subset \text{Sim}(W, p)$ eine Komposition $\phi: S \times W \rightarrow W$, sofern die Norm von Ähnlichkeitsabbildungen auf S eine reguläre quadratische Form induziert. Es genügt also, lineare Teilräume von $\text{Sim}(W, p)$ zu studieren um das Kompositionsproblem zu lösen. Mit ähnlichen Methoden hat J. Junker in seiner Diplomarbeit [Jun80] das Problem für Körper von Charakteristik 2 behandelt. Er hat auch für Körper von Charakteristik 2 eine Funktion $\rho': \mathbb{N} \rightarrow \mathbb{N}$ mit der Eigenschaft gefunden, dass Kompositionen $\phi: V \times W \rightarrow W$ mit $\dim V = s$, $\dim W = n$ dann und nur dann existieren, falls $s \leq \rho'(n)$. Diese Funktion unterscheidet sich jedoch von der Radon-Hurwitz Funktion für Körper von Charakteristik $\neq 2$. Es ist $\rho'(n_0 \cdot 2^{2a+b}) = 4a + 4^b$ für n_0 ungerade und $b = 0, 1$ falls $2a + b > 2$ und $\rho'(n_0 \cdot 2^{2a+b}) = 2^{2a+b}$ falls $2a + b \leq 2$.

Das Kompositionsproblem steht auch im Zusammenhang mit Cliffordalgebren und ihren Darstellungen. In [Lam73] wird mit ihrer Hilfe das Hurwitzproblem (über den reellen Zahlen) gelöst. Lam reduziert das Problem auf Kompositionen $\phi: V \times W \rightarrow W$, in denen ϕ_z für ein $z \in V$ die Identität ist. Sei V_0 das orthogonale Komplement von $F \cdot z$ und q_0 die Restriktion der quadratischen Form von V auf V_0 . Dann erlaubt die Cliffordalgebra $C(V_0, -q_0)$ eine Darstellung auf W durch $C(V_0, -q_0) \rightarrow \text{End}_F(W)$, $v \mapsto \phi_v$. Durch die Analyse der Struktur der Cliffordalgebren $C(\langle -1, \dots, -1 \rangle)$ und durch Konstruktion von Kompositionen mit Hilfe der (komplexen) Darstellungstheorie erhält Lam das gleiche Resultat wie zuvor Radon und Hurwitz.

Die vorliegende Arbeit basiert vor allem auf den Arbeiten [Züg95] und [Eld02], welche beide zur Lösung des Kompositionsproblems Cliffordalgebren einsetzen und grundlegende Eigenschaften der kanonischen Involution und der Standardinvolution einer Cliffordalgebra, sowie ihrer Restriktion auf die gerade Teilalgebra verwenden. Während Elduques Arbeit nur für Körper von Charakteristik 2 geschrieben ist, betrachtet Züger Kompositionen über einem beliebigen kommutativen Ring R . Ausserdem untersucht Züger nicht nur Kompositionen mit quadratischen Formen, sondern auch mit antisymmetrischen Formen und hermiteschen Formen über quadratischen und Quaternionen-Algebren.

Der Text ist wie folgt aufgebaut: Im 1. Kapitel werden die Grundbegriffe eingeführt. Im 2. Kapitel werden Kompositionen über kommutativen Ringen betrachtet. Wir geben zuerst ein allgemeines Theorem, welches hermitesche Kompositionen in der Sprache der Algebren mit Involutionen beschreibt. Dann untersuchen wir den Zusammenhang von Kompositionen mit quadratischen Formen und Kompositionen mit symmetrischen Bilinearformen. Mit Hilfe dieser Untersuchung kann ein Fehler aus R. Zügers Arbeit korrigiert werden, welcher von A. Elduque bemerkt wurde und für Ringe, in denen 2 nicht invertierbar ist, Zügers Resultate zu quadratischen Kompositionen in Frage stellt. Das 3. Kapitel schränkt sich wieder auf Kompositionen über einem Körper F ein. Allerdings verallgemeinern wir dort das Kompositionsproblem auf quadratische Paare und (anti-)hermitesche Formen über beliebigen Azumaya-Algebren, deren Zentrum entweder F oder eine quadratische separable Erweiterung von F ist. Unsere Verallgemeinerung beruht auf der im 2. Kapitel gegebenen Charakterisierung von Komposition und auf der Tatsache, dass es auf quadratischen Paaren eine Verallgemeinerung der geraden Cliffordalgebra und ihrer kanonischen Involution gibt. Wir konstruieren für beliebige quadratische Paare Kompositionen und zeigen, dass diese Konstruktionen optimal sind für Kompositionen mit (anti-)hermiteschen Formen über einer vorgegebenen Azumaya-Algebra. In der Folge erhalten wir notwendige und hinreichende Bedingungen für Kompositionen die nicht nur optimal für ein vorgegebenes quadratisches Paar sind, sondern unter allen Kompositionen bei festem Grad des quadratischen Paares. Die Arbeit wird mit einer Anwendung zur Verallgemeinerung von Kompositionsalgebren auf quadratische Paare und einigen Beispielen zu Ende geführt.

An dieser Stelle möchte ich dem Betreuer dieser Diplomarbeit, Prof. Knus, herzlich für die inspirierenden Besprechungen und hilfreichen Literaturhinweise danken.

Kapitel 1

Grundbegriffe

In diesem Kapitel sind einige Begriffe und Sätze aus der Theorie der quadratischen und hermiteschen Formen sowie der Azumaya-Algebren wiedergegeben. Die meisten Beweise für die im Folgenden formulierten Theoreme befinden sich in [Knu91].

1.1 Azumaya-Algebren

In dieser Arbeit werden Ringe als assoziativ mit 1 vorausgesetzt. Moduln werden als Rechts-Moduln betrachtet. Für einen Ring A und einen Teilring $B \subset A$ bezeichnet $C_A(B) = \{r \in A \mid ab = ba \ \forall b \in B\}$ den *Zentralisator* von B in A und $Z(A) = C_A(A)$ das *Zentrum* von A . Mit R bezeichnen wir jeweils einen kommutativen Ring und mit F einen beliebigen Körper. Unter einer Algebra über R wird ein Ring A zusammen mit einem Ringhomomorphismus $\iota: R \rightarrow Z(A)$ verstanden. Für eine R -Algebra A bezeichnet A^{op} die *entgegengesetzte Algebra* mit Elementen $\{a^{\text{op}} \mid a \in A\}$, welche die gleiche R -Modul-Struktur wie A trägt, jedoch die umgekehrte Multiplikation: $a^{\text{op}} \cdot b^{\text{op}} = (ba)^{\text{op}}$. Weiter bezeichnet $A^e = A \otimes A^{\text{op}}$ die *einhängende Algebra*. Die Algebra A ist auf natürliche Weise ein A^e -Modul gegeben durch $(a \otimes b^{\text{op}}) \cdot x = axb$. Man nennt A *separabel*, falls A auf obige Weise ein projektiver A^e -Modul ist. Ausserdem heisst A *zentral*, falls $\iota: R \rightarrow Z(A)$ ein Isomorphismus ist.

Für einen Körper F fallen die endlich dimensional zentralen, separablen F -Algebren mit den endlich dimensional *zentral einfachen* Algebren zusammen. Matrizenalgebren über Körpern sind wichtige Beispiele von zentral einfachen Algebren. Unter Skalarerweiterung wird jede endlich dimensionale zentral einfache F -Algebra isomorph zu einer Matrizenalgebra. Wir betrachten eine Klasse von R -Algebren, genannt *Azumaya-Algebren*, welche

den Begriff von endlich dimensionalen zentral einfachen F -Algebren verallgemeinert. Azumaya R -Algebren von konstantem Rang lassen sich dadurch charakterisieren, dass sie unter einer (treu flachen, étalen) Erweiterung von R zu einer Matrizenalgebra zerfallen. Die genaue Definition der Azumaya-Algebren und verschiedene Charakterisierungen sind im Folgenden gegeben:

Definition 1.1.1 *Ein R -Modul M heisst treu flach, falls der Tensorprodukt-Funktor $- \otimes M$ exakt und treu ist. Eine R -Algebra S heisst treu flach, falls sie treu flach als R -Modul ist und étale, falls sie flach, endlich darstellbar und separabel ist. Ein R -Modul P heisst treu projektiv, falls P endlich erzeugt projektiv ist und für alle R -Module N aus $P \otimes N = 0$ folgt, dass $N = 0$ ist.*

Definition 1.1.2 *Eine R -Algebra A heisst Azumaya-Algebra (über R), falls sie folgende Bedingungen erfüllt:*

1. A ist zentral.
2. A ist separabel.
3. A ist als R -Modul treu projektiv.

Lemma 1.1.3 *Ist A eine Azumaya-Algebra über R und S eine kommutative R -Algebra, so ist $A \otimes S$ eine Azumaya-Algebra über S . Das Tensorprodukt zweier Azumaya-Algebren über R ist eine Azumaya-Algebra über R .*

Theorem 1.1.4 *Sei A eine treu projektive R -Algebra. Dann sind folgende Aussagen äquivalent:*

- A ist eine Azumaya-Algebra.
- $A^e \xrightarrow{\text{can}} \text{End}_R(A)$, $\text{can}(a \otimes b^{\text{op}})(x) = axb$ ist ein Isomorphismus.
- Es gibt eine treu flache, étale R -Algebra S und einen treu projektiven S -Modul P mit $A \otimes S \simeq \text{End}_S(P)$.

Theorem 1.1.5 *Sei A eine treu projektive R -Algebra von konstantem Rang. Dann sind folgende Aussagen äquivalent:*

- A ist eine Azumaya-Algebra.
- Es gibt eine treu flache, étale R -Algebra S mit $A \otimes S \simeq M_m(S)$ für $m \in \mathbb{N}$, $m^2 = \text{Rg } A$. Wir nennen m den Grad von A , notiert $\text{deg } A$.

Lemma 1.1.6 *Sei A eine R -Azumaya Algebra. Jedes beidseitige Ideal $J \subset A$ ist von der Form $J = IA$ für ein maximales Ideal $I \subset R$. Jeder Homomorphismus $f: A \rightarrow B$ in eine als R -Modul treue R -Algebra B ist injektiv. Es gilt $B \simeq A \otimes C_B(f(A))$. Ist B ebenfalls Azumaya über R , so auch $C_B(f(A))$. Jeder Homomorphismus von R -Azumaya-Algebren gleichen Ranges ist ein Isomorphismus.*

Bemerkung Für Azumaya-Algebren über einem Körper F kennt man einen Kürzungssatz: Ist $A \otimes B \simeq A \otimes C$ für F -Azumaya-Algebren A, B, C , so gilt $B \simeq C$. Allgemein ist diese Aussage jedoch falsch. Immerhin gilt der Kürzungssatz für halblokale Ringe R (siehe [Knu91, S. 144]), insbesondere für $R = F \times F$.

Wie für endlich dimensionale zentral einfache Algebren lässt sich auch für Azumaya-Algebren eine Brauer-Gruppe definieren. Zwei Azumaya-Algebren A und B über R heissen *Brauer-äquivalent*, falls eine der folgenden äquivalenten Bedingungen zutrifft:

- Es gibt treu projektive R -Moduln P_1, P_2 mit $A \otimes \text{End}_R(P_1) \simeq B \otimes \text{End}_R(P_2)$.
- Es gibt einen treu projektiven A -Modul P mit $B \simeq \text{End}_A(P)$.

Die Klasse der R -Azumaya-Algebren bildet eine Menge und ein abelsches Monoid mit Neutralelement bezüglich des Tensorprodukts. Nimmt man den Quotient modulo Braueräquivalenz, so erhält man eine Gruppe.

Definition 1.1.7 *Der Quotient des Monoids von R -Azumaya-Algebren modulo Braueräquivalenz heisst Brauergruppe, notiert $\text{Br}(R)$. Die Äquivalenzklasse einer R -Azumaya-Algebra A wird mit $[A]$ notiert.*

Wir führen noch eine andere Gruppe ein, die in engem Zusammenhang mit der Brauergruppe steht und später relevant wird. Der Grund liegt darin, dass wir es in dieser Arbeit fast ausschliesslich mit Azumaya-Algebren von konstantem Rang zu tun haben werden, auch wenn das Zentrum nicht zusammenhängendes Spektrum hat. Wir möchten eine solche Azumaya-Algebra nicht als äquivalent betrachten zu einer Azumaya-Algebra von nicht konstantem Rang. Die Klasse der R -Azumaya-Algebren von konstantem Rang bildet ein Monoid mit Neutralelement und die Klasse der Endomorphismenalgebren von konstantem Rang ein Untermonoid. Nimmt man den Quotient, so erhält man wiederum eine Gruppe.

Definition 1.1.8 Nenne zwei R -Azumaya konstant Brauer-äquivalent, falls treu projektive R -Moduln P_1, P_2 von konstantem Rang existieren mit $A \otimes \text{End}_R(P_1) \simeq B \otimes \text{End}_R(P_2)$. Der Quotient des Monoids von R -Azumaya-Algebren von konstantem Rang modulo konstante Braueräquivalenz heisst konstante Brauergruppe, notiert $\text{Br}_c(R)$. Die Äquivalenzklasse einer R -Azumaya-Algebra A von konstantem Rang wird mit $[A]_c$ notiert.

Für Ringe mit zusammenhängendem Spektrum bringt die Definition nichts Neues. Im allgemeinen Fall gibt es einen Homomorphismus $\psi: \text{Br}_c(R) \rightarrow \text{Br}(R)$, $[A]_c \mapsto [A]$. Jener ist sogar ein Isomorphismus:

Lemma 1.1.9 1. Für eine beliebige R -Azumaya-Algebra A gibt es einen treu projektiven R -Modul P , so dass $A \otimes \text{End}_R(P)$ konstanten Rang hat.

2. Die Abbildung $\text{Br}(R) \rightarrow \text{Br}_c(R)$, $[A] \mapsto [A \otimes \text{End}_R(P)]_c$ für ein R -Modul P wie oben ist wohldefiniert und bildet die Inverse zu ψ .

Beweis Für die erste Aussage zerlegen wir R in ein endliches Produkt $R = R_1 \times \cdots \times R_l$ und schreiben A als $A = A_1 \times \cdots \times A_l$ derart, dass A_i eine R_i -Azumaya-Algebra von konstantem Rang n_i^2 ist. Sei $n = n_1 \cdots n_l$ und $P_i = R_i^{n/n_i}$, $i = 1, \dots, l$. Dann ist $P_1 \oplus \cdots \oplus P_l$ ein treu projektives R -Modul und $A \otimes \text{End}_R(P)$ hat konstanten Rang n^2 . Zeigen wir die zweite Aussage: Falls $A \otimes \text{End}_R(P_1)$ und $A \otimes \text{End}_R(P_2)$ konstanten Rang haben, so ist $(A \otimes \text{End}_R(P_1)) \otimes (A \otimes \text{End}_R(P_2))^{\text{op}} \simeq \text{End}_R(A \otimes P_1 \otimes P_2)$ eine Endomorphismenalgebra eines R -Moduls von konstantem Rang. Es folgt $[A \otimes \text{End}_R(P_1)]_c = [A \otimes \text{End}_R(P_2)]_c$ und Wohldefiniertheit ist gezeigt. Dass die beiden Abbildungen invers sind, folgt nun einfach daraus, dass Endomorphismenalgebren triviale Brauerklasse haben. \square

Für eine R -Azumaya Algebra von konstantem Rang definieren wir einen Index, der den Index einer Azumaya-Algebren über einem Körper F verallgemeinert. Jener ist gegeben durch $\deg D$ falls $A \simeq M_r(D)$ für ein $r \in \mathbb{N}$ und eine Divisionsalgebra D .

Definition 1.1.10 Sei A eine R -Azumaya Algebra von konstantem Rang. Wir nennen das Minimum $\min \deg B$ über alle Azumaya-Algebren B mit $[B]_c = [A]_c$ den Index von A und schreiben $\text{ind } A$.

Besonders wichtig im 3. Kapitel werden die Spezialfälle 1) $R = F$ und 2) $R = F \times F$ für einen Körper F sein. Die Struktur von Azumaya-Algebren über diesen Ringen und ihre Brauergruppe lassen sich genau beschreiben.

Theorem 1.1.11 1. $R = F$: (Wedderburn): Jede R -Azumaya Algebra ist isomorph zu $M_r(D)$ für ein $r \in \mathbb{N}$ und eine zentral einfache Divisionsalgebra D , welche bis auf Isomorphie eindeutig bestimmt ist. Umgekehrt ist jede Algebra von dieser Form Azumaya über R .

2. $R = F \times F$: Jede R -Azumaya Algebra ist isomorph zu einer Algebra der Form $M_{r_1}(D_1) \times M_{r_2}(D_2)$ für $r_1, r_2 \in \mathbb{N}$ und zentral einfache Divisionsalgebren D_1, D_2 , welche bis auf Isomorphie eindeutig bestimmt sind. Umgekehrt ist jede Algebra von dieser Form Azumaya über R . Die R -Azumaya Algebren A von konstantem Rang sind genau diejenigen für welche $r_1 \deg(D_1) = r_2 \deg(D_2)$ ($= \deg A$) gilt.

Lemma 1.1.12 Sei A eine Azumaya-Algebra über $R = F \times F$ von konstantem Rang, also $A = A_1 \times A_2$ für zentral einfache Algebren A_1, A_2 von gleichem Grad. Der oben definierte Index von A ist $\text{ind } A = \text{kgV}(\text{ind } A_1, \text{ind } A_2)$. Ausserdem teilt der Index von A den Grad von A .

Beweis Laut obigem Theorem existieren $r_1, r_2 \in \mathbb{N}$ und zentral einfache Divisionsalgebren D_1, D_2 mit $A_1 \simeq M_{r_1}(D_1)$, $A_2 \simeq M_{r_2}(D_2)$ und $r_1 \deg(D_1) = r_2 \deg(D_2) = \deg A$. Es folgt $\text{ind } A_1 \mid \deg A$, $\text{ind } A_2 \mid \deg A$ und insbesondere $\text{kgV}(\text{ind } A_1, \text{ind } A_2) \mid \deg A$. Da jede R -Azumaya-Algebra $B \simeq B_1 \times B_2$ von konstantem Rang mit $[B]_c = [A]_c$ von dieser Form ist, gilt auch $\text{kgV}(\text{ind } A_1, \text{ind } A_2) \mid \text{ind } A$. Für $k_1 = \frac{\text{kgV}(\text{ind } A_1, \text{ind } A_2)}{\text{ind } A_1}$, $k_2 = \frac{\text{kgV}(\text{ind } A_1, \text{ind } A_2)}{\text{ind } A_2}$ ist $k_1 \text{ind } A_1 = k_2 \text{ind } A_2$ und die Azumaya-Algebra $B = M_{k_1}(D_1) \times M_{k_2}(D_2)$ erfüllt $\deg B = \text{kgV}(\text{ind } A_1, \text{ind } A_2)$ und $[B]_c = [A]_c$. \square

Bemerkung Nach Theorem (1.1.4) gibt es für eine R -Azumaya Algebra eine treu flache, étale R -Algebra S für welche $A \otimes S \simeq M_m(S)$. In den beiden Spezialfällen $R = F$, $R = F \times F$ lässt sich S als $S = L$ bzw. $S = L \times L$ für eine (galoissche) Körpererweiterung $L \supset F$ wählen. Für $R = F$ ist dies wohlbekannt. Für $R = F \times F$, $A \simeq M_{r_1}(D_1) \times M_{r_2}(D_2)$ existieren (galoissche) Körpererweiterungen L_1, L_2 mit $M_{r_i}(D_i) \otimes L_i \simeq M_{r_i \deg D_i}(L_i)$, $i = 1, 2$. Wähle nun für L eine (galoissche) Körpererweiterung von F , die sowohl L_1 wie auch L_2 enthält. Damit ist $A \otimes (L \times L) \simeq M_{r_1 \deg D_1}(L) \times M_{r_2 \deg D_2}(L)$.

