MASTERARBEIT

Titel der Masterarbeit

„Clifford-Algebren zu quadratischen Moduln über Ringen“

Verfasserin

Mag.art. Karen Klein, BSc

angestrebter akademischer Titel

Master of Science (MSc)

Wien, 2015

Studienkennzahl lt. Studienblatt:	A 066 821
Studienrichtung lt. Studienblatt:	Masterstudium Mathematik
Betreuer:	Univ.-Prof. Dr. Joachim Schwermer

CLIFFORD-ALGEBREN ZU QUADRATISCHEN MODULN ÜBER RINGEN

Inhaltsverzeichnis

Einleitung	3
Terminologie	7
1. Grundlagen zu Clifford-Algebren	9
1.1. Konstruktion und Eindeutigkeit	9
1.2. Erzeugende	12
1.3. Involutionen von C(E,q)	13
1.4. Graduierung	16
1.5. Das graduierte Tensorprodukt	18
1.6. Clifford-Algebren zu freien quadratischen Moduln	20
1.7. Erweiterung der Skalare	22
1.8. Einbettungen in C(E,q)	25
1.9. Äußere Algebren	27
2. Die Struktur von Clifford-Algebren	30
2.1. Standard-Involutionen	30
2.2. Freie Quaternionen-Algebren	33
2.3. Arf-Algebren	39
2.4. Konjugation	41
2.5. Spezielle Elemente	45
2.6. Spezielle Elemente und die Struktur von Clifford-Algebren	50
2.7. Skalierte quadratische Formen und das Tensorprodukt von Clifford-Algebren	53
2.8. Die Struktur von C(E,q) und C_0(E,q)	55
2.9. Verallgemeinerung für den Fall ungeraden Ranges	57
3. Quadratische Moduln von Rang 2	59
3.1. Standardinvolutionen auf projektiven Algebren von Rang 2	59
3.2. Formen von Typ A	61
3.3. Verschränkte Produkte	64
3.4. Similaritäten, Radikal und Kern	65
3.5. Kompositionsabbildungen	67
3.6. Existenz und Eindeutigkeit der Komposition	70
3.7. Die Gruppe G(A)	72
ANHANG	74
Quadratische Moduln über lokalen Ringen	74
Separabilität	75
Literatur	76
Zusammenfassung	77
Abstract	78
Curriculum Vitae	79

Einleitung

Die Entwicklung der Theorie quadratischer Formen wurde entscheidend von Carl Friedrich Gauss beeinflusst, der dieses Thema in seinen von Formeln und expliziten Berechnungen geprägten *Disquisitiones Arithmeticae*, die er 1801 veröffentlichte, behandelte. Zunächst behandelt Gauss klassische Fragestellungen, wie etwa welche Zahlen sich durch eine gegebene quadratische Form mit ganzzahligen Koeffizienten darstellen lassen. In Artikel 234 seiner Abhandlung wendet er sich jedoch einem bis dahin noch völlig neuen Problem zu – nämlich der Komposition quadratischer Formen – und untersucht quadratische Formen, die sich durch gewisse Variablentransformationen als Produkt zweier Formen schreiben lassen. An diesem Punkt knüpfte Adolf Hurwitz im Jahr 1898 an. In einem privaten Notizbuch notierte er seine Gedanken zu Gauss Resultaten über die Komposition quadratischer Formen. Im Gegensatz zu Gauss verließ Hurwitz sich weniger auf explizite Berechnungen, sondern nutzte seine Erkenntnisse aus der Theorie linearer Transformationen. Sowohl Gauss als auch Hurwitz beschränkten sich bei ihren Untersuchungen auf quadratische Formen vom Grad 2 mit ganzzahligen Koeffizienten. Knapp hundert Jahre später betrachtete Martin Kneser in [7] einen völlig neuen Ansatz zu diesem Thema: Indem er einen gegebenen quadratischen Modul (E, q) als Modul über der Teilalgebra $C_0(E, q)$ der zugehörigen Clifford-Algebra auffasst, gelingt es ihm auf elegante Weise, eine allgemeine Theorie für die Komposition binärer quadratischer Moduln (also projektiver Moduln von konstantem Rang 2) über beliebigen kommutativen Ringen R (mit Eins) aufzubauen. Einen sehr guten Überblick über diese historischen Entwicklungen gibt [2].
Ziel meiner Arbeit ist es nun, Knesers algebraischen Zugang zu verstehen und die zugrundeliegenden Resultate, die sich auf quadratische Moduln über Ringen und ihre zugehörigen Clifford-Algebren beziehen, auszuarbeiten. Ich werde daher zunächst die Theorie der Clifford-Algebren zu endlich erzeugten, projektiven quadratischen Moduln erläutern. Darauf aufbauend werde ich die Struktur dieser Algebren untersuchen, wobei ich mich vor allem an Alexander J. Hahns Ausführungen in [4] zu diesem Thema orientieren werde. Zuletzt werde ich speziell den Fall projektiver quadratischer Moduln von konstantem Rang 2 behandeln, um zum Abschluss auf Knesers Ergebnisse über die Komposition quadratischer Formen einzugehen.

Im ersten Kapitel werde ich zu Beginn die Existenz und Eindeutigkeit von Clifford-Algebren zu beliebigen quadratischen Moduln (E, q) über kommutativen Ringen R beweisen und ein Erzeugendensystem für diese angeben. Mithilfe der einer Clifford-Algebra eigenen universellen Eigenschaft lassen sich gewisse Involutionen auf der Clifford-Algebra $C(E, q)$ konstruieren, die im folgenden sehr nützlich sein werden. Weiters werde ich eine $\mathbb{Z}/2\mathbb{Z}$-Graduierung auf $C(E, q)$ definieren, bezeichnet durch $C(E, q) = C_0(E, q) \oplus C_1(E, q)$. Um zu zeigen, dass im Fall einer orthogonalen Zerlegung $E = E_1 \perp E_2$ die Clifford-Algebra zu (E, q) durch die jeweiligen Clifford-Algebren zu $(E_1, q|_{E_1})$ und $(E_2, q|_{E_2})$ bereits eindeutig bestimmt ist, werde ich das graduierte Tensorprodukt verwenden. In einem dem Spezialfall freier quadratischer Moduln von endlichem Rang gewidmeten Abschnitt wird ersichtlich, dass das zuvor angegebene Erzeugendensystem in diesem Fall eine Basis bildet und die Clifford-Algebra (als Modul über R) dann frei und von endlichem Rang ist. Um Resultate über freie Moduln auf den projektiven Fall zu übertragen, werde ich zeigen, dass die Struktur der Clifford-Algebren zu endlich erzeugten projektiven quadratischen Moduln mit skalarer Erweiterung „verträglich“ ist. Damit lassen sich auch in diesem allgemeinen Fall sowohl der Grundring R, als auch der quadratische Modul E in die Clifford-Algebra $C(E, q)$ einbetten und auch im Fall einer orthogonalen Zerlegung $E = E_1 \perp E_2$ gibt es (für $i = 1, 2$) einen injektiven Homomorphismus von R-Algebren $C(E_i, q|_{E_i}) \hookrightarrow C(E, q)$. Zum Abschluss dieses Kapitels werde ich die äußere Algebra zu einem R-Modul betrachten und die entsprechende Theorie verwenden, um zu zeigen, dass die Clifford-Algebra $C(E, q)$ zu einem endlich erzeugten, projektiven quadratischen R-Modul und ihre Teilalgebra $C_0(E, q)$ beide endlich erzeugt und projektiv sind.

Das zweite Kapitel behandelt nun die Struktur von Clifford-Algebren. Ähnlich wie Hahn in [4] werde auch ich zunächst Eigenschaften von Standard-Involutionen auf treuen Algebren untersuchen. Der darauffolgende Abschnitt befasst sich mit dem Spezialfall von *freien Quaternionen-Algebren*, also Clifford-Algebren zu freien, nichtsingulären quadratischen Moduln von Rang 2: Ich werde zeigen, dass für den Zentralisator von $C_0(E, q)$ in $C(E, q)$ und die Zentren von $C(E, q)$ und $C_0(E, q)$ die folgenden Identitäten gelten:

$$Z_{C(E,q)}C_0(E, q) = Z(C_0(E, q)) = C_0(E, q) \quad \textit{und} \quad Z(C(E, q)) = R.$$

Zudem werde ich beweisen, dass die Algebra $C(E, q)$ in diesem Fall separabel ist. Für entsprechende Verallgemeinerungen auf den Fall beliebiger endlich erzeugter, projektiver, nichtsingulärer quadratischer Moduln ist jedoch einiges an Theorie aufzubauen. Von besonderer Bedeutung ist hierbei die Analyse des Zentralisators von $C_0(E, q)$ in $C(E, q)$ – der sogenannten *Arf-Algebra* $A(E, q)$. Dazu werde ich eine Konjugation auf $A(E, q)$ definieren und Eigenschaften gewisser *spezieller Elemente* (siehe [4]) in der Arf-Algebra untersuchen. Existieren solche Elemente in $A(E, q)$, so lassen sich die Zentren der Clifford-Algebra $C(E, q)$ und deren Teilalgebra $C_0(E, q)$ bestimmen. Mithilfe skalierter quadratischer Formen kann ein Zusammenhang zwischen dem graduierten Tensorprodukt von Clifford-Algebren und dem üblichen Tensorprodukt hergestellt werden. Nimmt die Rangfunktion eines endlich erzeugten, projektiven, nichtsingulären quadratischen R-Moduls nur gerade Werte an, so werde ich zeigen, dass in diesem Fall die Clifford-Algebra $C(E, q)$ zentral und separabel ist. Im Fall ungeraden Ranges werde ich ein analoges Ergebnis für die Teilalgebra $C_0(E, q)$ beweisen. Zum Abschluss dieses Kapitels werde ich noch auf gewisse weiterführende Resultate aus [4] sowie die in [9] ausgeführte Verallgemeinerung für den Fall ungeraden Ranges auf sogenannte *semireguläre* (und nicht notwendig nichtsinguläre) quadratische Moduln hinweisen.

Im dritten und letzten Kapitel meiner Arbeit werde ich gesondert projektive quadratische Moduln von konstantem Rang 2 betrachten. Ich werde $C_0(E, q)$ mit einer eindeutigen Standard-Involution versehen und zeigen, dass der quadratische Modul E in diesem Fall *von Typ* $C_0(E, q)$ ist: E kann also als projektiver $C_0(E, q)$-Modul von Rang 1 aufgefasst werden, sodass für alle $y \in C_0(E, q),\ x \in E$ die Gleichung

$$q(yx) = n(y)q(x)$$

erfüllt ist, wobei n die durch die eindeutig bestimmte Standardinvolution auf $C_0(E, q)$ festgelegte Norm sei. Im Zusammenhang zum vorangegangenen Kapitel möchte ich hier – als Verallgemeinerung der freien Quaternionen-Algebren – auch verschränkten Produkten projektiver quadratischer R-Moduln von Rang 2 einen Abschnitt widmen.

Weiters werde ich Similaritäten von quadratischen R-Moduln untersuchen sowie Radikal und Kern eines quadratischen Moduls definieren. Der darauffolgende Abschnitt behandelt ein grundlegendes Resultat über die Komposition von primitiven, projektiven quadratischen Moduln von konstantem Rang 2, welches einen Zusammenhang zwischen Kompositionsabbildungen und Homomorphismen von R-Algebren zeigt: Es besagt, dass es zu einer beliebigen Kompositionsabbildung $\nu : E_1 \times E_2 \to E$, wobei E_1, E_2, E primitive, projektive quadratische R-Moduln von konstantem Rang 2 seien, eindeutig bestimmte Homomorphismen $\eta_i : C_0(E_i, q_i) \to C_0(E, q)$ $(i = 1, 2)$ von R-Algebren gibt, sodass für alle $y_i \in C_0(E_i, q_i)$, $x_i \in E_i$ $(i = 1, 2)$ gilt:

$$\nu(y_1 x_1, y_2 x_2) = \eta_1(y_1)\eta_2(y_2)\nu(x_1, x_2).$$

Weiters werde ich die Existenz und Eindeutigkeit der Komposition beweisen. Zuletzt werde ich zeigen, dass die Isomorphieklassen primitiver, projektiver quadratischer Moduln von Rang 2, die von vorgegebenem Typ A sind, bezüglich entsprechender Komposition eine abelsche Gruppe bilden.

Terminologie

Die in dieser Arbeit betrachteten Ringe R seien stets kommutativ und besitzen ein Einselement 1. Die multplikative Gruppe der Einheiten in R sei bezeichnet mit R^*. Sämtliche Moduln seien unitäre Links-Moduln, Algebren seien assoziative Links-Algebren mit Eins.

Ein R-Modul heißt *treu*, falls $r = 0$ das einzige Element in R ist, sodass $rx = 0$ für alle $x \in E$ gilt. Der *Annihilator* von $x \in E$ ist definiert durch $Ann_R(x) := \{r \in R \mid rx = 0\}$. Es ist also E genau dann treu, wenn $Ann_R(E) := \bigcap_{x \in E} Ann_R(x) = \{0\}$ gilt. Ist A eine R-Algebra, so bezeichnet man A als treu, falls A als Modul über R treu ist; dies ist äquivalent dazu, dass die durch $i : r \mapsto r1_A$ definierte Abbildung von R ins Zentrum $Zen(A)$ von A injektiv ist. Falls i auch surjektiv ist, nennt man A eine *zentrale* R-Algebra.

Ist $q : E \to R$ eine quadratische Form auf einem R-Modul E, so sei b die zugehörige symmetrische Bilinearfom, welche durch

$$b(x, y) = q(x + y) - q(x) - q(y)$$

gegeben ist (für x, $y \in E$). Sind $E_1, E_2, \ldots, E_n$ Untermoduln von E, so bezeichnet man E als die *orthogonale Summe* von $E_1, E_2, \ldots, E_n$, falls E die direkte Summe der E_i ($i = 1, 2, \ldots, n$) ist und die Untermoduln E_i bezüglich b paarweise orthogonal sind; wir schreiben dann $E = E_1 \perp E_2 \perp \ldots \perp E_n$.

Bezeichnet $Hom_R(E, R)$ die Menge der R-Modul-Homomorphismen, so bildet diese bezüglich komponentenweiser Addition eine abelsche Gruppe. Durch die Zuordnung $x \mapsto b(x, .)$ erhalten wir einen R-Modul-Homomorphismus $b_E : E \to Hom_R(E, R)$. Die Bilinearform b heißt *nichtsingulär*, falls b_E ein Isomorphismus ist. Wir nennen einen quadratischen R-Modul (E, q) nichtsingulär, falls die zu q assoziierte Bilinearform b nichtsingulär ist. Ist E frei von endlichem Rang, so ist die *Gram-Matrix* von b bezüglich der Basis $\{e_1, e_2, \ldots, e_n\}$ definiert durch $B := (b(e_i, e_j)_{i,j=1}^n)$. Ein freier quadratischer R-Modul (E, q) ist genau dann nichtsingulär, wenn die Determinante der Gram-Matrix invertierber ist.

Ein quadratischer R-Modul heißt *primitiv*, falls der von $q(E)$ erzeugte R-Modul $Rq(E) =< q(x) \mid x \in E >_R$ mit R übereinstimmt.

1. Grundlagen zu Clifford-Algebren

1.1. **Konstruktion und Eindeutigkeit.**

Sei (E, q) ein quadratischer Modul über einem kommutativen Ring R mit Eins.

Definition 1.1. *Eine* Clifford-Algebra *zu (E, q) ist eine R-Algebra C gemeinsam mit einem R-Modul-Homomorphismus $\iota : E \to C$ mit*

$$\iota(x)^2 = q(x) \cdot 1_C$$

für alle $x \in E$ derart, dass die folgende universelle Eigenschaft erfüllt ist: Zu jedem R-Modul-Homomorphismus $\alpha : E \to A$ in eine R-Algebra A mit $\alpha(x)^2 = q(x) \cdot 1_A$ für alle $x \in E$ existiert genau ein R-Algebren-Homomorphismus $\bar{\alpha} : C \to A$, sodass $\bar{\alpha} \circ \iota = \alpha$ gilt.

Die universelle Eigenschaft der Clifford-Algebra $C(E, q)$ besagt also, dass es für jede R-Algebra A und jeden R-Modul-Homomorphismus $\alpha : E \to A$, der $\alpha(x)^2 = q(x) \cdot 1_A$ für alle $x \in E$ erfüllt, genau einen R-Algebren-Homomorphismus $\bar{\alpha} : C \to A$ gibt, sodass das folgende Diagramm kommutiert:

$$\begin{tikzcd} E \arrow[r, "\iota"] \arrow[dr, "\alpha"'] & C \arrow[d, dotted, "\bar{\alpha}"] \\ & A \end{tikzcd}$$

Für jeden R-Modul-Homomorphismus $\alpha : E \to A$ in eine R-Algebra A mit $\alpha(x)^2 = q(x) \cdot 1_A$ für alle $x \in E$ folgt aus der Definition der zur quadratischen Form q assoziierten symmetrischen Bilinearform b_q automatisch auch:

$$\begin{aligned} \alpha(x)\alpha(y) + \alpha(y)\alpha(x) = \alpha(x+y)^2 - \alpha(x)^2 - \alpha(y)^2 = \\ = (q(x+y) - q(x) - q(y)) \cdot 1_A = b(x, y) \cdot 1_A \end{aligned}$$

für alle $x, y \in E$.

Wir werden zeigen, dass jeder quadratische R-Modul (E, q) eine Clifford-Algebra besitzt. Diese ist bis auf Isomorphie eindeutig bestimmt:

Lemma 1.1. *Seien (C, ι) und (C', ι') zwei Clifford-Algebren zu (E, q). Dann gibt es genau einen R-Algebren-Isomorphismus $\varphi : C \to C'$ mit $\iota' = \varphi \circ \iota$, also derart, dass das folgende Diagramm kommutiert:*

$$\begin{tikzcd} E \arrow[r, "\iota"] \arrow[dr, "\iota'"'] & C \arrow[d, dotted, "\varphi"] \\ & C' \end{tikzcd} .$$

Beweis. Aus der universellen Eigenschaft von (C, ι) folgt, dass es genau einen Homomorphismus von R-Algebren $\varphi : C \to C'$ mit $\varphi \circ \iota = \iota'$ gibt. Ebenso ergibt sich aus der universellen Eigenschaft von (C', ι') die Existenz eines eindeutig bestimmten R-Algebren-Homomorphismus $\psi : C' \to C$ mit $\psi \circ \iota' = \iota$.

Es gilt daher: $\iota = \psi \circ \iota' = \psi \circ \varphi \circ \iota$. Nach Definition gibt es genau einen R-Algebren-Homomorphismus $\chi : C \to C$ mit $\chi \circ \iota = \iota$. Da die identische Abbildung Id_C diese

Identität erfüllt, folgt $\chi = \psi \circ \varphi = Id_C$. Analog folgt aus $\iota' = \varphi \circ \iota = \varphi \circ \psi \circ \iota'$, dass $\varphi \circ \psi = Id_{C'}$. φ und ψ sind also zueinander inverse Isomorphismen. $\square$

Definition 1.2. *Die* Tensorpotenzen $T^r E, r \in \mathbb{N}$, *sind induktiv definiert durch:*

$$T^0 E := R, \quad T^1 E := E, \quad T^{r+1} := T^r \otimes_R E \quad f\ddot{u}r\, r \geq 1.$$

Die Familie aller $T^r E$ wird zusammengefasst zum R-Modul

$$TE := \bigoplus_{r \geq 0} T^r E.$$

Die Elemente aus TE sind also Folgen $(z_0, z_1, z_2, \dots)$ mit $z_r \in T^r E$, sodass nur endlich viele Folgenglieder ungleich 0 sind.

Wir wollen nun eine Multiplikation auf TE definieren, die TE zu einer R-Algebra – der sogenannten *Tensoralgebra* von E – macht. Sei $\{e_i\}_{i \in S}$ ein Erzeugendensystem von E. Für $r \in \mathbb{N}, r \geq 1$ bilden alle $e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_r}$ mit $i_k \in S$ für alle $1 \leq k \leq r$ ein Erzeugendensystem von $T^r E$. Zur einfacheren Notation schreiben wir im folgenden

$$[e_{i_1}, e_{i_2}, \dots e_{i_r}] := e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_r}$$

und $1 \in T^0 E = R$ schreiben wir als $[\,]$. Offenbar erzeugen alle $[e_{i_1}, e_{i_2}, \dots e_{i_r}]$ mit beliebigem $r \geq 0$ den R-Modul TE.

Lemma 1.2. *Es gibt auf TE eine Struktur als R-Algebra, so dass*

$$[e_{i_1}, e_{i_2}, \dots e_{i_r}][e_{j_1}, e_{j_2}, \dots e_{j_s}] = [e_{i_1}, e_{i_2}, \dots e_{i_r}, e_{j_1}, e_{j_2}, \dots e_{j_s}](*)$$

für alle $r, s \in \mathbb{N}$ und alle Indizes $i_k, i_l \in S$ ($k \in \{1, \dots, r\},\ l \in \{1, \dots, s\}$) gilt. TE hat die folgende universelle Eigenschaft:
Ist $\alpha : E \to A$ ein R-Modul-Homomorphismus in eine R-Algebra A, so existiert ein eindeutig bestimmter R-Algebren-Homomorphismus $\varphi : TE \to A$ mit $\varphi(x) = \alpha(x)$ für alle $x \in E = T^1 E \subset TE$.