1.2 Involutionen

Definition 1.2.1 Sei B eine R -Azumaya-Algebra. Eine Abbildung $\tau: B \rightarrow B$ heisst Involution, falls sie folgende Bedingungen erfüllt:

1. $\tau(x + y) = \tau(x) + \tau(y)$ für alle $x, y \in B$.

2. $\tau(xy) = \tau(y)\tau(x)$ für alle $x, y \in B$.

3. $\tau^2(x) = x$ für alle $x \in B$.

Die Restriktion von τ auf R ist eine Involution von R . Ist τ R -linear, so heisst sie von 1. Art, ansonsten von 2. Art oder unitär.

Seien σ und τ zwei Involutionen auf einer Azumaya-Algebra A . Haben σ und τ die gleiche Restriktion auf das Zentrum, so ist auch $\sigma \otimes \tau$ eine Involution. Die Existenz eines Zerfällungsrings $S \supset R$, d.h. einer treu flachen, étalen Erweiterung mit $A \otimes S \simeq M_m(S)$, kann dazu benutzt werden, jeder Involution 1. Art einen Typ zuzuweisen. Wir machen das hier nur für Azumaya-Algebren über einem Körper F . Dazu brauchen wir die Beschreibung der Automorphismen einer Azumaya-Algebra durch den Satz von Skolem-Noether:

Theorem 1.2.2 Sei A eine F -Azumaya-Algebra und f ein Automorphismus von A . Dann existiert $u \in A^\times$ mit $f(x) = uxu^{-1}$ für alle $x \in A$.

Definition 1.2.3 Sei τ eine Involution 1. Art auf einer F -Azumaya-Algebra A . Sei $\beta: A \otimes L \xrightarrow{\cong} M_r(L)$ eine Zerfällung und $\tilde{\tau} = \beta(\tau \otimes \text{id}_L)\beta^{-1}$ die auf $M_r(L)$ transportierte Involution. Dann ist $\forall x: \tilde{\tau}(x) = ux^t u^{-1}$ für ein $u \in M_r(L)^\times$ mit $u^t = \pm u$. Die Involution τ heisst symplektisch, falls u eine alternierende Matrix ist, sonst heisst τ orthogonal.

Falls $\text{char } F \neq 2$, so ist das Tensorprodukt zweier Involutionen 1. Art σ und τ orthogonal gdw. σ und τ den gleichen Typ haben. Ist hingegen $\text{char } F = 2$, so ist $\sigma \otimes \tau$ symplektisch gdw. mindestens eine der Involutionen σ und τ symplektisch ist.

1.3 Quadratische und hermitesche Räume

Der Rang aller betrachteten quadratischen und hermiteschen Module wird als konstant vorausgesetzt.

Definition 1.3.1 Sei M ein endlich erzeugtes projektives R -Modul und sei $q: M \rightarrow R$ eine Abbildung. Das Paar (M, q) heisst quadratisches Modul, falls folgende Bedingungen erfüllt sind:

- $q(rx) = r^2q(x)$ für alle $x \in M, r \in R$,
- Die Polare b_q definiert durch $b_q(x, y) = q(x + y) - q(x) - q(y)$ ist R -bilinear.

Falls b_q zudem nichtsingulär ist, d.h. falls $\hat{b}_q: M \rightarrow M^*$, $\hat{b}_q(x)(y) = b_q(x, y)$ ein Isomorphismus ist, so heisst (M, q) ein regulärer quadratischer Raum. Existiert zudem ein Element $z \in M$ mit $q(z) = 1$, so nennen wir (M, q) einen punktierten Raum.

Beispiel Sei $(M, q) = (R^{2k}, q_H)$ mit $q_H(x_1, y_1, \dots, x_k, y_k) = x_1y_1 + \dots + x_ky_k$. Das Paar (M, q_H) ist ein regulärer quadratischer Raum über R vom Rang $2k$, bezeichnet als *hyperbolischer Raum* über R^k und notiert $H(R^k)$.

Für Ringe R mit $2 \notin R^\times$ gibt es keine regulären quadratischen Räume (M, q) von ungeradem Rang. Man betrachtet daher sogenannte halbreguläre quadratische Räume, welche einer schwächeren Bedingung genügen, jedoch viele gute Eigenschaften mit regulären quadratischen Räumen teilen. Für die Definition brauchen wir folgendes Lemma:

Lemma 1.3.2 Sei n ungerade, $R_0 = \mathbb{Z}[\xi_i, \xi_{ij}]$ der Polynomring über Unbestimmten ξ_i, ξ_{ij} für $i, j = 1, \dots, n, i < j$. Sei M der freie Modul R_0^n mit Basis e_1, \dots, e_n und q_0 die quadratische Form gegeben durch $q_0(e_i) = \xi_i, b_{q_0}(e_i, e_j) = b_{q_0}(e_j, e_i) = \xi_{ij}, i < j$. Dann existiert ein Polynom $P_n(\xi_i, \xi_{ij}) \in \mathbb{Z}[\xi_i, \xi_{ij}]$ mit $\det(b_{q_0}(e_i, e_j)) = 2P_n(\xi_i, \xi_{ij})$.

Definition 1.3.3 Sei (M, q) ein quadratisches R -Modul von Rang $n = 2k + 1$ und P_n das Polynom aus obigem Lemma. Das Ideal von R , welches von allen Elementen der Form $d_0(x_1, \dots, x_n) = P_n(q(x_i), b_q(x_i, x_j))$ für $x_i \in M$ erzeugt wird, heisst halb-Diskriminanten Ideal, notiert $d_0(M, q)$. Ist $d_0(M, q) = R$, so heisst (M, q) ein halbregulärer quadratischer Raum. Ein quadratischer Raum (M, q) ist ein halbregulärer quadratischer Raum, falls $\text{Rg } M$ ungerade ist, bzw. ein regulärer quadratischer Raum, falls $\text{Rg } M$ gerade ist.

Für quadratische Räume erweist es sich häufig als nützlich, den Ring so zu erweitern, dass die Struktur des quadratischen Raumes möglichst einfach wird. Wir bezeichnen für einen quadratischen Raum (M, q) und eine kommutative R -Algebra S den quadratischen Raum $(M \otimes S, q \otimes id_S)$ mit $(M, q) \otimes S$.

Lemma 1.3.4 Sei (M, q) ein quadratischer Raum von Rang n . Es gibt eine treu flache kommutative R -Algebra S mit $(M, q) \otimes S \simeq H(S^k)$ (falls $n = 2k$) bzw. $(M, q) \otimes S \simeq H(S^k) \perp \langle 1_S \rangle$ (falls $n = 2k + 1$).

Definition 1.3.5 Sei A ein (nicht notwendigerweise kommutativer) Ring mit einer Involution $a \mapsto \bar{a}$. Sei E ein treu projektives, endlich erzeugtes A -Rechtsmodul. Sei $h: E \times E \rightarrow A$ eine Abbildung und $\varepsilon = \pm 1$. Wir nennen (E, h) einen ε -hermiteschen Raum, falls folgende Bedingungen erfüllt sind:

1. $h(x_1 + x_2, y) = h(x_1, y) + h(x_2, y)$ für alle $x_1, x_2, y \in E$.
 $h(x, y_1 + y_2) = h(x, y_1) + h(x, y_2)$ für alle $x, y_1, y_2 \in E$.
2. $h(xa, yb) = \bar{a}h(x, y)b$ für alle $x, y \in E, a, b \in A$.
3. $h(y, x) = \varepsilon \overline{h(x, y)}$ für alle $x, y \in E$.
4. Die Abbildung $\hat{h}: E \rightarrow E^*$, $\hat{h}(x)(y) = h(x, y)$ ist ein Isomorphismus von A -Rechtsmoduln.

Anstatt von ε -hermiteschen Räumen sprechen wir auch von hermiteschen Räumen (falls $\varepsilon = 1$) bzw. antihermiteschen Räumen (falls $\varepsilon = -1$). Ein ε -hermitescher Raum (E, h) heisst alternierender Raum falls $h(y, y) = 0$ für alle $y \in E$.

Lemma 1.3.6 Sei (E, h) ein ε -hermitescher Raum über einer R -Algebra A mit Involution σ und S eine kommutative R -Algebra. Sei $h_S: E \otimes S \times E \otimes S \rightarrow A \otimes S$ definiert durch $h(x \otimes s_1, y \otimes s_2) = h(x, y) \otimes (s_1 s_2)$. Dann ist $(E, h) \otimes S = (E \otimes S, h_S)$ ein ε -hermitescher Raum über der S -Algebra $A \otimes S$ mit Involution $\sigma \otimes \text{id}_S$.

Jedem ε -hermiteschen Raum (E, h) über A lässt sich eine Involution σ_h auf $\text{End}_A(E)$ zuordnen mit der Eigenschaft:

$$h(f(x), y) = h(x, \sigma_h(f)(y)) \text{ für alle } x, y \in E, f \in \text{End}_A(E).$$

Man nennt σ_h die adjungierte Involution bezüglich h und definiert sie durch

$$\sigma_h(f) = \hat{h}^{-1} \circ f^* \circ \hat{h}.$$

Für R -Azumaya-Algebren A mit Involution gibt es eine Umkehrung dieser Aussage: Jede Involution auf $\text{End}_A(E)$ gehört zu einer ε -hermiteschen Form, welche Werte auf $A \otimes I$ für ein invertierbares R -Modul I (d.h. ein R -Modul mit $I \otimes I^* \simeq R$) annimmt. Die allgemeine Aussage findet man in [Züg95] mit ergänzenden Beweisen in [Knu70]. Wir benötigen diese Umkehrung nur in den Spezialfällen von Kapitel 3. Dazu ist folgende Tatsache relevant:

Lemma 1.3.7 Seien A und B zwei Azumaya-Algebren über $R = F$ oder $R = F \times F$ mit $[A]_c = [B]_c$. Besitzt B eine Involution τ , so existiert auf A eine Involution θ mit $\theta|_R = \tau|_R$.

Das Lemma folgt im Wesentlichen daraus, dass Matrizenalgebren der Form $M_k(R)$ Involutionen besitzen, die auf R mit τ übereinstimmen. Für Details siehe [KMRT98] Proposition (3.15) und Bemerkung (3.20).

Bemerkung Für $R = F \times F$ und unitäre Involutionen ist es wesentlich, die konstante Brauergruppe zu verwenden. Zum Beispiel ist $[F \times M_2(F)] = 1$ in $\text{Br}(R)$, jedoch besitzt $F \times M_2(F)$ keine Involution, welche die Faktoren vertauscht. In [KMRT98] Bemerkung 3.20 wurde dem nicht Rechnung getragen.

Wie in [KMRT98] setzen wir für eine unitäre Involution τ einer Azumaya-Algebra über $R = F \times F$ voraus, dass $\tau|_R$ die Faktoren vertauscht. Das folgende Theorem ergibt sich aus obigem Lemma und aus Theorem (4.2) in [KMRT98]:

Theorem 1.3.8 *Sei B eine Azumaya-Algebra über einem Körper K . Schreibe $B = \text{End}_A(E)$ für eine beliebige K -Azumaya-Algebra A mit $[A] = [B]$ und ein treu projektives A -Modul E . Gibt es auf B eine Involution 1. Art (2. Art), so besitzt auch A eine Involution θ von 1. Art (bzw. 2. Art) und es gibt folgenden Zusammenhang zwischen ε -hermiteschen Formen auf E und Involutionen auf B :*

- *Falls θ von 1. Art ist, so definiert die Zuordnung $h \mapsto \sigma_h$ eine Bijektion zwischen nichtsingulären (bzgl. θ) ε -hermiteschen Formen auf E bis auf einen Faktor in K^\times und Involutionen erster Art auf B . Falls $\text{char } K \neq 2$, so haben die Involutionen σ_h auf $B = \text{End}_A(E)$ und θ auf A den gleichen Typ gdw. h hermitesch ist, bzw. entgegengesetzte Typen gdw. h antihermitesch ist. Falls $\text{char } K = 2$, so ist σ_h symplektisch gdw. h alternierend ist.*
- *Falls θ von 2. Art ist und $F \subset K$ der Teilkörper von zentral Invarianten ist, so definiert die Abbildung $h \mapsto \sigma_h$ eine Bijektion zwischen nichtsingulären (bzgl. θ) hermiteschen Formen auf E bis auf einen Faktor in F^\times und Involutionen von 2. Art auf B , welche F invariant lassen.*

Theorem 1.3.9 *Sei B eine Azumaya-Algebra über $R = F \times F$ und τ eine unitäre Involution auf B . Dann existiert eine F -Azumaya-Algebra B_0 mit*

$$(B, \tau) \simeq (B_0 \times B_0^{\text{op}}, \sigma),$$

wobei σ durch $\sigma(x, y^{\text{op}}) = (y, x^{\text{op}})$ definiert ist. Insbesondere hat B konstanten R -Rang. Schreibe $B = \text{End}_A(E)$ für eine beliebige R -Azumaya-Algebra mit $[A]_c = [B]_c$. Dann existiert auf A eine unitäre Involution θ und die Abbildung $h \mapsto \sigma_h$ definiert eine Bijektion zwischen nichtsingulären (bzgl. θ) hermiteschen Formen auf E bis auf einen Faktor in F^\times und Involutionen von 2. Art auf B , welche auf $R = F \times F$ die Faktoren vertauscht.

1.4 Quadratische und hermitesche Kompositionen

In diesem Abschnitt definieren wir quadratische und ε -hermitesche Kompositionen und geben ihre grundlegendsten Eigenschaften an.

Definition 1.4.1 *Seien (M, q) und (E, p) quadratische Räume. Eine Komposition von (M, q) mit (E, p) , genannt quadratische Komposition, ist eine bilineare Abbildung $\phi: M \times E \rightarrow E$, so dass*

$$\forall x \in M, \forall y \in E : p(\phi(x, y)) = q(x)p(y).$$

Wir schreiben dafür $\phi: (M, q) \times (E, p) \rightarrow (E, p)$.

Definition 1.4.2 *Sei (M, q) ein quadratischer Raum und (E, h) ein ε -hermitescher Raum über einer R -Algebra A mit Involution $a \mapsto \bar{a}$. Eine Komposition von (M, q) mit (E, h) , genannt ε -hermitesche Komposition, ist eine Abbildung $\phi: M \times E \rightarrow E$ mit folgenden Eigenschaften:*

- ϕ ist R -linear in der 1. Variablen und A -linear in der 2. Variablen
- $\forall x \in M, \forall y_1, y_2 \in E : h(\phi(x, y_1), \phi(x, y_2)) = q(x)h(y_1, y_2)$.

Wir schreiben dafür $\phi: (M, q) \times (E, h) \rightarrow (E, h)$. Falls die Involution auf A die Identität ist, so nennen wir ε -hermitesche Formen und Kompositionen auch ε -symmetrische Bilinearformen bzw. ε -symmetrische Kompositionen.

Notation Für eine Komposition $\phi: (M, q) \times (E, p) \rightarrow (E, p)$ oder $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ schreiben wir auch öfters $\phi_x \in \text{End}_A(E)$ für den Endomorphismus $E \rightarrow E$, $y \mapsto \phi(x, y)$.

Lemma 1.4.3 *Sei $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ eine ε -hermitesche Komposition und sei S eine kommutative R -Algebra. Dann ist auch die durch Erweiterung der Skalare gewonnene Abbildung $\phi_S: (M, q) \otimes S \times (E, h) \otimes S \rightarrow (E, h) \otimes S$ eine ε -hermitesche Komposition.*

Proposition 1.4.4 *Sei (M, q) ein quadratischer Raum über R und (E, h) ein ε -hermitescher Raum über einer R -Algebra A . Sei $\phi: M \times E \rightarrow E$ eine Abbildung, welche R -linear in der 1. Variablen und A -linear in der 2. Variablen ist. Sei $\phi_x \in \text{End}_A(E)$ definiert durch $\phi_x(y) = \phi(x, y)$. Dann sind folgende Aussagen äquivalent:*

1. $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ ist eine Komposition.

2. Es gilt $\sigma_h(\phi_x)\phi_x = q(x)\text{id}_E$ für alle $x \in M$.
3. Es gilt $\phi_x\sigma_h(\phi_x) = q(x)\text{id}_E$ für alle $x \in M$.
4. Die Abbildung $\tilde{\phi}$ definiert durch $\tilde{\phi}(x, y) = \sigma_h(\phi_x)(y)$ ist eine Komposition von (M, q) mit (E, h) .

Beweis Da h nichtsingulär ist, beweist folgende Rechnung die Äquivalenz von 1) und 2):

$$h(\sigma_h(\phi_x)\phi_x(y_1), y_2) = h(\phi_x(y_1), \phi_x(y_2)) = q(x)h(y_1, y_2).$$

Aus dem gleichen Grund sind auch 3) und 4) äquivalent. Es bleibt die Äquivalenz von 2) und 3) zu zeigen. Wir zeigen "2) \Rightarrow 3)". Für Elemente $x \in M$ mit $q(x) \in R^\times$ impliziert $\sigma_h(\phi_x)\phi_x = q(x)\text{id}_E$ die Gleichung $\phi_x\sigma_h(\phi_x) = q(x)\text{id}_E$. Ausserdem folgt für ein solches x aus $\sigma_h(\phi_x)\phi_y + \sigma_h(\phi_y)\phi_x = \lambda\text{id}_E$ für $\lambda \in R$ und beliebiges $y \in M$ die Gleichung $\phi_y\sigma_h(\phi_x) + \phi_x\sigma_h(\phi_y) = \lambda\text{id}_E$ (mittels Multiplikation von links mit $\phi_x q(x)^{-1}$ und von rechts mit $\sigma_h(\phi_x)$). Sei $M' \subset M$ die Menge der Elemente von M , welche diese beiden Eigenschaften haben. Wegen der R -Linearität von ϕ in der ersten Variablen und der R -Linearität von σ_h bildet M' einen linearen Teilraum von M . Besitzt (M, q) eine Basis e_1, \dots, e_n von Elementen mit $q(e_i) \in R^\times$, $i = 1, \dots, n$, so folgt $M' = M$ und insbesondere $\phi_x\sigma_h(\phi_x) = q(x)\text{id}_E$ für alle $x \in M$. Es genügt zu zeigen, dass eine solche Basis über einer (kommutativen) Ringweiterung $S \supset R$ existiert. Dazu erweitern wir in einem ersten Schritt die Skalare wie in Lemma 1.3.4, so dass $(M, q) \otimes S \simeq H(S^k)$ oder $(M, q) \otimes S \simeq H(S^k) \perp \langle 1_S \rangle$. Der Raum $\langle 1_S \rangle$ besitzt eine entsprechende Basis und es gilt $H(S^k) = H(S) \perp \dots \perp H(S)$ (k -mal). Es bleibt übrig, für eine hyperbolische Ebene $H(S) = (S^2, q_H)$ zu zeigen, dass sie über einer Ringweiterung $S' \supset S$ eine Basis von Elementen e', f' mit $q_H(e'), q_H(f') \in S'^\times$ besitzt. Wir betten S im kommutativen Ring $S' = S[X]/(X^2 + X - 1)$ ein. Sei e, f eine Basis der hyperbolischen Ebene $H(S)$ mit $q_H(e) = q_H(f) = 0, b_{q_H}(e, f) = 1$. Wir setzen $e' = X(e+f)$ und $f' = X(Xe-f)$. Wegen $e = e' + f', f = Xe' - f'$ bilden auch e', f' eine Basis von $H(S)$. Die Werte $q_H(e') = X^2$ und $q_H(f') = -X^3$ liegen in S'^\times , denn es gilt $X(X+1) = 1$ in S' . Damit ist die Aussage gezeigt und der Beweis vollendet. \square

1.5 Die Clifford-Algebra

Definition 1.5.1 Sei (M, q) ein quadratischer Raum über einem Ring R . Es gibt eine R -Algebra $C(M, q)$ und eine R -lineare Abbildung $i: M \rightarrow C(M, q)$,

so dass $\forall x \in M : i(x)^2 = q(x) \cdot 1_A$. Das Paar $(C(M, q), i)$ ist universell mit der folgenden Eigenschaft: Es gibt für jede R -Algebra A und jede R -lineare Abbildung $f: M \rightarrow A$ mit $f(x)^2 = q(x) \cdot 1_A$ genau einen Algebren-Homomorphismus $\tilde{f}: C(M, q) \rightarrow A$, so dass $\tilde{f} \circ i = f$. Man nennt $C(M, q)$ die Clifford-Algebra von (M, q) .