Beweis. Die Multiplikation auf TE sei die lineare Fortsetzung von $(*)$, also die eindeutig bestimmte bilineare Abbildung $TE \times TE \to TE$, $(z, z') \mapsto zz'$, die auf dem gegebenen Erzeugendensystem durch $(*)$ gegeben ist. Diese Verknüpfung ist assoziativ, denn für drei Elemente des Erzeugendensystems $z_1 = [e_{i_1}, e_{i_2}, \dots e_{i_r}], z_2 = [e_{j_1}, e_{j_2}, \dots e_{j_s}], z_3 = [e_{k_1}, e_{k_2}, \dots e_{k_t}]$ gilt:

$$\begin{aligned}(z_1 z_2) z_3 &= ([e_{i_1}, e_{i_2}, \dots e_{i_r}, e_{j_1}, e_{j_2}, \dots e_{j_s}])[e_{k_1}, e_{k_2}, \dots e_{k_t}] = \\ &= [e_{i_1}, e_{i_2}, \dots e_{i_r}, e_{j_1}, e_{j_2}, \dots e_{j_s}, e_{k_1}, e_{k_2}, \dots e_{k_t}] = \\ &= [e_{i_1}, e_{i_2}, \dots e_{i_r}][e_{j_1}, e_{j_2}, \dots e_{j_s}, e_{k_1}, e_{k_2}, \dots e_{k_t}] = z_1(z_2 z_3).\end{aligned}$$

Das Eins-Element ist gegeben durch $[\,]$. Damit wird TE zu einer (assoziativen) R-Algebra (mit Eins).
Ist $\alpha : E \to A$ ein R-Modul-Homomorphismus in eine R-Algebra A, so definiere $\varphi : TE \to A$ durch

$$\varphi([e_{i_1}, e_{i_2}, \dots e_{i_r}]) := \alpha(e_{i_1})\alpha(e_{i_2}) \dots \alpha(e_{i_r})$$

für $r \geq 1$ und $\varphi([\,]) := 1_A$. Für zwei Elemente $z_1, z_2 \in TE$ des Erzeugendensystems gilt dann:

$$\begin{aligned}\varphi(z_1 z_2) &= \varphi([e_{i_1}, e_{i_2}, \dots e_{i_r}, e_{j_1}, e_{j_2}, \dots e_{j_s}]) = \\ &= \alpha(e_{i_1})\alpha(e_{i_2})\alpha(e_{i_r})\alpha(e_{j_1})\alpha(e_{j_2})\alpha(e_{j_s}) = \\ &= \varphi([e_{i_1}, e_{i_2}, \dots e_{i_r}])\varphi([e_{j_1}, e_{j_2}, \dots e_{j_s}]) = \varphi(z_1)\varphi(z_2).\end{aligned}$$

φ ist also ein R-Algebren-Homomorphismus. Für alle $i \in S$ gilt: $\varphi(e_i) = \varphi([e_i]) = \alpha(e_i)$ und da $\{e_i\}_{i \in S}$ ein Erzeugendensystem von E ist, folgt, dass $\varphi(x) = \alpha(x)$

für alle $x \in E$. Da TE als R-Algebra von $E = T^1E \subset TE$ erzeugt wird, ist der R-Algebren-Homomorphismus φ dadurch eindeutig bestimmt. □

Die Tensoralgebra TE ist durch die universelle Eigenschaft bis auf Isomorphie eindeutig bestimmt:

Lemma 1.3. *Sei B eine weitere R-Algebra, die obige universelle Eigenschaft erfüllt, und seien $i : E \hookrightarrow TE$ und $j : E \hookrightarrow B$ die jeweiligen Einbettungen von E in TE bzw. B. Dann gibt es genau einen R-Algebren-Isomorphismus $\varphi : TE \to B$ mit $\varphi(i(x)) = j(x)$ für alle $x \in E$.*

Beweis. Aus der universellen Eigenschaft von TE folgt, dass es einen eindeutig bestimmten R-Algebren-Homomorphismus $\varphi : TE \to B$ mit $\varphi(i(x)) = j(x)$ für alle $x \in E$ gibt. Ebenso folgt aus der universellen Eigenschaft von B, dass es einen eindeutig bestimmten R-Algebren-Homomorphismus $\psi : B \to TE$ mit $\psi(j(x)) = i(x)$ für alle $x \in E$ gibt. Es gilt nun für $\psi \circ \varphi : TE \to TE$, dass $\psi \circ \varphi(i(x)) = \psi(j(x)) = i(x)$ für alle $x \in E$. Da auch Id_{TE} dies erfüllt, folgt aus der universellen Eigenschaft von TE, dass $\psi \circ \varphi = Id_{TE}$. Analog erhält man $\varphi \circ \psi = Id_B$. φ und ψ sind also zueinander inverse Isomorphismen. □

Nun haben wir sämtliche Vorbereitungen getroffen, um zu beliebigen quadratischen R-Moduln eine Clifford-Algebra zu konstruieren.

Satz 1.4. *Sei (E,q) ein quadratischer R-Modul und sei i die Einbettung $E \hookrightarrow TE$. Es sei $J(q)$ das zweiseitige Ideal in TE, das von allen $i(x)^2 - q(x)[\,]$ mit $x \in E$ erzeugt wird und $\pi : TE \to TE/J(q)$ der kanonische Homomorphismus. Setzt man*

$$C(E,q) := TE/J(q), \quad \iota := \pi \circ i : E \to C(E,q),$$

so ist $(C(E.q), \iota)$ eine Clifford-Algebra zu (E,q).

Beweis. Nach Konstruktion gilt:

$$\iota(x)^2 = i(x)^2 + J(q) = q(x)[\,] + J(q) \quad \textit{für alle}\, x \in E,$$

es stimmt also $\iota(x)^2$ mit der Restklasse von $q(x)[\,]$ in $C(E,q)$ überein.
Es bleibt die universelle Eigenschaft von Clifford-Algebren zu überprüfen. Sei also $\alpha : E \to A$ ein R-Modul-Homomorphismus in einen R-Modul A mit $\alpha(x)^2 = q(x)1_A$ für alle $x \in E$. Wegen der universellen Eigenschaft der Tensoralgebra TE, gibt es genau einen R-Algebren-Homomorphismus $\varphi : TE \to A$ mit $\varphi(i(x)) = \alpha(x)$ für alle $x \in E$. Es gilt:

$$\varphi(i(x)^2 - q(x)[\,]) = \alpha(x)^2 - q(x)1_A = 0 \quad \textit{für alle}\, x \in E.$$

Das Ideal $J(q)$ liegt also im Kern von φ. Sei $\bar{\varphi} : C(E,q) \to A$ der induzierte R-Algebren-Homomorphismus, der gegeben ist durch

$$\bar{\varphi} : i(x) + J(q) \mapsto \varphi(i(x)) = \alpha(x).$$

Es gilt insbesondere $\bar{\varphi}(\iota(x)) = \alpha(x)$ für alle $x \in E$, also $\bar{\varphi} \circ \iota = \alpha$. Da TE als Algebra von $i(E)$ und somit $C(E,q)$ von $\iota(E)$ erzeugt wird, ist $\bar{\varphi}$ dadurch eindeutig bestimmt. □

Beispiele:

(1) Ist $E = \{0\}$, so ist $q = 0$ die einzige quadratische Form $q : E \to R$. Nach obigem Satz ist $C(E,q) := TE/J(q) = R/\{0\} = R$ gemeinsam mit der Nullabbildung $E \to R$ eine Clifford-Algebra.

(2) Ist E ein freier R-Modul von Rang 1, q eine quadratische Form auf E und $\{e\}$ eine Basis von E, so ist die Tensoralgebra gegeben durch $TE = R[X]$, die Inklusionsabbildung $i : E \to TE$ durch $e \mapsto X$ und das Ideal $J(q)$ durch $J(q) =< i(x)^2 - q(x)[] \mid x \in E >_R =< X^2 - q(e) >_R$. Daher ist $C(E,q) = R[X]/(X^2 - q(e))$ gemeinsam mit dem durch $re \mapsto rX + (X^2 - q(e))$ gegebenen Homomorphismus $E \to C(E,q)$ von R-Moduln eine Clifford-Algebra zu (E,q). Ist $\alpha : E \to A$ ein R-Modul-Homomorphismus in eine R-Algebra A, der $\alpha(x)^2 = q(x)1_A$ für alle $x \in E$ erfüllt, so ist der eindeutige Homomorphismus $\bar{\alpha} : C(E,q) \to A$ gegeben durch $r_0 + r_1X + (X^2 - q(e)) \mapsto r_0 1_A + r_1\alpha(e)$.

1.2. **Erzeugende.**

Lemma 1.5. *Sei (E,q) ein quadratischer R-Modul und $\{e_i\}_{i\in S}$ ein Erzeugendensystem von E. Ist die Indexmenge S linear geordnet, so wird C(E,q) als R-Modul von $1_{C(E,q)} = [] + J(q)$ und allen Produkten $\iota(e_{i_1})\iota(e_{i_2})\dots\iota(e_{i_r})$ mit $r > 0$ und $i_1 < i_2 < \dots < i_r$ aufgespannt.*

Beweis. Die Clifford-Algebra $C(E,q)$ wird nach Konstruktion als R-Modul von allen Produkten $\iota(e_{i_1})\iota(e_{i_2})\dots\iota(e_{i_r})$ mit $r \geq 0$ und $i_k \in S$ für $1 \leq k \leq r$ erzeugt, wobei wir $1_{C(E,q)}$ als Produkt der Länge $r = 0$ betrachten. Wir nennen diese Produkte im Folgenden *Standardprodukte.*
Behauptung: Jedes Standardprodukt $\iota(e_{i_1})\iota(e_{i_2})\dots\iota(e_{i_r})$ ist eine Linearkombination von Produkten $\iota(e_{j_1})\iota(e_{j_2})\dots\iota(e_{j_s})$ mit $s \leq r$, $\{j_1, j_2, \dots j_s\} \subset \{i_1, i_2, \dots i_r\}$ und $j_1 < j_2 < \dots < j_s$ – sogenannten *zulässigen Standardprodukten.*
Beweis mittels Induktion über die Länge r der Produkte: Für $r = 0$ und $r = 1$ ist die Behauptung trivial. Sei nun $r > 1$ und $z := \iota(e_{i_1})\iota(e_{i_2})\dots\iota(e_{i_r})$. Aus der Induktionsannahme folgt, dass $\iota(e_{i_2})\iota(e_{i_3})\dots\iota(e_{i_r})$ eine Linearkombination von zulässigen Standardprodukten ist. Ohne Beschränkung der Allgemeinheit kann man daher annehmen, dass $i_2 < i_3 < \dots < i_r$. Gilt nun $i_1 < i_2$, so ist z selbst bereits ein zulässiges Standardprodukt. Ist $i_1 = i_2$, so folgt:

$$z = \iota(e_{i_1})^2\iota(e_{i_3})\dots\iota(e_{i_r}) = q(e_{i_1})\iota(e_{i_3})\dots\iota(e_{i_r})$$

und z ist also ein Vielfaches des zulässigen Standardproduktes $\iota(e_{i_3})\iota(e_{i_4})\dots\iota(e_{i_r})$. Ist $i_1 > i_2$, so gilt:

$$z = \iota(e_{i_1})\iota(e_{i_2})\iota(e_{i_3})\dots\iota(e_{i_r}) =$$
$$= b_q(e_{i_1}, e_{i_2})\iota(e_{i_3})\dots\iota(e_{i_r}) - \iota(e_{i_2})\iota(e_{i_1})\iota(e_{i_3})\dots\iota(e_{i_r}). \quad (*)$$

Der erste Summand ist ein Vielfaches eines zulässigen Standardproduktes. Für den zweiten Summand folgt aus der Induktionsannahme, dass $\iota(e_{i_1})\iota(e_{i_3})\dots\iota(e_{i_r})$ eine Linearkombination von Produkten $\iota(e_{j_1})\iota(e_{j_2})\dots\iota(e_{j_s})$ mit $s \leq r-1$, $\{j_1, j_2, \dots j_s\} \subset \{i_1, i_3, \dots i_r\}$ und $j_1 < j_2 < \dots < j_s$ ist. Wegen $i_1 > i_2$ und der Annahme, dass $i_2 < i_3 < \dots < i_r$ erfüllt ist, gilt: $j_k > i_2$ für alle $1 \leq k \leq s$, $k \neq 2$. Also sind die Produkte $\iota(e_{i_2})\iota(e_{j_1})\iota(e_{j_2})\dots\iota(e_{j_s})$ zulässig und somit ist auch der erste Summand von z in $(*)$ eine Linearkombination von zulässigen Standardprodukten. □

Beispiel: Sei (E,q) ein freier quadratischer R-Modul mit Basis $\{x_1, x_2\}$, sodass $q(x_1) = q(x_2) = 0$ und $b(x_1, x_2) = 1_R$. Eine solche Basis nennt man *hyperbolische Basis*, den R-Modul E bezeichnet man dann als *hyperbolische Ebene.* Es sei $(C(E,q), \iota)$

eine Clifford-Algebra zu (E, q). Für $x = r_1x_1 + r_2x_2 \in E$ gilt offenbar:

$$q(x) = q(r_1x_1 + r_2x_2) = b(r_1x_1, r_2x_2) + q(r_1x_1) + q(r_2x_2) = r_1r_2 \cdot 1_R + 0 = r_1r_2.$$

Wir betrachten nun die folgende Abbildung:

$$\alpha : E \to M_2(R), \quad x = r_1x_1 + r_2x_2 \mapsto \begin{pmatrix} 0 & r_1 \\ r_2 & 0 \end{pmatrix}.$$

α ist ein R-Modul-Homomorphismus und es gilt für alle $x = r_1x_1 + r_2x_2 \in E$:

$$\alpha(x)^2 = \begin{pmatrix} 0 & r_1 \\ r_2 & 0 \end{pmatrix}^2 = \begin{pmatrix} r_1r_2 & 0 \\ 0 & r_1r_2 \end{pmatrix} = r_1r_2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = q(x) \cdot 1_{M_2(R)}.$$

Wegen der universellen Eigenschaft der Clifford-Algebra existiert daher ein eindeutiger R-Algebren-Homomorphismus $\bar{\alpha} : C(E, q) \to M_2(R)$, sodass $\bar{\alpha} \circ \iota = \alpha$. Als R-Modul wird $C(E, q)$ nach obigem Lemma von der Menge $\{1_{C(E,q)}, \iota(x_1), \iota(x_2), \iota(x_1)\iota(x_2)\}$ aufgespannt. Für beliebiges $z = r_0 1_{C(E,q)} + r_1\iota(x_1) + r_2\iota(x_2) + r_3\iota(x_1)\iota(x_2) \in C(E, q)$ gilt:

$$\bar{\alpha}(z) = r_0 \cdot 1_{M_2(R)} + r_1\alpha(x_1) + r_2\alpha(x_2) + r_3\alpha(x_1)\alpha(x_2) =$$

$$= \begin{pmatrix} r_0 & 0 \\ 0 & r_0 \end{pmatrix} + \begin{pmatrix} 0 & r_1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ r_2 & 0 \end{pmatrix} + \begin{pmatrix} r_3 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} r_0 + r_3 & r_1 \\ r_2 & r_0 \end{pmatrix}.$$

Es ist die Menge

$$\{\bar{\alpha}(1_{C(E,q)}), \bar{\alpha}(\iota(x_1)), \bar{\alpha}(\iota(x_2)), \bar{\alpha}(\iota(x_1)\iota(x_2))\} =$$

$$= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

linear unabhängig in $M_2(R)$. Es müssen daher auch $1_{C(E,q)}, \iota(x_1), \iota(x_2), \iota(x_1)\iota(x_2)$ linear unabhängig sein und bilden somit eine Basis von $C(E, q)$ als R-Modul. Damit ist aber auch klar, dass $\bar{\alpha}$ ein Isomorphismus ist und daher $C(E, q) \tilde{=} M_2(R)$.

Bemerkung: Ist $E \neq 0$ ein freier R-Modul mit endlicher Basis $\{e_1, e_2, \dots e_n\}$, so wird $C(E, q)$ als R-Modul von

$$\left\{1_{C(E,q)},\ \iota(e_{i_1})\iota(e_{i_2}) \dots \iota(e_{i_r}) : 1 \leq r \leq n,\ 1 \leq i_1 < i_2 < \dots < i_r \leq n\right\}$$

aufgespannt. Wir werden zeigen, dass dies dann sogar eine Basis von $C(E, q)$ ist. Die Clifford-Algebra zu einem freien quadratischen R-Modul von endlichem Rang ist also wieder ein freier R-Modul und es gilt: $rg_R(C(E, q)) = 2^n$.

1.3. **Involutionen von C(E,q).**

Sei $\delta : (E, q) \to (E', q')$ ein R-Modul-Homomorphismus zwischen zwei quadratischen R-Moduln, sodass $q'(\delta(x)) = q(x)$ für alle $x \in E$ gilt und seien $(C, \iota), (C', \iota')$ Clifford-Algebren zu (E, q) bzw. (E', q'). Für den R-Modul-Homomorphismus $\iota' \circ \delta : E \to C'$ in die R-Algebra C' gilt:

$$(\iota' \circ \delta)(x)^2 = \iota'(\delta(x))^2 = q'(\delta(x))1_{C'} = q(x)1_{C'} \quad f\ddot{u}r\, alle\, x \in E.$$

Daher folgt aus der universellen Eigenschaft der Clifford-Algebra $C = C(E, q)$, dass es einen eindeutig bestimmten R-Algebren-Homomorphismus $C(\delta) : C \to C'$ mit

$C(\delta) \circ \iota = \iota' \circ \delta$ gibt. Man betrachte hierzu das folgende kommutative Diagramm:

$$\begin{tikzcd} E \arrow[r, "\iota"] \arrow[d, "\delta"'] & C \arrow[d, dotted, "C(\delta)"] \\ E' \arrow[r, "\iota'"'] & C' \end{tikzcd}$$

Sei $\delta' : (E', q') \to (E'', q'')$ ein weiterer R-Modul-Homomorphismus, der die *quadratischen Formen respektiert*, für den also $q''(\delta'(x)) = q'(x)$ für alle $x \in E'$ gilt. (C'', ι'') sei die (bis auf Isomorphie eindeutig bestimmte) Clifford-Algebra zu (E'', q''). Wie oben erhalten wir einen R-Algebren-Homomorphismus $C(\delta') : C' \to C''$ mit $C(\delta') \circ \iota' = \iota'' \circ \delta'$. Das Diagramm

$$\begin{tikzcd} E \arrow[r, "\iota"] \arrow[d, "\delta"'] & C \arrow[d, dotted, "C(\delta)"] \\ E' \arrow[r, "\iota'"] \arrow[d, "\delta'"'] & C' \arrow[d, dotted, "C(\delta')"] \\ E'' \arrow[r, "\iota''"'] & C'' \end{tikzcd}$$

kommutiert somit und es gilt also: $C(\delta') \circ C(\delta) \circ \iota = \iota'' \circ \delta' \circ \delta$. Wegen der Eindeutigkeit des R-Algebren-Homomorphismus $C(\delta' \circ \delta) : C \to C''$ mit $C(\delta' \circ \delta) \circ \iota = \iota'' \circ (\delta' \circ \delta)$ folgt: $C(\delta' \circ \delta) = C(\delta') \circ C(\delta)$. Ist δ ein R-Modul-Isomorphismus, so ist $C(\delta)$ ein R-Algebren-Isomorphismus.

Definition 1.3. *Als* Involution *auf einer R-Algebra A bezeichnen wir einen Homomorphismus oder Anti-Homomorphismus $\rho : A \to A$ von R-Algebren, der $\rho^2 = id_A$ erfüllt.*

Ist nun $(E, q) = (E', q')$ und $\delta = -id_E$, so erhalten wir nach Obigem einen eindeutigen R-Algebren-Isomorphismus σ auf $C(E, q)$ mit $\sigma \circ \iota = \iota \circ (-id_E)$, also

$$\sigma(\iota(x)) = -\iota(x) \quad \textit{für alle } x \in E \tag{1}$$

und da $C(E, q)$ als Algebra über R von $\iota(E)$ erzeugt wird, gilt daher $\sigma^2 = id_{C(E,q)}$, σ ist also eine Involution auf $C(E, q)$.

Das Beispiel aus Abschnitt 1.2 lässt sich nun folgendermaßen verallgemeinern:

Lemma 1.6. *Sei (E, q) ein endlich erzeugter, projektiver quadratischer R-Modul, für den es eine orthogonale Zerlegung $E = E_1 \perp E_2$ gibt, sodass E_1 eine hyperbolische Ebene ist. Dann gibt es einen R-Algebren-Isomorphismus $C(E, q) \tilde{=} M_2(C(E_2, q_2))$.*

Beweis. Sei $(C(E, q), \iota)$ eine Clifford-Algebra zu (E, q) und $(C(E_2, q_2), \iota_2)$ eine Clifford-Algebra zu $(E_2, q_2 = q|_{E_2})$. Weiters sei $\{x_1, x_2\}$ eine hyperbolische Basis von E_1. Wir betrachten die folgende Abbildung:

$$\alpha : E \to M_2(C(E_2, q_2)),\ x = r_1x_1 + r_2x_2 + y \mapsto \begin{pmatrix} \iota_2(y) & r_1 \cdot 1_{C(E_2,q_2)} \\ r_2 \cdot 1_{C(E_2,q_2)} & -\iota_2(y) \end{pmatrix}$$

für $r_1,\ r_2 \in R,\ y \in E_2$. Offenbar ist α ein R-Modul-Homomorphismus und wegen $b(r_1x_1 + r_2x_2, y) = 0$ gilt für alle $x = r_1x_1 + r_2x_2 + y \in E_1 \perp E_2$:

$$\alpha(x)^2 = \begin{pmatrix} \iota_2(y) & r_1 \cdot 1_{C(E_2,q_2)} \\ r_2 \cdot 1_{C(E_2,q_2)} & -\iota_2(y) \end{pmatrix}^2 =$$

$$= \begin{pmatrix} \iota_2(y)^2 + r_1 r_2 \cdot 1_{C(E_2,q_2)} & r_1\iota_2(y) - r_1\iota_2(y) \\ r_2\iota_2(y) - r_2\iota_2(y) & \iota_2(y)^2 + r_1 r_2 \cdot 1_{C(E_2,q_2)} \end{pmatrix} =$$

$$= (r_1 r_2 + \iota_2(y)^2) \cdot 1_{M_2(C(E_2,q_2))} = (q(r_1 x_1 + r_2 x_2) + q_2(y)) \cdot 1_{M_2(C(E_2,q_2))} =$$

$$= q(x) \cdot 1_{M_2(C(E_2,q_2))}.$$

Es gibt daher einen eindeutigen R-Algebren-Homomorphismus $\bar{\alpha} : C(E,q) \to M_2(C(E_2,q_2))$ mit $\bar{\alpha} \circ \iota = \alpha$.
Andererseits gibt es einen eindeutigen R-Algebren-Homomorphismus $j : C(E_2,q_2) \to C(E,q)$ mit $j \circ \iota_2 = \iota|_{E_2}$.

$$\begin{tikzcd} E_2 \arrow[r, "\iota_2"] \arrow[dr, "\iota|_{E_2}"'] & C(E_2,q_2) \arrow[d, "j"] \\ & C(E,q) \end{tikzcd}$$

Für $y \in E_2$ gilt dann:

$$\bar{\alpha} \circ j \circ \iota_2(y) = \bar{\alpha} \circ \iota(y) = \alpha(y) = \begin{pmatrix} \iota_2(y) & 0 \\ 0 & -\iota_2(y) \end{pmatrix}.$$

Ist $\sigma := C(-Id_{E_2})$ wie in (1), so gilt:

$$\bar{\alpha} \circ j \circ \iota_2(y) = \begin{pmatrix} \iota_2(y) & 0 \\ 0 & \sigma(\iota_2(y)) \end{pmatrix}.$$

Als R-Algebra wird $C(E_2,q_2)$ von allen $\iota_2(y)$ mit $y \in E_2$ erzeugt und wir erhalten daher für alle $z_2 \in C(E_2,q_2)$:

$$\bar{\alpha} \circ j(z_2) = \begin{pmatrix} z_2 & 0 \\ 0 & \sigma(z_2) \end{pmatrix}.$$

Ist $\{x_1, x_2, \ldots, x_m\}$ ein Erzeugendensystem von E, so wird $C(E,q)$ als R-Modul von $1_{C(E,q)}$ und allen Produkten $\iota(x_{i_1})\iota(x_{i_2})\ldots\iota(x_{i_k})$ mit $k > 0,\ 1 \le i_1 < i_2 < \cdots < i_k \le m$ erzeugt. Daher gilt:

$$C(E,q) = j(C(E_2,q_2)) + \iota(x_1)j(C(E_2,q_2)) +$$
$$+\iota(x_2)j(C(E_2,q_2)) + \iota(x_1)\iota(x_2)j(C(E_2,q_2)).$$

Ist nun $z \in C(E,q)$ beliebig, so lässt sich z schreiben als $z = j(z_{2,0}) + \iota(x_1)j(z_{2,1}) + \iota(x_2)j(z_{2,2}) + \iota(x_1)\iota(x_2)j(z_{2,3})$ mit $z_{2,i} \in C(E_2,q_2)$ für $i \in \{0,1,2,3\}$ und es gilt:

$$\bar{\alpha}(z) = \begin{pmatrix} z_{2,0} & 0 \\ 0 & \sigma(z_{2,0}) \end{pmatrix} + \begin{pmatrix} 0 & 1_{C(E_2,q_2)} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} z_{2,1} & 0 \\ 0 & \sigma(z_{2,1}) \end{pmatrix} +$$

$$+ \begin{pmatrix} 0 & 0 \\ 1_{C(E_2,q_2)} & 0 \end{pmatrix} \begin{pmatrix} z_{2,2} & 0 \\ 0 & \sigma(z_{2,2}) \end{pmatrix} + \begin{pmatrix} 0 & 1_{C(E_2,q_2)} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1_{C(E_2,q_2)} & 0 \end{pmatrix} \begin{pmatrix} z_{2,3} & 0 \\ 0 & \sigma(z_{2,3}) \end{pmatrix} =$$

$$= \begin{pmatrix} z_{2,0} + z_{2,3} & \sigma(z_{2,1}) \\ z_{2,2} & \sigma(z_{2,0}) \end{pmatrix}.$$

Da σ ein Isomorphismus ist, ist $\bar{\alpha}$ offensichtlich surjektiv und auch injektiv, also ein Isomorphismus $C(E,q) \to M_2(C(E_2,q_2))$. $\square$

Definition 1.4. *Sei $(C,+,\cdot)$ eine R-Algebra. Dann bezeichnet $(C^{op},+,*)$ die entgegengesetzte R-Algebra, welche als Gruppe mit $(C,+)$ übereinstimmt, deren Multiplikation $*$ jedoch durch*

$$z_1 * z_2 := z_2 \cdot z_1$$

für $z_1,\ z_2 \in C$ definiert ist.