Theorem 1.5.2 • Sei $T(M) = \bigoplus M^{\otimes i}$ die Tensoralgebra von M und $J(q)$ das Ideal, welches von allen Elementen der Form $x \otimes x - q(x) \cdot 1$ für $x \in M$ erzeugt wird. Dann erfüllt $T(M)/J(q)$ mit der Inklusion $i: M \rightarrow T(M)/J(q)$ induziert durch $M = M^{\otimes 1} \subset T(M)$ die universelle Eigenschaft der Clifford-Algebra.

- Für jeden quadratischen Raum (M, q) ist die Clifford Algebra $C(M, q)$ durch die universelle Eigenschaft bis auf Isomorphie bestimmt.

Die Clifford-Algebra besitzt eine kanonische $\mathbb{Z}/2\mathbb{Z}$ -Graduierung $C(M, q) = C_0(M, q) \oplus C_1(M, q)$, wobei $C_0(M, q)$ von Produkten gerader Länge aus $i(M)$ erzeugt wird und $C_1(M, q)$ von Produkten ungerader Länge. Der gerade Teil $C_0(M, q)$ ist eine Teilalgebra von $C(M, q)$ und wird in dieser Arbeit die wesentliche Rolle spielen.

Theorem 1.5.3 Sei (M, q) ein quadratischer Raum vom Rang n . Dann ist $C(M, q)$ ein projektives R -Modul vom Rang 2^n und die kanonische Abbildung $i: M \rightarrow C(M, q)$ ist injektiv. Die gerade Clifford-Algebra $C_0(M, q)$ sowie $C_1(M, q)$ haben beide Rang 2^{n-1} .

Anbetracht obigen Theorems können wir M mit $i(M) \subset C(M, q)$ identifizieren. Da $C(M, q)^{\text{op}}$ ebenfalls die universelle Eigenschaft der Clifford-Algebra erfüllt, existieren auf $C(M, q)$ Involutionen τ^\pm mit $\tau^\pm|_M = \pm \text{id}$. Die beiden Involutionen induzieren auf $C_0(M, q)$ die gleiche Involution, welche wir die *kanonische Involution* der geraden Clifford-Algebra $C_0(M, q)$ nennen und mit τ_0 notieren. Um die Struktur der Clifford-Algebra anzugeben unterscheiden wir zwei Fälle: 1) $\text{Rg } M$ gerade und (M, q) regulär, 2) $\text{Rg } M$ ungerade und (M, q) halbregulär.

Theorem 1.5.4 (Strukturtheorem) Sei (M, q) ein quadratischer Raum von Rang n und $C(M, q) = C_0(M, q) \oplus C_1(M, q)$ die Clifford-Algebra.

- $n = 2k$: $C(M, q)$ ist Azumaya über R , $Z = Z(C_0(M, q))$ ist eine separable quadratische R -Algebra und $C_0(M, q)$ ist Azumaya über Z . Ausserdem ist $Z = C_{C(M, q)}(C_0(M, q))$. Falls $Z \simeq R \times R$, so ist $C_0(M, q) \simeq C_0^+(M, q) \times C_0^-(M, q)$, wobei $C_0^\pm(M, q)$ R -Azumaya-Algebren von Rang 2^{2k-2} sind mit $[C^+] = [C(M, q)] = [C^-]$ in $\text{Br}(R)$.

- $n = 2k + 1$: $C_0(M, q)$ ist Azumaya über R . Es gilt $Z(C(M, q)) \simeq C_{C(M, q)}(C_0(M, q))$ und die durch die Multiplikation in $C(M, q)$ induzierte Abbildung $C_0(M, q) \otimes Z(C(M, q)) \rightarrow C(M, q)$ ist ein Isomorphismus.

Man kann für hyperbolische Räume $H(R^k)$ die Clifford-Algebra explizit berechnen. Für den Beweis der obigen Theoreme verwendet man Lemma 1.3.4 zusammen mit folgender Tatsache:

Lemma 1.5.5 *Sei (M, q) ein quadratischer Raum und S eine kommutative R -Algebra. Dann gilt $C((M, q) \otimes S) \simeq C(M, q) \otimes S$, $C_0((M, q) \otimes S) \simeq C_0(M, q) \otimes S$, $Z(C((M, q) \otimes S)) \simeq Z(C(M, q)) \otimes S$ und $Z(C_0((M, q) \otimes S)) \simeq Z(C_0(M, q)) \otimes S$.*

Kapitel 2

Kompositionen über kommutativen Ringen

2.1 Charakterisierung von hermiteschen Kompositionen

Theorem 2.1.1 *Sei (M, q) ein quadratischer Raum, $z \in M$ mit $q(z) = 1$ und sei (E, h) ein ε -hermitescher Raum über einer R -Algebra A . Dann existiert eine Komposition $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ gdw. ein Homomorphismus $\alpha: (C_0(M, q), \tau_0) \rightarrow (\text{End}_A(E), \sigma_h)$ von Algebren mit Involutionen existiert.*

Beweis “ \Leftarrow “: Sei $\alpha: (C_0(M, q), \tau_0) \rightarrow (\text{End}_A(E), \sigma_h)$ ein Homomorphismus von Algebren mit Involutionen. Definiere $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ durch $\phi(x, y) = \alpha(zx)(y)$. Aus der Definition ersichtlich ist ϕ R -linear in der ersten Variablen und A -linear in der zweiten Variablen und aus der Rechnung

$$\begin{aligned} h(\phi(x, y_1), \phi(x, y_2)) &= h(\alpha(zx)y_1, \alpha(zx)y_2) \\ &= h(y_1, \sigma_h(\alpha(zx))\alpha(zx)y_2) \\ &= h(y_1, \alpha(\tau_0(zx))\alpha(zx)y_2) = h(y_1, \alpha(\overbrace{zxzx}^{q(x) \cdot 1})y_2) \\ &= q(x)h(y_1, y_2) \end{aligned}$$

folgt die Behauptung.

“ \Rightarrow “: Sei $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ eine ε -hermitesche Komposition. Für die Definition von $\alpha: (C_0(M, q), \tau_0) \rightarrow (\text{End}_A(E), \sigma_h)$ wird der Kürze wegen der Isomorphismus

$$(C_0(M, q), \tau_0) \simeq \left(\frac{T(M \otimes M)}{J_1(q) + J_2(q)}, \sigma \right)$$

benutzt, wobei die Ideale $J_1(q), J_2(q) \subset T(M \otimes M)$ von den Elementen der Form $x \otimes x - q(x) \cdot 1$ bzw. $(x \otimes y) \otimes (y \otimes z) - q(y)x \otimes z$ erzeugt werden und die Involution $\underline{\sigma}$ von der Vertauschung $\sigma(x \otimes y) = y \otimes x$ auf $M \otimes M$ induziert ist (vgl. Seite 31). Wir definieren nun

$$\beta: T(M \otimes M) \rightarrow \text{End}_A(E) \quad \text{durch} \quad \beta(x_1 \otimes x_2) = \sigma_h(\phi_{x_1})\phi_{x_2}.$$

Aus Lemma (1.4.4) folgt $\beta(x \otimes x) = \sigma_h(\phi_x)\phi_x = q(x) \cdot \text{id}_E$ und $\alpha((x \otimes y) \otimes (y \otimes z)) = \sigma_h(\phi_x)\phi_y \circ \sigma_h(\phi_y)\phi_z = q(y)\sigma_h(\phi_x)\phi_z = q(y)\alpha(x \otimes z)$. Also verschwindet β auf den Idealen $J_1(q)$ und $J_2(q)$ und faktorisiert durch die gerade Cliffordalgebra. Der induzierte Homomorphismus $\alpha: (C_0(M, q)) \rightarrow \text{End}_A(E)$ ist mit den Involutionsen verträglich, denn $\beta(\sigma(x_1 \otimes x_2)) = \beta(x_2 \otimes x_1) = \sigma_h(\phi_{x_2})\phi_{x_1} = \sigma_h(\sigma_h(\phi_{x_1})\phi_{x_2}) = \sigma_h(\beta(x_1 \otimes x_2))$. \square

Bemerkung Durch die im Beweis verwendete Konstruktion:

$$\begin{aligned} \phi &\rightsquigarrow \alpha : \alpha(x_1 x_2) = \sigma_h(\phi_{x_1}) \circ \phi_{x_2} \\ \alpha &\rightsquigarrow \phi : \phi(x, y) = \alpha(zx)(y) \end{aligned}$$

erhält man aus einer Komposition ϕ auch dann einen Homomorphismus α , wenn kein $z \in M$ mit $q(z) = 1$ existiert. Die obige Zuordnung $\phi \rightsquigarrow \alpha$ ist $1 - 1$ eingeschränkt auf Kompositionen mit $\phi_z = \text{id}_E$. Ist diese Bedingung nicht erfüllt, so liefert $\phi \rightsquigarrow \alpha \rightsquigarrow \phi'$ (explizit: $\phi'(x, y) = \sigma_h(\phi_z) \circ \phi(x, y)$) eine Komposition, in der ϕ'_z die Identität ist.

2.2 Minimale Kompositionen

Definition 2.2.1 Eine quadratische Komposition $\phi: (M, q) \times (E, p) \rightarrow (E, p)$ über R heisst minimale quadratische Komposition (im Sinne von R. Züger), falls keine quadratische Komposition $\phi': (M', q') \rightarrow (E', p')$ über R existiert mit $\text{Rg } M' = \text{Rg } M$ und $\text{Rg } E' < \text{Rg } E$.

Eine hermitesche oder antihermitesche Komposition $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ über einer festen R -Algebra A mit Involution θ heisst minimale hermitesche Komposition bzw. minimale antihermitesche Komposition (im Sinne von R. Züger), falls keine (bzgl. θ) hermitesche bzw. antihermitesche Komposition $\phi': (M', q') \rightarrow (E', h')$ existiert mit $\text{Rg } M' = \text{Rg } M$ und $\text{Rg } E' < \text{Rg } E$.

Die Antwort auf die Frage, wie klein $\text{Rg } E$ sein kann für Kompositionen $\phi: M \times E \rightarrow E$ mit vorgegebenem Rang von M war für quadratische und anti-symmetrische Kompositionen über den reellen oder komplexen Zahlen schon früher bekannt. Der Rang von E für eine minimale quadratische Komposition $\phi: (M, q) \times (E, p) \rightarrow (E, p)$ oder für eine minimale anti-symmetrische

Komposition $\phi: (M, q) \times (E, b) \rightarrow (E, b)$ beträgt genau $\pi_+(\operatorname{Rg} M)$ bzw. $\pi_-(\operatorname{Rg} M)$, gegeben in der folgenden Tabelle gegeben. Wir listen zum Vergleich die Grösse $\pi_h(\operatorname{Rg} M)$ auf, welche für Räume von geradem Rang die Dimension von $C_0(M, q)$ angibt und für Räume von ungeradem Rang die halbe Dimension von $C_0(M, q)$. Sie bedeutet eine untere Schranke für den Rang von E und ergibt sich direkt aus Theorem (2.1.1).

Notation Sei $m = 8a + b \in \mathbb{N}$ mit $a, b \in \mathbb{N}_0$ und $0 \leq b < 8$.

b	0	1	2	3	4	5	6	7
$\pi_+(m)$	2^{4a-1}	2^{4a}	2^{4a+1}	2^{4a+2}	2^{4a+2}	2^{4a+3}	2^{4a+3}	2^{4a+3}
$\pi_-(m)$	2^{4a}	2^{4a+1}	2^{4a+1}	2^{4a+1}	2^{4a+1}	2^{4a+2}	2^{4a+3}	2^{4a+4}
$\pi_h(m)$	2^{4a-1}	2^{4a}	2^{4a}	2^{4a+1}	2^{4a+1}	2^{4a+2}	2^{4a+2}	2^{4a+3}

Der einzige Fall, in dem die triviale Schranke $\pi_h(m)$ weder mit der Schranke für quadratische noch mit der Schranke für anti-symmetrische Kompositionen übereinstimmt, ist der Fall $\operatorname{Rg} M \equiv 2 \pmod{4}$. Der eigentliche Grund liegt darin, dass die kanonische Involution auf $C_0(M, q)$ in diesem Fall unitär ist, so dass für triviales Zentrum, $C_0(M, q) \simeq C^+ \times C^-$ die Projektion auf eine Komponente kein Homomorphismus von Algebren mit Involutions darstellen kann. Es stellt sich heraus, dass die gleichen minimalen Ränge π_\pm für Kompositionen über beliebigen Körpern von Charakteristik ungleich 2 gelten. Über kommutativen Ringen mit $2 \notin R^\times$ ist dies nicht genau der Fall.

Nicht jeder quadratische Raum (M, q) lässt eine minimale quadratische, hermitesche oder antihermitesche Komposition zu. R. Züger gibt in seiner Dissertation [Züg95] für punktierte Räume hinreichende und (in den meisten Fällen) notwendige Bedingungen an (M, q) für die Existenz einer minimalen Komposition. Er untersucht quadratische Kompositionen, antisymmetrische Kompositionen, hermitesche Kompositionen über quadratischen separablen Algebren mit Standardinvolution, sowie hermitesche Kompositionen über Quaternionenalgebren mit Standardinvolution. Dabei erlaubt er den quadratischen Räumen (E, p) und den (anti-)symmetrischen Räumen (E, b) Werte in einem invertierbaren R -Modul zu nehmen und den hermiteschen Räumen (E, h) über S oder Q Werte in einem invertierbaren S -Modul, bzw. in $A \otimes I$ für ein invertierbares R -Modul zu nehmen. Wir geben im Folgenden seine Resultate zu minimalen Kompositionen wieder:

Theorem 2.2.2 1. *Der Rang für eine minimale Komposition ist wie folgt gegeben:*

- (a) *Symmetrische Kompositionen: Der minimale Rang l von E , für den eine Komposition $\phi: (M, q) \times (E, b) \rightarrow (E, b)$ eines quadratischen Raumes (M, q) von Rang m mit einem symmetrischen*

Raum (E, b) existiert ist genau $l = \pi_+(m)$, ausser in den Fällen $m \equiv 3, 4, 5 \pmod{8}$ und $2 = 0$ in R , wo $l = \frac{\pi_+(m)}{2}$.

(b) *Antisymmetrische Kompositionen:* Der minimale Rang l von E , für den eine Komposition $\phi: (M, q) \times (E, b) \rightarrow (E, b)$ eines quadratischen Raumes (M, q) von Rang m mit einem anti-symmetrischen Raum (E, b) existiert ist genau $l = \pi_-(m)$, ausser in den Fällen $m \equiv 0, 1, 7 \pmod{8}$ und $2 = 0$ in R , wo $l = \frac{\pi_-(m)}{2}$.

(c) *Hermitesche Kompositionen über einer quadratischen, separablen Algebra S :* Der minimale S -Rang l von E , für den eine Komposition $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ eines quadratischen Raumes (M, q) von Rang m mit einem hermiteschen Raum (E, h) über S existiert, wobei h bzgl. der Standardinvolution von S hermitesch ist, ist genau $l = \pi_h(m)$.

(d) *Hermitesche Kompositionen über einer Quaternionen-Algebra Q :* Der minimale Rang l von E , für den eine Komposition $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ eines quadratischen Raumes (M, q) von Rang m mit einem hermiteschen Raum (E, h) über Q existiert, wobei h bzgl. der Standardinvolution von Q hermitesch ist, ist genau $l = 2\pi_-(m)$, ausser in den Fällen $m \equiv 0, 1, 7 \pmod{8}$, wo $l = \pi_-(m)$.

2. Sei (M, q) ein punktierter quadratischer Raum von Rang m und $C = C(M, q)$, $C_0 = C_0(M, q)$, $Z = Z(C_0(M, q))$ die (gerade) Cliffordalgebra bzw. das Zentrum der geraden Cliffordalgebra. Es gibt in den Fällen (a), (b), (c), (d) folgende hinreichende Bedingungen für die Existenz einer Komposition von Rang $\pi_+(m)$, $\pi_-(m)$, $\pi_h(m)$ bzw. $2\pi_-(m)$:

(a) *Symmetrische Kompositionen:*

i. $m \equiv 0 \pmod{8}$: $[C] = 1$ in $\text{Br}(R)$ und $Z \simeq R \times R$.

ii. $m \equiv \pm 1 \pmod{8}$: $[C_0] = 1$ in $\text{Br}(R)$.

iii. $m \equiv \pm 2 \pmod{8}$: $[C_0] = 1$ in $\text{Br}(Z)$.

iv. $m \equiv \pm 3 \pmod{8}$: $[C_0] = [Q]$ in $\text{Br}(R)$ für Quaternionen Q .

v. $m \equiv 4 \pmod{8}$: $Z \simeq R \times R$ und $[C] = [Q]$ in $\text{Br}(R)$ für Quaternionen Q .

Die obigen Bedingungen sind notwendig für punktierte Räume, ausser wenn 2 ein Nullteiler in R ist und $m \equiv 4 \pmod{8}$.

(b) *Antisymmetrische Kompositionen:*

i. $m \equiv 0 \pmod{8}$: $Z \simeq R \times R$ und $[C] = [Q]$ in $\text{Br}(R)$ für Quaternionen Q .

- ii. $m \equiv \pm 1 \pmod{8}$: $[C_0] = [Q]$ in $\text{Br}(R)$ für Quaternionen Q .
- iii. $m \equiv \pm 2 \pmod{8}$: $[C_0] = 1$ in $\text{Br}(Z)$.
- iv. $m \equiv \pm 3 \pmod{8}$: $[C_0] = 1$ in $\text{Br}(R)$.
- v. $m \equiv 4 \pmod{8}$: $[C] = 1$ in $\text{Br}(R)$ und $Z \simeq R \times R$.

Die obigen Bedingungen sind notwendig für punktierte Räume, ausser wenn 2 ein Nullteiler in R ist und $m \equiv 0 \pmod{8}$.

(c) *Hermitesche Kompositionen über einer quadratischen, separablen Algebra S :*

- i. $m \equiv 0 \pmod{4}$: $Z \simeq R \times R$ und $[C] = [Q]$ in $\text{Br}(R)$ für Quaternionen Q mit einer Graduierung $Q = Q_0 \oplus Q_1$ mit $Q_0 = S$.
- ii. $m \equiv 1 \pmod{2}$: $[C_0] = [Q]$ in $\text{Br}(R)$ für Quaternionen Q mit einer Graduierung $Q = Q_0 \oplus Q_1$ mit $Q_0 = S$.
- iii. $m \equiv \pm 2 \pmod{8}$: $Z = S$ und $[C_0] = 1$ in $\text{Br}(Z)$.

Die obigen Bedingungen sind notwendig für punktierte Räume.

(d) *Hermitesche Kompositionen über einer Quaternionen-Algebra Q :*

- i. $m \equiv 0 \pmod{8}$: $Z \simeq R \times R$ und $[C] = [Q \otimes Q']$ in $\text{Br}(R)$ für Quaternionen Q' .
- ii. $m \equiv \pm 1 \pmod{8}$: $[C_0] = [Q \otimes Q']$ in $\text{Br}(R)$ für Quaternionen Q' .
- iii. $m \equiv \pm 2 \pmod{8}$: $[C_0] = [Q \otimes Z]$ in $\text{Br}(Z)$.
- iv. $m \equiv \pm 3 \pmod{8}$: $[C_0] = [Q]$ in $\text{Br}(R)$.
- v. $m \equiv 4 \pmod{8}$: $[C] = [Q]$ in $\text{Br}(R)$ und $Z \simeq R \times R$.

Die obigen Bedingungen sind notwendig für punktierte Räume, ausser wenn 2 ein Nullteiler in R ist und $m \equiv 0 \pmod{8}$.

Bemerkung In den Fällen, in welchen die Bedingungen an (M, q) für eine minimale Komposition durch die Brauerklasse von $C(M, q)$ ausgedrückt werden, ist $Z \simeq R \times R$. Schreibt man die Clifford-Algebra als $C^+ \times C^-$, so ist gemäss Theorem (1.5.4) $[C^\pm] = [C(M, q)]$ in $\text{Br}(R)$. Man kommt also immer nur mit der geraden Clifford-Algebra aus.

In [Züg95] wird der minimale Rang einer quadratischen Komposition mit dem minimalen Rang einer symmetrischen Komposition gleichgesetzt. Dies führt jedoch auf falsche Ergebnisse für Räume von Rang 3, 4 und 5 und Ringe mit $2 = 0$, was sich anhand einer kurzen Überlegung zeigen lässt:

Lemma 2.2.3 *Es gibt für quadratische Räume (M, q) keine quadratische Komposition $\phi: (M, q) \times (E, p) \rightarrow (E, p)$ mit $\text{Rg } M > \text{Rg } E$, sofern p einen Nicht-Nullteiler $p(y_0)$ darstellt.*

Beweis Die Abbildung $\phi(\cdot, y_0) : M \rightarrow E$ ist injektiv, denn $\phi(x, y_0) = 0 \Rightarrow \forall x' \in M : 0 = b_p(\phi(x, y_0), \phi(x', y_0)) = b_q(x, x')p(y_0) \Rightarrow x \in \ker \hat{b}_q$. Da (M, q) als regulär oder halbreulär vorausgesetzt wurde, folgt $x = 0$ oder $q(x) \neq 0$, aber $q(x)p(y_0) = p(\phi(x, y_0)) = 0$ führt im letzteren Fall zu einem Widerspruch. \square

Für Räume von Rang $m = 3$, $m = 4$ oder $m = 5$ und Ringe mit $2 = 0$ liegt der minimale Rang für eine symmetrische Komposition gemäss Theorem (2.2.2) bei 2, 2 bzw. 4, also kleiner m . Ein ganz konkretes explizites Beispiel ist das folgende:

Beispiel Sei $(M, q) = (R^4, q_H)$ mit der hyperbolischen quadratischen Form $q_H(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$ und $(E, b) = (R^2, b_a)$ mit der alternierenden Form $b_a((y_1, y_2), (y'_1, y'_2)) = y_1y'_2 - y'_1y_2$. Die bilineare Abbildung $\phi : M \times E \rightarrow E$ definiert durch $\phi((x_1, x_2, x_3, x_4), (y_1, y_2)) = (x_1y_1 + x_3y_2, -x_4y_1 + x_2y_2)$ ist eine antisymmetrische (und symmetrische falls $2 = 0$ in R) Komposition mit $\text{Rg } M = 4 > 2 = \text{Rg } E$. Sei nun R ein Ring mit $2 = 0$. Dann ist b_a die Polare der quadratischen Form p auf E definiert durch $p(y_1, y_2) = y_1y_2 + \alpha y_1^2 + \beta y_2^2$ für $\alpha, \beta \in R$. Zudem ist jede quadratische Form mit Polaren b_a von dieser Form. Für $x_3 = 1 = y_2, y_1 = x_4 = 0$ ist $p(\phi((x_1, x_2, x_3, x_4), (y_1, y_2))) = p(1, x_2) = x_2 + \alpha + \beta x_2^2$ und $q_H(x_1, x_2, x_3, x_4)p(y_1, y_2) = \beta x_1x_2$. Falls $\alpha = 0$ sind die Werte verschieden, wenn man $x_1 = 1 = x_2$ einsetzt. Falls hingegen $\alpha \neq 0$ ergibt Einsetzen von $x_1 = x_2 = 0$, dass ϕ keine Komposition von (M, q) mit (E, p) sein kann.

Der Fehler wurde von A. Elduque in [Eld02] bemerkt. Er hat für Körper von Charakteristik 2 den Rang $l = \text{Rg } E$ für eine minimale quadratische Komposition $\phi : (M, q) \times (E, p) \rightarrow (E, p)$ in Abhängigkeit von $\text{Rg } M$ gegeben, was wir wie folgt formulieren können:

Proposition 2.2.4 *Für eine minimale quadratische Komposition $\phi : (M, q) \times (E, p) \rightarrow (E, p)$ über einem Körper von Charakteristik 2 ist der Rang von E bestimmt durch $\text{Rg } E = \gamma(\text{Rg } M) = \min\{\pi_+(\text{Rg } M), \pi_-(\text{Rg } M)\}$ mit den folgenden Ausnahmen (für die zweite Gleichung): $\gamma(3) = 4, \gamma(4) = 4, \gamma(5) = 8$.*

Es stellen sich für Ringe R , in denen 2 ein Nullteiler ist, folgende Fragen:

- Gibt es auch für Kompositionen über R nur diese Ausnahmen?
- Warum gibt es nur Gegenbeispiele für Räume von kleinem Rang?
- Unter welchen Bedingungen und mit welcher Methode erhält man aus einer symmetrischen Komposition $\phi : (M, q) \times (E, b) \rightarrow (E, b)$ eine quadratische Komposition $\phi : (M, q) \times (E, p) \rightarrow (E, p)$?

Wir versuchen diese Fragen in den nächsten beiden Abschnitten befriedigend zu beantworten.

2.3 Zusammenhang von symmetrischer und quadratischer Komposition

Die folgende Beobachtung ist im Weiteren von Interesse:

Proposition 2.3.1 *Sei $\phi: (M, q) \times (E, b) \rightarrow (E, b)$ eine symmetrische Komposition und $\text{Rg } M \geq 2$. Dann existiert höchstens eine quadratische Form p auf E mit $b_p = b$ und der Eigenschaft, dass $\phi: (M, q) \times (E, p) \rightarrow (E, p)$ eine quadratische Komposition ist.*

Beweis Seien p_1 und p_2 quadratische Formen auf E mit $b_{p_1} = b = b_{p_2}$ und der Eigenschaft, dass $\phi: (M, q) \times (E, p_i) \rightarrow (E, p_i)$ für $i = 1, 2$ quadratische Kompositionen sind. Es genügt, die Behauptung der Proposition für alle Lokalisierungen von R zu zeigen. Nehmen wir also an, R sei lokal. Wegen $\text{Rg } M \geq 2$ existieren nun $x_1, x_2 \in M$ derart, dass $b_q(x_1, x_2) = 1$. Durch Linearisierung in der ersten Variablen erhält man die Gleichungen

$$b_q(x_1, x_2)p_1(y) = b(x_1 \cdot y, x_2 \cdot y) = b_q(x_1, x_2)p_2(y) \text{ für alle } y \in E$$

und damit $p_1 = p_2$. □

Bemerkung Falls $\text{Rg } M = 1$, so ist die Eindeutigkeits-Aussage von Proposition (2.3.1) im Allgemeinen falsch. Sei (M, q) der quadratische Raum mit Basis e , $q(e) = 1$ und $\phi: (M, q) \times (E, b) \rightarrow (E, b)$, $\phi(\lambda e, x) = \lambda x$ für $\lambda \in R, x \in E$. Sofern eine quadratische Form auf E mit Polaren b existiert, so gibt es, falls 2 ein Nullteiler ist, mehrere solche Formen und jede liefert mit ϕ eine Komposition von quadratischen Formen.

Theorem 2.3.2 *Sei (M, q) ein quadratischer Raum von Rang $\text{Rg } M \geq 6$ und sei $\phi: (M, q) \times (E, b) \rightarrow (E, b)$ eine symmetrische Komposition. Es existiere $z \in M$ mit $q(z) = 1$. Wir können annehmen, dass $\phi(z, \cdot) = \text{id}_E$. Existiert ein von z linear unabhängiges Element $c \in M$, für welches $b_q(z, c) = 1$ und $q|_{Rz \oplus Rc}$ regulär ist, so ist b Polare einer eindeutig bestimmten quadratischen Form p welche durch ϕ eine quadratische Komposition $\phi: (M, q) \times (E, p) \rightarrow (E, p)$ liefert.*

Beweis Der Beweis benützt den in der Charakterisierung von Komposition gegebenen Homomorphismus $\alpha: (C_0(M, q), \tau_0) \rightarrow (\text{End}_R(E), \sigma_b)$ von

Algebren mit Involutionen. Sei für beliebiges $c \in M$ mit $b_q(z, c) = 1$ die quadratische Form p_c auf E definiert durch:

$$p_c(y) = b(y, \alpha(zc)y).$$

Die Polare zu p_c ist b , denn $b_{p_c}(y_1, y_2) = b(y_1, \alpha(zc)y_2) + b(y_2, \alpha(zc)y_1) = b(y_1, (\alpha(zc) + \sigma_b(\alpha(zc)))y_2) = b(y_1, \alpha(zc + cz)y_2) = b(y_1, y_2)$, d.h.

$$b_{p_c} = b \quad (2.1)$$

Mit Hilfe der Identität $czx = xcz + b_q(z, x)c - b_q(c, x)z$ ergibt sich weiter:

$$\begin{aligned} p_c(x \cdot y) &= b(x \cdot y, \alpha(zc)(x \cdot y)) = b(\alpha(zx)y, \alpha(zczx)y) \\ &= b(\alpha(zx)y, \alpha(zx)\alpha(cz)y) + b(\alpha(zx)y, b_q(z, x)\alpha(zc)y - b_q(c, x)y) \\ &= b(x \cdot y, x \cdot (\alpha(cz)y)) + b(y, b_q(z, x)\alpha(xzzc)y - b_q(c, x)\alpha(xz)y) \\ &= q(x)p_c(y) + b(y, b_q(z, x)\alpha(xc)y - b_q(c, x)\alpha(xz)y), \end{aligned}$$

also

$$p_c(x \cdot y) = q(x)p_c(y) + b_q(z, x)b(y, \alpha(xc)y) - b_q(c, x)b(y, \alpha(xz)y). \quad (2.2)$$

Wir wählen nun ein Element $c \in M$, das die Voraussetzungen des Theorems erfüllt und schreiben $x \in M$ als $x = \mu z + \nu c + a$ mit $\mu, \nu \in R, a \in (Rz \oplus Rc)^\perp$. Dann ergibt sich aus obiger Rechnung:

$$\begin{aligned} p_c(x \cdot y) &= q(x)p_c(y) \\ &\quad + b_q(z, x) \left(\overbrace{b(y, \mu\alpha(zc)y)}^{\mu p_c(y)} + \overbrace{b(y, \nu q(c)y)}^{2\nu q(c)p_c(y)} + b(y, \alpha(ac)y) \right) \\ &\quad - b_q(c, x) \left(\overbrace{b(y, \mu y)}^{2\mu p_c(y)} + \overbrace{b(y, \nu\alpha(cz)y)}^{\nu p_c(y)} + b(y, \alpha(az)y) \right) \\ &= q(x)p_c(y) + p_c(y) \overbrace{\left(b_q(z, x)(\mu + 2\nu q(c)) - b_q(c, x)(2\mu + \nu) \right)}^{=0} \\ &\quad + b_q(z, x)b(y, \alpha(ac)y) - b_q(c, x)b(y, \alpha(az)y) \end{aligned}$$

$$\Rightarrow p_c(x \cdot y) = q(x)p_c(y) + b_q(z, x)b(y, \alpha(ac)y) - b_q(c, x)b(y, \alpha(az)y), \quad (2.3)$$

wobei $c \in M$ wie in den Voraussetzungen des Theorems und $x = \mu z + \nu c + a$ mit $\mu, \nu \in R$ und $a \in (Rz + Rc)^\perp$. Das Ziel besteht nun darin zu zeigen, dass

$$b(y, \alpha(ac)y) = 0 = b(y, \alpha(az)y) \quad \text{für alle } y \in E, a \in (Rz + Rc)^\perp \quad (2.4)$$

Wir können annehmen, dass R ein lokaler Ring ist, denn gilt (2.4) für alle Lokalisierungen von R , dann auch für R selbst. In der Folge lässt sich M als $M = (Rz \oplus Rc) \perp M_1 \perp M_2 \perp \cdots \perp M_k$ mit regulären M_i von Rang $\text{Rg } M_i \leq 2$, $i = 1, \dots, k-1$ und (evtl. halb-)regulärem M_k mit $\text{Rg } M_k \in \{1, 2\}$ schreiben und $a \in (Rz + Rc)^\perp$ als $a = a_1 + a_2 + \cdots + a_k$ mit $a_i \in M_i$, $i = 1, \dots, k$. Gilt (2.4) für alle a_i , so folgt sie wegen der Linearität von (2.4) auch für a . Wir schreiben im Folgenden a für a_i und i_a für i . Sei \tilde{c} von der Form $\tilde{c} = \lambda z + (1 - 2\lambda)c + a$ für beliebiges $\lambda \in R$. Da $b_q(\tilde{c}, z) = 2\lambda + (1 - 2\lambda) + 0 = 1$, gelten die Gleichungen (2.1) und (2.2) auch mit \tilde{c} anstelle c . Unter der weiteren Voraussetzung an den Rang des Moduls ($\text{Rg } M \geq 6$) gibt es in der obigen Zerlegung des Moduls ein reguläres M_j mit $j \neq i_a$. Wir wählen Elemente $x_1, x_2 \in M_j$ mit $b_q(x_1, x_2) = 1$. Setze $x_3 = x_1 + x_2$. Dadurch ist $b_q(z, x_i) = b_q(c, x_i) = b_q(\tilde{c}, x_i) = 0$ für $i = 1, 2, 3$ und Gleichung (2.2) liefert

$$p_c(x_i \cdot y) = q(x_i)p_c(y) \quad (2.5)$$

$$p_{\tilde{c}}(x_i \cdot y) = q(x_i)p_{\tilde{c}}(y) \quad (2.6)$$

und somit

$$\begin{aligned} b_q(x_1, x_2)p_c(y) &= (q(x_3) - q(x_1) - q(x_2))p_c(y) \\ &= p_c(x_3 \cdot y) - p_c(x_1 \cdot y) - p_c(x_2 \cdot y) \\ &= b_{p_c}(x_1 \cdot y, x_2 \cdot y) \\ &= b(x_1 \cdot y, x_2 \cdot y) \end{aligned}$$

und analog

$$b_q(x_1, x_2)p_{\tilde{c}}(y) = b(x_1 \cdot y, x_2 \cdot y)$$

Wegen $b_q(x_1, x_2) = 1$ folgt

$$p_c(y) = p_{\tilde{c}}(y) \quad \text{für alle } y \in E \quad (2.7)$$

Gleichung (2.2) mit $x = \tilde{c}$ liefert

$$\begin{aligned} p_{\tilde{c}}(\tilde{c} \cdot y) &= q(\tilde{c})p_{\tilde{c}}(y) + b_q(z, \tilde{c})b(y, \alpha(\tilde{c}\tilde{c})y) - b_q(\tilde{c}, \tilde{c})b(y, \alpha(\tilde{c}z)y) \\ &= q(\tilde{c})p_{\tilde{c}}(y) + 2q(\tilde{c})p_{\tilde{c}}(y) - 2q(\tilde{c})p_{\tilde{c}}(y) \\ &= q(\tilde{c})p_{\tilde{c}}(y) \end{aligned}$$

Gleichung (2.3) liefert

$$p_c(\tilde{c} \cdot y) = q(\tilde{c})p_c(y) + b(y, \alpha(ac)y) - b_q(c, \tilde{c})b(y, \alpha(az)y)$$

Mit (2.7) folgt deshalb

$$\begin{aligned}
b(y, \alpha(ac)y) &= b_q(c, \tilde{c})b(y, \alpha(az)y) \\
&= (\lambda + 2q(c)(1 - 2\lambda))b(y, \alpha(az)y) \\
&= (2q(c) + \underbrace{\lambda(1 - 4q(c))}_{=: r \in R^\times})b(y, \alpha(az)y)
\end{aligned}$$

Wir wählen nun für $\lambda \in R$ die folgenden Werte:

- $\lambda = -2q(c)r^{-1} \Rightarrow b(y, \alpha(ac)y) = 0$
- $\lambda = (1 - 2q(c))r^{-1} \Rightarrow b(y, \alpha(az)y) = b(y, \alpha(ac)y) = 0$

Einsetzen in (2.3) liefert schliesslich $p_c(x \cdot y) = q(x)p_c(y)$, wie behauptet. \square

Beispiel Enthält (M, q) eine hyperbolische Ebene, d.h. einen Teilraum $(H, q|_H) \subset (M, q)$ mit Basis e_1, e_2 und $q(e_1) = 0 = q(e_2), b_q(e_1, e_2) = 1$ oder ist R ein Körper, so ergibt sich aus jeder symmetrischen Komposition von (M, q) mit (E, b) eine Komposition von (M, q) mit einer quadratischen Form p auf E mit Polaren b .

Bemerkung Die Definition von p durch $p(y) = b(y, \alpha(zc)y)$ ist zwingend und ausserdem ist die Definition ganz unabhängig von der Wahl eines Elements c mit $b_q(z, c) = 1$. Nämlich ergibt sich aus der Gleichung $p(x \cdot y) = q(x)p(y)$ durch Linearisierung die Identität $b(x_1 \cdot y, x_2 \cdot y) = b_q(x_1, x_2)p(y)$. Einsetzen von $x_1 = z, x_2 = c$ führt auf $b(y, \alpha(zc)y) = b(z \cdot y, c \cdot y) = b_q(z, c)p(y) = p(y)$.

Die Idee, die quadratische Form so zu definieren und zu zeigen, dass die Definition unabhängig von c ist, stammt aus [Eld02, Theorem 1 III)]. Elduque benützt sie nur für quadratische Räume (über Körpern von char 2) von Rang $4r, r > 1$ mit trivialer Clifford-Invariante und verwendet anstelle der C_0 -Modulstruktur die C -Modulstruktur.

2.4 Spur von Kompositionen

Für quadratische Räume von Rang $\text{Rg } M \equiv 3, 4, 5$ (8) konstruiert R. Züger in [Züg95] im Abschnitt über den „Zusammenhang zwischen minimalen hermiteschen und quadratischen Formen“ quadratische Kompositionen $\phi: (M, q) \times (E, p) \rightarrow (E, p)$ mit Rang $\text{Rg } E = \pi_+(\text{Rg } M)$. Diese Kompositionen sind minimale quadratische Kompositionen für $\text{Rg } M = 3, 4, 5$ und ergänzen unser Resultat aus dem vorangehenden Abschnitt, in dem wir für Räume von Rang

≥ 6 den Zusammenhang zwischen quadratischer und symmetrischen Komposition zu klären versucht haben. Beachte, dass für quadratische Räume von Rang $\text{Rg } M \equiv 3, 4, 5 \pmod{8}$ die Bedingungen für die Existenz von quadratischen Kompositionen mit $\text{Rg } E = \pi_+(m)$ und hermiteschen Kompositionen über einer Quaternionenalgebra Q mit $\text{Rg } E = 2\pi_-$ übereinstimmen. Wir geben im Folgenden Zügers Konstruktion wieder.

Proposition 2.4.1 *Sei (M, q) ein quadratischer Raum und (E, h) ein hermitescher Raum über einer Quaternionen-Algebra Q , wobei h bzgl. der Standardinvolution $a \mapsto \bar{a}$ auf Q hermitesch sei. Es existiere eine hermitesche Komposition $\phi: (M, q) \times (E, h) \rightarrow (E, h)$ von (M, q) mit (E, h) . Dann liefert Spurbildung eine reguläre symmetrische Bilinearform $b = \text{Tr} \circ h: E \times E \rightarrow R$ und ϕ induziert eine symmetrische Komposition $\phi: (M, q) \times (E, b) \rightarrow (E, b)$. Falls h gerade ist, d.h. von der Form $h(x, y) = h_0(x, y) + \overline{h_0(y, x)}$ für eine Sesquilinearform h_0 , so ist die Abbildung $p: E \rightarrow R$ definiert durch $p(y) = h(y, y)$ eine quadratische Form mit Werten in R und Polaren b und $\phi: (M, q) \times (E, p) \rightarrow (E, p)$ liefert eine quadratische Komposition.*

Beweis Symmetrie von b ist eine Konsequenz von $\text{Tr}(a) = \text{Tr}(\bar{a})$ für alle $a \in Q$, Regularität folgt aus der Regularität von h und der Regularität der bilinearen Spurform $T_Q: Q \times Q \rightarrow R$, $T_Q(y_1, y_2) = \text{Tr}(y_1 y_2)$. Die Kompositionseigenschaft ergibt sich direkt aus Spurbildung. Falls h gerade ist, so liegen die Werte von p in R und p ist eine reguläre quadratische Form. Die Kompositionseigenschaft ergibt sich durch Gleichsetzen von y_1 und y_2 in $h(\phi(x, y_1), \phi(x, y_2)) = q(x)h(y_1, y_2)$. \square

Korollar 2.4.2 *Sei R ein beliebiger kommutativer Ring. Der minimale Rang für quadratische Kompositionen $\phi: (M, q) \times (E, p) \rightarrow (E, p)$ mit $\text{Rg } M = 3, 4, 5$ ist 4, 4 bzw. 8.*

Beweis Dies folgt aus den Resultaten von R. Züger zu symmetrischen Kompositionen und der Hilfe von obiger Proposition. \square

Bemerkung Der Beweis der Proposition überträgt sich auch auf den Fall, wo die hermitesche Form Werte in $Q \otimes I$ für ein invertierbares Modul I hat. Die Formen b und h haben dann Werte in I . Die von R. Züger konstruierten hermiteschen Formen sind tatsächlich gerade.