Ist (C, ι) eine Clifford-Algebra zu einem quadratischen R-Modul (E, q), so kann man die Struktur-Abbildung $\iota : E \to C(E, q)$ auch als R-Modul-Homomorphismus $\tilde{\iota} : E \to C(E, q)^{op}$ auffassen. Es gilt dann:

$$\tilde{\iota}(x)^2 = \tilde{\iota}(x) * \tilde{\iota}(x) = q(x) \cdot 1_{C(E,q)^{op}}$$

für alle $x \in E$. Aus der universellen Eigenschaft der Clifford-Algebra $C(E, q)$ folgt daher, dass es einen eindeutigen R-Algebren-Homomorphismus $\tau : C(E, q) \to C(E, q)^{op}$ mit $\tau(\iota(x)) = \tilde{\iota}(x) = \iota(x)$ für alle $x \in E$ gibt.

$$\begin{tikzcd} E \arrow[r, "\iota"] \arrow[dr, "\tilde{\iota}"'] & C(E,q) \arrow[d, dotted, "\tau"] \\ & C(E,q)^{op} \end{tikzcd}$$

Fasst man τ als Abbildung von $C(E, q)$ in sich selbst auf, so erhält man: $\tau(z_1 z_2) = \tau(z_2)\tau(z_1)$ für alle $z_1, z_2 \in C(E, q)$. Da τ^2 ein R-Algebren-Homomorphismus mit $\tau^2(\iota(x)) = \iota(x)$ für alle $x \in E$ ist, muss $\tau^2 = Id_{C(E,q)}$ gelten und τ ist daher eine (Anti-)Involution von $C(E, q)$.

1.4. **Graduierung.**

Definition 1.5. *Sei A eine R-Algebra. Eine* $\mathbb{Z}/2\mathbb{Z}$-Graduierung *auf A ist eine Zerlegung $A = A_0 \oplus A_1$ als direkte Summe zweier R-Untermoduln, sodass $1_A \in A_0$ und $A_i \cdot A_j \subset A_{i+j}$ gilt, wobei wir $i, j \in \{0, 1\}$ als Restklassen in $\mathbb{Z}/2\mathbb{Z}$ betrachten. Gibt es eine solche Zerlegung, so nennt man die Algebra A auch* modulo 2 graduiert*. Die Elemente in A_i, $i = 0, 1$, heißen* homogen vom Grad i*. Sind $A = A_0 \oplus A_1$ und $B = B_0 \oplus B_1$ zwei $\mathbb{Z}/2\mathbb{Z}$-graduierte R-Algebren, so heißt eine Abbildung $\alpha : A \to B$ ein* Homomorphismus von graduierten R-Algebren*, falls α ein R-Algebren-Homomorphismus ist und $\alpha(A_i) \subset B_i$ für $i = 0, 1$ gilt.*

Für eine $\mathbb{Z}/2\mathbb{Z}$-graduierte R-Algebra $A = A_0 \oplus A_1$ gilt also insbesondere $A_1 \cdot A_1 \subset A_0$. Für den R-Untermodul A_0 hingegen gilt: $1_A \in A_0$ und $A_0 \cdot A_0 \subset A_0$; also ist A_0 eine Unteralgebra von A.
Sei nun I ein zweiseitiges Ideal von A. Ist $I = I_0 \oplus I_1$ mit $I_0 = I \cap A_0$ und $I_1 = I \cap A_1$, so gilt: $A/I \tilde{=} A_0/I_0 \oplus A_1/I_1$. Wir setzen $S_i := A_i/I_i$ für $i = 0, 1$ und erhalten eine Zerlegung $A/I = S_0 + S_1$ mit $S_i \cdot S_j \subset S_{i+j}$ $(i, j \; mod\, 2)$. Daher ist A/I wieder $\mathbb{Z}/2\mathbb{Z}$-graduiert.
Die Tensoralgebra TE des R-Moduls E wird durch

$$TE_0 = \bigoplus_{r \geq 0} T^{2r}E \quad und \quad TE_1 = \bigoplus_{r \geq 0} T^{2r+1}E$$

zu einer $\mathbb{Z}/2\mathbb{Z}$-graduierten Algebra: TE_0 und TE_1 sind R-Untermoduln von TE und es gilt: $TE = TE_0 \oplus TE_1$ mit $1_{TE} = [\,] \in TE_0$. Wegen $T^rE \cdot T^sE \subset T^{r+s}E$ für alle r, $s \geq 0$ folgt auch $TE_i \cdot TE_j \subset TE_{i+j}$ $(i, j \; mod\, 2)$.
Ist nun (E, q) ein quadratischer R-Modul und $C(E, q) = TE/J(q)$ die in Kapitel 1.1 konstruierte Clifford-Algebra zu E, wobei $J(q)$ das von den Elementen $x^2 - q(x)1_{TE}$ mit $x \in E$ erzeugte zweiseitige Ideal ist. Alle erzeugenden Elemente von $J(q)$ gehören zu TE_0 und es gilt: $J(q) = J(q)_0 \oplus J(q)_1$ mit $J(q)_i = J(q) \cap TE_i$ für $i = 0, 1$. Nach Obigem erhalten wir daher eine $\mathbb{Z}/2\mathbb{Z}$-Graduierung

$$C(E, q) = TE/J(q) = C_0(E, q) \oplus C_1(E, q)$$

mit $C_i(E,q) = TE_i/J(q)_i$ $(i = 0,1)$.
Ist $\{e_i\}_{i\in S}$ ein Erzeugendensystem von E, so wird $C_0(E,q)$ nach Lemma 1.5 als R-Modul von allen Produkten $\iota(e_{i_1})\iota(e_{i_2})\dots\iota(e_{i_r})$ mit $i_1 < i_2 < \cdots < i_r$ und r gerade erzeugt; $C_1(E,q)$ wird als R-Modul von allen solchen Produkten mir r ungerade erzeugt. $C_0(E,q)$ ist eine Unteralgebra von $C(E,q)$ und wird als solche von $1_{C(E,q)}$ und allen $\iota(e_i)\iota(e_j)$ mit $i < j$ erzeugt.

Beispiele:

(1) Sei (E,q) die hyperbolische Ebene und $\{x_1,\, x_2\}$ eine hyperbolische Basis von E. Wir haben bereits früher gezeigt, dass in diesem Fall $C(E,q) \tilde{=} M_2(R)$ gilt. Auf $C(E,q)$ haben wir die Graduierung $C(E,q) = C_0(E,q) \oplus C_1(E,q)$, wobei die Summanden durch

$$C_0(E,q) = \{r_0 1_{C(E,q)} + r_3\iota(x_1)\iota(x_2) \mid r_0, r_3 \in R\},$$
$$C_1(E,q) = \{r_1\iota(x_1) + r_2\iota(x_2) \mid r_1, r_2 \in R\}$$

gegeben sind. Wir wollen nun eine entsprechende Graduierung auf $M_2(R)$ finden. Dazu definieren wir

$$M_2(R)_0 := \left\{ r_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + r_3 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \;\middle|\; r_0, r_3 \in R \right\},$$
$$M_2(R)_1 := \left\{ r_1 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + r_2 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \;\middle|\; r_1, r_2 \in R \right\}.$$

Es sind $M_2(R)_0$ und $M_2(R)_1$ Untermoduln von $M_2(R)$ mit $M_2(R) = M_2(R)_0 \oplus M_2(R)_1$ und es gilt: $1_{M_2(R)} \in M_2(R)_0$ und

$$M_2(R)_0 \cdot M_2(R)_0 \subset M_2(R)_0, \quad M_2(R)_0 \cdot M_2(R)_1 \subset M_2(R)_1,$$
$$M_2(R)_1 \cdot M_2(R)_0 \subset M_2(R)_1, \; \textit{sowie} \; M_2(R)_1 \cdot M_2(R)_1 \subset M_2(R)_0.$$

Wir erhalten somit eine $\mathbb{Z}/2\mathbb{Z}$-Zerlegung auf $M_2(R)$. Nach Konstruktion gilt für den Isomorphismus $\bar{\alpha}$ aus Abschnitt 1.2:

$$\bar{\alpha}(C_i(E,q)) = M_2(R)_i$$

für $i = 0,1$. $\bar{\alpha}$ ist also ein graduierter R-Algebren-Isomorphismus.

(2) Sei nun (E,q) ein endlich erzeugter projektiver quadratischer R-Modul, für den es eine orthogonale Zerlegung $E = E_1 \perp E_2$ gibt, sodass E_1 eine hyperbolische Ebene ist. Wir definieren nun:

$$M_2(C(E_2,q_2))_0 := \left\{ \begin{pmatrix} z_0 & z_1 \\ z_2 & z_3 \end{pmatrix} \;\middle|\; z_0, z_3 \in C_0(E_2,q_2),\; z_1, z_2 \in C_1(E_2,q_2) \right\},$$
$$M_2(C(E_2,q_2))_1 := \left\{ \begin{pmatrix} z_0 & z_1 \\ z_2 & z_3 \end{pmatrix} \;\middle|\; z_0, z_3 \in C_1(E_2,q_2),\; z_1, z_2 \in C_0(E_2,q_2) \right\}.$$

Dadurch erhalten wir eine $\mathbb{Z}/2\mathbb{Z}$-Graduierung auf $M_2(C(E_2,q_2))$:
Es sind $M_2(C(E_2,q_2))_0$ und $M_2(C(E_2,q_2))_1$ Untermoduln von $M_2(C(E_2,q_2))$ und es gilt $M_2(C(E_2,q_2)) = M_2(C(E_2,q_2))_0 \oplus M_2(C(E_2,q_2))_1$, sowie $1_{M_2(C(E_2,q_2))} \in M_2(C(E_2,q_2))_0$. Sind $Z = \begin{pmatrix} z_0 & z_1 \\ z_2 & z_3 \end{pmatrix}$, $Z' = \begin{pmatrix} z_0' & z_1' \\ z_2' & z_3' \end{pmatrix} \in M_2(C(E_2,q_2))$, so sind $z_0, z_3, z_0', z_3' \in C_0(E_2,q_2)$, $z_1, z_2, z_1, z_2' \in C_1(E_2,q_2)$ und daher $z_0z_0', z_1z_2', z_2z_1', z_3z_3' \in C_0(E_2,q_2)$ und $z_0z_1', z_1z_3', z_2z_0', z_3z_2' \in C_1(E_2,q_2)$; es gilt somit

$$ZZ' = \begin{pmatrix} z_0z_0' + z_1z_2' & z_0z_1' + z_1z_3' \\ z_2z_0' + z_3z_2' & z_2z_1' + z_3z_3' \end{pmatrix} \in M_2(C(E_2,q_2))_0.$$

Wir erhalten also $M_2(C(E_2,q_2))_0 \cdot M_2(C(E_2,q_2))_0 \subset M_2(C(E_2,q_2))_0$ und analog auch die anderen Fälle. Es gilt somit:

$$M_2(C(E_2,q_2))_i \cdot M_2(C(E_2,q_2))_j \subset M_2(C(E_2,q_2))_{i+j} \quad (i,j=0,1,\ i+j \mod 2).$$

Unter dem R-Algebren-Isomorphismus $\bar{\alpha} : C(E,q) \to M_2(C(E_2,q_2))$ aus dem Beweis von Lemma 1.6 entspricht diese Zerlegung von $M_2(C(E_2,q_2))$ gerade der Zerlegung $C(E,q) = C_0(E,q) \oplus C_1(E,q)$.

Der R-Algebren-Homomorphismus $C(\delta) : C(E,q) \to C(E',q')$ zu einem die quadratischen Formen q, q' respektierenden R-Modul-Homomorphismus $\delta(E,q) \to (E',q')$ erfüllt für $i = 0,1$:

$$C(\delta)(C_i(E,q)) \subset C_i(E',q').$$

Daher sind insbesondere die Abbildungen σ und τ aus Abschnitt ein Automorphismus und ein Anti-Automorphismus von graduierten R-Algebren. Für σ gilt:

$$\sigma(z) = z \quad \forall\, z \in C_0(E,q) \ \ \mathit{und} \quad \sigma(z) = -z \quad \forall\, z \in C_1(E,q).$$

Ist $2 \cdot 1_R$ kein Nullteiler in R, also $z \neq -z$ für alle $z \in C(E,q)$ mit $z \neq 0_{C(E,q)}$, so erhalten wir:

$$C_0(E,q) = \{z \in C(E,q) : \sigma(z) = z\} \ \mathit{und}\ C_1(E,q) = \{z \in C(E,q) : \sigma(z) = -z\}.$$

1.5. **Das graduierte Tensorprodukt.**

Zunächst wollen wir die Clifford-Algebra $(C(E,q),\iota)$ im Falle einer orthogonalen Zerlegung $E = E_1 \perp E_2$ untersuchen und zeigen, dass die Algebren-Strukturen der (bis auf Isomorphie eindeutig bestimmten) Clifford-Algebren zu E_1 und E_2 dann bereits $C(E,q)$ bestimmen.

Satz 1.7. *Ist (E,q) ein quadratischer R-Modul, für den eine orthogonale Zerlegung* $E = E_1 \perp E_2$ *existiert, so gibt es einen Isomorphismus*

$$\phi : C(E_1, q|_{E_1}) \hat{\otimes}_R C(E_2, q|_{E_2}) \tilde{\to} C(E,q)$$

von graduierten R-Algebren.

Beweis. Seien also $(C(E_1,q|_{E_1}),\iota_1)$ und $(C(E_2,q|_{E_2}),\iota_2)$ Clifford-Algebren zu $(E_1,q|_{E_1})$ bzw. $(E_2,q|_{E_2})$. Wegen der universellen Eigenschaft der Clifford-Algebren $C(E_i,q|_{E_i})$, $i = 0,1$, existieren eindeutig bestimmte R-Algebren-Homomorphismen $g_i : C(E_i,q|_{E_i}) \to C(E,q)$, $i = 0,1$, sodass die folgenden Diagramme kommutieren.

$$\begin{tikzcd} E_1 \arrow[r, "\iota_1"] \arrow[dr, "\iota|_{E_1}"'] & C(E_1,q|_{E_1}) \arrow[d, dotted, "g_1"] \\ & C(E,q) \end{tikzcd} \qquad \begin{tikzcd} E_2 \arrow[r, "\iota_2"] \arrow[dr, "\iota|_{E_2}"'] & C(E_2,q|_{E_2}) \arrow[d, dotted, "g_2"] \\ & C(E,q) \end{tikzcd}$$

Die Abbildung $C(E_1,q|_{E_1}) \times C(E_2,q|_{E_2}) \to C(E,q),\ (z_1,z_2) \mapsto g_1(z_1)g_2(z_2)$ induziert wegen der universellen Eigenschaft des Tensorproduktes einen R-Modul-Homomorphismus

$$\phi : C(E_1,q|_{E_1}) \otimes_R C(E_2,q|_{E_2}) \to C(E,q),\ \phi(z_1 \otimes z_2) = g_1(z_1)g_2(z_2).$$

Wir wollen nun eine Algebren-Multiplikation auf dem R-Modul $C(E_1,q|_{E_1}) \otimes_R C(E_2,q|_{E_2})$ definieren, die ϕ zu einem R-Algebren-Homomorphismus macht. Die übliche Definition $(z_1 \otimes z_2)(z_1' \otimes z_2') := (z_1 z_1') \otimes (z_2 z_2')$ für $z_1,\ z_1' \in C(E_1, q|_{E_1}),\ z_2,\ z_2' \in C(E_2, q|_{E_2})$ ist dafür jedoch nicht geeignet, da im Allgemeinen

$$\phi((z_1 z_1') \otimes (z_2 z_2')) = g_1(z_1) g_1(z_1') g_2(z_2) g_2(z_2')$$
$$\neq g_1(z_1) g_2(z_2) g_1(z_1') g_2(z_2') = \phi(z_1 \otimes z_2)\phi(z_1' \otimes z_2')$$

gilt. Ist nun $z_1' = \iota_1(x_1)$, $z_2 = \iota_2(x_2)$ für $x_1 \in E_1$, $x_2 \in E_2$, so folgt wegen $b(x_1, x_2) = 0$, dass

$$g_2(z_2) g_1(z_1') = g_2(\iota_2(x_2)) g_1(\iota_1(x_1)) = \iota(x_2)\iota(x_1) = -\iota(x_1)\iota(x_2) = -g_1(z_1') g_2(z_2).$$

Für beliebige $z_1,\ z_1' \in C(E_1, q|_{E_1}),\ z_2,\ z_2' \in C(E_2, q|_{E_2})$ erhält man daher:

$$g_2(z_2) g_1(z_1') = (-1)^{ij} g_1(z_1') g_2(z_2),\ falls\ z_1' \in C_i(E_1, q|_{E_1}),\ z_2 \in C_j(E_2, q|_{E_2}).$$

Man erhält dann also:

$$\phi(z_1 \otimes z_2)\phi(z_1' \otimes z_2') = (-1)^{ij} g_1(z_1) g_1(z_1') g_2(z_2) g_2(z_2') = \phi\big((-1)^{ij}(z_1 z_1') \otimes (z_2 z_2')\big).$$

Wir definieren daher:

$$(z_1 \otimes z_2)(z_1' \otimes z_2') := (-1)^{ij}(z_1 z_1') \otimes (z_2 z_2')$$

für $z_1' \in C_i(E_1, q|_{E_1}),\ z_2 \in C_j(E_2, q|_{E_2})$ $(i, j = 0, 1)$. Da $C(E_i, q|_{E_i}) = C_0(E_i, q|_{E_i}) \oplus C_1(E_i, q|_{E_i}),\ i = 0, 1,$ ist damit die Multiplikation für beliebige Elemente $(z_1 \otimes z_2), (z_1' \otimes z_2') \in C(E_1, q|_{E_1}) \otimes_R C(E_2, q|_{E_2})$ gegeben. Wir bezeichnen die resultierende R-Algebra mit

$$C(E_1, q|_{E_1}) \hat{\otimes}_R C(E_2, q|_{E_2});$$

diese ist wieder $\mathbb{Z}/2\mathbb{Z}$-graduiert. ϕ wird dadurch zu einem Homomorphismus

$$C(E_1, q|_{E_1}) \hat{\otimes}_R C(E_2, q|_{E_2}) \to C(E, q)$$

von graduierten R-Algebren.

Wir wollen nun zeigen, dass ϕ sogar ein Isomorphismus ist. Es gilt:

$$\phi(\iota_1(x_1) \otimes 1_{C(E_2, q|_{E_2})}) = g_1(\iota_1(x_1)) = \iota|_{E_1}(x_1) = \iota(x_1)\ \ f\ddot{u}r\ x_1 \in E_1,$$
$$\phi(1_{C(E_1, q|_{E_1})} \otimes \iota_2(x_2)) = g_2(\iota_2(x_2)) = \iota|_{E_2}(x_2) = \iota(x_2)\ \ f\ddot{u}r\ x_2 \in E_2.$$

Wir definieren einen R-Modul-Homomorphismus

$$f : E = E_1 \perp E_2 \to C(E_1, q|_{E_1}) \hat{\otimes}_R C(E_2, q|_{E_2}),$$
$$f(x_1 + x_2) := \iota_1(x_1) \otimes 1_{C(E_2, q|_{E_2})} + 1_{C(E_1, q|_{E_1})} \otimes \iota_2(x_2)\ \ f\ddot{u}r\ x_1 \in E_1,\ x_2 \in E_2.$$

Schreiben wir 1 für die jeweiligen Einselemente in $C(E_1, q|_{E_1})$ und $C(E_2, q|_{E_2})$, so gilt wegen $b(x_1, x_2) = 0$ für alle $x = x_1 + x_2 \in E = E_1 \perp E_2$:

$$f(x)^2 = f(x_1 + x_2)^2 = (\iota_1(x_1) \otimes 1 + 1 \otimes \iota_2(x_2))^2 =$$
$$= (\iota_1(x_1))^2 \otimes 1 + 1 \otimes (\iota_2(x_2))^2 + \iota_1(x_1) \otimes \iota_2(x_2) - \iota_1(x_1) \otimes \iota_2(x_2) =$$
$$= (q(x_1) + q(x_2))(1 \otimes 1) = q(x_1 + x_2)(1 \otimes 1) = q(x)(1 \otimes 1).$$

Aus der universellen Eigenschaft der Clifford-Algebra folgt nun, dass es genau einen R-Modul-Homomorphismus

$$\psi : C(E, q) \to C(E_1, q|_{E_1}) \hat{\otimes}_R C(E_2, q|_{E_2})$$

mit $\psi \circ \iota = f$ gibt.

$$\begin{tikzcd} E_1 \perp E_2 = E \arrow[r, "\iota"] \arrow[dr, "f"'] & C(E, q) \arrow[d, dotted, "\psi"] \\ & C(E_1, q|_{E_1}) \hat{\otimes}_R C(E_2, q|_{E_2}) \end{tikzcd}$$

Es gilt also $\psi(\iota(x_1)) = \iota_1(x_1) \otimes 1$ und $\psi(\iota(x_2)) = 1 \otimes \iota_2(x_2)$. Es sind daher ϕ und ψ zueinander inverse Isomorphismen und die Behauptung ist somit bewiesen. □

1.6. **Clifford-Algebren zu freien quadratischen Moduln.**

Beispiel: Sei (E, q) ein freier quadratischer R-Modul mir einem erzeugenden Element e, also $E = Re$. In Beispiel (2) aus Abschnitt 1.1 haben wir gesehen, dass die bis auf Isomorphie eindeutig bestimmte Clifford-Algebra zu (E, q) gegeben ist durch $C(E, q) = R[X]/(X^2 - q(e))$ gemeinsam mit dem Homomorphismus ι, der $re \in E$ auf $rX + (X^2 - q(e)) \in C(E, q)$ abbildet. Die Clifford-Algebra ist in diesem Fall also ein freier R-Modul von Rang 2 und $\{1_{C(E,q)}, \iota(e)\}$ ist eine Basis von $C(E, q)$ (als R-Modul).