Kapitel 3

Komposition von quadratischen Paaren

Wie im 2. Kapitel beobachtet wurde, lassen sich quadratische und hermitesche Kompositionen eines quadratischen Raumes (M, q) in vielen Fällen alleine durch die gerade Clifford-Algebra $C_0(M, q)$ zusammen mit ihrer kanonischen Involution beschreiben. Für die gerade Clifford-Algebra von regulären quadratischen Räumen über Körpern gibt es eine Verallgemeinerung auf sogenannte quadratische Paare, die im Folgenden definiert und beschrieben werden. Die Beweise der Theoreme über quadratische Paare findet man in [KMRT98], wo quadratische Paare erstmals eingeführt wurden.

3.1 Quadratische Paare

Definition 3.1.1 Sei A eine Azumaya-Algebra über einem Körper F und σ eine Involution 1. Art auf A . Die Mengen von symmetrischen, antisymmetrischen, symmetrisierten und alternierenden Elemente sind definiert durch:

$$\begin{aligned}\text{Sym}(A, \sigma) &= \{a \in A \mid \sigma(a) = a\} \\ \text{Skew}(A, \sigma) &= \{a \in A \mid \sigma(a) = -a\} \\ \text{Symd}(A, \sigma) &= \{a + \sigma(a) \mid a \in A\} \\ \text{Alt}(A, \sigma) &= \{a - \sigma(a) \mid a \in A\}\end{aligned}$$

Für $\text{char } F \neq 2$ ist $\text{Symd}(A, \sigma) = \text{Sym}(A, \sigma) \neq \text{Skew}(A, \sigma) = \text{Alt}(A, \sigma)$ und für $\text{char } F = 2$ ist $\text{Symd}(A, \sigma) = \text{Alt}(A, \sigma) \subsetneq \text{Skew}(A, \sigma) = \text{Sym}(A, \sigma)$.

Definition 3.1.2 Sei A eine F -Azumaya-Algebra und $\beta: A \otimes L \xrightarrow{\cong} M_r(L)$ eine (galoissche) Zerfällung. Für $a \in A$ liegt die reduzierte Spur $\text{Tr}(\beta(a \otimes 1))$ von a in F . Wir schreiben dafür $\text{Trd}_A(a)$.

Lemma 3.1.3 Sei A eine F -Azumaya-Algebra und σ eine Involution 1. Art auf A . Es gilt $\dim(\text{Sym}(A, \sigma)) + \dim(\text{Alt}(A, \sigma)) = n^2$ und

$$\begin{aligned}\text{Alt}(A, \sigma) &= \{a \in A \mid \text{Trd}_A(as) = 0 \text{ für alle } s \in \text{Sym}(A, \sigma)\} \\ \text{Symd}(A, \sigma) &= \{a \in A \mid \text{Trd}_A(as) = 0 \text{ für alle } s \in \text{Skew}(A, \sigma)\}\end{aligned}$$

Falls $\text{char } F = 2$, so ist σ symplektisch genau dann wenn $1 \in \text{Alt}(A, \sigma)$.

Definition 3.1.4 Sei A eine F -Azumaya-Algebra von Grad n . Ein quadratisches Paar (σ, f) auf A besteht aus einer Involution 1. Art σ , welche orthogonal ist falls $\text{char } F \neq 2$ bzw. symplektisch falls $\text{char } F = 2$, und einer linearen Abbildung $f: \text{Sym}(A, \sigma) \rightarrow F$, welche folgende Bedingung erfüllt:

$$f(x + \sigma(x)) = \text{Trd}_A(x) \text{ für alle } x \in A.$$

Ist A nicht aus dem Kontext bekannt, so schreiben wir auch (A, σ, f) für ein quadratisches Paar.

Bemerkung Die Definition macht Sinn, da $x + \sigma(x) = x' + \sigma(x') \Leftrightarrow x' - x \in \text{Skew}(A)$ und wegen Lemma (3.1.3) $\text{Trd}(\text{Skew}(A, \sigma)) = \{0\} \Leftrightarrow 1 \in \text{Symd}(A, \sigma)$, was für Involutionen 1. Art in $\text{char } F \neq 2$ immer erfüllt ist und in $\text{char } F = 2$ genau dann wenn σ symplektisch ist.

Falls $\text{char } F \neq 2$, so ist f durch die Bedingung $f(x + \sigma(x)) = \text{Trd}_A(x)$ für alle $x \in A$ eindeutig bestimmt: $f(x) = \frac{1}{2} \text{Trd}_A(x)$. Falls $\text{char } F = 2$, so ist f nur auf $\text{Symd}(A, \sigma) \subsetneq \text{Sym}(A, \sigma)$ festgelegt und es gibt im Allgemeinen verschiedene Abbildungen f , mit welcher σ ein quadratisches Paar auf A bildet. Dies entspricht im Fall von $[A] = 1$ in $\text{Br}(F)$ der Tatsache, dass es verschiedene quadratische Formen auf V mit vorgegebener Polaren gibt.

Lemma 3.1.5 Sei (A, σ, f) ein quadratisches Paar. Es existiert ein bis auf Addition von Elementen in $\text{Alt}(A, \sigma)$ eindeutig bestimmtes Element $\ell \in A$ mit

$$f(s) = \text{Trd}_A(\ell s) \text{ für alle } s \in \text{Sym}(A, \sigma) \quad \text{und } \ell + \sigma(\ell) = 1.$$

Falls $\text{char } F \neq 2$, so kann $\ell = \frac{1}{2}$ gewählt werden.

Im Folgenden beschreiben wir quadratische Paare für triviale F -Azumaya-Algebren, d.h. von der Form $A = \text{End}_F(V)$. Es weist sich heraus, dass sich diese mit regulären quadratischen Räumen modulo F^\times identifizieren lassen.

Lemma 3.1.6 Sei A Azumaya über F mit einer Involution σ von 1. Art.

- $\deg A = 2k + 1$: A zerfällt über F und σ ist notwendigerweise orthogonal. Es gibt insbesondere keine quadratischen Paare auf A falls $\text{char } F = 2$.

- $\deg A = 2k$: Der Index von A ist eine Zweierpotenz und A hat sowohl Involutionen von symplektischem als auch von orthogonalem Typ.

Lemma 3.1.7 Sei (V, q) ein regulärer quadratischer Raum. Definiere eine Abbildung

$$V \otimes V \rightarrow \text{End}_F(V), \quad \varphi_q(v \otimes w)(x) = vb_q(w, x).$$

Diese Abbildung ist ein Isomorphismus und induziert einen Isomorphismus von Algebren mit Involutionen:

$$\varphi_q: (V \otimes V, \sigma_{\text{sw}}) \xrightarrow{\cong} (\text{End}_F(V), \sigma_q),$$

wobei $\sigma_{\text{sw}}(v \otimes w) = w \otimes v$ und σ_q die zu b_q adjungierte Involution bezeichnet. Es existiert eine eindeutige lineare Abbildung $f_q: \text{Sym}(\text{End}_F(V), \sigma_q) \rightarrow F$ mit

$$f_q \circ \varphi_q(v \otimes v) = q(v) \text{ für alle } x, y \in V.$$

Das Paar (σ_q, f_q) ist ein quadratisches Paar auf $\text{End}_F(V)$.

Theorem 3.1.8 Sei (σ, f) ein quadratisches Paar auf einer Endomorphismenalgebra $\text{End}_F(V)$. Dann ist (σ, f) von der Form (σ_q, f_q) für eine reguläre quadratische Form q auf V , welche bis auf einen Faktor in F^\times eindeutig bestimmt ist.

3.2 Clifford-Algebra von quadratischen Paaren

Im Folgenden wird für quadratische Paare (A, σ, f) eine Clifford-Algebra eingeführt auf eine Weise, dass $C(\text{End}_F(V), \sigma_q, f_q) \simeq C_0(V, q)$ für einen regulären quadratischen Raum (V, q) .

Die Relationen in $C_0(V, q) \subset T_0(V)/J(q)$ sind von zweierlei Art: Die einen kommen von der Gleichung $x \otimes x = q(x) \cdot 1$, die zweiten von der Gleichung $x \otimes y \otimes y \otimes z = q(y)x \otimes z$. Die gerade Clifford-Algebra $C_0(V, q)$ kann direkt als Quotient der Tensoralgebra $T(V \otimes V)$ definiert werden durch

$$C_0(V, q) = \frac{T(V \otimes V)}{J_1(q) + J_2(q)},$$

wobei die Ideale $J_1(q), J_2(q) \subset T(V \otimes V)$ von den Elementen der Form $x \otimes x - q(x) \cdot 1$ bzw. $(x \otimes y) \otimes (y \otimes z) - q(y) \cdot x \otimes z$ erzeugt werden. Sei $A = \text{End}_F(V)$ und \underline{A} der unterliegende F -Vektorraum der F -Algebra A . Wir identifizieren

im Folgenden die Vektorräume $V \otimes V$ und \underline{A} mittels $\varphi_q: (V \otimes V, \sigma_{\text{sw}}) \xrightarrow{\cong} (\text{End}_F(V), \sigma_q)$. Unter dieser Identifizierung wird $J_1(q)$ von den bzgl. σ_q symmetrischen Elementen von \underline{A} erzeugt. Das Ideal $J_2(q)$ kann wie folgt beschrieben werden: Es bezeichne $\text{Sand}: \underline{A} \otimes \underline{A} \rightarrow \text{End}_F(\underline{A})$ definiert durch $\text{Sand}(a \otimes b)(x) = axb$ den „Sandwich“-Isomorphismus. Dann ist $J_2(q)$ von allen Elementen der Form

$$u - \text{Sand}(u)(\ell), \text{ für } u \in A \otimes A \text{ mit } \text{Sand}(u)(x) = \text{Sand}(u)(\sigma_q(x)), \forall x \in \underline{A}$$

erzeugt. Wir überprüfen dies für Körper F von Charakteristik $\neq 2$, für welche wir $\ell = \frac{1}{2}$ wählen können. Sei u von der Form $u = a \otimes b$ mit $a = \varphi_q(v_1 \otimes v_2)$, $b = \varphi_q(v_3 \otimes v_4)$ und sei $x = \varphi_q(w_1 \otimes w_2)$. Dann ergibt eine kurze Rechnung

$$\begin{aligned} \text{Sand}(u)(x) &= b_q(v_2, w_1)b_q(w_2, v_3)\varphi_q(v_1, v_4), \\ \text{Sand}(u)(\sigma_q(x)) &= b_q(v_2, w_2)b_q(w_1, v_3)\varphi_q(v_1, v_4) \end{aligned}$$

und es folgt, dass die Elemente u mit $\text{Sand}(u)(x) = \text{Sand}(u)(\sigma_q(x))$, $\forall x \in \underline{A}$ von den Elementen der Form $u = \varphi_q(v_1 \otimes w) \otimes \varphi_q(w \otimes v_2)$ erzeugt werden. Für ein solches u ist $\text{Sand}(u)(\ell) = \frac{1}{2}b_q(w, w)\varphi_q(v_1, v_2) = q(w)\varphi_q(v_1, v_2)$, womit die Behauptung folgt. Die allgemeine Definition eines quadratischen Paares ist nun naheliegend:

Definition 3.2.1 Sei (σ, f) ein quadratisches Paar auf einer F -Azumaya Algebra A . Die Clifford-Algebra ist definiert als

$$C(A, \sigma, f) = \frac{T(\underline{A})}{J_1(\sigma, f) + J_2(\sigma, f)}$$

wobei die Ideale $J_1(\sigma, f)$, $J_2(\sigma, f) \subset T(\underline{A})$ wie folgt gegeben sind:

$J_1(\sigma, f)$ ist von allen Elementen der Form $s - f(s)$, für $s \in \underline{A}$ mit $\sigma(s) = s$, erzeugt.

$J_2(\sigma, f)$ ist von allen Elementen der Form $u - \text{Sand}(u)(\ell)$, für $u \in \underline{A} \otimes \underline{A}$ mit $\text{Sand}(u)(x) = \text{Sand}(u)(\sigma(x))$ für alle x , erzeugt.

Die Involution σ auf A induziert auf der Tensoralgebra $T(\underline{A})$ eine Involution, welche die beiden Ideale $J_1(\sigma, f)$, $J_2(\sigma, f)$ in sich abbildet. Sie vererbt sich daher auf eine Involution der Clifford-Algebra $C(A, \sigma, f)$, welche wir die *kanonische Involution* nennen, notiert $\underline{\sigma}$. Es gilt nach Konstruktion:

$$\underline{\sigma}(a_1 \otimes \cdots \otimes a_k) = \sigma(a_k) \otimes \cdots \otimes \sigma(a_1) \text{ für alle } k \in \mathbb{N}, a_1, \dots, a_k \in \underline{A},$$

betrachtet als Elemente der Cliffordalgebra.

Lemma 3.2.2 Sei (A, σ, f) ein quadratisches Paar über einem Körper F und sei $L \supset F$ eine Körpererweiterung. Dann ist (A_L, σ_L, f_L) definiert als $(A \otimes L, \sigma \otimes \text{id}_L, f \otimes \text{id}_L)$ ein quadratisches Paar und es gilt $C(A_L, \sigma_L, f_L) \simeq C(A, \sigma, f) \otimes L$.

Theorem 3.2.3 (Strukturtheorem) Sei (A, σ, f) ein quadratisches Paar, $\deg A = n$ und $C(A, \sigma, f)$ die Clifford-Algebra.

1. $n = 2k$: $Z = Z(C_0(M, q))$ ist eine separable quadratische F -Algebra und $C(A, \sigma, f)$ ist Z -Azumaya von Z -Rang $2^{2(k-1)}$. Falls $Z \simeq F \times F$, so ist $C(A, \sigma, f) \simeq C^+ \times C^-$ für F -Azumaya-Algebren C^\pm von Grad 2^{k-1} und es gilt: $[C^+][C^-][A] = 1$ in $\text{Br}(F)$ falls k gerade ist, bzw. $[C^+][C^-] = 1$ falls k ungerade ist.
2. $n = 2k + 1$: $(A, \sigma, f) \simeq (\text{End}_F(V), \sigma_q, f_q)$ für einen regulären quadratischen Raum (V, q) ; es gilt $C(A, \sigma, f) \simeq C_0(V, q)$ und diese Algebra ist F -Azumaya.

Wir wenden im Weiteren häufig stillschweigend folgende Tatsache an:

Lemma 3.2.4 Sei $\beta: (A, \sigma, f) \xrightarrow{\simeq} (B, \tau, g)$ ein Isomorphismus, d.h. β ist ein Isomorphismus von Algebren mit Involutionen und $g \circ \beta = f$. Dann sind die Cliffordalgebren $C(A, \sigma, f)$ und $C(B, \tau, g)$ kanonisch isomorph. Sind (V, q) und (V', q') zwei ähnliche quadratische Räume, so sind die geraden Cliffordalgebren $C_0(V, q)$ und $C_0(V', q')$ kanonisch isomorph.

3.3 Verallgemeinerung des Kompositionsproblems

Wir verallgemeinern das Kompositionsproblem von quadratischen Formen über Körpern auf quadratische Paare folgendermassen:

Definition 3.3.1 Sei (A, σ, f) ein quadratisches Paar über einem Körper F . Sei B eine Azumaya-Algebra mit Zentrum F oder S , wobei S eine quadratische, separable Erweiterung von F mit Standardinvolution i bezeichnet. Sei τ eine Involution von B mit $\tau|_F = \text{id}$ bzw. $\tau|_S = i$. Eine Komposition von (A, σ, f) mit (B, τ) ist ein Homomorphismus von F -Algebren mit Involutionen:

$$\alpha: (C(A, \sigma, f), \underline{\sigma}) \longrightarrow (B, \tau)$$

Aus den Theoremen (1.3.8), (2.1.1), und (2.3.2) ergibt sich folgender Satz:

Proposition 3.3.2 Sei $(\sigma, f) = (\sigma_q, f_q)$ ein quadratisches Paar auf $A = \text{End}_F(V)$ und $\alpha: (C(A, \sigma, f), \underline{\sigma}) \longrightarrow (B, \tau)$ eine Komposition. Der quadratische Raum (V, q) kann so gewählt werden, dass ein z existiert mit $q(z) = 1$. Sei D eine Azumaya-Algebra mit $[B]_c = [D]_c$. Dann gibt es eine Involution θ auf D und es existiert ein treues D -Modul E , sowie eine (bzgl. θ) nichtsinguläre ε -hermitesche Form h mit $(B, \tau) \simeq (\text{End}_D(E), \sigma_h)$ und eine Komposition $\phi: (M, q) \times (E, h) \rightarrow (E, h)$.

Proposition 3.3.3 Sei $\alpha: (C(A, \sigma, f), \underline{\sigma}) \longrightarrow (B, \tau)$ eine Komposition über einem Körper F und $L \supset F$ eine Körpererweiterung. Dann ist $\alpha \otimes \text{id}_L$ eine Komposition von $C(A_L, \sigma_L, f_L)$ mit $(B \otimes_F L, \tau \otimes_F \text{id}_L)$. Insbesondere liefert jede Komposition durch Erweiterung der Skalare zu einem Zerfällungskörper von A eine (klassische) Komposition eines quadratischen Raumes mit einem ε -hermiteschen Raum.

Beispiel Sei $(\sigma, f) = (\sigma_q, f_q)$ ein quadratisches Paar auf $A = \text{End}_F(V)$ und sei $\alpha: (C(A, \sigma, f), \underline{\sigma}) \longrightarrow (B, \tau)$ eine Komposition, wobei B eine F -Azumaya-Algebra von Index ≤ 2 und τ eine symplektische Involution bezeichne. Dann ist (B, τ) von der Form $(\text{End}_Q(E), \sigma_h)$ für eine Quaternionen-Algebra Q und einer nichtsingulären, bzgl. der Standardinvolution auf Q hermiteschen Form h und wir erhalten eine Komposition von (V, q) mit (E, h) , sofern q so gewählt ist, dass $1 \in q(V)$.

Wie schon bemerkt gibt es in Charakteristik 2 für Räume ungeraden Ranges keine quadratischen Paare. Wir betrachten in diesem Fall anstatt quadratischen Paaren halbreguläre quadratische Räume und führen folgende Notation ein:

Notation Es bezeichnet P ein quadratisches Paar (A, σ, f) oder einen halbregulären quadratischen Raum (M, q) (in ungerader Dimension, $\text{char } F = 2$). Wir nennen P ein *erweitertes quadratisches Paar*. Dabei sei $(C(P), \underline{\sigma})$ die (gerade) Clifford-Algebra $C(A, \sigma, f)$ bzw. $C_0(M, q)$ mit kanonischer Involution. Wir schreiben $\text{deg } P$ für $\text{deg } A$ bzw. $\dim V$.

Wie aus der Definition der Komposition von quadratischen Paaren ersichtlich ist, spielt die kanonische Involution $\underline{\sigma}$ der Clifford-Algebra $C(P)$ eine wichtige Rolle. Der Typ der kanonischen Involution und die Restriktion auf $Z(C(P))$ (für $\text{deg } P$ gerade) ist wie folgt bestimmt:

Theorem 3.3.4 Sei P ein erweitertes quadratisches Paar von Grad n und $(C(P), \underline{\sigma})$ die zugehörige Clifford-Algebra mit kanonischer Involution.

- $n = 2k$: Die Involution $\underline{\sigma}$ ist unitär falls k ungerade, orthogonal falls $\text{char } F \neq 2$, $k \equiv 0 \pmod{4}$, bzw. symplektisch falls $\text{char } F = 2$ oder $k \equiv 2 \pmod{4}$.
- $n = 2k + 1$: Die Involution $\underline{\sigma}$ ist orthogonal falls $\text{char } F \neq 2$, $n \equiv \pm 1 \pmod{8}$, bzw. symplektisch falls $\text{char } F = 2$, $n > 1$ oder $n \equiv \pm 3 \pmod{8}$. Die einzige Ausnahme bildet $n = 1$, $\text{char } F = 2$. In diesem Fall ist $C(P) = F$ und $\underline{\sigma}$ notwendigerweise orthogonal.

Definition 3.3.5 Wir unterscheiden verschiedene Typen von Kompositionen $\alpha: (C(P), \underline{\sigma}) \longrightarrow (B, \tau)$ durch die Klasse $[B]_c$ in der konstanten Brauergruppe und danach, ob die Involution τ unitär, orthogonal oder symplektisch ist. Es bedeute $\text{Typ } \alpha = ([D], t)$ mit $t = \pm 1 \in F$, dass B F -Azumaya mit Brauerklasse $[B] = [D]$ und τ von symplektischem Typ sei falls $t = -1$, bzw. von orthogonalem Typ falls $t \neq -1$. Es bedeute $\text{Typ } \alpha = ([D']_c, 0)$, dass B Azumaya über $Z(D') \supset F$ sei mit $[B]_c = [D']_c$ und τ unitär sei mit dem Körper von zentral Invarianten gleich F . Wir betrachten keine Kompositionen mit orthogonalen Involutionsen, falls $\text{char } F = 2$.

Bemerkung Die Kompositionen von den Typen $([F], \pm 1)$, $([Q], -1)$ und $([S]_c, 0)$ mit $\deg Q = 2$ entsprechen Zügers Kompositionen von quadratischen Räumen mit (anti-)symmetrischen Bilinearformen, mit bzgl. der Standardinvolution hermiteschen Formen über Quaternionen Q , bzw. mit hermiteschen Formen über einer quadratischen Algebra S .

3.4 Minimale Kompositionen

Definition 3.4.1 Eine Komposition $\alpha: (C(P), \underline{\sigma}) \longrightarrow (B, \tau)$ heisst minimal, falls keine Komposition $\beta: (C(P), \underline{\sigma}) \longrightarrow (B', \tau')$ mit $\text{Typ } \alpha = \text{Typ } \beta$ und $\text{Rg } B' < \text{Rg } B$ existiert.

In diesem Abschnitt wird die Frage untersucht, wie der entsprechende minimale Grad $\deg B$ einer minimalen Komposition $\alpha: (C(A, \sigma, f), \underline{\sigma}) \longrightarrow (B, \tau)$ bestimmt ist. Die allgemeine Antwort lässt sich mit Hilfe einer Metrik auf der konstanten Brauergruppe ausdrücken:

Lemma 3.4.2 Sei R ein kommutativer Ring und $\text{Br}_c(R)$ die konstante Brauergruppe (siehe Definitionen (1.1.8) und (1.1.10)). Die Abbildung

$$d: \text{Br}_c(R) \times \text{Br}_c(R) \rightarrow \mathbb{R}, \quad d([B_1]_c, [B_2]_c) = \log_2 \text{ind}(B_1 \otimes B_2^{\text{op}})$$

ist wohldefiniert und erfüllt die Axiome einer Metrik. Sie besitzt die zusätzlichen Eigenschaften

$$d(A \otimes B, A \otimes C) = d(B, C) \quad \text{und} \quad d(B^{\text{op}}, C^{\text{op}}) = d(B, C)$$

für R -Azumaya-Algebren A, B, C von konstantem Rang.

Beweis Nach Konstruktion hängt der Index einer Azumaya-Algebra von konstantem Rang nur von ihrer Klasse in der konstanten Brauergruppe ab. Unter Verwendung der Eigenschaften 1) $[A]_c^{-1} = [A^{\text{op}}]_c$, 2) $\text{ind } A = \text{ind } A^{\text{op}}$ und 3) $\text{ind}(A_1 \otimes A_2) \leq \text{ind}(A_1) \text{ind}(A_2)$ lassen sich die Behauptungen des Lemmas einfach zeigen: Wohldefiniertheit folgt aus 1), positive Definitheit aus 1) und $\deg R = 1$, Symmetrie folgt aus 2) und die Dreiecksungleichung aus 3). Eigenschaft 1) folgt direkt aus der Charakterisierung von Azumaya-Algebren (Theorem (1.1.4)). Um Eigenschaft 2) zu zeigen schreiben wir $\text{ind } A = \text{deg } A_0$ für einen Repräsentanten A_0 der Brauerklasse $[A]_c$ von minimalem Grad, womit mit Hilfe von 1) folgt: $\text{ind } A^{\text{op}} \leq \text{deg } A_0^{\text{op}} = \text{deg } A_0 = \text{ind } A$. Die umgekehrte Ungleichung ergibt sich aus dem gleichen Argument und $(A^{\text{op}})^{\text{op}} = A$. Genauso wählt man für 3) Repräsentanten von minimalem Grad und erhält die Ungleichung sofort. \square

Bemerkung Die Brauerklassen von Azumaya-Algebren mit einer Involution erster Art bilden eine Untergruppe der Brauergruppe. Sei nun F ein Körper. Die Brauergruppe und die konstante Brauergruppe stimmen überein. Aus Lemma (3.1.6) erhalten wir, dass die induzierte Metrik auf der obigen Untergruppe nach \mathbb{N} abbildet. Dadurch erklärt sich die Wahl der Basis 2 des Logarithmus in der Definition der Metrik.

Die Bedeutung dieser Metrik für die Lösung des Kompositionsproblem zeigt sich in den beiden folgenden Lemmata.

Lemma 3.4.3 *Seien B und C R -Azumaya-Algebren von konstantem Rang. Der minimale Rang einer R -Azumaya-Algebra A von konstantem Rang mit $[A]_c = [B]_c$ für welche ein Homomorphismus von R -Algebren $f: C \rightarrow A$ existiert, ist genau $\text{deg } A = \text{deg } C \cdot 2^{d(B,C)}$. Ist ferner $R = F$ oder $R = F \times F$ und A wie oben, jedoch nicht unbedingt minimal, so teilt $\text{deg } C \cdot 2^{d(B,C)}$ den Grad von A .*

Beweis Falls $f: C \rightarrow A$ ein Homomorphismus ist, so ist $A \simeq C \otimes G$ wobei $G = C_A(f(C))$ eine R -Azumaya-Algebra von konstantem Rang mit $[G]_c = [A]_c [C]_c^{-1} = [B \otimes C^{\text{op}}]_c$ ist. Es folgt die Ungleichung: $\text{deg } A = \text{deg } C \text{deg } G \geq \text{deg } C \text{ind } G = \text{deg } C \text{ind}(B \otimes C^{\text{op}}) = \text{deg } C \cdot 2^{d(B,C)}$. Im Falle $R = F$ oder

$R = F \times F$ teilt wegen Lemma (1.1.12) der Index von G den Grad von G . Umgekehrt existiert nach Definition von Metrik und Index eine R -Azumaya Algebra G mit $2^{d(B,C)} = \deg G$ und $[B \otimes C^{\text{op}}]_{\mathfrak{c}} = [G]_{\mathfrak{c}}$. Definiere $f: C \rightarrow A = C \otimes G$ durch die Inklusion. Es gilt $\deg A = \deg C \deg G = \deg C \cdot 2^{d(B,C)}$ und $[A]_{\mathfrak{c}} = [C]_{\mathfrak{c}}[G]_{\mathfrak{c}} = [C]_{\mathfrak{c}}[B \otimes C^{\text{op}}]_{\mathfrak{c}} = [B]_{\mathfrak{c}}$. \square

Lemma 3.4.4 *Sei P ein erweitertes quadratisches Paar von Grad n . Sei B eine Azumaya-Algebra von konstantem Rang und $Z(B) = F$ oder $Z(B) = S$ für eine separable quadratische Erweiterung $S \supset F$ und sei $\alpha: C = C(P) \rightarrow B$ ein Homomorphismus von F -Algebren. Es lässt sich Folgendes über den Grad von B aussagen:*

1. $n = 2k + 1$:

- (a) $Z(B) = F$ und $[B] = [D]$: Es gilt $2^{k+d(D,C)} \mid \deg B$.
- (b) $Z(B) = S$ und $[B]_{\mathfrak{c}} = [D']_{\mathfrak{c}}$: Es gilt $2^{k+d(D',C \otimes S)} \mid \deg B$.

2. $n = 2k$: Sei $Z = Z(C(P))$.

- (a) $Z(B) = F$ und $[B] = [D]$: Ist $Z = K$ ein Körper, so gilt $2^{k+d(D \otimes K, C)} \mid \deg B$. Ist $Z \simeq F \times F$, $C \simeq C^+ \times C^-$, so können wir folgendes aussagen: Falls $\ker \alpha = \{0\} \times C^-$ gilt $2^{k-1+d(D, C^+)} \mid \deg B$; falls $\ker \alpha = C^+ \times \{0\}$ gilt $2^{k-1+d(D, C^-)} \mid \deg B$; falls α injektiv ist, so ist $\deg B = 2^{k-1} \cdot (n_1 \cdot 2^{d(D, C^+)} + n_2 \cdot 2^{d(D, C^-)})$ für gewisse $n_1, n_2 \in \mathbb{N}$.

Ist $\deg P \equiv 2 \pmod{4}$ und $B \simeq B^{\text{op}}$, so ist im letzten Fall $\deg B = n \cdot 2^{k-1+d(D, C^+)} = n \cdot 2^{k-1+d(D \otimes Z, C(P))}$ für ein $n \geq 2$.

- (b) $Z(B) = S$ und $[B]_{\mathfrak{c}} = [D']_{\mathfrak{c}}$: Wir betrachten nur 2 Spezialfälle: $\ker \alpha \neq \{0\}$ oder $Z = S$.

i. $\ker \alpha \neq \{0\}$: Es folgt $Z \simeq F \times F$, $C \simeq C^+ \times C^-$: Falls $\ker \alpha = \{0\} \times C^-$, so gilt $2^{k-1+d(D', C^+ \otimes S)} \mid \deg B$; falls $\ker \alpha = C^+ \times \{0\}$, so gilt $2^{k-1+d(D', C^- \otimes S)} \mid \deg B$.

ii. $Z = S$, α injektiv: Es gilt $2^{k-1+d(C(P), D')} \mid \deg B$ falls S ein Körper ist, bzw. $\deg B = 2^{k-2} \cdot (n_1 2^{d(D_1, C^+)} + n_2 2^{d(D_2, C^-)})$ für gewisse $n_1, n_2 \in \mathbb{N}$ falls $S \simeq F \times F$, $D' = D_1 \times D_2$.

Beweis 1. $\deg P = 2k + 1$: Dann ist $\deg C = 2^k$.

- (a) $Z(B) = F$ und $[B] = [D]$: Die Aussage ergibt sich direkt aus Lemma (3.4.3).

- (b) $Z(B) = S$ und $[B]_c = [D']_c$: Die Algebra B lässt sich als $B = \alpha(C) \otimes G = (\alpha(C) \otimes S) \otimes_S G$ für eine S -Algebra G schreiben. Also ist $\alpha \otimes \text{id}_S: C \otimes S \rightarrow \alpha(C) \otimes S \hookrightarrow B$ ein Homomorphismus von S -Azumaya-Algebren und Lemma (3.4.3) gibt die behauptete Schranke.

2. $n = 2k$: Dann ist $\deg C = 2^{k-1}$. Sei $Z = Z(C(P))$.

- (a) $Z(B) = F$ und $[B] = [D]$: Sei zuerst α injektiv: Man könnte einen Homomorphismus $C \rightarrow B \hookrightarrow B \otimes Z$ konstruieren, aber dieser ist nicht Z -linear. Wir gehen deshalb wie folgt vor: Wegen $[B \otimes B^{\text{op}}] = 1$ existiert ein F -Vektorraum E mit $\alpha \otimes 1: C \otimes B^{\text{op}} \rightarrow B \otimes B^{\text{op}} \simeq \text{End}_F(E)$. Wir führen auf E eine Z -Modulstruktur ein durch $\lambda y = ((\alpha \otimes 1) \circ i(\lambda))(y)$ für $\lambda \in Z, y \in E$ und $i: Z \hookrightarrow C$. Da $\alpha \otimes 1$ und i injektiv sind, ist E ein treuer Z -Modul. Also ist $\text{End}_Z(E)$ eine Z -Azumaya-Algebra. Falls $Z = K$ ein Körper ist, so hat $\text{End}_Z(E)$ konstanten Rang. Falls $Z \simeq F \times F$, so muss dies jedoch nicht der Fall sein. Wir behandeln zuerst den Fall $Z = K$ ein Körper. Das Bild von $(\alpha \otimes 1) \circ i$ liegt in $\text{End}_K(E)$. Der Homomorphismus $C \otimes B^{\text{op}} \rightarrow \text{End}_K(E)$ ist nach Konstruktion K -linear und liefert mit Lemma (3.4.3) ein $n \in \mathbb{N}$ mit $\frac{1}{2}(\deg B)^2 = \deg \text{End}_K(E) = n \deg B \deg C \cdot 2^{d(K, C \otimes B^{\text{op}})} = n \deg B \cdot 2^{k-1+d(B \otimes K, C)} = n \deg B \cdot 2^{k-1+d(D \otimes K, C)}$. Kürzen von $\frac{1}{2} \deg B$ ergibt die behauptete Relation $2^{k+d(D \otimes K, C)} \mid \deg B$.
Nun zum Fall $Z \simeq F \times F$. Sei e ein nichttriviales zentrales Idempotentes von C und $E^+ = \alpha(e)E$, $E^- = \alpha(1-e)E$, $C^+ = eC$, $C^- = (1-e)C$. Wegen $E = E_1 \oplus E_2$, $\text{End}_Z(E) \simeq \text{End}_F(E_1) \times \text{End}_F(E_2)$ erhalten wir Homomorphismen $\alpha_{\pm}: C^{\pm} \otimes B^{\text{op}} \rightarrow \text{End}_F(E_{\pm})$. Lemma (3.4.3) liefert $n_{\pm} \in \mathbb{N}$ mit $\dim E_{\pm} = n_{\pm} \deg B \cdot 2^{k-1+d(D, C^{\pm})}$. Also ergibt sich die Gleichung $(\deg B)^2 = \dim E = \dim E_- + \dim E_+ = \deg B \cdot 2^{k-1}(n_+ 2^{d(D, C^+)} + n_- 2^{d(D, C^-)})$ und damit die Behauptung.

Ist α nicht injektiv, so ist der Kern eines der nichttrivialen Ideale $C^+ \times \{0\}$ und $\{0\} \times C^-$. Die Abbildung faktorisiert deshalb durch $C^+ \simeq C/(\{0\} \times C^-)$ oder $C^- \simeq C/(C^+ \times \{0\})$. Lemma (3.4.3) liefert wie behauptet $2^{k-1+d(D, C^+)} \mid \deg B$ bzw. $2^{k-1+d(D, C^-)} \mid \deg B$. Die letzte Behauptung folgt aus $d(D, C^+) = d(D^{\text{op}}, (C^+)^{\text{op}}) = d(D, C^-)$ und $d(D \otimes Z, C) = \text{kgV}(d(D, C^+), d(D, C^-))$.

- (b) $Z(B) = S$ und $[B]_c = [D']_c$:
i. $Z \simeq F \times F$, $C \simeq C^+ \times C^-$: Falls $\ker \alpha = C^+ \times \{0\}$, so faktorisiert α durch C^- . Wie im Fall 1a) folgt die Aussage.

Der Fall $\ker \alpha = \{0\} \times C^-$ ist analog.

- ii. $Z = S$: Sei zuerst $Z = K$ ein Körper. Es existiert ein K -Vektorraum E mit $B \otimes B^{\text{op}} \simeq \text{End}_K(E)$. Sei $\beta: C(P) \otimes B^{\text{op}} \rightarrow \text{End}_F(E)$ der Homomorphismus $C \otimes B^{\text{op}} \xrightarrow{\alpha \otimes 1} B \otimes B^{\text{op}} \subset \text{End}_F(E)$. Wir definieren auf E mittels $i: K \hookrightarrow C$ und β eine neue K -Vektorraum-Struktur und schreiben $\text{End}'_K(E)$ für die Endomorphismenalgebra bezüglich der neuen Vektorraum-Struktur. Das Bild von β liegt in $\text{End}'_K(E)$ und wir erhalten einen K -linearen Homomorphismus $C \otimes B^{\text{op}} \xrightarrow{\beta} \text{End}'_K(E)$. Das Lemma (3.4.3) liefert die Beziehung $\deg C \deg B \cdot 2^{d(C \otimes B^{\text{op}}, K)} \mid \deg \text{End}'_K(E) = (\deg B)^2$ und die Aussage folgt.

Sei nun $Z = S = F \times F$. Wie oben erhalten wir einen Z -linearen Homomorphismus $C \otimes B^{\text{op}} \rightarrow \text{End}'_Z(E)$, wobei $\dim_F(E) = 2(\deg B)^2$. Die Algebra $\text{End}'_Z(E)$ zerfällt in zwei Teile $\text{End}_F(E_1) \times \text{End}_F(E_2)$ mit $\dim E_1 + \dim E_2 = \dim E$. Sei $B = B_1 \times B_2$. Wir erhalten Homomorphismen $C^+ \otimes B_1^{\text{op}} \rightarrow \text{End}_F(E_1)$ und $C^- \otimes B_2^{\text{op}} \rightarrow \text{End}_F(E_2)$. Lemma (3.4.3) liefert $n_1, n_2 \in \mathbb{N}$ mit $\dim E_i = n_i \deg C \deg B \cdot 2^{d(F, C^+ \otimes B_i^{\text{op}})}$, $i = 1, 2$. Es folgt $2(\deg B)^2 = \deg C \deg B \cdot (n_1 2^{d(B_1, C^+)} + n_2 2^{d(B_2, C^-)})$ und damit die Aussage. □

Theorem 3.4.5 (Grad von minimalen Kompositionen) *Sei P ein erweitertes quadratisches Paar von Grad $n > 1$ und $\alpha: (C(P), \underline{\sigma}) \rightarrow (B, \tau)$ eine minimale Komposition (bzw. allgemein eine beliebige Komposition). Dann ist der Grad von B wie folgt bestimmt:*

1. $n = 2k + 1$:

- (a) Typ $\alpha = (D, \pm 1)$: *Der minimale Grad beträgt $2^{k+d(D, C(P))+\delta}$, wobei $\delta = 1$ gdw. $[C(P)] = [D]$ und*

$$\left\{ \begin{array}{l} \text{char } F \neq 2 \text{ und } (\tau \text{ symplektisch und } \deg P \equiv \pm 1 \text{ (8)}) \\ \text{oder } (\tau \text{ orthogonal und } \deg P \equiv \pm 3 \text{ (8)}) \end{array} \right\}$$

sonst $\delta = 0$. Im Allgemeinen ist $\deg B$ ein Vielfaches des minimalen Grades.