Wie bereits früher angekündigt, wollen wir nun dieses Resultat auf freie R-Moduln endlichen Ranges verallgemeinern.

Satz 1.8. *Sei (E,q) ein freier quadratischer R-Modul und* $\{e_1, e_2, \dots, e_n\}$ *eine Basis von E. Dann bilden* $1_{C(E,q)}$ *und alle Produkte* $\iota(e_{i_1})\iota(e_{i_2})\dots\iota(e_{i_r})$ *mit* $1 \le r \le n$ *und* $1 \le i_1 < i_2 < \dots < i_r \le n$ *eine Basis von C(E,q) als R-Modul. Die Clifford-Algebra C(E,q) ist daher ein freier R-Modul vom Rang* $2^{rg_R E}$.

Beweis. Produkte der obigen Form nennen wir zulässige Standardprodukte (vgl. Beweis von Lemma 1.5), $1_{C(E,q)}$ fassen wir als Produkt der Länge 0 auf. In Lemma 1.5 haben wir bereits gesehen, dass die Menge der zulässigen Standardprodukte die Clifford-Algebra $C(E, q)$ als R-Modul aufspannt. Es bleibt also die R-lineare Unabhängigkeit zu zeigen. Dazu bemerken wir zunächst: Gibt es eine Zerlegung $E = E_1 \perp E_2$ und ist die Behauptung für E_1 und E_2 erfüllt, so gilt nach Satz 1.7 die Isomorphie von R-Moduln

$$C(E, q) \tilde{=} C(E_1, q_1) \perp C(E_2, q_2)$$

und die Aussage folgt daher aus den entsprechenden Eigenschaften des Tensorproduktes freier R-Moduln:
Sei $\{e_1, e_2, \dots, e_m\}$ eine Basis von E_1 und $\{e_{m+1}, \dots, e_n\}$ eine Basis von E_2. Da die Behauptung für E_1 erfüllt ist, bilden alle Produkte $\iota_1(e_{i_1})\iota_1(e_{i_2})\dots\iota_1(e_{i_r})$ mit $0 \le r \le m$ und $1 \le i_1 < i_2 < \dots < i_r \le m$ eine Basis von $C(E_1, q|_{E_1})$, wobei $\iota_1 : E_1 \to C(E_1, q|_{E_1})$ die Strukturabbildung sei. Ebenso bilden alle zulässigen Standardprodukte (bzgl. der gegebenen Basis von E_2) in $C(E_2, q|_{E_2})$ eine Basis von $C(E_2, q|_{E_2})$. Daher bildet die Menge

$$\big\{\iota_1(e_{i_1})\dots\iota_1(e_{i_r}) \otimes \iota_2(e_{j_1})\dots\iota_2(e_{j_s}) \mid 0 \le r \le m,\ 0 \le s \le n - m,$$
$$1 \le i_1 < \dots < i_r \le m < j_1 < \dots < j_s \le n\big\}$$

eine Basis von $C(E_1, q|_{E_1}) \otimes_R C(E_2, q|_{E_2})$. Wendet man den Isomorphismus ϕ aus Satz 1.7 nun auf ein Basiselement an, so erhält man

$$\phi\big(\iota_1(e_{i_1})\dots\iota_1(e_{i_r}) \otimes \iota_2(e_{j_1})\dots\iota_2(e_{j_s})\big) = g_1\big(\iota_1(e_{i_1})\dots\iota_1(e_{i_r})\big)g_2\big(\iota_2(e_{j_1})\dots\iota_2(e_{j_s})\big) =$$
$$= \iota(e_{i_1})\dots\iota(e_{i_r})\iota(e_{j_1})\dots\iota(e_{j_s}).$$

Der Isomorphismus ϕ bildet also die gegebene Basis von $C(E_1, q|_{E_1}) \otimes_R C(E_2, q|_{E_2})$ gerade auf die Menge der zulässigen Standardprodukte bezüglich der Basis $\{e_1, e_2, \dots, e_n\}$ von $E = E_1 \perp E_2$ ab und es folgt somit die Behauptung.

Ist R ein Körper der Charakteristik $\neq 2$, so besitzt der quadratische R-Modul E eine Orthogonalbasis, also eine Zerlegung $E = E_1 \perp E_2 \perp \ldots \perp E_n$ mit $E_i = Re_i$ für $1 \leq i \leq n$. Nach obigem Beispiel gilt die Behauptung für alle E_i $(1 \leq i \leq n)$. Induktion über den Rang n von E zeigt, dass die zulässigen Standardprodukte bzgl. einer Orthogonalbasis von E eine Basis von $C(E,q)$ bilden. Ist nun $\{e_1, e_2, \ldots, e_n\}$ eine beliebige Basis von E, so wissen wir bereits, dass die Menge der zulässigen Standardprodukte bzgl. dieser Basis ein Erzeugendensystem bildet. Aus Kardinalitätsgründen muss dieses wieder eine Basis sein.

Sei nun R ein Integritätsring der Charakteristik $\neq 2$. Es sei S der Quotientenkörper von R und F der freie S-Modul mit derselben Basis $\{e_1, e_2, \ldots, e_n\}$ wie E. Wir betten nun R in S und E in F ein. Es ergibt sich folgendes Diagramm:

$$\begin{array}{ccc} E & \longrightarrow & F \\ {\scriptstyle \iota_E}\downarrow & & \downarrow{\scriptstyle \iota_F} \\ C(E,q) & \longrightarrow & C(F,\bar{q}) \end{array}$$

wobei die quadratische Form $\bar{q}$ auf F durch

$$\bar{q}(\sum_{i=1}^{n} \frac{a_i}{b_i} e_i) = (b_1 b_2 \ldots b_n)^{-2} q(\sum_{i=1}^{n} b_1 \ldots b_{i-1} b_{i+1} \ldots b_n \, a_i \, e_i)$$

für $a_i, b_i \in R, b_i \neq 0, 1 \leq i \leq n$ gegeben ist. Betrachten wir nun das durch die Produkte $\iota(e_{i_1})\iota(e_{i_2}) \ldots \iota(e_{i_r})$ mit $0 \leq r \leq n$ und $1 \leq i_1 < i_2 < \cdots < i_r \leq n$ gegebene Erzeugendensystem von $C(E,q)$. Wären diese Erzeugenden linear abhängig über R, dann wären auch die Erzeugenden von $C(F,\bar{q})$ linear abhängig über dem Körper S; dies steht im Widerspruch zu Obigem.

Wir wollen den Satz nun für einen quadratischen Modul E über einem beliebigen (kommutativen) Ring (mit Eins) beweisen. Sei $\tilde{R}$ ein Polynomring über $\mathbb{Z}$ (also insbesondere ein Integritätsring der Charakteristik 0) mit so vielen Unbestimmten, wie R Erzeugende (als Ring) hat. Sei I der Kern des Homomorphismus $\tilde{R} \to R$, der die Unbestimmten auf die Erzeugenden abbildet. Es gilt dann also: $R \tilde{=} \tilde{R}/I$; wir bezeichnen diesen Isomorphismus mit φ. Es sei $\tilde{E}$ der freie $\tilde{R}$-Modul mit der Basis $\{\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_n\}$ der Länge n; es gilt also $E \tilde{=} \tilde{E}/I\tilde{E}$, wobei der Isomorphismus gegeben ist durch $\psi : e_i \mapsto \tilde{e}_i + I\tilde{E}$. Die quadratische Form $\tilde{q}$ auf $\tilde{E}$ definieren wir derart, dass

$$\tilde{q}(\sum_{i=1}^{n} \tilde{a}_i \tilde{e}_i) + I = \varphi(q(\sum_{i=1}^{n} a_i e_i))$$

für $\tilde{a}_i \in \tilde{R}$, $a_i = \varphi^{-1}(\tilde{a}_i + I) \in R$ gilt.
Da $\tilde{R}$ ein Integritätsring der Charakteristik $\neq 0$ ist, bilden die Produkte $\tilde{\iota}(\tilde{e}_{i_1})\tilde{\iota}(\tilde{e}_{i_2}) \ldots \tilde{\iota}(\tilde{e}_{i_r})$ mit $0 \leq r \leq n$ und $1 \leq i_1 < i_2 < \cdots < i_r \leq n$ eine Basis von $(C(\tilde{E},\tilde{q}), \tilde{\iota})$ als $\tilde{R}$-Modul. Es ist daher $C(\tilde{E},\tilde{q})/IC(\tilde{E},\tilde{q})$ ein freier $\tilde{R}/I$-Modul mit Basis $\{\tilde{\iota}(\tilde{e}_{i_1})\tilde{\iota}(\tilde{e}_{i_2}) \ldots \tilde{\iota}(\tilde{e}_{i_r}) + IC(\tilde{E},\tilde{q}) : \ 0 \leq r \leq n, 1 \leq i_1 < i_2 < \cdots < i_r \leq n\}$. Wir fassen nun $C(\tilde{E},\tilde{q})/IC(\tilde{E},\tilde{q})$ via dem Isomorphismus $R \simeq \tilde{R}/I$ als R-Algebra auf.
Definieren wir den R-Modul-Homomorphismus $f : E \to C(\tilde{E},\tilde{q})/IC(\tilde{E},\tilde{q})$ durch:

$$f(\sum_{i=1}^{n} a_i e_i) = \sum_{i=1}^{n} a_i(\tilde{\iota}(\tilde{e}_i) + IC(\tilde{E},\tilde{q}))$$

für $a_i \in R$ $(i = 1, \ldots, n)$, so gilt:

$$f(\sum_{i=1}^n a_i e_i)^2 = \big(\sum_{i=1}^n a_i(\tilde{\iota}(\tilde{e}_i) + IC(\tilde{E}, \tilde{q}))\big)^2 =$$

$$= \sum_{i=1}^n a_i^2 \big(\tilde{q}(\tilde{e}_i) \cdot 1_{C(\tilde{E},\tilde{q})} + IC(\tilde{E}, \tilde{q})\big) \cdot 1 + \sum_{\substack{i,j=1 \\ i<j}}^n a_i a_j \big(\tilde{b}(\tilde{e}_i, \tilde{e}_j) \cdot 1_{C(\tilde{E},\tilde{q})} + IC(\tilde{E}, \tilde{q})\big) \cdot 1 =$$

$$= \big(\sum_{i=1}^n \tilde{a}_i^2 \tilde{q}(\tilde{e}_i) + \sum_{\substack{i,j=1 \\ i<j}}^n \tilde{a}_i \tilde{a}_j \tilde{b}(\tilde{e}_i, \tilde{e}_j)\big) \cdot (1_{C(\tilde{E},\tilde{q})} + IC(\tilde{E}, \tilde{q})) = \tilde{q}(\sum_{i=1}^n \tilde{a}_i \tilde{e}_i) \cdot 1 =$$

$$= (\tilde{q}(\sum_{i=1}^n \tilde{a}_i \tilde{e}_i) + I)(1_{C(\tilde{E},\tilde{q})} + IC(\tilde{E}, \tilde{q})) = q(\sum_{i=1}^n a_i e_i) \cdot 1,$$

wobei 1 das Einselement in $C(\tilde{E}, \tilde{q})/IC(\tilde{E}, \tilde{q})$ bezeichnet. Wegen der universellen Eigenschaft der Clifford-Algebra $(C(E, q), \iota)$ gibt es daher einen eindeutigen Homomorphismus $g : C(E, q) \to C(\tilde{E}, \tilde{q})/IC(\tilde{E}, \tilde{q})$ von R-Algebren mit $g(\iota(e_i)) = f(e_i) = \tilde{\iota}(\tilde{e}_i) + IC(\tilde{E}, \tilde{q})$ und es gilt für diesen:

$$g(\iota(e_{i_1})\iota(e_{i_2}) \ldots \iota(e_{i_r})) = \tilde{\iota}(\tilde{e}_{i_1})\tilde{\iota}(\tilde{e}_{i_2}) \ldots \tilde{\iota}(\tilde{e}_{i_r}) + IC(\tilde{E}, \tilde{q}).$$

Diese Produkte sind nach Obigem linear unabhängig über R. Daher sind auch die Produkte $\iota(e_{i_1})\iota(e_{i_2}) \ldots \iota(e_{i_r})$ linear unabhängig über R und bilden also eine Basis von $C(E, q)$ als R-Modul. $\square$

Bemerkungen:

(1) Es folgt daher für freie quadratische R-Moduln mit endlicher Basis $\{e_1, e_2, \ldots, e_n\}$, dass $1_{C(E,q)}$ und $\iota(e_i)$ $(i = 1, \ldots, n)$ linear unabhängig sind; der Ringhomomorphismus $R \to C(E, q)$, $a \mapsto a \cdot 1_{C(E,q)}$ und auch der R-Modul-Homomorphismus $\iota : E \to C(E, q)$ sind also injektiv. In Zukunft werden wir für freie Moduln oft R mit dem Unterring $R \cdot 1_{C(E,q)}$ von $C(E, q)$ und E mit dem Untermodul $\iota(E)$ identifizieren und schreiben dann a statt $a \cdot 1_{C(E,q)}$ und x statt $\iota(x)$.

(2) Wir haben im vorigen Kapitel bereits gesehen, dass alle Produkte $\iota(e_{i_1})\iota(e_{i_2}) \ldots \iota(e_{i_r})$ mit $r \geq 0$ und $1 \leq i_1 < i_2 < \cdots < i_r \leq n = rg_R E$ mit r gerade den R-Untermodul $C_0(E, q)$ von $C(E, q)$, alle solchen Produkte mit r ungerade den R-Untermodul $C_1(E, q)$ aufspannen. Aus dem Satz folgt nun, dass die beiden Erzeugendensysteme jeweils linear unabhängig sind und wir erhalten daher Basen für $C_0(E, q)$ und $C_1(E, q)$. Die beiden Untermoduln sind also wieder frei und es gilt:

$$rg_R C_0(E, q) = rg_R C_1(E, q) = 2^{rg_R E - 1}.$$

1.7. **Erweiterung der Skalare.**

Wir haben im vorigen Abschnitt gesehen, dass Clifford-Algebren zu freien quadratischen R-Moduln von endlichem Rang wieder (als R-Modul) frei und von endlichem Rang sind. Dies wird für die Analyse der Struktur sehr nützlich sein. Ich möchte mich in dieser Arbeit jedoch nicht auf den Spezialfall freier Moduln beschränken und wir werden sehen, dass sich viele Resultate, die für freie quadratische Moduln von endlichem Rang gelten, mittels Lokalisierungstheorie auch auf den Fall endlich erzeugter, projektiver Moduln übertragen lassen. Das folgende Beispiel soll dies motivieren:

Beispiel: Sei $R := \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ der Ring der ganzen Zahlen im quadratischen Zahlkörper $K := \mathbb{Q}(\sqrt{-5})$. Wir betrachten die beiden Ideale $I_1 := (3,\, 1+2\sqrt{-5})$ und $I_2 := (3,\, 1-2\sqrt{-5})$ in R und definieren eine quadratische Form $q : I_1 \to R$ auf I_1 durch $q(x) := \lambda x^2$ für $x \in I_1$ und ein fixes Element $\lambda \in R$. Wir werden sehen, dass (I_1, q) ein endlich erzeugter, projektiver quadratischer R-Modul ist, der nicht frei ist. Wegen

$$1 = 3 - (1+2\sqrt{-5}) - (1-2\sqrt{-5}) \in I_1 + I_2$$

gilt offenbar $I_1 + I_2 = R$. Andererseits gilt: $I_1 \cap I_2 = (3)$. Wir definieren nun $f : I_1 \cap I_2 \to I_1 \oplus I_2$ durch $f(x) := (x, -x)$ und $g : I_1 \oplus I_2 \to R$ durch $g(x, y) := x + y$. Dann ist die Sequenz

$$\{0\} \longrightarrow I_1 \cap I_2 \xrightarrow{f} I_1 \oplus I_2 \xrightarrow{g} R \longrightarrow \{0\}$$

eine kurze exakte Folge von R-Moduln und wir erhalten daher die Isomorphie

$$I_1 \oplus I_2 \tilde{=} R \oplus (I_1 \cap I_2) = R \oplus (3) \tilde{=} R^2.$$

Da R^2 als R-Modul frei von Rang 2 ist, sind I_1 und I_2 direkte Summanden eines freien R-Moduls und daher projektive R-Moduln. Da I_1 und I_2 aber keine Hauptideale sind, sind sie nicht frei über R.

Für die Verallgemeinerung von Resultaten über freie Moduln von endlichem Rang auf den Fall endlich erzeugter, projektiver Moduln werden wir verwenden, dass für beliebige Primideale $\mathfrak{p} \subset R$ die Lokalisierung $E_\mathfrak{p} = E \otimes_R R_\mathfrak{p}$ eines endlich erzeugten, projektiven R-Moduls E in $\mathfrak{p}$ frei und von endlichem Rang über dem lokalen Ring $R_\mathfrak{p}$ ist. Der nachfolgende Satz zeigt nun, dass die Struktur von Clifford-Algebren zu quadratischen Moduln mit Erweiterung der Skalare „verträglich“ ist.

Sei E endlich erzeugt und projektiv. Ist A eine kommutative R-Algebra, so erhalten wir in natürlicher Weise einen quadratischen A-Modul $(E \otimes_R A, q_A)$ mit $q_A : E \otimes_R A \to A$, indem wir die quadratische Form q und die assoziierte Bilinearform b durch

$$q_A(x \otimes a) = q(x)a^2 \quad \textit{und} \quad b_A(x \otimes a, x' \otimes a') = b(x, x')aa'$$

(für $x, x' \in E,\ a, a' \in A$) auf $E \otimes_R A$ fortsetzen.

Satz 1.9. *Sei (E,q) ein endlich erzeugter, projektiver quadratischer R-Modul und sei A eine kommutative R-Algebra. Dann gibt es einen A-Algebren-Isomorphismus* $\varphi : C(E \otimes_R A, q_A) \to C(E, q) \otimes_R A$.

Beweis. Seien $\iota : E \to C(E, q)$, $\iota_A : E \otimes_R A \to C(E \otimes_R A, q_A)$ die Strukturabbildungen und $\alpha := \iota \otimes id_A : E \otimes_R A \to C(E, q) \otimes_R A$, also $\alpha(x \otimes a) = \iota(x) \otimes a$ für alle $x \in E, a \in A$. Dann ist α ein A-Modul-Homomorphismus und erfüllt für alle $x_1, x_2, \ldots, x_r \in E$, $a_1, a_2, \ldots, a_r \in A$ $(r > 0)$:

$$\alpha\big(\sum_{i=1}^{r} x_i \otimes a_i\big)^2 = \big(\sum_{i=1}^{r} \iota(x_i) \otimes a_i\big)^2 =$$

$$= \sum_{i=1}^{r} \iota(x_i)^2 \otimes a_i^2 + \sum_{\substack{i,j=1 \\ i<j}}^{r} \Big((\iota(x_i)\iota(x_j)) \otimes (a_i a_j) + (\iota(x_j)\iota(x_i)) \otimes (a_i a_j)\Big) =$$

$$= \sum_{i=1}^{r} q(x_i) 1_{C(E,q)} \otimes a_1^2 + \sum_{\substack{i,j=1\\ i<j}}^{r} b(x_i, x_j) 1_{C(E,q)} \otimes (a_i a_j) =$$

$$= \sum_{i=1}^{r} q(x_i) a_i^2 (1_{C(E,q)} \otimes 1_A) + \sum_{\substack{i,j=1\\ i<j}}^{r} b(x_i, x_j) a_i a_j (1_{C(E,q)} \otimes 1_A) =$$

$$= q_A\Big(\sum_{i=1}^{r} x_i \otimes a_i\Big)(1_{C(E,q)} \otimes 1_A).$$

Daher gibt es wegen der universellen Eigenschaft der Clifford-Algebra genau einen A-Algebren-Homomorphismus $\varphi : C(E \otimes_R A, q_A) \to C(E,q) \otimes_R A$ mit $\varphi \circ \iota_A = \alpha$.

$$\begin{tikzcd} (E \otimes_R A, q_A) \arrow[r, "\iota_A"] \arrow[dr, "\alpha"'] & C(E \otimes_R A, q_A) \arrow[d, dotted, "\varphi"] \\ & C(E,q) \otimes_R A \end{tikzcd}$$

Wir fassen nun durch Einschränkung der Skalare $C(E \otimes_R A, q_A)$ als R-Algebra auf und definieren die Abbildung $\alpha' : E \to C(E \otimes_R A, q_A)$ durch $\alpha'(x) = \iota_A(x \otimes 1_A)$. Es ist α' ein R-Modul-Homomorphismus und erfüllt

$$\alpha'(x)^2 = \iota_A(x \otimes 1)^2 = q_A(x \otimes 1) = q(x) \cdot 1_{C(E \otimes_R A, q_A)}$$

für alle $x \in E$. Daher existiert genau ein R-Algebren-Homomorphismus $\psi : C(E,q) \to C(E \otimes_R A, q_A)$ mit $\psi \circ \iota = \alpha'$.

$$\begin{tikzcd} E \arrow[r, "\iota"] \arrow[dr, "\alpha'"'] & C(E,q) \arrow[d, dotted, "\psi"] \\ & C(E \otimes_R A, q_A) \end{tikzcd}$$

ψ induziert einen A-Algebren-Homomorphismus

$$\psi' : C(E,q) \otimes_R A \to C(E \otimes_R A, q_A) \; mit \; \psi'(z \otimes a) = a\psi(z)$$

für alle $z \in C(E,q)$, $a \in A$. Es gilt für alle $x \in E,\ a \in A$:

$$\psi' \circ \varphi(\iota_A(x \otimes a)) = \psi'(\alpha(x \otimes a)) = \psi'(\iota(x) \otimes a) = a\psi(\iota(a)) = a\alpha'(x) =$$

$$= a\iota_A(x \otimes 1_A) = \iota_A(x \otimes a),$$

$$\varphi \circ \psi'(\iota(x) \otimes a) = \varphi(a\psi(\iota(x)) = a\varphi(\alpha'(x)) = a\varphi(\iota_A(x \otimes 1_A)) = a\alpha(x \otimes 1_A) =$$

$$= a(\iota(x) \otimes 1_A) = \iota(x) \otimes a.$$

Da $\iota_A(E \otimes_R A)$ bzw. $\iota(E) \otimes_R A$ die Algebren $C(E \otimes_R A, q_A)$ bzw. $C(E,q) \otimes_R A$ erzeugen, sind daher ψ' und φ zueinander inverse Isomorphismen von A-Algebren. $\square$

Bemerkung: Der A-Algebren-Isomorphismus φ bildet $C_0(E \otimes_R A, q_A)$ auf $C_0(E,q) \otimes_R A$ und $C_1(E \otimes_R A, q_A)$ auf $C_1(E,q) \otimes_R A$ ab. Versieht man $C(E,q) \otimes_R A$ mit der $\mathbb{Z}/2\mathbb{Z}$-Graduierung, die $C(E,q)$ induziert, so ist φ also ein graduierter A-Algebren-Isomorphismus. Die Einschränkung $\varphi|_{C_0(E \otimes_R A, q_A)}$ ist ein A-Algebren-Isomorphismus nach $C_0(E,q) \otimes_R A$.

1.8. Einbettungen in C(E,q).

Wir werden nun Satz 1.9 verwenden, um zu zeigen, dass sowohl die Abbildung $i : R \to C(E,q)$ definiert durch $r \mapsto r1_{C(E,q)}$, als auch die Strukturabbildung $\iota : E \to C(E,q)$ injektiv sind. Für den Fall, dass E frei ist, wissen wir das bereits.

Proposition 1.10. *Sei (E,q) ein endlich erzeugter, projektiver quadratischer R-Modul. Dann ist die durch $r \mapsto r1_{C(E,q)}$ definierte Abbildung $i : R \to C(E,q)$ injektiv – also $C(E,q)$ treu.*

Beweis. Sei $\mathfrak{p} \subset R$ ein Primideal und $R_\mathfrak{p}$ die kommutative R-Algebra, die man durch Lokalisierung in $\mathfrak{p}$ erhält. Wir bezeichnen den quadratischen $R_\mathfrak{p}$-Modul $(E \otimes_R R_\mathfrak{p}, q_{R_\mathfrak{p}})$, den man durch Erweiterung der Skalare wie in Abschnitt 1.7 erhält, nun im Folgenden mit $(E_\mathfrak{p}, q_\mathfrak{p})$. Sei weiters $f : C(E,q) \to C(E,q) \otimes_R R_\mathfrak{p}$ durch $f(z) = z \otimes 1_{R_\mathfrak{p}}$ definiert und $g := \varphi^{-1} : C(E,q) \otimes_R R_\mathfrak{p} \to C(E \otimes_R R_\mathfrak{p}, q_{r_\mathfrak{p}}) = C(E_\mathfrak{p}, q_\mathfrak{p})$, wobei φ der $R_\mathfrak{p}$-Algebren-Isomorphismus aus Satz 1.9 ist. Wir betrachten das folgende Diagramm:

$$\begin{tikzcd} R \arrow[r, "i"] \arrow[d, "j"'] & C(E,q) \arrow[d, "F"] \\ R_\mathfrak{p} \arrow[r, "i'"'] & C(E_\mathfrak{p}, q_\mathfrak{p}) \end{tikzcd}$$

wobei $j : R \to R_\mathfrak{p}$ durch $r \mapsto r/1 =: r_\mathfrak{p}$ und $i' : R_\mathfrak{p} \to C(E_\mathfrak{p}, q_\mathfrak{p})$ durch $a \mapsto a1_{C(E_\mathfrak{p}, q_\mathfrak{p})}$ für alle $a = r/s \in R_\mathfrak{p}$ gegeben sei. Die Abbildung $F : C(E,q) \to C(E_\mathfrak{p}, q_\mathfrak{p})$ sei die Komposition $F = g \circ f$. Für $r \in R$ gilt:

$$i' \circ j(r) = i'(r_\mathfrak{p}) = r_\mathfrak{p} 1_{C(E_\mathfrak{p}, q_\mathfrak{p})}, \text{ sowie}$$

$$\begin{aligned} F \circ i(r) &= g \circ f(r1_{C(E,q)}) = g(r1_{C(E,q)} \otimes 1_{R_\mathfrak{p}}) = g(1_{C(E,q)} \otimes r_\mathfrak{p}) = \\ &= g(r_\mathfrak{p}(1_{C(E,q)} \otimes 1_{R_\mathfrak{p}})) = r_\mathfrak{p} g(1_{C(E,q)} \otimes 1_{R_\mathfrak{p}}) = r_\mathfrak{p} 1_{C(E_\mathfrak{p}, q_\mathfrak{p})}. \end{aligned}$$

Das obige Diagramm kommutiert also.
Da $E_\mathfrak{p}$ ein projektiver Modul über dem lokalen Ring $R_\mathfrak{p}$ ist, ist $E_\mathfrak{p}$ frei. Ist $\{e_1, e_2, \dots, e_n\} \subset E$ ein Erzeugendensystem des R-Moduls E, so wird $E_\mathfrak{p}$ als $R_\mathfrak{p}$-Modul von $\{e_1 \otimes 1_{R_\mathfrak{p}}, e_2 \otimes 1_{R_\mathfrak{p}}, \dots, e_n \otimes 1_{R_\mathfrak{p}}\}$ erzeugt. Insbesondere ist $E_\mathfrak{p}$ endlich erzeugt, also freier $R_\mathfrak{p}$-Modul von endlichem Rang. Wir wissen daher von unseren früheren Beobachtungen, dass die Abbildung $i' : R_\mathfrak{p} \to C(E_\mathfrak{p}, q_\mathfrak{p})$ injektiv ist.
Sei nun $r \in \ker i$. Da i' injektiv ist, muss $a \in \ker j$ gelten. Die obige Konstruktion gilt für jedes Primideal $\mathfrak{p} \subset R$ und es folgt daher: $r_\mathfrak{p} = 0$ für alle Primideale $\mathfrak{p} \subset R$. Es muss also $r = 0$ gelten und $i : R \to C(E,q)$ ist daher injektiv. □

Proposition 1.11. *Sei (E,q) ein endlich erzeugter, projektiver quadratischer R-Modul. Dann ist die Strukturabbildung $\iota : E \to C(E,q)$ injektiv.*

Beweis. Man überprüft leicht, dass das Diagramm

$$\begin{tikzcd} E \arrow[r, "\iota"] \arrow[d, "j'"'] & C(E,q) \arrow[d, "F"] \\ E_\mathfrak{p} \arrow[r, "\iota'"'] & C(E_\mathfrak{p}, q_\mathfrak{p}) \end{tikzcd}$$

mit $j'(x) = x \otimes 1_{R_\mathfrak{p}}$ für $x \in E$ und ι, ι' die jeweiligen Strukturabbildungen, sowie F wie im Beweis von Proposition 1.10, kommutativ ist. Da $E_\mathfrak{p}$ frei ist, wissen wir, dass ι' injektiv ist. Für $x \in \ker \iota$ muss daher auch $x \in \ker j'$ gelten. Es gibt also ein $s \in R \setminus \mathfrak{p}$, sodass $sx = 0$. Dies gilt für jedes Primideal $\mathfrak{p} \subset R$. Wir können voraussetzen, dass $E \neq 0$, da andernfalls die Aussage trivial ist. Wäre $x \neq 0$, so würde für den Annihilator gelten: $Ann_R(x) \neq R$. Also gäbe es ein Primideal $\mathfrak{p} \subset R$, sodass $Ann_R(x) \subset \mathfrak{p}$ – ein Widerspruch. Es folgt $x = 0$ und somit die Injektivität von ι. □

Wir werden im Folgenden daher auch für endlich erzeugte, projektive quadratische R-Moduln (E, q) meist R und E als Teilmengen von $C(E, q)$ auffassen und die Injektionen i und ι notationell unterdrücken.

Sei nun (E, q) ein endlich erzeugter, projektiver quadratischer R-Modul, für den es eine orthogonale Zerlegung $E = E_1 \perp E_2$ gibt. Es sind dann E_1 und E_2 wieder projektiv und wegen $E_1 \tilde{=} E/E_2$ bzw. $E_2 \tilde{=} E/E_1$ auch endlich erzeugt. Sei $(C(E_1, q_1), \iota_1)$ eine Clifford-Algebra zu $(E_1, q_1 = q|_{E_1})$. Wir zeigen nun, dass man $C(E_1, q_1)$ in $C(E, q)$ einbetten kann.

Proposition 1.12. *Sei (E, q) ein endlich erzeugter, projektiver quadratischer R-Modul mit orthogonaler Zerlegung $E = E_1 \perp E_2$. Für $i = 0, 1$ sei $g_i : C(E_i, q_i) \to C(E, q)$ der eindeutige R-Algebren-Homomorphismus, der durch die Inklusion $E_i \hookrightarrow E$ induziert wird, der also $g_i \circ \iota_i = \iota|_{E_i}$ erfüllt, wobei $\iota : E \to C(E, q)$, $\iota_i : E_i \to C(E_i, q_i)$ die jeweiligen Strukturabbildungen sind. Dann ist g_i injektiv.*

Beweis. Wir zeigen die Behauptung für $i = 1$. Wir identifizieren E_1 mit $\iota_1(E_1) \subset C(E_1, q_1)$ und E mit $\iota(E) \subset C(E, q)$. Es gilt dann: $g_1(x) = x$ für alle $x \in E_1$ und das folgende Diagramm kommutiert:

$$\begin{tikzcd} E_1 \arrow[r, "\iota_1"] \arrow[d, hook] & C(E_1, q_1) \arrow[d, dotted, "g_1"] \\ E \arrow[r, "\iota"'] & C(E, q) \end{tikzcd}$$

Seien nun zunächst E_1 und E frei. Dann sind auch die zugehörigen Clifford-Algebren frei von endlichem Rang. Sei $\{z_1, z_2, \ldots, z_m\}$ eine Basis von $C(E_1, q_1)$ und $z = \sum_{i=1}^m r_i z_i \in \ker g_1$. Für den graduierten R-Algebren-Homomorphismus $\phi : C(E_1, q_1) \hat{\otimes}_R C(E_2, q_2) \to C(E, q)$ aus Satz 1.7 gilt dann: $\phi(z \otimes 1_{C(E_2,q_2)}) = g_1(z) g_2(1) = 0$. Weil ϕ ein Isomorphismus ist, folgt daher $z \otimes 1_{C(E_2,q_2)} = 0$ und somit:

$$\sum_{i=1}^m (z_i \otimes 0) = 0 = \Big(\sum_{i=1}^m r_i z_i \Big) \otimes 1_{C(E_2,q_2)} = \sum_{i=1}^m (z_i \otimes r_i 1_{C(E_2,q_2)}).$$

Da $\{z_1, z_2, \ldots, z_m\}$ eine Basis von $C(E_1, q_1)$ als R-Modul ist, lässt sich jedes Element in $C(E_1, q_1) \otimes_R C(E_2, q_2)$ eindeutig in der Form $\sum_{i=1}^m z_i \otimes z_i'$ für gewisse $z_i' \in C(E_2, q_2)$ schreiben (siehe [5, Theorem 5.11]). Es folgt daher: $r_i 1_{C(E_2,q_2)} = 0$, also $r_i = 0$ für alle $i = 1, 2, \ldots, m$ und wir erhalten $z = 0$. Also ist g_1 in diesem Fall injektiv.

Nun zum allgemeinen Fall: Ist $\mathfrak{p} \subset R$ ein Primideal, so erhalten wir das folgende Diagramm:

$$\begin{tikzcd} E_{1,\mathfrak{p}} \arrow[r, "\iota_{1,\mathfrak{p}}"] \arrow[d, hook] & C(E_{1,\mathfrak{p}}, q_{1,\mathfrak{p}}) \arrow[r, "\varphi_1"] \arrow[d, dotted, "g_1'"'] & C(E_1, q_1) \otimes_R R_\mathfrak{p} \arrow[d, dotted, "g_1 \otimes id_{R_\mathfrak{p}}"] \\ E_\mathfrak{p} \arrow[r, "\iota_\mathfrak{p}"'] & C(E_\mathfrak{p}, q_\mathfrak{p}) \arrow[r, "\varphi"'] & C(E, q) \otimes_R R_\mathfrak{p} \end{tikzcd}$$

wobei $\iota_{1,\mathfrak{p}}$, $\iota_{\mathfrak{p}}$ die Strukturabbildungen in die jeweiligen Clifford-Algebren und φ_1, φ die jeweiligen Isomorphismen wie in Satz 1.9 seien. g_1' sei der eindeutige Homomorphismus von $R_{\mathfrak{p}}$-Moduln $C(E_{1,\mathfrak{p}}, q_{1,\mathfrak{p}}) \to C(E_{\mathfrak{p}}, q_{\mathfrak{p}})$ mit $g_1' \circ \iota_{1,\mathfrak{p}} = \iota_{\mathfrak{p}}|_{E_{1,\mathfrak{p}}}$. Wegen $\varphi_1 \circ \iota_{1,\mathfrak{p}} = \iota_1 \otimes id_{R_{\mathfrak{p}}}$ und $\varphi \circ \iota_{\mathfrak{p}} = \iota \otimes id_{R_{\mathfrak{p}}}$ sieht man leicht, dass das Diagramm kommutiert.
Da $E_{1,\mathfrak{p}}$ und $E_{\mathfrak{p}}$ freie $R_{\mathfrak{p}}$-Moduln sind, folgt die Injektivität von g_1' aus obigem Spezialfall. Es muss daher auch $g_1 \otimes id_{R_{\mathfrak{p}}}$ injektiv sein. Ist nun $z \in \ker g_1$, so folgt $z \otimes 1_{R_{\mathfrak{p}}} \in \ker(g_1 \otimes id_{R_{\mathfrak{p}}})$ und wegen der Injektivität von $g_1 \otimes id_{R_{\mathfrak{p}}}$ weiter $z \otimes 1_{R_{\mathfrak{p}}} = 0 \in C(E_1, q_1) \otimes_R R_{\mathfrak{p}}$; es gibt also ein Element $s \in R \setminus \mathfrak{p}$, sodass $sz = 0$. Da dies für alle Primideale $\mathfrak{p} \subset R$ gilt, muss schon $z = 0$ gelten und der R-Algebren-Homomorphismus $g_1 : C(E_1, q_1) \to C(E, q)$ ist somit injektiv. □

Im Fall von endlich erzeugten, projektiven quadratischen R-Moduln (E, q) mit einer orthogonalen Zerlegung $E = E_1 \perp E_2$ können wir daher $C(E_1, q|_{E_1})$ und $C(E_2, q|_{E_2})$ als Teilalgebren von $C(E, q)$ auffassen.

1.9. **Äußere Algebren.**

Definition 1.6. *Sei (E, q) ein endlich erzeugter, projektiver quadratischer R-Modul. Gilt $q(x) = 0$ für alle $x \in E$, so nennt man die Clifford-Algebra $\Lambda(E) := C(E, q)$ die* äußere Algebra *von E. Die Multiplikation in $\Lambda(E)$ notieren wir mit $\wedge$.*

Wegen $q(x) = 0$ für alle $x \in E$ folgt $b(x, y) = 0$ für alle $x, y \in E$ und es gilt daher:

$$x \wedge y = -y \wedge x$$

für alle $x, y \in E$.
Sei $\{e_1, e_2, \ldots, e_m\}$ ein Erzeugendensystem von E. Wir definieren:

$$\Lambda^0(E) := R,$$

$$\Lambda^k(E) :=< e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k} \mid i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, m\} >_R \quad (k \geq 1).$$

Ist $k > m$, so enthält jedes der $\Lambda^k(E)$ erzeugenden Produkte $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k}$ zumindest ein e_i doppelt. Wegen $e_i \wedge e_j = -e_j \wedge e_i$ können wir durch Vorzeichenwechsel zwei aufeinanderfolgende Elemente im Produkt vertauschen. Wiederholen wir diesen Schritt so oft, bis zwei gleiche Elemente direkt hintereinander stehen, so sehen wir, dass wegen $e_i \wedge e_i = q(e_i) = 0$ bereits $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k} = 0$ gelten muss. Für $k > m$ gilt also $\Lambda^k(E) = 0$.
Für $1 \leq k \leq m$ wird der Untermodul $\Lambda^k(E)$ von $\Lambda(E)$ von jenen Produkten $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k}$ mit e_{i_j} $(j = 1, 2, \ldots k)$ paarweise verschieden erzeugt.
Sei nun $\{e_1', e_2', \ldots, e_n'\}$ ein weiteres Erzeugendensystem von E . Jedes Produkt $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k}$ lässt sich dann als Linearkombination von Produkten $e_{j_1}' \wedge e_{j2}' \wedge \cdots \wedge e_{jk}'$ schreiben und umgekehrt. Die Definition von $\Lambda^k(E)$ ist daher unabhängig von der Wahl des Erzeugendensystems.
Da $1_{\Lambda(E)}$ und alle Produkte $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k}$ mit $1 \leq k \leq m$ die äußere Algebra $\Lambda(E)$ als R-Modul erzeugen, gilt offenbar $\Lambda(E) = \Lambda^0(E) + \Lambda^1(E) + \cdots + \Lambda^m(E)$.

Lemma 1.13. *Ist E ein endlich erzeugter projektiver R-Modul, $\{e_1, e_2, \ldots, e_m\}$ ein Erzeugendensystem von E, so gilt:*

$$\Lambda(E) = \Lambda^0(E) \oplus \Lambda^1(E) \oplus \cdots \oplus \Lambda^m(E).$$

Beweis. Ist R ein lokaler Ring, so ist E frei von endlichem Rang. Ist $\{e_1, e_2, \dots, e_n\}$ eine Basis von E, so ist $\{1_{\Lambda(E)}, e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_k} | 1 \leq k \leq n, 1 \leq i_1 < i_2 < \dots < i_k \leq n\}$ eine Basis von $\Lambda(E)$ als R-Modul. Es gilt also

$$\Lambda^k(E) \cap \sum_{\substack{j=0 \\ j \neq k}}^{n} \Lambda^j(E) = \{0\}$$

für alle $k = 0, 1, \dots, m$ und die Behauptung ist bewiesen.
Für den Fall eines beliebigen (kommutativen) Ringes (mit Eins) sei nun $\mathfrak{p} \subset R$ ein Primideal. Dann gilt $q_{R_\mathfrak{p}} = 0$ und daher nach Satz 1.9:

$$\Lambda(E)_\mathfrak{p} := \Lambda(E) \otimes_R R_\mathfrak{p} \tilde{=} \Lambda(E \otimes_R R_\mathfrak{p}) =: \Lambda(E_\mathfrak{p}).$$

Da E endlich erzeugt und projektiv ist und $R_\mathfrak{p}$ ein lokaler Ring ist, ist $E_\mathfrak{p}$ ein freier $R_\mathfrak{p}$-Modul von endlichem Rang n und daher auch $\Lambda(E \otimes_R R_\mathfrak{p})$ als $R_\mathfrak{p}$-Modul frei von endlichem Rang n. Es gilt daher $\Lambda(E_\mathfrak{p}) = \Lambda^0(E_\mathfrak{p}) \oplus \Lambda^1(E_\mathfrak{p}) \oplus \dots \oplus \Lambda^n(E_\mathfrak{p})$ und der $R_\mathfrak{p}$-Algebren-Isomorphismus $\varphi : \Lambda(E_\mathfrak{p}) \to \Lambda(E)_\mathfrak{p}$ lässt sich einschränken zu einem $R_\mathfrak{p}$-Modul-Isomorphismus $\varphi_j : \Lambda^j(E_\mathfrak{p}) \to \Lambda^j(E)_\mathfrak{p}$ für alle $j = 0, 1, \dots, n$.
Für ein beliebiges festes $k \in \{0, 1, \dots, m\}$ betrachten wir die Inklusion $\Lambda^k(E) \cap \sum_{\substack{j=0 \\ j \neq k}}^{n} \Lambda^j(E) \hookrightarrow \Lambda^k(E)$. Durch Lokalisierung in $\mathfrak{p}$ und Komposition mit φ_j erhalten wir eine Abbildung:

$$\Big(\Lambda^k(E) \cap \sum_{\substack{j=0 \\ j \neq k}}^{n} \Lambda^j(E)\Big)_\mathfrak{p} \to \Lambda^k(E_\mathfrak{p}).$$

Diese ist klarerweise injektiv und ihr Bild liegt in $\Lambda^k(E_\mathfrak{p}) \cap \sum_{\substack{j=0 \\ j \neq k}}^{n} \Lambda^j(E_\mathfrak{p})$. Aus Obigem folgt jedoch, dass dieser Durchschnitt $\{0\}$ ist, und es muss daher auch $\Big(\Lambda^k(E) \cap \sum_{\substack{j=0 \\ j \neq k}}^{n} \Lambda^j(E)\Big)_\mathfrak{p} = \{0\}$ gelten. Da dies für alle Primideale $\mathfrak{p} \subset R$ gilt, folgt $\Lambda^k(E) \cap \sum_{\substack{j=0 \\ j \neq k}}^{n} \Lambda^j(E) = \{0\}$ für beliebiges $k \in \{0, 1, \dots, m\}$ und die Summe ist daher direkt. □

Satz 1.14. *Sei (E, q) ein endlich erzeugter, projektiver quadratischer R-Modul. Dann sind auch die Clifford-Algebra $C(E, q)$ und ihre Teilalgebra $C_0(E, q)$ (als R-Moduln) endlich erzeugt und projektiv.*

Beweis. Dass $C(E, q)$ und $C_0(E, q)$ endlich erzeugt sind, haben wir bereits früher gesehen.
Da E endlich erzeugt und projektiv ist, gibt es einen endlich erzeugten, projektiven R-Modul E', sodass $E \oplus E'$ frei von endlichem Rang ist. Wir statten nun E' mit der quadratischen Form $q' = 0$ aus und betrachten die orthogonale Summe $E \perp E'$ mit der quadratischen Form $\bar{q}$, die definiert ist durch: $\bar{q}(x + x') = q(x) + q(x') = q(x)$ für $x \in E,\ x' \in E'$. Es gilt die R-Modul-Isomorphie

$$C(E \perp E', \bar{q}) \tilde{=} C(E, q) \otimes_R \Lambda(E').$$

Da $E \perp E'$ frei von endlichem Rang ist, gilt dies auch für $C(E \perp E', \bar{q})$. Nach vorangegangenem Lemma gilt

$$\Lambda(E') = \Lambda^0(E') \oplus \Lambda^1(E') \oplus \dots \oplus \Lambda^m(E')$$

für ein $m \geq 0$. Es ist also $R = \Lambda^0(E')$ ein direkter Summand von $\Lambda(E')$. Wir erhalten damit:

$$C(E \perp E', \bar{q}) \tilde{=} \big(C(E,q) \otimes_R R\big) \oplus \big(C(E,q) \otimes_R \Lambda^1(E')\big) \oplus \cdots \oplus \big(C(E,q) \otimes_R \Lambda^m(E')\big).$$

Daher ist $C(E,q) \tilde{=} C(E,q) \otimes_R R$ isomorph zu einem direkten Summand des freien R-Moduls $C(E \perp E', \bar{q})$, also projektiv.
Wegen $C(E,q) = C_0(E,q) \oplus C_1(E,q)$ ist die Teilalgebra $C_0(E,q)$ direkter Summand eines projektiven R-Moduls und somit selbst projektiv. $\square$

Wir betrachten nun wieder den Fall $q = 0$. Hat E konstanten Rang n, so haben wir oben bereits gesehen, dass dann $\Lambda^k(E) = 0$ für alle $k > n$ und $\Lambda(E) = \Lambda^0(E) \oplus \Lambda^1(E) \oplus \cdots \oplus \Lambda^n(E)$ gilt. Wir wollen nun die Summanden $\Lambda^1(E)$ und $\Lambda^n(E)$ genauer betrachten.