- (b) Typ $\alpha = (D', 0)$: *Der minimale Grad beträgt $2^{k+d(D', C(P) \otimes Z(D'))}$. Im Allgemeinen ist $\deg B$ ein Vielfaches des minimalen Grades.*

2. $n = 4k$: *Sei $Z = Z(C(P))$.*

- (a) Typ $\alpha = (D, \pm 1)$: Ist $Z = K$ ein Körper, so beträgt der minimale Grad $2^{2k+d(D \otimes K, C(P))+\delta}$ und im Allgemeinen ein Vielfaches davon; ist $Z \simeq F \times F$, $C(P) \simeq C^+ \times C^-$, so beträgt der minimale Grad $2^{2k-1+\min\{d(D, C^+), d(D, C^-)\}+\delta}$, wobei in beiden Fällen $\delta = 1$ gdw. $[C(P)] = [D \otimes Z]$ bzw. ($[C^+] = [D]$ oder $[C^-] = [D]$) und $\left. \begin{array}{l} \text{char } F \neq 2 \text{ und } (\tau \text{ symplektisch und } \deg P \equiv 0 \pmod{8}) \\ \text{oder } (\tau \text{ orthogonal und } \deg P \equiv 4 \pmod{8}) \end{array} \right\}$, sonst $\delta = 0$.
- (b) Typ $\alpha = (D', 0)$: Unter der Bedingung $\ker \alpha \neq \{0\}$ beträgt der minimale Grad $2^{2k-1+\min\{d(D', C^+ \otimes S), d(D', C^- \otimes S)\}}$.

3. $n = 4k + 2$:

- (a) Typ $\alpha = (D, \pm 1)$: Der minimale Grad beträgt $2^{2k+1+d(D \otimes Z, C(P))}$. Im Allgemeinen ist $\deg B = n \cdot 2^{2k+d(D \otimes Z, C(P))}$ mit $n \geq 2$ und n gerade falls Z ein Körper ist.
- (b) Typ $\alpha = (D', 0)$: Unter der Bedingung $Z \simeq S$ beträgt der minimale Grad $2^{2k+d(D', C(P))}$ und allgemein gilt $\deg B = n \cdot 2^{2k-1+d(D', C(P))}$ mit $n \geq 2$ und n gerade falls Z ein Körper ist.

Bemerkung Im Fall 2a) kommt $\delta = 1$ nur vor, falls $[A] = 1$ ist.

Der Beweis von Theorem (3.4.5) besteht aus 2 Teilen: Existenz und Minimalität. Für beides wird ausser Lemma (3.4.4) ein Lemma zur Ausdehnung von Involutionen benötigt, welches man in [KMRT98, Seite 52] findet und hier, soweit erforderlich, wiedergegeben ist:

Lemma 3.4.6 Sei B eine einfache Teilalgebra einer Azumaya-Algebra A über einem Körper K . Nehme an, dass A und B Involutionen σ bzw. τ besitzen mit $\sigma|_K = \tau|_K$. Dann hat A eine Involution σ' , deren Restriktion auf B gleich τ ist. Falls σ von erster Art ist, dann stehen die Typen von σ' und τ wie folgt in Beziehung:

- Falls $\text{char } K \neq 2$, so kann σ' beliebig von orthogonalem oder symplektischem Typ gewählt werden, ausser wenn $\deg C_A(B)$ ungerade ist. In diesem Fall hat jede Erweiterung σ' von τ den gleichen Typ wie τ .
- Angenommen $\text{char } K = 2$: Ist τ symplektisch oder unitär, so ist jede Erweiterung σ' von τ symplektisch.

Für unitäre Involutionen auf Azumaya-Algebren über $F \times F$ verwenden wir folgende Konstruktionen:

Lemma 3.4.7 *Sei $R = F \times F$.*

1. *Sei B eine R -Azumaya-Teilalgebra einer R -Azumaya-Algebra A . Nehme an, dass A und B unitäre Involutionen σ bzw. τ besitzen. Dann hat A eine Involution σ' , deren Restriktion auf B gleich τ ist.*
2. *Sei D eine F -Azumaya-Divisionsalgebra mit einer Involution 1. Art $d \mapsto \bar{d}$ und sei B eine R -Azumaya-Algebra der Form $B = \text{End}_{D \otimes R}(E)$ für ein treu projektives $D \otimes R$ -Modul E . Sei τ eine unitäre Involution auf B . Dann existiert auf $\text{End}_D(E) \supset \text{End}_{D \otimes R}(E)$ eine Involution 1. Art σ' , welche τ ausdehnt und der Typ kann beliebig symplektisch oder orthogonal gewählt werden falls $\text{char } F \neq 2$, bzw. symplektisch falls $\text{char } F = 2$.*

Beweis 1. Gemäss dem ersten Teil von Theorem 1.3.9 haben A und B konstanten Rang. Es existiert eine R -Azumaya-Algebra C von konstantem Rang mit $A = B \otimes C$. Da A und B^{op} unitäre Involutionen besitzen und $[A \otimes B^{\text{op}}]_c = [C]_c$, besitzt wegen Lemma (1.3.7) auch C eine unitäre Involution ρ . Die Involution $\sigma' = \tau \otimes \rho$ ist eine Involution auf A , welche τ ausdehnt.

2. Sei $\text{deg } B = k$. Sei $*$ die Involution auf $M_k(D)$ gegeben durch $(d_{ij})^* = (\bar{d}_{ij})^t$. Wir können $\text{End}_D(E)$ mit $M_{2k}(D)$ und $(\text{End}_{D \otimes R}(E), \tau)$ mit $(M_k(D) \times M_k(D), \rho)$, $\rho(m_1, m_2) = (m_2^*, m_1^*)$ identifizieren. Sei σ_{\pm} die Involution auf $M_2(F)$ definiert durch $\sigma_{\pm} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & \pm b \\ \pm c & a \end{pmatrix}$. Die Involution σ_- ist unabhängig der Charakteristik von F symplektisch, σ_+ ist orthogonal falls $\text{char } F \neq 2$. Definiere σ' als Tensorprodukt $* \otimes \sigma_{\pm}$ auf $M_{2k}(D) = M_2(M_k(D))$, wobei je nach dem erwünschten Typ σ_+ oder σ_- gewählt wird. Nach Konstruktion ist $\sigma'|_{M_k(D) \times M_k(D)} = \rho$. \square

Beweis von Theorem (3.4.5) 1. $n = 2k + 1$:

- (a) Typ $\alpha = (D, t)$: Es existiert \tilde{B} und $f: C(P) \rightarrow \tilde{B}$ mit $[\tilde{B}] = [D]$ und $\text{deg } \tilde{B} = 2^{k+d(D,C)}$. Da f injektiv ist, können wir $C(P)$ mit dem Bild in \tilde{B} identifizieren. Falls $\underline{\sigma}$ den Typ t hat, so lässt sich $\underline{\sigma}$ mit Hilfe von Lemma (3.4.6) auf \tilde{B} zu einer Involution τ von Typ t ausdehnen. Dies trifft ausser in den in der Aussage des Theorems umklammerten Fällen immer zu. Falls $[C(P)] \neq [D]$, so ist $\text{deg } C_{\tilde{B}}(C(P)) = 2^{d(D,C(P))}$ gerade. Also lässt sich $\underline{\sigma}$ auch in diesem Fall zu einer Involution τ auf $B = \tilde{B}$ vom Typ t ausdehnen. In den umklammerten Fällen mit $[C(P)] = [D]$ lässt sich

$\underline{\sigma}$ hingegen nicht zu einer Involution von Typ t auf \tilde{B} (oder einer ungerade-gradigen Erweiterung von \tilde{B}) ausdehnen. Da dies für alle Homomorphismen $C(P) \rightarrow B$ mit $\deg B = 2^{k+d(D,C)}$ zutrifft, existiert keine Komposition vom Grad $2^{k+d(D,C)}$. Der minimale Grad ist somit ein gerades Vielfaches davon und insbesondere mindestens $2 \cdot 2^{k+d(D,C)}$. Dieser Grad wird erreicht durch $C(P) \rightarrow B \hookrightarrow B = \tilde{B} \otimes M_2(F)$ und Ausdehnung der Involution.

- (b) Typ $\alpha = (D', 0)$: Sei $S = Z(D')$. Es existiert \tilde{B} und $f: C(P) \hookrightarrow C(P) \otimes S \rightarrow \tilde{B}$ injektiv, mit $[\tilde{B}]_c = [D']_c$, $\deg \tilde{B} = 2^{k+d(D',C(P) \otimes S)}$. Sei κ der nichttriviale Automorphismus von $S \supset F$. Die Involution $\underline{\sigma} \otimes \kappa$ auf $C(P) \otimes S$ dehnt $\underline{\sigma}$ aus. Die Involution $\underline{\sigma} \otimes \kappa$ ist unitär und lässt sich mit Hilfe von Lemma (3.4.6) oder Lemma (3.4.7) zu einer Involution auf \tilde{B} ausdehnen. Der Rest der Behauptung folgt direkt aus Lemma (3.4.4).

2. $n = 4k$: Sei $Z = Z(C(P))$.

- (a) Typ $\alpha = (D, t)$: Falls $Z = K$ ein Körper ist, so folgt die Aussage aus Lemma (3.4.4, 2a) und der gleichen Argumentation wie in 1a). Beachte, dass $C(P) \rightarrow \text{End}_{D \otimes K}(E) \hookrightarrow \text{End}_D(E)$ mit $\deg \text{End}_{D \otimes K}(E) = \deg C(P) \cdot 2^{d(D \otimes K, C(P))}$ tatsächlich einen Homomorphismus in eine F -Azumaya-Algebra vom erforderlichen Grad liefert. Falls $Z \simeq F \times F$, $C(P) \simeq C^+ \times C^-$ so liefert Projektion auf C^+ sowie C^- unter Anwendung von Lemma (3.4.3) zwei F -Azumaya-Algebren B_{\pm} mit $[B_{\pm}] = [D]$, $\deg B_{\pm} = 2^{2k-1+d(D, C^{\pm})}$ und Homomorphismen $f_{\pm}: C(P) \rightarrow C^{\pm} \rightarrow B_{\pm}$. Die Involution $\underline{\sigma}$ induziert auf C^{\pm} zwei Involutionen $\underline{\sigma}_{\pm}$ vom gleichen Typ wie $\underline{\sigma}$. Sei oBdA $d(D, C^+) \leq d(D, C^-)$. Die Involution $\underline{\sigma}_+$ lässt sich zu einer Involution auf B_+ vom Typ t erweitern, ausser wenn einer der umklammerten Fälle zutrifft und $[C^+] = [D]$. In letzterem Fall ist der Grad von B für eine minimale Komposition $\alpha: (C(P), \underline{\sigma}) \rightarrow (B, \tau)$ mindestens $2 \cdot \deg B_{\pm} = 2^{2k+d(D, C^{\pm})}$ (im Allgemeinen ein gerades Vielfaches) und dies wird erreicht durch Tensorieren von B^+ mit $M_2(F)$ und Erweiterung der Involution von C^+ auf $M_2(B^+)$.
- (b) Typ $\alpha = (D', 0)$, $Z \simeq F \times F$: Sei κ der nichttriviale Automorphismus von $S \supset F$. Projektion auf C^{\pm} und Tensorieren mit (S, κ) liefert Homomorphismen von F -Algebren mit Involutionen $(C(P), \underline{\sigma}) \rightarrow (C^{\pm} \otimes S, \underline{\sigma}_{\pm} \otimes \kappa)$. Durch Anwendung von Lemma (3.4.3) erhalten wir zwei S -Azumaya-Algebren B_{\pm} mit $[B_{\pm}]_c = [D']_c$, $\deg B_{\pm} = 2^{2k-1+d(D', C^{\pm} \otimes S)}$ und Homomorphismen

$f_{\pm}: C^{\pm} \otimes S \rightarrow B_{\pm}$. Die unitären Involutionen auf $C^{\pm} \otimes S$ können zu unitären Involutionen auf B_{\pm} ausgedehnt werden. Minimalität des Grades folgt aus Lemma (3.4.4).

3. $n = 4k + 2$:

- (a) Typ $\alpha = (D, t)$: Da $\underline{\sigma}$ in diesem Fall unitär ist, muss jede Komposition $\alpha: (C(P), \underline{\sigma}) \rightarrow (B, \tau)$ injektiv sein, denn angenommen α sei nicht injektiv, dann ist $Z \simeq F \times F$ und es gibt ein nichttriviales zentral Idempotentes $e \in \ker \alpha$. Die Gleichung $0 = \tau(\alpha(e)) = \alpha(\underline{\sigma}(e)) = \alpha(1 - e) = 1$ führt diese Annahme zu einem Widerspruch. Aus Lemma (3.4.4) ergibt sich die Schranke $\deg B \geq 2^{2k+1+d(D \otimes Z, C(P))}$ und die gesuchte allgemeine Aussage über den Grad von B . Die Schranke kann wie folgt erreicht werden: Wegen Lemma (3.4.3) existiert eine Z -Azumaya-Algebra \tilde{B} von der Form $\tilde{B} = \text{End}_{D \otimes Z}(E)$, $\deg B = 2^{2k+1+d(D \otimes Z, C(P))}$ und ein Homomorphismus $C(P) \rightarrow \tilde{B} = \text{End}_{D \otimes Z}(E) \subset \text{End}_D(E)$. Die unitäre Involution auf $C(P)$ kann zu einer unitären Involution $\tilde{\tau}$ auf $\text{End}_{D \otimes Z}$ ausgedehnt werden. Da D eine Involution 1. Art trägt, liefert Lemma (3.4.6) oder Lemma (3.4.7) eine Involution τ von Typ t auf $B = \text{End}_D(E)$, welche $\tilde{\tau}$ ausdehnt.
- (b) Typ $\alpha = (D', 0)$, $Z = S$: Es existiert eine S -Azumaya-Algebra B mit $[B]_c = [D']_c$, $\deg B = 2^{2k+d(D', C(P))}$ und ein Homomorphismus von S -Algebren $f: C(P) \rightarrow B$. Die unitäre Involution auf $C(P)$ kann zu einer unitären Involution auf B erweitert werden. Die Minimalität des Grades und die allgemeine Aussage über den Grad von B wird durch Lemma 3.4.4 garantiert. Für $S \simeq F \times F$, $D' = D_1 \times D_2$ benützt man dabei die Gleichung $d(C^+, D_1) = d(C^-, D_2)$, welche durch die Existenz von unitären Involutionen auf $C(P)$ und D' sichergestellt wird.

□

Bemerkung Es existieren für jedes erweiterte quadratische Paar P über F und für jeden vorgegebenen Typ $(D, \pm 1)$ oder $(D', 0)$ Kompositionen. Eine solche kann wie folgt konstruiert werden: Als erstes bettet man $C(P)$ in $C(P) \otimes C(P)^{\text{op}} \simeq \text{End}_Z(E) \subset \text{End}_F(E)$ ein. Die Involution auf $C(P)$ kann mit Hilfe von Lemma (3.4.6) und Lemma (3.4.7) zu einer Involution 1. Art ρ auf $\text{End}_F(E)$ ausgedehnt werden. Als zweites tensoriert man (über F) mit (D, τ) bzw. (D', τ') , wobei τ eine Involution 1. Art auf D und τ' eine unitäre Involution auf D' bezeichnet. Im ersten Fall mag der Typ von $\rho \otimes \tau$ noch

nicht der gewünschte sein. Tensorieren mit $M_2(F)$ versehen mit der Standardinvolution schafft dem Abhilfe. Man erhält also immer eine Komposition. Die Schwierigkeit besteht nur darin, den minimalen Grad herauszufinden und zu erreichen.

In Theorem (3.4.5) lässt sich eine von der Struktur der Cliffordalgebra $C(P)$ unabhängige Schranke ablesen. Das Theorem sagt auch, wann diese Schranke erreicht wird:

Korollar 3.4.8 *Sei P ein erweitertes quadratische Paar von Grad n und $\alpha: (C(P), \underline{\sigma}) \longrightarrow (B, \tau)$ eine Komposition.*

1. $n = 2k + 1$:

(a) Typ $\alpha = (D, \pm 1)$: *Es gilt $\deg B \geq 2^{k+\delta}$, wobei $\delta = 1$ gdw.*

$$\left\{ \begin{array}{l} \text{char } F \neq 2 \text{ und } (\tau \text{ symplektisch und } \deg P \equiv \pm 1 \text{ (8)}) \\ \text{oder } (\tau \text{ orthogonal und } \deg P \equiv \pm 3 \text{ (8)}) \end{array} \right\},$$
sonst $\delta = 0$.

Gleichheit trifft genau dann ein, wenn $[C(P)] = [D]$ in den Fällen mit $\delta = 0$, bzw. $[C(P)] = [D \otimes Q]$ für eine Quaternionen-Algebra Q in den Fällen mit $\delta = 1$.

(b) Typ $\alpha = (D', 0)$: *Es gilt $\deg B \geq 2^k$ mit Gleichheit gdw. $[D']_c = [C(P) \otimes Z(D')]_c$.*

2. $n = 4k$: *Sei $Z = Z(C(P))$.*

(a) Typ $\alpha = (D, \pm 1)$: *$\deg B \geq 2^{2k-1+\delta}$, wobei $\delta = 1$ gdw.*

$$\left\{ \begin{array}{l} \text{char } F \neq 2 \text{ und } (\tau \text{ symplektisch und } \deg P \equiv 0 \text{ (8)}) \\ \text{oder } (\tau \text{ orthogonal und } \deg P \equiv 4 \text{ (8)}) \end{array} \right\},$$
sonst $\delta = 0$.

Gleichheit trifft genau dann ein, wenn $Z \simeq F \times F$ sowie $([C^+] = [D] \text{ oder } [C^-] = [D])$ in den Fällen mit $\delta = 0$, bzw. $([C^+] = [D \otimes Q] \text{ oder } [C^-] = [D \otimes Q])$ für eine Quaternionen-Algebra Q in den Fällen mit $\delta = 1$.

(b) Typ $\alpha = (D', 0)$: *Es gilt $\deg B \geq 2^{2k-1}$ mit Gleichheit gdw. $Z \simeq F \times F$ und $([C^+ \otimes S]_c = [D']_c \text{ oder } [C^- \otimes S]_c = [D']_c)$.*

3. $n = 4k + 2$

(a) Typ $\alpha = (D, \pm 1)$: *Es gilt $\deg B \geq 2^{2k+1}$ mit Gleichheit gdw. $[C(P)]_c = [D \otimes Z]_c$.*

(b) Typ $\alpha = (D', 0)$: *Es gilt $\deg B \geq 2^{2k}$ mit Gleichheit gdw. $Z \simeq S$ und $[D']_c = [C(P)]_c$.*

Beweis Es folgt alles direkt aus Theorem (3.4.5), ausser die Aussagen über das Zentrum der Cliffordalgebra in 2b) und 3b). In beiden Fällen stimmt der Grad für ein minimales B mit dem Grad der Clifford-Algebra überein. Da eine Komposition eines quadratischen Paares von $\deg A = 4k + 2$ injektiv sein muss (da die kanonische Involution der Cliffordalgebra unitär und mit der Involution auf B verträglich ist), sind die beiden Algebren isomorph und insbesondere sind die Zentren isomorph. Ist hingegen $\deg A = 4k$, so kann eine minimale Komposition nicht injektiv sein, denn sonst müssten die Involutionen auf den Zentren von gleicher Art sein. Es folgt insbesondere $Z \simeq F \times F$. \square

Um mit den Resultaten aus [Züg95] zu vergleichen, mag der Leser Korollar (3.4.8) auf die Spezialfälle von (anti-)symmetrischen Kompositionen und hermiteschen Kompositionen über quadratischen und Quaternionen-Algebren anwenden. Wir machen das hier nur für quadratische Räume (V, q) von Rang $4k$ und Kompositionen mit symplektischen Involutionen. Dies entspricht Kompositionen mit antisymmetrischen Formen und hermiteschen Formen über Quaternionen. Gemäss dem Korollar ist der minimale Grad von B für eine Komposition der Form $\alpha: (C(\text{End}_F(V), \sigma_q, f_q), \underline{\sigma}_q) \rightarrow (B, \tau)$, τ symplektisch gegeben durch 2^{2k} falls $\dim V \equiv 0 \pmod{8}$ und $\text{char } F \neq 2$, bzw. 2^{2k-1} falls $\dim V \equiv 4 \pmod{8}$ oder $\text{char } F = 2$. Zudem trifft Gleichheit genau dann ein wenn $Z \simeq F \times F$ und $[C^\pm] = [B]$ bzw. $[C^\pm] = [B \times Q']$ für eine Quaternionenalgebra Q' . Wegen der Bemerkung nach 2.2.2 ist in diesen Fällen $[C^\pm] = [C(M, q)]$. Es bleibt bloss noch zu bemerken, dass $\deg B = \dim E$ falls $B = \text{End}_F(E)$, bzw. $\deg B = \frac{1}{2} \dim E$ falls $B = \text{End}_Q(E)$.