Proposition 1.15. *Sei E ein endlich erzeugter, projektiver R-Modul von konstantem Rang n. Dann gilt $\Lambda^1(E) \tilde{=} E$ und $\Lambda^n(E)$ ist ein endlich erzeugter, projektiver R-Modul von konstantem Rang 1.*

Beweis. Ist E frei und $\{e_1, e_2, \ldots, e_n\}$ eine Basis von E, so bilden $1_{\Lambda(E)}$ und alle Produkte $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k}$ mit $1 \leq k \leq n$, $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ eine Basis von $\Lambda(E)$ als R-Modul. Es gilt daher in diesem Fall:

$$\Lambda^1(E) = < e_i \mid 1 \leq i \leq n >_R \tilde{=} E \quad \textit{und} \quad \Lambda^n(E) = < e_1 \wedge e_2 \wedge \cdots \wedge e_n >_R \tilde{=} R.$$

Sei nun E ein endlich erzeugter, projektiver R-Modul von konstantem Rang n mit quadratischer Form $q = 0$. Dann ist die Strukturabbildung $\iota : E \to \Lambda(E)$ injektiv und ihr Bild ist gerade $\Lambda^1(E)$, es gilt also auch in diesem Fall $\Lambda^1(E) \tilde{=} E$. Es bleibt das zweite Resultat zu zeigen. Zunächst bemerken wir, dass $\Lambda^n(E)$ als direkter Summand von $\Lambda(E)$ projektiv ist. Sei $\{e_1, e_2, \ldots, e_n\}$ ein Erzeugendensystem von E, dann wird $\Lambda^n(E)$ von $e_1 \wedge e_2 \wedge \cdots \wedge e_n$ erzeugt, da ein beliebiges Produkt $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n}$ (mit e_{i_j} $(j = 1, \ldots, n)$ paarweise verschieden) des Erzeugendensystems von $\Lambda^n(E)$ durch Schritte der Form $e_{i_j} \wedge e_{i_{j+1}} = -e_{i_{j+1}} \wedge e_{i_j}$ (für $j = 1, 2, \ldots, n-1$) auf die Form $\pm e_1 \wedge e_2 \wedge \cdots \wedge e_n$ gebracht werden kann. Sei nun $\mathfrak{p} \subset R$ ein Primideal, so ist $E_\mathfrak{p} = E \otimes_R R_\mathfrak{p}$ frei über $R_\mathfrak{p}$ und es gilt daher nach Obigem:

$$\Lambda^n(E)_\mathfrak{p} \tilde{=} \Lambda^n(E_\mathfrak{p}) \tilde{=} R_\mathfrak{p}.$$

Wie betrachten nun das folgende Diagramm:

$$\begin{tikzcd} R \arrow[r, "i"] \arrow[d, "j"'] & \Lambda^n(E) \arrow[d, "J"] \\ R_\mathfrak{p} \arrow[r] & \Lambda^n(E)_\mathfrak{p} \end{tikzcd}$$

wobei die Abbildungen j, J und i durch $j(r) := r_\mathfrak{p} := r/1 \in R_\mathfrak{p}$, $J(z) := z \otimes 1_{R_\mathfrak{p}}$ und $i(r) := re_1 \wedge e_2 \wedge \cdots \wedge e_n$ gegeben seien. Offensichtlich ist i surjektiv. Ist $r \in \ker i$, so folgt $r \in \ker j$, also $r_\mathfrak{p} = 0$. Da dies für jedes Primideal $\mathfrak{p} \subset R$ gilt, folgt $r = 0$. Also ist i injektiv und es gilt $R \tilde{=} \Lambda^n(E) = < e_1 \wedge e_2 \wedge \cdots \wedge e_n >_R$. Daher ist $\Lambda^n(E)$ ein endlich erzeugter, projektiver R-Modul vom Rang 1. $\square$

Gibt es eine Zerlegung $E = E_1 \oplus E_2$, so gilt falls $q = 0$ automatisch auch $E = E_1 \perp E_2$ und daher die Isomorphie $\Lambda(E) \tilde{=} \Lambda(E_1) \otimes_R \Lambda(E_2)$ von R-Moduln. Für die direkten Summanden $\Lambda^k(E)$, $k = 1, \ldots, m$, von $\Lambda(E)$ gilt dann:

$$\Lambda^k(E) \tilde{=} \bigoplus_{i+j=k} \Big(\Lambda^i(E_1) \otimes_R \Lambda^j(E_2)\Big).$$

Hat nun E_1 Rang 1 und E_2 ist frei von Rang $n-1$, so gilt $\Lambda^j(E_1) = 0$ für alle $j > 1$ und $\Lambda^n(E_2) = 0$. Es folgt daher in diesem Fall:

$$\Lambda^n(E) \,\tilde{=}\, \Lambda^1(E_1) \otimes_R \Lambda^{n-1}(E_2) \,\tilde{=}\, E_1 \otimes_R R \,\tilde{=}\, E_1.$$

Daraus folgt unmittelbar:

Lemma 1.16. *Sei E ein endlich erzeugter projektiver R-Modul von konstantem Rang n. Weiters seien Zerlegungen $E = E_1 \oplus E_2 = E_1' \oplus E_2'$ gegeben, wobei E_1, E_1' Rang 1 haben und E_2, E_2' frei von Rang $n-1$ seien. Dann gilt $E_1 \tilde{=} E_1'$.*

2. Die Struktur von Clifford-Algebren

2.1. **Standard-Involutionen.**

Sei A eine treue R-Algebra. Da dann die durch $r \mapsto r \cdot 1_A$ gegebene Abbildung $R \to A$ injektiv ist, identifizieren wir R mit der Teilmenge $R \cdot 1_A$ von A. Sei $\rho : z \mapsto \bar{z}$ ein R-Algebren-Antiautomorphismus auf A, sodass folgende Eigenschaften für alle $z \in A$ erfüllt sind:

(2) $$s(z) := z + \bar{z} \in R, \quad n(z) := z\bar{z} \in R.$$

Es folgt dann:

$$\rho^2(z) = \bar{\bar{z}} = \overline{s(z) - z} = s(z) - \bar{z} = z$$

und ρ ist daher eine Involution.

Definition 2.1. *Sind für einen R-Algebren-Antiautomorphismus ρ auf einer treuen R-Algebra A die Eigenschaften (2) erfüllt, so nennen wir ρ eine* Standard-Involution *auf A. Die Abbildung $s : A \to R \subset A$ heißt die* Spur *von A, $n : A \to R \subset A$ die* Norm *von A. Existiert eine Standard-Involution auf A, so sagt man, dass A eine* R-Algebra mit Standard-Involution *ist.*

Bemerkung: Alternativ zu dieser Definition würde es genügen $n(z) = z\bar{z} \in R$ vorauszusetzen, da dann wegen

$$n(1_A + z) = (1_A + z)(1_A + \bar{z}) = (1_R + z + \bar{z} + z\bar{z})1_A$$

auch $s(z) = z + \bar{z} \in R \cdot 1_A = R$ folgt.

Beispiele:

(1) Ist $A = R$ und $\rho = id_R$, so ist A die *triviale* R-Algebra mit Standard-Involution.

(2) Ist A eine freie R-Algebra von Rang 2, so lässt sich A darstellen als Restklassenring $A = R[X]/(X^2 - cX - d)$ für gewisse $c, d \in R$. Die *Konjugation* ς auf A ist in der Basis $\{1_A,\ x = X + (X^2 - cX - d)\}$ definiert durch:

$$\varsigma : r_0 1_A + r_1 x \mapsto (r_0 + r_1 c)1_A - r_1 x$$

für $r_0,\ r_1 \in R$. Offenbar ist ς R-linear und für $a = r_0 1_A + r_1 x,\ a' = r_0' 1_A + r_1' x \in A$ gilt:

$$\varsigma(a)\varsigma(a') = ((r_0 + r_1 c)1_A - r_1 x)((r_0' + r_1' c)1_A - r_1' x) =$$

$$= (r_0 r_0' + r_0 r_1' c + r_1 r_0' c + r_1 r_1' c^2)1_A - (r_0 + r_1 c) r_1' x - r_1(r_0' + r_1' c)x + r_1 r_1' x^2 =$$

$$= (r_0r_0' + r_1r_1'd + r_0r_1'c + r_1r_0'c + r_1r_1'c^2)1_A - (r_0r_1' + r_1r_0' + r_1r_1'c)x =$$
$$= \varsigma\big((r_0r_0' + r_1r_1'd)1_A + (r_0r_1' + r_1r_0' + r_1r_1'c)x\big) =$$
$$= \varsigma\big((r_01_A + r_1x)(r_0'1_A + r_1'x)\big) = \varsigma(aa').$$

Also ist ς ein R-Algebren-Homomorphismus. Wegen

$$\varsigma^2(a) = \varsigma^2(r_01_A + r_1x) = \varsigma\big((r_01_A + r_1c)1_A - r_1x\big) =$$
$$= (r_0 + r_1c - r_1c)1_A + r_1x = a$$

für alle $a = r_01_A + r_1x \in A$ folgt $\varsigma^2 = id_A$ und ς ist somit eine Involution. Es gilt:

$$s(a) := a + \varsigma(a) = r_01_A + r_1x + (r_0 + r_1c)1_A - r_1x = (2r_0 + r_1c)1_A \in R1_A,$$
$$n(a) := a\varsigma(a) = (r_01_A + r_1x)((r_0 + r_1c)1_A - r_1x) =$$
$$= (r_0^2 + r_0r_1c)1_A - r_0r_1x + r_0r_1x + r_1^2cx - r_1^2x^2 = (r_0^2 + r_0r_1c - r_1^2d)1_A \in R1_A.$$

Da A – als freie R-Algebra von Rang 2 – kommutativ ist, sind die Antiautomorphismen auf A gerade die Automorphismen auf A und die Konjugation ς ist somit eine Standard-Involution auf A.

(3) Wir betrachten die R-Algebra $M_2(R)$ der 2×2-Matrizen über R gemeinsam mit der Abbildung $\rho : M_2(R) \to M_2(R)$, die gegeben ist durch:

$$\rho : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Offensichtlich ist ρ R-linear und für $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in M_2(R)$ gilt:

$$\rho(M')\rho(M) = \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} cb' + dd' & -ab' - bd' \\ -ca' - dc' & aa' + bc' \end{pmatrix} = \rho(MM').$$

Also ist ρ ein R-Algebren-Antiautomorphismus auf $M_2(R)$. Offensichtlich gilt $\rho^2 = id_{M_2(R)}$. Wegen

$$s(M) := M + \rho(M) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (a+d)1_{M_2(R)} \in R1_{M_2(R)},$$
$$n(M) = M\rho(M) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & -ab + ab \\ cd - cd & -bc + ad \end{pmatrix} =$$
$$= (ad - bc)1_{M_2(R)} \in R1_{M_2(R)}$$

ist ρ eine Standard-Involution und die Spur der R-Algebra $M_2(R)$ stimmt gerade mit der Spur von Matrizen überein, während die Norm durch die Determinantenabbildung auf $M_2(R)$ gegeben ist.

Wir betten nun die R-Algebra $A = R[X]/(X^2 - cX - d)$ aus Beispiel (2) in $M_2(R)$ ein via

$$i : A \to M_2(R), \ \ r_01_A + r_1x \mapsto \begin{pmatrix} r_0 & r_1d \\ r_1 & r_0 + r_1c \end{pmatrix}.$$

Diese Abbildung ist R-linear und für alle $z = r_01_A + r_1x$, $z' = r_0'1_A + r_1'x \in A$ gilt:

$$i(z)i(z') = \begin{pmatrix} r_0 & r_1d \\ r_1 & r_0 + r_1c \end{pmatrix}\begin{pmatrix} r_0' & r_1'd \\ r_1' & r_0' + r_1'c \end{pmatrix} =$$
$$= \begin{pmatrix} r_0r_0' + r_1r_1'd & (r_0r_1' + r_1r_0' + r_1r_1'c)d \\ r_0r_1' + r_1r_0' + r_1r_1'c & r_0r_0' + r_1r_1'd + (r_0r_1' + r_1r_0' + r_1r_1'c)c \end{pmatrix} =$$

$$= i\big((r_0r_0' + r_1r_1'd)1_A + (r_0r_1' + r_1r_0' + r_1r_1'c)x\big) = i(zz').$$

Da i offensichtlich injektiv ist, ist i somit ein injektiver Homomorphismus von R-Algebren. Wir werden nun zeigen, dass die Standard-Involution ρ eingeschränkt auf das Bild von i gerade der Konjugation ς auf A entspricht, dass also $\rho \circ i = i \circ \varsigma$ gilt. Sei also $z = r_0 1_A + r_1 x \in A$ beliebig. Dann gilt:

$$\rho \circ i(z) = \rho \begin{pmatrix} r_0 & r_1 d \\ r_1 & r_0 + r_1 c \end{pmatrix} = \begin{pmatrix} r_0 + r_1 c & -r_1 d \\ -r_1 & r_0 \end{pmatrix}, \quad \textit{sowie}$$

$$i \circ \varsigma(z) = i((r_0 + r_1 c)1_A - r_1 x) = \begin{pmatrix} r_0 + r_1 c & -r_1 d \\ -r_1 & r_0 + r_1 c - r_1 c \end{pmatrix}$$

und die Behauptung ist gezeigt.

Ist A eine R-Algebra mit Standard-Involution ρ, so gilt für alle $z \in A$:

$$z^2 + z\bar{z} = z(z + \bar{z}) = zs(z) = s(z)z = (z + \bar{z})z = z^2 + \bar{z}z,$$

wobei wir verwendet haben, dass die durch $r \mapsto r \cdot 1_A$ definierte Abbildung R ins Zentrum von A einbettet. Zudem gilt:

$$n(z) = z\bar{z} = z(s(z) - z) = s(z)z - z^2$$

und es folgt daher:

$$z\bar{z} = \bar{z}z \quad \textit{und} \quad z^2 - s(z)z + n(z) = 0. \tag{3}$$

Weiters gilt für alle $z, z' \in A$:

$$n(zz') = (zz')(\overline{zz'}) = zz'\bar{z}'\bar{z} = n(z')z\bar{z} = n(z)n(z')$$

und wir erhalten daher, dass $z \in A$ genau dann invertierbar ist, wenn $n(z) \in R$ invertierbar ist.
Definieren wir nun für $z, z' \in A$

$$f(z, z') := s(z\bar{z}') = z\bar{z}' + \overline{z\bar{z}'} = z\bar{z}' + z'\bar{z},$$

so erhalten wir eine symmetrische Bilinearform $f : A \times A \to R$ und es gilt:

$$n(z + z') = (z + z')(\overline{z + z'}) = z\bar{z} + z\bar{z}' + z'\bar{z} + z'\bar{z}' = n(z) + n(z') + f(z, z'),$$

$$\textit{sowie} \quad n(rz) = (rz)(\overline{rz}) = r^2 n(z)$$

für alle $r \in R$. Es ist also $n : A \to R$ eine quadratische Form auf A mit assoziierter symmetrischer Bilinearform f.

Der folgende Satz wird in Zukunft sehr nützlich sein:

Satz 2.1. *Sei A eine (treue) R-Algebra mit Standard-Involution $\rho : x \mapsto \bar{x}$. Für ein beliebiges Element $z \in A$ sind äquivalent:*

(1) $z - \bar{z} \in A^*$
(2) $(z - \bar{z})^2 \in R^*$
(3) $R + Rz = R \oplus Rz$ *ist eine separable freie R-Algebra vom Rang 2.*

Beweis. (1) $\Longleftrightarrow$ (2): Wir setzten $z' := z - \bar{z}$. Es gilt $\bar{z}' = \overline{z - \bar{z}} = \bar{z} - z = -z'$ und daher $R \ni n(z') = z'\bar{z}' = -z'^2$. Es gilt nun genau dann $z' \in A^*$, wenn $n(z') = -z'^2 \in R^*$ und (1) und (2) sind daher äquivalent.
(2) $\Longleftrightarrow$ (3): Gilt $R + Rz = R \oplus Rz$, so ist $R + Rz$ eine freie R-Algebra von Rang 2. Nach Gleichung (3) im Vorangegangenen gilt: $z^2 - s(z)z + n(z) = 0$. Setzen wir $S := s(z)$, $N := -n(z)$, so gilt daher: $R \oplus Rz \tilde{=} R[X]/(X^2 - SX - N)$, wobei der

Isomorphismus durch $z \mapsto X + (X^2 - SX - N)$ gegeben ist. Es gilt nun allgemein, dass $R[X]/(X^2 - SX - N)$ genau dann separabel ist, wenn $S^2 + 4N \in R^*$. Wegen

$$S^2 + 4N = (z + \bar{z})^2 - 4z\bar{z} = z^2 + 2z\bar{z} + \bar{z}^2 - 4z\bar{z} = (z - \bar{z})^2$$

ist also $R \oplus Rz$ genau dann separabel, wenn $(z - \bar{z})^2 \in R^*$ gilt.
Es bleibt zu zeigen, dass aus $(z - \bar{z})^2 \in R^*$ folgt, dass $\{1_A, z\}$ eine Basis von $R + Rz$ bildet. Seien also $r_0, r_1 \in R$ derart, dass $r_0 + r_1 z = 0$. Dann gilt:

$$r_1(z - \bar{z}) = r_1 z - r_1 \bar{z} = r_1 z - \overline{r_1 z} = -r_0 + \bar{r}_0 = 0.$$

Ist nun $(z - \bar{z})^2 \in R^*$, so kann $z - \bar{z}$ kein Nullteiler sein und es folgt daher $r_1 = 0$ und auch $r_0 = 0$; also sind 1_A und z linear unabhängig. □

2.2. **Freie Quaternionen-Algebren.**

Sei in diesem Abschnitt (E, q) ein freier quadratischer R-Modul vom Rang 2 und $C(E, q)$ eine Clifford-Algebra zu (E, q). Man nennt $C(E, q)$ dann auch eine *freie Quaternionen-Algebra*. Wir wollen nun eine Standard-Involution auf $C(E, q)$ konstruieren.
Zunächst sei (E, q) ein beliebiger quadratischer R-Modul und $(C(E, q), \iota)$ eine Clifford-Algebra. Sei $\sigma = C(-id_E)$ und $\tau : C(E, q) \to C(E, q)^{op}$ der eindeutige Homomorphismus von R-Algebren mit $\tau \circ \iota = \tilde{\iota}$, wobei $\tilde{\iota} : E \to C(E, q)^{op}$ gerade der Strukturabbildung ι, aufgefasst als Abbildung in die R-Algebra $C(Eq)^{op}$, entspricht (vgl. Abschnitt 1.3). Wir fassen nun τ als Antiautomorphismus auf $C(E, q)$ auf. Durch Komposition von σ mit τ erhalten wir einen R-Algebren-Antiautomorphismus $\gamma := \sigma \circ \tau$, der

$$\gamma(x) = -x$$

für alle $x \in E$ erfüllt. Da $C(E, q)$ als R-Algebra von $E = \iota(E)$ erzeugt wird, ist γ offensichtlich eine Involution auf $C(E, q)$ und als Antiautomorphismus durch $\gamma(x) = -x$ eindeutig festgelegt. Weiters erhält γ die Graduierung $C(E, q) = C_0(E, q) \oplus C_1(E, q)$.

Definition 2.2. *Den R-Algebren-Antiautomorphismus $\gamma := \sigma \circ \tau$ (mit der Notation aus Abschnitt 1.3) nennt man die* kanonische Involution *auf $C(E, q)$.*

Im Spezialfall freier Quaternionen-Algebren hat diese Involution die Eigenschaften, die für eine Standard-Involution gefordert werden:

Proposition 2.2. *Sei (E, q) ein freier quadratischer R-Modul von Rang 2. Dann ist die kanonische Involution γ eine Standard-Involution auf $C(E, q)$.*

Beweis. Sei $\{x_1, x_2\}$ eine Basis von E. Es ist γ ein Antiautomorphismus und es gilt für alle $z = r_0 1_{C(E,q)} + r_1 x_1 + r_2 x_2 + r_3 x_1 x_2 \in C(E, q)$:

$$\begin{aligned} \bar{z} := \gamma(z) = r_0 1_{C(E,a)} - r_1 x_1 - r_2 x_2 + r_3 x_2 x_1 = \\ = r_0 1_{C(E,q)} - r_1 x_1 - r_2 x_2 + r_3(b(x_1, x_2) 1_{C(E,q)} - x_1 x_2) = \\ = (r_0 + r_3 b(x_1, x_2)) 1_{C(E,q)} - r_1 x_1 - r_2 x_2 - r_3 x_1 x_2 \end{aligned}$$

und daher:

$$\begin{aligned} n(z) 1_{C(E,q)} = z\bar{z} = r_0(r_0 + r_3 b(x_1, x_2)) 1_{C(E,q)} - r_0 r_1 x_1 - r_0 r_2 x_2 - r_0 r_3 x_1 x_2 + \\ +(r_0 + r_3 b(x_1, x_2)) r_1 x_1 - r_1^2 x_1^2 - r_1 r_2 x_1 x_2 - r_1 r_3 x_1^2 x_2 + \\ +(r_0 + r_3 b(x_1, x_2)) r_2 x_2 - r_1 r_2 x_2 x_1 - r_2^2 x_2^2 - r_2 r_3 x_2 x_1 x_2 + \end{aligned}$$

$$+(r_0 + r_3 b(x_1,x_2))r_3 x_1 x_2 - r_1 r_3 x_1 x_2 x_1 - r_2 r_3 x_1 x_2^2 - r_3^2 x_1 x_2 x_1 x_2 =$$

$$= \Big(r_0^2 + r_0 r_3 b(x_1,x_2) - r_1^2 q(x_1) - r_2^2 q(x_2) - r_1 r_2 b(x_1,x_2) + r_3^2 q(x_1)q(x_2)\Big) 1_{C(E,q)} +$$
$$+\Big(-r_0 r_1 + r_0 r_1 + r_1 r_3 b(x_1,x_2) + r_2 r_3 q(x_2) - r_1 r_3 b(x_1,x_2) - r_2 r_3 q(x_2)\Big) x_1 +$$
$$+\Big(-r_0 r_2 - r_1 r_3 q(x_1) + r_0 r_2 + r_2 r_3 b(x_1,x_2) - r_2 r_3 b(x_1,x_2) + r_1 r_3 q(x_1)\Big) x_2 +$$
$$+\Big(-r_0 r_3 - r_1 r_2 + r_1 r_2 + r_0 r_3 + r_3^2 b(x_1,x_2) - r_3^2 b(x_1,x_2)\Big) x_1 x_2 =$$

$$= \Big(r_0^2 + r_0 r_3 b(x_1,x_2) + r_3^2 q(x_1)q(x_2) - (r_1^2 q(x_1) + r_1 r_2 b(x_1,x_2) + r_2^2 q(x_2))\Big) 1_{C(E,q)}.$$

Es ist also $n(z) \in R$ und aus der Bemerkung zu Definition 2.1 folgt, dass dann auch $s(z) \in R$ gilt. □

Bemerkung: Im Allgemeinen gilt die Aussage obiger Proposition jedoch nicht. Ist nämlich $C(E,q)$ eine Clifford-Algebra zu einem beliebigen projektiven quadratischen R-Modul (E,q), der von $m > 2$ Elementen erzeugt wird, so müsste eine Standard-Involution ρ auf $C(E,q)$ die quadratische Gleichung $z^2 - s(z)z + n(z) = 0$ für alle $z \in C(E,q)$ erfüllen (siehe Gleichung (3) in Abschnitt 2.1). Wegen $x^2 = q(x)$ für alle $x \in E$ würde $q(x) - s(x)x + n(x) = 0$ für alle $x \in E$ folgen. Es müsste also $q(x) = -n(x)$ und $s(x) = x + \rho(x) = 0$ gelten. Aus Letzterem folgt: $\rho(x) = -x$ für alle $x \in E$. Da $C(E,q)$ als R-Algebra von E erzeugt wird, folgt daher, dass ρ (als Antiautomorphismus) mit der kanonischen Involution γ übereinstimmen müsste. Für beliebige Elemente $x, y, z \in E$ muss allerdings

$$s(xyz) = xyz + \gamma(xyz) = xyz + \gamma(z)\gamma(y)\gamma(x) = xyz - zyx.$$

nicht mehr in R liegen und es muss daher im Allgemeinen keine Standard-Involution auf $C(E,q)$ existieren.

Ist $C(E,q)$ nun eine freie Quaternionen-Algebra über R, so definiert die kanonische Involution γ (als Standard-Involution $z \mapsto \bar{z} = \gamma(z)$) eine quadratische Form auf $C(E,q)$, die durch die Normfunktion $n(z) = z\bar{z}$ (für $z \in C(E,q)$) gegeben ist. Die zugehörige symmetrische Bilinearform ist durch $f(z,z') = z\bar{z'} + z'\bar{z}$ (für $z, z' \in C(E,q)$) gegeben. $C(E,q)$ erhält damit die Struktur eines quadratischen R-Moduls. Sei $\{x_1,\ x_2\}$ eine Basis von E. Dann ist $\{1_{C(E,q)},\ x_1,\ x_2,\ x_1x_2\}$ eine Basis von $C(E,q)$ als R-Modul. Betrachten wir die Graduierung $C(E,q) = C_0(E,q) \oplus C_1(E,q)$, so bilden $\{1_{C(E,q)},\ x_1x_2\}$ und $\{x_1,\ x_2\}$ Basen von $C_0(E,q)$ bzw. $C_1(E,q)$. Offenbar gilt $C_1(E,q) = E$ und wegen

$$f(1_{C(E,q)}, x_1) = \bar{x}_1 + x_1 = -x_1 + x_1 = 0$$
$$f(1_{C(E,q)}, x_2) = \bar{x}_2 + x_2 = -x_2 + x_2 = 0$$
$$f(x_1x_2, x_1) = (x_1x_2)\bar{x}_1 + x_1(\overline{x_1x_2}) = -x_1x_2x_1 + x_1x_2x_1 = 0$$
$$f(x_1x_2, x_2) = (x_1x_2)\bar{x}_2 + x_2(\overline{x_1x_2}) = -q(x_2)x_1 + q(x_2)x_1 = 0$$

sind $C_0(E,q)$ und $C_1(E,q)$ bezüglich f zueinander orthogonal. Es folgt somit:

$$C(E,q) = C_0(E,q) \perp E.$$

Satz 2.3. *Sei (E,q) ein freier quadratischer R-Modul von Rang 2 und $C(E,q)$ eine Clifford-Algebra. Dann sind äquivalent:*

(1) *(E,q) ist nichtsingulär,*

(2) *(C(E,q),n) ist als quadratischer R-Modul nichtsingulär, wobei* $n : C(E,q) \to R$ *die durch die Standard-Involution* γ *gegebene Norm auf* $C(E,q)$ *sei,*
(3) $C_0(E,q)$ *ist eine separable freie R-Algebra von Rang 2,*
(4) $x_1x_2 - \overline{x_1x_2}$ *ist invertierbar in* $C(E,q)$.

Beweis. Ein freier quadratischer R-Modul (E',q') mit Basis $\{x_1,x_2,\ldots,x_n\}$ und assoziierter Bilinearform b' ist genau dann nichtsingulär, wenn die Determinante der Gram-Matrix $\Big(b(x_i,x_j)\Big)_{i,j=1}^{n}$ in R invertierbar ist. Die Aussage (1) ist daher äquivalent zu

$$(1') \quad \det\begin{pmatrix} 2q(x_1) & b(x_1,x_2) \\ b(x_1,x_2) & 2q(x_2)\end{pmatrix} = 4q(x_1)q(x_2) - b(x_1,x_2)^2 \in R^*.$$

Um Aussage (2) umzuformulieren, müssen wir nun auch die Gram-Matrix von $(C(E,q),f)$ bezüglich der Basis $\{1 = 1_{C(E,q)}, x_1, x_2, x_1x_2\}$ berechnen:

$$f(1,1) = 1+1 = 2, \quad f(1,x_1) = f(1,x_2) = 0 \ (\textit{siehe oben}),$$
$$f(1,x_1x_2) = \overline{x_1x_2} + x_1x_2 = x_2x_1 + x_1x_2 = b(x_1,x_2),$$
$$f(x_1,x_1) = x_1\bar{x}_1 + x_1\bar{x}_1 = -2q(x_1), \quad f(x_1,x_2) = x_1\bar{x}_2 + x_2\bar{x}_1 = -b(x_1,x_2),$$
$$f(x_1,x_1x_2) = f(x_2,x_1x_2) = 0 \ (\textit{siehe oben}), \quad f(x_2,x_2) = -2q(x_2),$$
$$f(x_1x_2,x_1x_2) = x_1x_2(\overline{x_1x_2}) + x_1x_2(\overline{x_1x_2}) = 2x_1x_2\bar{x}_2\bar{x}_1 = 2q(x_1)q(x_2).$$

Wir erhalten somit die Gram-Matrix

$$B(C(E,q),f) := \begin{pmatrix} 2 & 0 & 0 & b(x_1,x_2) \\ 0 & -2q(x_1) & -b(x_1,x_2) & 0 \\ 0 & -b(x_1,x_2) & -2q(x_2) & 0 \\ b(x_1,x_2) & 0 & 0 & 2q(x_1)q(x_2)\end{pmatrix}$$

und berechnen deren Determinante:

$$\begin{aligned}\det B(C(E,q),f) &= 2\big(8q(x_1)^2q(x_2)^2 - 2q(x_1)q(x_2)b(x_1,x_2)^2\big) - \\ &\quad -b(x_1,x_2)\big(4q(x_1)q(x_2)b(x_1,x_2) - b(x_1,x_2)^3\big) = \\ &= 16q(x_1)^2q(x_2)^2 - 8q(x_1)q(x_2)b(x_1,x_2)^2 + b(x_1,x_2)^4 = \\ &= \big(4q(x_1)q(x_2) - b(x_1,x_2)^2\big)^2.\end{aligned}$$

Aussage (2) ist daher äquivalent zu

$$(2') \quad \det B(C(E,q),f) = \big(4q(x_1)q(x_2) - b(x_1,x_2)^2\big)^2 \in R^*.$$

Da $r \in R$ genau dann invertierbar ist, wenn r^2 invertierbar ist, folgt die Äquivalenz von (1) und (2).

Wie setzen nun $z := x_1x_2$. Dann gilt:

$$z - \bar{z} = x_1x_2 - \overline{x_1x_2} = x_1x_2 - x_2x_1 = 2x_1x_2 - (x_1x_2 + x_2x_1) = 2x_1x_2 - b(x_1,x_2)$$

und daher

$$\begin{aligned}(z-\bar{z})^2 &= 4x_1x_2x_1x_2 - 4b(x_1,x_2)x_1x_2 + b(x_1,x_2)^2 = \\ &= 4b(x_1,x_2)x_1x_2 - 4q(x_1)q(x_2) - 4b(x_1,x_2)x_1x_2 + b(x_1,x_2)^2 = \\ &= -4q(x_1)q(x_2) + b(x_1,x_2)^2.\end{aligned}$$

Mit Satz 2.1 folgt daher, dass $x_1x_2 - \overline{x_1x_2} \in C(E,q)^*$ – also Aussage (4) – genau dann gilt, wenn $4q(x_1)q(x_2) - b(x_1,x_2)^2 \in R^*$ – also Aussage (1) – erfüllt ist. Dies ist wiederum äquivalent dazu, dass $C_0(E,q) = R + Rx_1x_2$ eine freie separable R-Algebra mit Basis $\{1,\ x_1x_2\}$ ist – das entspricht gerade Aussage (3). $\square$

Dieses Wissen wollen wir nun nutzen, um die Struktur freier Quaternionen-Algebren zu untersuchen.

Definition 2.3. *Der* Zentralisator *von $C_0(E,q)$ in $C(E,q)$ ist definiert als*

$$Z_{C(E,q)}C_0(E,q) := \{z \in C(E,q) \mid zy = yz \ \ \forall y \in C_0(E,q)\}.$$

Der Zentralisator bildet eine Teilalgebra von $C(E,q)$ und es gilt für die Zentren von $C(E,q)$ bzw. $C_0(E,q)$ offensichtlich:

$$Z(C(E,q)) \subset Z_{C(E,q)}C_0(E,q),$$
$$Z(C_0(E,q)) = Z_{C(E,q)}C_0(E,q) \cap C_0(E,q) \subset Z_{C(E,q)}C_0(E,q).$$

Satz 2.4. *Ist (E,q) ein freier quadratischer R-Modul von Rang 2 und nichtsingulär, dann gilt für die Clifford-Algebra $C(E,q)$:*

$$Z_{C(E,q)}C_0(E,q) = Z(C_0(E,q)) = C_0(E,q) \quad \textit{und} \ \ Z(C(E,q)) = R.$$

Beweis. Ist $\{x_1, x_2\}$ eine Basis von E, so ist $\{1_{C(E,q)},\, x_1x_2\}$ eine Basis der Teilalgebra $C_0(E,q)$ von $C(E,q)$ und $C_0(E,q)$ ist offensichtlich kommutativ – es gilt daher $Z(C_0(E,q)) = C_0(E,q)$. Weiters gilt (wie oben bereits bemerkt): $Z(C_0(E,q)) \subset Z_{C(E,q)}C_0(E,q)$.
Um die umgekehrte Inklusion zu zeigen, sei nun $z := z_0 + z_1 \in Z_{C(E,q)}C_0(E,q) \subset C_0(E,q) \oplus C_1(E,q) = C(E,q)$. Dann gilt nach Definition des Zentralisators für alle $y \in C_0(E,q)$: $zy = yz$, also $z_0y + z_1y = yz_0 + yz_1$. Da $C_0(E,q)$ kommutativ ist, lässt sich diese Bedingung reduzieren zu

$$z_1y = yz_1.$$

Wir haben oben gesehen, dass $C_0(E,q)$ und $C_1(E,q)$ zueinander orthogonal sind bezüglich der von der Standardinvolution γ induzierten Bilinearform f auf $C(E,q)$. Daher muss für $z = z_0 + z_1 \in Z_{C(E,q)}C_0(E,q)$ gelten:

$$0 = f(y, z_1) = y\bar{z}_1 + z_1\bar{y} = -yz_1 + z_1\bar{y}$$

für alle $y \in C_0(E,q)$. Damit gilt also für alle $z = z_0 + z_1 \in Z_{C(E,q)}C_0(E,q)$:

$$z_1y = yz_1 = z_1\bar{y}$$

und somit $z_1(y - \bar{y}) = 0$ für alle $y \in C_0(E,q)$. Da (E,q) nichtsingulär ist, ist nach dem vorangegangenen Satz $x_1x_2 - \overline{x_1x_2}$ invertierbar in $C(E,q)$. Wir setzen nun $y = x_1x_2$ und erhalten damit $z_1 = 0$, also $z \in C_0(E,q)$. Somit haben wird auch die Inklusion $Z_{C(E,q)}C_0(E,q) \subset C_0(E,q) = Z(C_0(E,q))$ bewiesen und es gilt daher Gleichheit.
Wegen $Z(C(E,q)) \subset Z_{C(E,q)}C_0(E,q) = C_0(E,q)$ hat jedes $z \in Z(C(E,q))$ die Form $z = r_0 + r_1x_1x_2$ $(r_0, r_1 \in R)$ und muss insbesondere $zx_1 = x_1z$ erfüllen und somit auch

$$(r_0 + r_1b(x_1,x_2))x_1 - r_1q(x_1)x_2 = r_0x_1 + r_1(x_1x_2)x_1 = zx_1 =$$
$$= x_1z = r_0x_1 + r_1x_1(x_1x_2) = r_0x_1 + r_1q(x_1)x_2.$$

Weil $\{x_1, x_2\}$ eine Basis von E ist, folgt daher:

$$r_1b(x_1,x_2) = 0 \ \ \textit{und} \ \ 2r_1q(x_1) = 0.$$

Es gilt also $r_1b(x_1,x_2) = r_1b(x_1,x_1) = 0$ und weil $\{x_1, x_2\}$ den R-Modul E erzeugt, folgt $b(r_1x_1, \,.\,) = 0 \in Hom(E,R)$. Nach Voraussetzung ist (E,q) nichtsingulär und es muss daher $r_1x_1 = 0$ gelten. Da x_1 R-linear unabhängig ist, folgt $r_1 = 0$. Somit haben wir auch $Z(C(E,q)) = R$ gezeigt. □

Bemerkung: Betrachten wir nun den Spezialfall eines nichtsingulären freien quadratischen R-Moduls (E,q) mit Orthogonalbasis $\{x_1,x_2\}$. Da (E,q) nichtsingulär ist, muss die Determinante der Gram-Matrix $\Big(b(x_i,x_j)\Big)_{i,j=1}^2$ in R invertierbar sein, also

$$\det\begin{pmatrix} 2q(x_1) & 0 \\ 0 & 2q(x_2)\end{pmatrix} = 4q(x_1)q(x_2) \in R^*$$

gelten. Daraus folgt insbesondere $2 \in R^*$. Die Clifford-Algebra $C(E,q)$ ist ein freier R-Modul von Rang 4 und für die Basis $\{x_0 := 1_{C(E,q)},\ x_1,\ x_2, x_3 := x_1x_2\}$ gilt:

$$x_0 = 1, \quad x_1^2 = q(x_1)x_0, \quad x_2^2 = q(x_2)x_0,$$
$$x_1x_2 = -x_2x_1 = x_3, \quad x_3^2 = x_1x_2x_1x_2 = -q(x_1)q(x_2)x_0.$$

Die freien Quaternionen-Algebren über kommutativen Ringen verallgemeinern also das Konzept der verallgemeinerten Quaternionen-Algebren $Q(a,b \mid K)$ über Körpern K. Daher macht die Bezeichnung

$$C(E,q) = Q(q(x_1), q(x_2) \mid R)$$

Sinn. Sind $R = \mathbb{R},\ q(x_1) = q(x_2) = -1$, so erhalten wir gerade die Hamiltonschen Quaternionen.

Satz 2.5. *Sei (E,q) ein nichtsingulärer, freier quadratischer R-Modul von Rang 2. Dann ist $C(E,q)$ separabel über R.*

Beweis. Sei $C(E,q)^e := C(E,q) \otimes_R C(E,q)^{op}$ und $\phi : C(E,q)^e \to C(E,q)$ der eindeutige $C(E,q)^e$-Modul-Homomorphismus mit $\phi(a \otimes b^{op}) = ab$ (siehe Anhang). Wir wollen nun ein separabilitäts-idempotentes Element $e \in C(E,q)^e$ konstruieren, also ein $e \in C(E,q)^{op}$ mit

$$\phi(e) = 1_{C(E,q)} =: 1 \quad \textit{und} \quad (1 \otimes z^{op})e = (z \otimes 1^{op})e$$

für alle $z \in C(E,q)$. Da (E,q) nichtsingulär ist, gilt $4q(x_1)q(x_2) - b(x_1,x_2)^2 \in R^*$. Wir definieren nun $u := (-4q(x_1)q(x_2) + b(x_1,x_2)^2)^{-1}$ und

$$e := u\Big((-q(x_1)q(x_2))1 \otimes 1^{op} - q(x_2)x_1 \otimes x_1^{op} - q(x_1)x_2 \otimes x_2^{op} +$$
$$+ b(x_1,x_2)x_2 \otimes x_1^{op} + (x_1x_2) \otimes (x_1x_2)^{op}\Big),$$

wobei zu beachten ist, dass $(x_1x_2)^{op} = x_2^{op} * x_1^{op} \in C(E,q)^{op}$ gilt. Wir schreiben die Multiplikation $*$ in $C(E,q)^{op}$ im Folgenden nicht mehr aus. Es gilt:

$$\phi(e) = u\Big(-q(x_1)q(x_2) - q(x_2)q(x_1) - q(x_1)q(x_2) + b(x_1,x_2)x_2x_1 + x_1x_2x_1x_2\Big) =$$
$$= u\Big(-3q(x_1)q(x_2) + b(x_1,x_2)^2 - b(x_1,x_2)x_1x_2 + b(x_1,x_2)x_1x_2 - q(x_1)q(x_2)\Big) =$$
$$= u\Big(-4q(x_1)q(x_2) + b(x_1,x_2)^2\Big) = 1.$$

Da $C(E,q)$ als R-Modul von $\{1, x_1, x_2, x_1x_2\}$ erzeugt wird, genügt es, $(1 \otimes z^{op})e = (z \otimes 1^{op})e$ für $z = x_1,\ x_2,\ x_1x_2$ zu überprüfen.
Für $\underline{z = x_1}$ erhält man einerseits:

$$u^{-1}(x_1 \otimes 1^{op})e = -q(x_1)q(x_2)x_1 \otimes 1^{op} - q(x_2)x_1^2 \otimes x_1^{op} - q(x_1)(x_1x_2) \otimes x_2^{op} +$$
$$+ b(x_1,x_2)(x_1x_2) \otimes x_1^{op} + (x_1^2x_2) \otimes (x_1x_2)^{op} =$$

$$= -q(x_1)q(x_2)x_1 \otimes 1^{op} - q(x_1)q(x_2)1 \otimes x_1^{op} - q(x_1)(x_1x_2) \otimes x_2^{op} +$$

$$+b(x_1,x_2)(x_1x_2)\otimes x_1^{op}+q(x_1)x_2\otimes(x_1x_2)^{op};$$

und andererseits:

$$u^{-1}(1\otimes x_1^{op})e=-q(x_1)q(x_2)1\otimes x_1^{op}-q(x_2)x_1\otimes(x_1^{op})^2-q(x_1)x_2\otimes(x_1^{op}x_2^{op})+$$
$$+b(x_1,x_2)x_2\otimes(x_1^{op})^2+(x_1x_2)\otimes x_1^{op}(x_1x_2)^{op}=$$

$$=-q(x_1)q(x_2)1\otimes x_1^{op}-q(x_1)q(x_2)x_1\otimes 1^{op}-q(x_1)b(x_1,x_2)x_2\otimes 1^{op}+q(x_1)x_2\otimes(x_2^{op}x_1^{op})+$$
$$+q(x_1)b(x_1,x_2)x_2\otimes 1^{op}+b(x_1,x_2)(x_1x_2)\otimes x_1^{op}-q(x_1)(x_1x_2)\otimes x_2^{op}=$$

$$=-q(x_1)q(x_2)1\otimes x_1^{op}-q(x_1)q(x_2)x_1\otimes 1^{op}+q(x_1)x_2\otimes(x_2^{op}x_1^{op})+$$
$$+b(x_1,x_2)(x_1x_2)\otimes x_1^{op}-q(x_1)(x_1x_2)\otimes x_2^{op}.$$

Es gilt also $u^{-1}(1\otimes x_1^{op})e=u^{-1}(x_1\otimes 1^{op})e$ und daher auch $(1\otimes x_1^{op})e=(x_1\otimes 1^{op})e$. Der Fall $\underline{z=x_2}$ verläuft völlig analog. Aufwendiger dagegen ist der Fall $\underline{z=x_1x_2}$: Einerseits berechnet man:

$$u^{-1}((x_1x_2)\otimes 1^{op})e=-q(x_1)q(x_2)(x_1x_2)\otimes 1^{op}-q(x_2)(x_1x_2x_1)\otimes x_1^{op}-$$
$$-q(x_1)(x_1x_2x_2)\otimes x_2^{op}+b(x_1,x_2)(x_1x_2x_2)\otimes x_1^{op}+(x_1x_2x_1x_2)\otimes(x_1x_2)^{op}=$$

$$=-q(x_1)q(x_2)(x_1x_2)\otimes 1^{op}-q(x_2)b(x_1,x_2)x_1\otimes x_1^{op}+q(x_1)q(x_2)x_2\otimes x_1^{op}-$$
$$-q(x_1)q(x_2)x_1\otimes x_2^{op}+q(x_2)b(x_1,x_2)x_1\otimes x_1^{op}+$$
$$+b(x_1,x_2)(x_1x_2)\otimes(x_1x_2)^{op}-q(x_1)q(x_2)1\otimes(x_1x_2)^{op}=$$

$$=-q(x_1)q(x_2)(x_1x_2)\otimes 1^{op}+q(x_1)q(x_2)x_2\otimes x_1^{op}-q(x_1)q(x_2)x_1\otimes x_2^{op}+$$
$$+b(x_1,x_2)(x_1x_2)\otimes(x_1x_2)^{op}-q(x_1)q(x_2)1\otimes(x_1x_2)^{op};$$

und andererseits:

$$u^{-1}(1\otimes(x_1x_2)^{op})e=-q(x_1)q(x_2)1\otimes(x_1x_2)^{op}-q(x_2)x_1\otimes((x_1x_2)^{op}x_1^{op})-$$
$$-q(x_1)x_2\otimes((x_1x_2)^{op}x_2^{op})+b(x_1,x_2)x_2\otimes((x_1x_2)^{op}x_1^{op})+(x_1x_2)\otimes(x_1x_2)^{op}(x_1x_2)^{op}=$$

$$=-q(x_1)q(x_2)1\otimes(x_1x_2)^{op}-q(x_1)q(x_2)x_1\otimes x_2^{op}-q(x_1)b(x_1,x_2)x_2\otimes x_2^{op}+$$
$$+q(x_1)q(x_2)x_2\otimes x_1^{op}+q(x_1)b(x_1,x_2)x_2\otimes x_2^{op}+$$
$$+b(x_1,x_2)(x_1x_2)\otimes(x_1x_2)^{op}-q(x_1)q(x_2)(x_1x_2)\otimes 1^{op}=$$

$$=-q(x_1)q(x_2)1\otimes(x_1x_2)^{op}-q(x_1)q(x_2)x_1\otimes x_2^{op}+q(x_1)q(x_2)x_2\otimes x_1^{op}+$$
$$+b(x_1,x_2)(x_1x_2)\otimes(x_1x_2)^{op}-q(x_1)q(x_2)(x_1x_2)\otimes 1^{op}.$$

Daher gilt auch $((x_1x_2)\otimes 1^{op})e=(1\otimes(x_1x_2)^{op})e$ und wir haben damit bewiesen, dass unser konstruiertes $e\in C(E,q)^e$ tatsächlich separabilitäts-idempotent für $C(E,q)$ ist. Somit ist $C(E,q)$ separabel. $\square$

2.3. Arf-Algebren.

Sei (E, q) ein endlich erzeugter, projektiver, nichtsingulärer quadratischer R-Modul.