3.5 Kompositionspaare

Definition 3.5.1 Ein regulärer quadratischer Raum (C, n) heisst unitäre Kompositionsalgebra, falls eine Komposition $\phi: (C, n) \times (C, n) \rightarrow (C, n)$ und ein Element $e \in C$ existiert mit $\phi(e, c) = c = \phi(c, e)$ für alle $c \in C$.

Proposition 3.5.2 Für eine Kompositionsalgebra (C, n) existiert eine Komposition $\alpha: (C(\text{End}_F(C), \sigma_n, f_n), \underline{\sigma}) \rightarrow (\text{End}_F(C), \sigma_n)$. Gibt es umgekehrt für einen regulären quadratischen Raum (C, n) eine solche Komposition und ist $\text{char } F \neq 2$ oder $\dim C \geq 6$, so existiert ein Skalar λ , so dass $(C, \lambda n)$ eine Kompositionsalgebra ist.

Beweis Wir wählen λ so, dass λn die Eins darstellt. Laut den Ergebnissen aus dem 2. Kapitel ist die Existenz einer Komposition von quadratischen

Formen $\phi: (C, \lambda n) \times (C, \lambda n) \rightarrow (C, \lambda n)$ unter obigen Bedingungen äquivalent zur Existenz eines Homomorphismus $\alpha: (C(\text{End}_F(C), \sigma_n, f_n), \underline{\sigma}) \rightarrow (\text{End}_F(C), \sigma_n)$. Es bleibt zu zeigen, dass ϕ so gewählt werden kann, dass ein Element $e \in C$ mit $\phi(e, c) = c = \phi(c, e)$ für alle $c \in C$ existiert. Sei $n' = \lambda n$ und $n'(z) = 1$. Wir haben bereits früher beobachtet, dass $\phi: (C, n') \times (C, n') \rightarrow (C, n')$ so gewählt werden kann, dass $\phi_z = \text{id}_C$. Sei $r_z \in \text{End}_F(C)$ die Rechtsmultiplikation gegeben durch $r_z(x) = \phi(x, z)$. Dieser Endomorphismus ist injektiv und daher invertierbar. Für die bilineare Abbildung $\phi': C \rightarrow C$ gegeben durch $\phi'(x, y) = r_z^{-1} \circ \phi_x \circ r_z(y)$ gilt $\phi'(x, z) = r_z^{-1} \circ \phi_x \circ r_z(z) = r_z^{-1} \circ \phi_x(z) = x$ und $\phi'(z, y) = r_z^{-1} \circ \phi_z \circ r_z(y) = r_z^{-1} \circ r_z(y) = y$. Auch erfüllt ϕ' die Kompositionsbedingung, denn $n'(\phi'(x, y)) = n'(r_z^{-1} \circ \phi_x \circ r_z(y)) = n'(\phi_x \circ r_z(y)) = n'(x)n'(r_z(y)) = n'(x)n'(y)$. Also ist (C, n') eine unitäre Kompositionsalgebra. \square

Definition 3.5.3 *Wir nennen ein quadratisches Paar (A, σ, f) ein Kompositionspaar, falls eine Komposition von (A, σ, f) mit (A, σ) existiert.*

Bemerkung Eigentlich möchten wir in Charakteristik 2 eine Komposition von (A, σ, f) mit (A, σ, f) voraussetzen, aber wir haben keine Definition für ein nichttriviales A . Es scheint, dass eine gute Definition der Komposition zweier quadratischen Paare (A, σ, f) und (B, τ, g) eine bilineare Abbildung $\text{Sym}(A, \sigma) \times \text{Sym}(B, \tau) \rightarrow \text{Sym}(B, \tau)$, welche mit dem Kompositionshomomorphismus und mit f und g verträglich ist, beinhalten sollte.

Bemerkung Aus Lemma (3.5.2) folgt, dass ein Kompositionspaar (A, σ, f) über einem Zerfällungskörper von A eine Kompositionsalgebra liefert, sofern $\text{char } F \neq 2$ oder $\text{deg } A \geq 6$. Insbesondere kann der Grad von A (in diesen Fällen) nur 1, 2, 4 oder 8 sein.

Theorem 3.5.4 *Sei (A, σ, f) ein Kompositionspaar, $Z = Z(C(A, \sigma, f))$. Dann ist $\text{deg } A = 1, 2, 4$ oder 8 und folgende Bedingungen sind erfüllt:*

1. $\text{deg } A = 2$: Falls $Z = K$ ein Körper ist, so ist $A \otimes K$ split; falls $Z \simeq F \times F$, so ist A split.
2. $\text{deg } A = 4$: Es gilt $Z = F \times F$, ausser falls $\text{char } F = 2$ und A trivial ist.
3. $\text{deg } A = 8$: Es gilt $Z \simeq F \times F$ und ein Faktor der Cliffordalgebra ist trivial.

Beweis Für eine Komposition $\alpha: (C(A, \sigma, f), \underline{\sigma}) \longrightarrow (B, \tau)$ muss der Grad von B mindestens $2^{\frac{1}{2} \deg A - 1}$ sein. Da $\deg A < 2^{\frac{1}{2} \deg A - 1}$ für $\deg A > 8$, fallen Paare von Grad > 8 schon mal weg. Ist $\deg A = 3, 5$ oder 7 , so erlaubt A laut Theorem (3.4.5) nur Kompositionen mit F -Azumaya-Algebren von geradem Grad. Ein quadratisches Paar mit $\deg A = 6$ lässt wiederum nur Kompositionen mit F -Azumaya-Algebren von Grad ≥ 8 zu. Es bleiben die Möglichkeiten $\deg A = 1$ (für $\text{char } F \neq 2$) und $\deg A = 2, 4, 8$. Für $\deg A = 8$ folgen die Behauptungen direkt aus Korollar (3.4.8) mit Berücksichtigung von $[C^+][C^-][A] = 1$ in $\text{Br}(F)$ (siehe Theorem 3.2.3). Die gleiche Argumentation lässt sich auf den Fall $\deg A = 4$ mit $\text{char } F \neq 2$ anwenden. Für $\deg A = 2$ gibt es laut Korollar (3.4.8) nur dann eine minimale Komposition, wenn $[C(A, \sigma, f)]_c = [A \otimes Z(C(A, \sigma, f))]_c$. Die Aussage folgt in diesem Fall aus $C(A, \sigma, f) = Z(C(A, \sigma, f))$. \square

Bemerkung Für $\text{char } F \neq 2$ ist bekannt, dass die obigen Bedingungen für Split-Paare $(\text{End}_F(V), \sigma_q, f_q)$ hinreichend dafür sind, dass q ähnlich zur Norm einer Kompositionsalgebra (C, n) ist, d.h. hinreichend um ein Kompositionspaar zu sein (vgl. [KMRT98, (35.2)], [Knu88, (9.11)]). Für $\deg A = 8$ ist die Bedingung auch in Charakteristik 2 hinreichend, siehe [Eld02, Corollary 2]. Für $\text{char } F = 2$ und $\deg A = 2$ ist die Bedingung ebenfalls hinreichend, denn für ein quadratisches Paar (σ, f) auf A muss σ symplektisch und somit die Standardinvolution ein. Unter der obigen Bedingung lässt sich Z in A einbetten und die Standardinvolution dehnt den nichttrivialen Automorphismus von Z aus (vgl. [Vil01, Proposition 2.1.2]). Jedoch muss für eine Kompositionsalgebra (C, n) von Dimension 4 das Zentrum trivial sein.

3.6 Beispiele von Kompositionen

1. Seien $(Q_1, \gamma_1), (Q_2, \gamma_2)$ Quaternionen über F mit Standardinvolutionsen. Es existiert ein kanonisches quadratisches Paar (A, σ, f) mit $A = Q \otimes Q_2$, $\sigma = \gamma_1 \otimes \gamma_2$ und die Cliffordalgebra ist isomorph zu $(Q_1, \gamma_1) \times (Q_2, \gamma_2)$, siehe [KMRT98, Example (8.19)]. Projektion auf den ersten Faktor und anschließende Tensorierung mit (Q_2, γ_2) liefert einen Homomorphismus: $(C(A, \sigma, f), \underline{\sigma}) \rightarrow (A, \sigma)$, also ein Kompositionspaar von Grad 4. Sei nun umgekehrt (A, σ, f) ein beliebiges quadratisches Paar von Grad 4 mit trivialer Diskriminante. Dann ist $C(A, \sigma, f) = Q_1 \times Q_2$ für zwei Quaternionen-Algebren Q_1, Q_2 . Wegen $[Q_1][Q_2][A] = 1$ in $\text{Br } F$ folgt $A \simeq Q_1 \otimes Q_2$. Falls die Involution σ eine (und damit beide) der Algebren Q_1, Q_2 in sich abbildet, so ist $(A, \sigma) \simeq (Q_1, \gamma_1) \otimes (Q_2, \gamma_2)$.

2. Für quadratische Paare von Grad 8 über Quaternionen lassen sich ebenfalls Kompositionspaare konstruieren. Man kann sich dabei A beliebig vorgeben und findet ein quadratisches Paar auf A , welches ein Kompositionspaar ist. Die Konstruktion ergibt sich aus einem Spezialfall aus [Vil01, Theorem 4.2.3].
3. Sei D' eine Divisions-Azumaya-Algebra von Grad 3 mit einer unitären Involution τ . Sei K das Zentrum von D' , F der Körper der zentral Invarianten und (A, σ, f) ein quadratisches Paar von Grad 2 über F mit $C(A, \sigma, f) = K$. Dann ist die Inklusion $C((A, \sigma, f), \underline{\sigma}) \subset (D', \tau)$ eine minimale Komposition von (A, σ, f) mit (D', τ) . Es gibt also auch Typen von unitären Kompositionen, für welche der minimale Grad (im Gegensatz zu den Fällen, die R. Züger behandelt) keine Zweierpotenz und sogar ungerade ist. Allgemeiner: Seien F, K und D' wie oben und (A, σ, f) ein quadratisches Paar mit $\deg A = 4k+2$ und $Z(C(A, \sigma, f)) = K$. Dann haben minimale Kompositionen vom Typ $(D' \otimes C(A, \sigma, f), 0)$ einen Grad mit Primfaktor 3.
4. Sei (A, σ, f) ein quadratisches Paar über einer Quaternionen Divisionsalgebra Q über F , d.h. $A = \text{End}_Q(V)$ für ein Q -(Rechts-)Vektorraum V . Sei $K \subset Q$ ein maximaler Körper in Q und $Q = [K, \mu]$, $\mu \in F^\times$ (d.h. $Q = K \oplus \ell K$ mit $\ell x \ell^{-1} = \bar{x}$ für $x \in K$ und $\ell^2 = \mu$). Dann ist $(A, \sigma, f) \otimes K$ ein quadratisches Paar über $A \otimes K \simeq \text{End}_K(V^0)$, wobei V^0 den Q -Vektorraum V aufgefasst als K -Vektorraum (durch Restriktion der Skalare) bezeichnet. Identifizieren wir $A \otimes K$ mit $\text{End}_K(V^0)$, so ist wegen Theorem (3.1.8) $(A, \sigma, f) \otimes K = (\text{End}_K(V_0), \sigma_q, f_q)$ für eine bis auf einen Faktor in K^\times eindeutig bestimmte reguläre quadratische Form q auf V^0 . Mit Lemma 3.2.2 erhalten wir

$$(C(A, \sigma, f) \otimes K, \underline{\sigma} \otimes \text{id}_K) \simeq (C_0(V^0, q), \tau_0).$$

Eine Komposition $\alpha: (C(A, \sigma, f), \underline{\sigma}) \longrightarrow (B, \tau)$ induziert deshalb eine Komposition

$$(C_0(V^0, q), \tau_0) \longrightarrow (B \otimes K, \tau \otimes \text{id}_K),$$

d.h. eine klassische Komposition des quadratischen Raumes (V^0, q) mit einer ε -hermiteschen Form (auf einem \tilde{D} -Modul, $[\tilde{D}]_c = [B \otimes K]_c$). Es stellt sich die Frage, wann und wie man aus einer (minimalen) Komposition eines quadratischen Raumes (V, q) mit einer ε -hermiteschen Form eine (minimale) Komposition eines quadratischen Paares über Quaternionen erhält. Sei (V, q) ein quadratischer Raum über einer

quadratischen Körpererweiterung K von F . Laut [Vil01] existiert ein quadratisches Paar (A, σ, f) über $Q = [K, \mu]$ für ein $\mu \in F^\times$ mit $(A, \sigma, f) \otimes K = (\text{End}_K V, \sigma_q, f_q)$ genau dann, wenn eine Abbildung $T: V \rightarrow V$ mit den folgenden Eigenschaften existiert:

- T ist additiv.
- $T^2 = \mu$.
- $T(v\lambda) = T(v)\bar{\lambda}$ für alle $v \in V, \lambda \in K$.
- $R(Tv) = -\mu\overline{R(v)}$ für alle $v \in V$.

Seien nun diese Bedingungen erfüllt und (A, σ, f) ein entsprechendes quadratisches Paar über $Q = [K, \mu]$. Wir betrachten Kompositionen der Form $(C_0(V, q), \tau_0) \rightarrow (B \otimes K, \tau \otimes \text{id}_K)$, oder äquivalent $\tilde{\alpha}: (C(A, \sigma, f) \otimes K, \underline{\sigma} \otimes \text{id}_K) \rightarrow (B \otimes K, \tau \otimes \text{id}_K)$. Falls $\tilde{\alpha}$ von der Form $\alpha \otimes \text{id}_K$ ist, so liefert α eine Komposition von (A, σ, f) mit (B, τ) . Dies muss jedoch nicht der Fall sein. Jedoch können wir K in $M_2(F)$ einbetten, die Identität auf K zu einer orthogonalen Involution ρ auf $M_2(F)$ erweitern und erhalten eine Komposition durch $(C(A, \sigma, f), \underline{\sigma}) \hookrightarrow (C(A, \sigma, f) \otimes K, \underline{\sigma} \otimes \text{id}_K) \rightarrow (B \otimes K, \tau \otimes \text{id}_K) \hookrightarrow (B \otimes M_2(F), \tau \otimes \rho)$. Man erhält also Zuordnungen von Kompositionen $\alpha: (C(A, \sigma, f), \underline{\sigma}) \rightarrow (B, \tau)$ mit $\text{Typ } \alpha = ([B]_c, t)$ und Kompositionen $\tilde{\alpha}: (C_0(V, q), \tau_0) \rightarrow (B \otimes K, \tau \otimes \text{id}_K)$ mit $\text{Typ } \tilde{\alpha} = ([B \otimes K]_c, t)$:

$$\alpha \rightsquigarrow \tilde{\alpha}: (C_0(V, q), \tau_0) \rightarrow (B \otimes K, \tau \otimes \text{id}_K) \quad (3.1)$$

$$\tilde{\alpha} \rightsquigarrow \alpha: (C(A, \sigma, f), \underline{\sigma}) \rightarrow (M_2(B), \tau \otimes \rho) \quad (3.2)$$

Beide Zuordnungen ordnen nur bedingt minimalen Kompositionen auch minimale Kompositionen zu. Bei Anwendung von $\alpha \rightsquigarrow \tilde{\alpha} \rightsquigarrow \alpha'$ oder $\tilde{\alpha} \rightsquigarrow \alpha \rightsquigarrow \tilde{\alpha}'$ geht ein Faktor 2 verloren. Betrachten wir dies an einem Beispiel: Sei $(A = Q_1 \otimes Q_2, \sigma = \gamma_1 \otimes \gamma_2, f)$ ein quadratisches Paar wie in Beispiel 1. Wir setzen $Q_1 = M_2(F)$ und nehmen an, dass Q_2 eine Divisionsalgebra ist. Das quadratische Paar (A, σ, f) besitzt dann eine minimale Komposition $\alpha: (C(A, \sigma, f), \underline{\sigma}) \rightarrow (Q_2, \gamma_2)$ vom Typ $(Q_2, -1)$. Wegen $\deg A \otimes K = 4$, $\deg Q \otimes K = 2$ ist dann auch die zugeordnete (klassische) Komposition $\tilde{\alpha}$ eine minimale Komposition. In diesem Falle geht also der Faktor 2 bei der Zuordnung $\tilde{\alpha} \rightsquigarrow \alpha'$ verloren. Sei nun $Q' = [K, \lambda]$ eine weitere Quaternionenalgebra mit einer orthogonalen Involution ρ . Wir setzen $Q' \not\cong Q_i$, $i = 1, 2$ voraus. Dann ist $\alpha: (C(A, \sigma, f), \underline{\sigma}) \rightarrow (Q_1 \otimes Q', \gamma_1 \otimes \rho)$ eine Komposition vom Typ $(Q', -1)$ und wegen Korollar 3.4.8 minimal. Die zugeordnete Komposition $\tilde{\alpha}$ von $(A, \sigma, f) \otimes K$ und $\text{Typ } (Q' \otimes K, -1) = (K, -1)$ ist hingegen

nicht optimal, denn es existiert eine Komposition $(C(A, \sigma, f) \otimes K, \underline{\sigma} \otimes \text{id}_K) \rightarrow (M_2(F) \otimes K, \gamma_1 \otimes \text{id}_K)$ mit $\deg M_2(F) \otimes K = 2 < 4$. Also geht in diesem Fall der Faktor 2 bei der Zuordnung $\alpha \rightsquigarrow \tilde{\alpha}$ verloren. Allgemeiner lässt sich aus Theorem 3.4.5 ablesen, bei welcher Zuordnung für gegebenen Kompositionstyp der Faktor 2 verloren geht.

Literaturverzeichnis

- [Eck43] Beno Eckmann. Gruppentheoretischer Beweis des Satzes von Hurwitz-Radon über die Komposition quadratischer Formen. *Comment. Math. Helv.*, 15:358–366, 1943.
- [Eld02] Alberto Elduque. Composition of Quadratic forms and the Hurwitz-Radon function in characteristic two. *Linear Algebra and its Applications*, 348:87–103, 2002.
- [Hur98] Adolf Hurwitz. Über die Komposition der quadratischen Formen von beliebig vielen Variablen. *Nachrichten Ges. Wiss. Göttingen, Math.-Phys. Klasse*, pages 309–316, 1898.
- [Jun80] J. Junker. Das Hurwitz Problem für quadratische Formen über Körpern der Charakteristik 2. Master's thesis, Saarbrücken, 1980.
- [KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The Book of Involutions*, volume 44 of *Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a préface by J. Tits.
- [Knu70] Max-Albert Knus. Algèbres d'Azumaya et modules projectifs. *Comment. Math. Helv.*, 45:372–383, 1970.
- [Knu88] Max-Albert Knus. Quadratic Forms, Clifford Algebras and Spinors. IMECC-UNICAMP, 1988.
- [Knu91] Max-Albert Knus. *Quadratic and Hermitian Forms over Rings*, volume 294 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1991. With a foreword by I. Bertuccioni.
- [Lam73] Tsit-Yuen Lam. *The Algebraic Theory of Quadratic Forms*. Mathematics Lecture Notes Series. W. A. Benjamin, Inc., Reading, Mass., 1973.

- [Rad22] Johann Karl August Radon. Lineare Scharen orthogonaler Matrizen. *Abh. Math. Sem. Univ. Hamburg*, 1:1–14, 1922.
- [Sha00] Daniel B. Shapiro. *Composition of Quadratic Forms*, volume 33 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter, 2000.
- [Vil01] Oliver Villa. *On Quadratic Quaternion Forms and Triality*. PhD thesis, ETH Zurich, 2001.
- [Züg95] Remo Züger. *Kompositionen von quadratischen Formen mit quadratischen, bilinearen oder hermiteschen Formen*. PhD thesis, Universität Bern, 1995.