Definition 2.4. *Den Zentralisator von $C_0(E,q)$ in $C(E,q)$ nennt man auch* Arf- *oder* Diskriminanten-Algebra*, im folgenden bezeichnet mit*

$$A(E,q) := Z_{C(E,q)}C_0(E,q).$$

Die Graduierung $C(E,q) = C_0(E,q) \oplus C_1(E,q)$ induziert eine Graduierung auf $A(E,q)$: Ist nämlich $z = z_0 + z_1 \in A(E,q)$ mit $z_i \in C_i(E,q)$ $(i = 0,1)$, so gilt für alle $y \in C_0(E,q)$

$$z_0 y + z_1 y = zy = yz = yz_0 + yz_1$$

und es folgt, dass $z_0 y = yz_0$ und $z_1 y = yz_1$, also sind z_0, $z_1 \in A(E,q)$. Wir erhalten daher eine $\mathbb{Z}/2\mathbb{Z}$-Graduierung $A(E,q) = A_0(E,q) \oplus A_1(E,q)$ mit $A_i(E,q) = C_i(E,q) \cap A(E,q)$ für $i = 0$, 1.

Proposition 2.6. *Ist E zusätzlich treu, so gibt es Elemente $x_1, x_2, \ldots, x_k \in E$ und $r_1, r_2, \ldots, r_k \in R$, sodass*

$$r_1 q(x_1) + r_2 q(x_2) + \cdots + r_k q(x_k) = 1_R.$$

Endlich erzeugte, projektive, nichtsinguläre, treue quadratische R-Moduln sind also primitiv.

Beweis. Sei $\mathfrak{a} \subset R$ das Ideal, welches von $\{q(x) \mid x \in E\}$ erzeugt wird. Die Elemente von $\mathfrak{a}$ sind also von der Form $r_1 q(x_1) + r_2 q(x_2) + \cdots + r_k q(x_k)$ für ein $k \geq 0$ und gewisse $r_1, r_2, \ldots, r_k \in R$, $x_1, x_2, \ldots, x_k \in E$. Es ist also zu zeigen, dass $\mathfrak{a} = R$ gilt.

Angenommen $\mathfrak{a} \subsetneq R$. Dann gibt es ein maximales Ideal $\mathfrak{m} \subset R$, sodass $\mathfrak{a} \subset \mathfrak{m}$. Durch Lokalisierung in $\mathfrak{m}$ erhalten wir den quadratischen $R_\mathfrak{m}$-Modul $(E_\mathfrak{m}, q_\mathfrak{m}) := (E \otimes_R R_\mathfrak{m}, q_{R_\mathfrak{m}})$ und dieser erfüllt:

$$q_\mathfrak{m}(E_\mathfrak{m}) = R_\mathfrak{m}^2 q(E) \subset R_\mathfrak{m} q(E) = R_\mathfrak{m}\mathfrak{a} \subset \mathfrak{m}R_\mathfrak{m}$$

Da E endlich erzeugt, projektiv und treu ist, gilt $E_\mathfrak{m} \neq \{0\}$ und $E_\mathfrak{m}$ ist frei von endlichem Rang über $R_\mathfrak{m}$. Sei $\{x_1, x_2, \ldots, x_n\}$ eine Basis von $E_\mathfrak{m}$ und $b_\mathfrak{m}$ die zu $q_\mathfrak{m}$ assoziierte symmetrische Bilinearform. Da $b_\mathfrak{m}(x, x') = q_\mathfrak{m}(x + x') - q_\mathfrak{m}(x) - q_\mathfrak{m}(x')$ für alle $x, x' \in E_\mathfrak{m}$ gilt, folgt nach Obigem für die Gram-Matrix $(b_\mathfrak{m}(x_i, x_j))_{i,j=1}^n$:

$$\det(b_\mathfrak{m}(x_i, x_j))_{i,j=1}^n \in \mathfrak{m}R_\mathfrak{m}.$$

Da nach Voraussetzung (E, b) nichtsingulär ist, ist auch $(E_\mathfrak{m}, b_\mathfrak{m})$ nichtsingulär. Daher gilt $\det(b_\mathfrak{m}(x_i, x_j))_{i,j=1}^n \in R_\mathfrak{m}^*$ – ein Widerspruch. Daher muss $\mathfrak{a} = R$ gelten und also $1_R \in \mathfrak{a}$. $\square$

Satz 2.7. *Sei E zusätzlich treu. Dann gibt es einen eindeutig bestimmten R-Algebren-Automorphismus $\mu : A(E,q) \to A(E,q)$, sodass*

$$\mu^2 = id_{A(E,q)} \quad \textit{und} \quad xz = \mu(z)x \ \textit{ für alle } x \in E, z \in A(E,q).$$

Für diesen gilt außerdem: $Z(C(E,q)) = \{z \in A(E,q) \mid \mu(z) = z\}$.

Beweis. Nach obiger Proposition gibt es $r_1, r_2, \ldots, r_k \in R$ und $x_1, x_2, \ldots, x_k \in E$, sodass $r_1 q(x_1) + r_2 q(x_2) + \cdots + r_k q(x_k) = 1$.

Wir zeigen zunächst die Eindeutigkeit: Sei $z \in A(E,q)$ beliebig. Falls es $\mu :$ $A(E,q) \to A(E,q)$ mit den geforderten Eigenschaften gibt, so folgt aus $x_i z x_i =$

$\mu(z)x_ix_i = \mu(z)q(x_i)$:

$$\mu(z) = \mu(z)\sum_{i=1}^{k} r_i q(x_i) = \sum_{i=1}^{k} r_i x_i z x_i.$$

Dadurch ist μ eindeutig festgelegt.

Nun zur Existenz: Wir definieren $\mu(z) := \sum_{i=1}^{k} r_i x_i z x_i$ für alle $z \in A(E,q)$. Für $x \in E$ gilt:

$$\mu(z)x = \sum_{i=1}^{k} r_i x_i z(x_i x) = \sum_{i=1}^{k} r_i x_i(x_i x)z = \sum_{i=1}^{k} r_i q(x_i)xz = xz$$

und ebenso:

$$x\mu(z) = x\sum_{i=1}^{k} r_i x_i z x_i = \sum_{i=1}^{k} r_i(xx_i)zx_i = \sum_{i=1}^{k} r_i z(xx_i)x_i = \sum_{i=1}^{k} r_i zxq(x_i) = zx.$$

Daher folgt für alle $x, x' \in E$:

$$\mu(z)xx' = xzx' = xx'\mu(z),$$

also gilt $\mu(z) \in A(E,q)$. Aus $x\mu(z) = zx$ folgt nun, dass $z \in A(E,q)$ genau dann im Zentrum $Z(C(E,q))$ liegt, wenn $\mu(z) = z$ gilt. Wegen $\mu(r) = r$ für alle $r \in R$ und der Linearität von μ, ist μ daher ein R-Modul-Automorphismus $A(E,q) \to A(E,q)$. Für $z, z' \in A(E,q)$ gilt:

$$\mu(z)\mu(z') = \Big(\sum_{i=1}^{k} r_i x_i z x_i\Big)\Big(\sum_{j=1}^{k} r_j x_j z' x_j\Big) = \sum_{i,j=1}^{k} r_i r_j x_i z(x_i x_j)z' x_j =$$

$$= \sum_{i,j=1}^{k} r_i r_j x_i(x_i x_j)zz' x_j = \sum_{i,j=1}^{k} r_i r_j q(x_i)x_j zz' x_j =$$

$$= \Big(\sum_{i=1}^{k} r_i q(x_i)\Big)\Big(\sum_{j=1}^{k} r_j x_j zz' x_j\Big) = \mu(zz').$$

Somit ist μ also ein R-Algebren-Automorphismus und es bleibt zu zeigen, dass $\mu^2 = id_{A(E,q)}$:

$$\mu^2(z) = \sum_{j=1}^{k} r_j x_j\Big(\sum_{i=1}^{k} r_i x_i z x_i\Big)x_j = \sum_{i,j=1}^{k} r_j r_i x_j x_i z(x_i x_j) = \sum_{i,j=1}^{k} r_i r_j x_j x_i(x_i x_j)z =$$

$$= \sum_{i,j=1}^{k} r_i r_j q(x_i)x_j x_j z = \sum_{i,j=1}^{k} r_i q(x_i) r_j q(x_j)z = \Big(\sum_{i=1}^{k} r_i q(x_i)\Big)\Big(\sum_{j=1}^{k} r_j q(x_j)\Big)z = z.$$

□

Bemerkung: Ist $z \in A_0(E,q)$, so gilt: $\mu(z)x = xz \in C_1(E,q)$ für alle $x \in E$ und daher folgt $\mu(z)x^2 \in C_0(E,q)$, also $\mu(z) \in C_0(E,q)$. Somit gilt: $\mu(A_0(E,q)) \subset A_0(E,q)$ und man zeigt analog, dass $\mu(A_1(E,q)) \subset A_1(E,q)$. μ ist also ein graduierter R-Algebren-Automorphismus.

2.4. **Konjugation.**

Sei (E,q) ein endlich erzeugter, projektiver, nichtsingulärer quadratischer R-Modul und $A(E,q)$ die Arf-Algebra von (E,q).

Sei $\sigma := C(-id_E)$ der eindeutige R-Algebren-Homomorphismus, den der R-Modul-Homomorphismus $-id_E$ induziert (siehe Abschnitt 1.3). Es gilt $\sigma = id_{C_0(E,q)} \oplus -id_{C_1(E,q)}$. Sei nun $\beta := \sigma|_{A(E,q)}$. Für $z = z_0 + z_1 \in A(E,q) = A_0(E,q) \oplus A_1(E,q)$, $y \in C_0(E,q)$ gilt dann:

$$\beta(z)y = (z_0 - z_1)y = z_0 y - z_1 y = y z_0 - y z_1 = y(z_0 - z_1) = y\beta(z),$$

also liegt $\beta(z)$ wieder in $A(E,q)$ und β ist somit ein R-Algebren-Automorphismus auf $A(E,q)$. Da auch μ ein graduierter R-Algebren-Automorphismus auf $A(E,q)$ ist, gilt für $z = z_0 + z_1 \in A(E,q) = A_0(E,q) \oplus A_1(E,q)$:

$$\beta\mu\beta^{-1}(z) = \beta\mu(z_0 - z_1) = \beta(\mu(z_0) - \mu(z_1)) = \mu(z_0) + \mu(z_1) = \mu(z).$$

Es gilt also: $\beta\mu\beta^{-1} = \mu$.

Definition 2.5. *Der graduierte R-Algebren-Automorphismus $\alpha := \beta\mu = \mu\beta : A(E,q) \to A(E,q)$ heißt* Konjugation von $A(E,q)$.

Offensichtlich gilt $\alpha^2 = \beta\mu\mu\beta = id_{A(E,q)}$ und α ist wieder eine Involution. In den beiden folgenden Beispielen wollen wir nun die Konjugationen von Arf-Algebren zu freien R-Moduln von Rang 1 und 2 betrachten.

Beispiele:

(1) Sei (E,q) frei von Rang 1 und $\{x\}$ sei eine Basis von E. Es ist dann $\{1_{C(E,q)}, x\}$ eine Basis von $C(E,q)$ und die Clifford-Algebra ist daher kommutativ. Es folgt

$$A(E,q) := Z_{C(E,q)}C_0(E,q) = C(E,q)$$

und $\mu = id_{A(E,q)}$. Die Konjugation von $A(E,q)$ ist daher gegeben durch $\alpha = \beta = \sigma$. Die Graduierung auf $A(E,q)$ ist offenbar $A(E,q) = R \oplus E$. Da $A(E,q)$ eine freie R-Algebra von Rang 2 ist, gilt wegen $x^2 = q(x)$

$$A(E,q) \tilde{=} R[X]/(X^2 - q(x)).$$

Nach Voraussetzung ist (E,q) nichtsingulär und es gilt deshalb $b(x,x) = 2q(x) \in R^*$. Es folgt $4q(x) \in R^*$ und $A(E,q)$ ist daher separabel. Versieht man $A := R[X]/(X^2 - q(x))$ mit der Graduierung $A = R1_A \oplus Ra$ mit $a = X + (X^2 - q(x))$, so erhält obiger Isomorphismus, in Folge mit ψ_1 bezeichnet, die Graduierung. Die Konjugation ς auf A ist gegeben durch $\varsigma(r_0 1_A + r_1 a) = r_0 1_A - r_1 a$. Es gilt:

$$\psi_1(\alpha(r_0 1_{C(E,q)} + r_1 x)) = r_0 1_A + r_1\psi_1(\alpha(x)) = r_0 1_A - r_1\psi_1(x) =$$

$$= r_0 1_A - r_1 a = \varsigma(r_0 1_A + r_1 a) = \varsigma(\psi_1(r_0 1_{C(E,q)} + r_1 x)).$$

ψ_1 erhält also die Konjugationen.

(2) Sei nun (E,q) frei von Rang 2 mit Basis $\{x_1, x_2\}$. Es gilt dann nach Satz 2.4

$$A(E,q) = Z(C_0(E,q)) = C_0(E,q)$$

und wir erhalten die triviale Graduierung $A(E,q) = A(E,q) \oplus \{0\}$. Für die kanonische Involution $\gamma : z \mapsto \bar{z}$ auf $C(E,q)$ (siehe Abschnitt 2.2) gilt

$\gamma(C_0(E,q)) = C_0(E,q)$ und γ lässt sich daher zu einem Antiautomorphismus auf $A(E,q)$ einschränken. Da $C_0(E,q)$ kommutativ ist, ist $\gamma|_{A(E,q)}$ ein Automorphismus. Es gilt:

$$x_1(x_1x_2) = q(x_1)x_2 = (x_2x_1)x_1 = (\overline{x_1x_2})x_1, \ \textit{sowie}\ x_2(x_1x_2) = (\overline{x_1x_2})x_2.$$

Aufgrund der Eindeutigkeit des R-Algebren-Automorphismus μ auf $A(E,q)$, folgt $\mu = \gamma|_{A(E,q)}$. Wegen $\beta = id_{A(E,q)}$, ist die Konjugation α auf $A(E,q)$ gegeben durch $\alpha = \gamma|_{A(E,q)}$. Weil (E,q) nichtsingulär ist, ist die Determinante der Gram-Matrix invertierbar – es gilt also $4q(x_1)q(x_2) - b(x_1,x_2)^2 \in R^*$. Setzen wir nun $a := b(x_1,x_2), b := -q(x_1)q(x_2)$, so ist wegen $a^2 + 4b \in R^*$ die R-Algebra $A := R[X]/(X^2 - aX - b)$ separabel. Wir definieren nun einen R-Modul-Isomorphismus

$$\psi_2 : A(E,q) \to R[X]/(X^2 - aX - b)$$

durch $1_{C(E,q)} \mapsto 1_A,\ x_1x_2 \mapsto x := X + (X^2 - aX - b)$. Wegen

$$\psi_2((x_1x_2)^2) = \psi_2(x_1(b(x_1,x_2)1_{C(E,q)} - x_1x_2)x_2) =$$

$$= \psi_2(ax_1x_2 + b1_{C(E,q)}) = ax + b1_A = x^2 = \psi_2(x_1x_2)^2$$

ist ψ_2 ein R-Algebren-Isomorphismus. $A(E,q) = C_0(E,q)$ ist somit separabel. Da wir auch auf A nur die triviale Graduierung $A = A \oplus \{0\}$ haben, ist ψ_2 graduiert. Die Konjugation ς auf A ist gegeben durch $\varsigma(r_01_A + r_1x) = (r_0 + ar_1)1_A - r_1x$. Auch in diesem Fall erhält ψ_2 die Konjugationen:

$$\psi_2(\alpha(r_01_{C(E,q)} + r_1x_1x_2)) = r_01_A + r_1\psi_2(x_2x_1) = r_01_A + r_1\psi_2(b(x_1,x_2) - x_1x_2) =$$

$$= (r_0 + ar_1)1_A - r_1x = \varsigma(\psi_2(r_01_{C(E,q)} + r_1x_1x_2)).$$

Sei (E,q) endlich erzeugt, projektiv, nichtsingulär und treu. Wir wollen nun die Arf-Algebra $A(E,q)$ im Falle einer orthogonalen Zerlegung $E = E_1 \perp E_2$ untersuchen. Da E endlich erzeugt, projektiv und nichtsingulär ist, gilt dies auch für die Untermoduln E_1 und E_2. Sei $A(E_i,q_i)$ für $i = 0,1$ die Arf-Algebra zu $(E_i, q_i = q|E_i)$. Wir betrachten nun die Kette von Inklusionen

$$A(E_1,q_1) \otimes_R A(E_2,q_2) \to A(E_1,q_1) \otimes_R C(E_2,q_2) \to C(E_1,q_1) \otimes_R C(E_2,q_2).$$

Wir erhalten damit einen graduierten R-Algebren-Homomorphismus

$$A(E_1,q_1)\hat{\otimes}_R A(E_2,q_2) \to C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2),$$

wobei die Algebren-Multiplikation des graduierten Tensorproduktes $C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2)$ gegeben ist durch: $(z_1 \otimes z_2)(z_1' \otimes z_2') = (-1)^{ij}(z_1z_1' \otimes z_2z_2')$ für $z_2 \in C_i(E_1,q_1),\ z_1' \in C_j(E_2,q_2)$ (siehe Abschnitt 1.7). Durch Komposition mit dem graduierten R-Algebren-Isomorphismus $\phi : C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2) \to C(E,q)$ erhalten wir einen Homomorphismus

$$\Phi : A(E_1,q_1)\hat{\otimes}_R A(E_2,q_2) \to C(E,q)$$

von graduierten R-Algebren. Sei nun $\alpha_i = \beta_i\mu_i = \mu_i\beta_i$ (für $i = 0,1$) die Konjugation von $A(E_i,q_i)$. Da α_i ein graduierter R-Algebren-Automorphismus ist, ist auch $\alpha_1 \otimes \alpha_2$ ein graduierter R-Algebren-Automorphismus auf $A(E_1,q_1)\hat{\otimes}_R A(E_2,q_2)$. Wir definieren nun die R-Algebra $A(E_1,q_1) * A(E_2,q_2)$ durch:

$$A(E_1,q_1) * A(E_2,q_2) := \{z \in A(E_1,q_1)\hat{\otimes}_R A(E_2,q_2) \mid (\alpha_1 \otimes \alpha_2)(z) = z\}.$$

Lemma 2.8. *Sei (E, q) ein nichtsingulärer, treuer, endlich erzeugter, projektiver quadratischer R-Modul, für den es eine Zerlegung $E = E_1 \perp E_2$ gibt, wobei die Untermoduln E_1, E_2 frei von endlichem Rang seien. Es seien weiters auch $A(E_1, q_1)$ und $A(E_1, q_2)$ freie R-Moduln von endlichem Rang, wobei q_i durch $q|_{E_i}$ gegeben ist $(i = 1, 2)$. Dann ist die Einschränkung von Φ auf $A(E_1, q_1) * A(E_2, q_2)$ ein R-Algebren-Isomorphismus*

$$A(E_1, q_1) * A(E_2, q_2) \to A(E, q)$$

und die Involution $\alpha_1 \otimes id_{A(E_2,q_2)} = id_{A(E_1,q_1)} \otimes \alpha_2$ von $A(E_1, q_1) * A(E_2, q_2)$ entspricht der Konjugation α von $A(E, q)$.

Beweis. Da $A(E_1, q_1)$ frei ist, ist die Abbildung $A(E_1, q_1)\hat{\otimes}_R A(E_2, q_2) \to A(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$ injektiv und weil auch $C(E_2, q_2)$ frei ist, ist $A(E_1, q_1)\hat{\otimes}_R C(E_2, q_2) \to C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$ ebenfalls injektiv. Somit ist auch die Komposition $A(E_1, q_1)\hat{\otimes}_R A(E_2, q_2) \to C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$ injektiv und wir betrachten daher $A(E_1, q_1)\hat{\otimes}_R A(E_2, q_2)$ als Teilalgebra von $C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$.

Sei $D := C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$ und $D = D_0 \oplus D_1$ die Graduierung von D. Weil $\phi : D \to C(E, q)$ ein graduierter R-Algebren-Isomorphismus ist, gilt für $z \in Z_D D_0$:

$$\phi(z)y' = \phi(z)\phi(y) = \phi(zy) = \phi(yz) = \phi(y)\phi(z) = y'\phi(z)$$

für alle $y' = \phi(y) \in C_0(E, q)$. Daher folgt: $\phi(Z_D D_0) \subset Z_{C(E,q)} C_0(E, q) = A(E, q)$. Analog kann man auch $\phi^{-1}(A(E, q)) \subset Z_D D_0$ zeigen und es gilt daher $\phi(Z_D D_0) = A(E, q)$. Um die Behauptung zu beweisen, müssen wir also zeigen, dass $A(E_1, q_1) * A(E_2, q_2) = Z_D D_0$ gilt. Wegen $\alpha_i = \beta_i\mu_i = \mu_i\beta_i$ und somit $\alpha_1 \otimes \alpha_2 = (\beta_1\mu_1) \otimes (\mu_2\beta_2) = (\beta_1 \otimes \mu_2) \circ (\mu_1 \otimes \beta_2)$ ist die Bedingung $(\alpha_1 \otimes \alpha_2)(z) = z$ in der Definition von $A(E_1, q_1) * A(E_2, q_2)$ äquivalent zu $(\mu_1 \otimes \beta_2)(z) = (\beta_1 \otimes \mu_2)(z)$. Wir zeigen nun also:

$$Z_D D_0 = \{z \in A(E_1, q_1)\hat{\otimes}_R A(E_2, q_2) \mid (\mu_1 \otimes \beta_2)(z) = (\beta_1 \otimes \mu_2)(z)\}.$$

Es gilt: $D_0 = \big(C_0(E_1, q_1) \otimes C_0(E_2, q_2)\big) \oplus \big(C_1(E_1, q_1) \otimes C_1(E_2, q_2)\big)$ und D_0 wird daher als R-Algebra von $C_0(E_1, q_1) \otimes 1_{C(E_2,q_2)}$, $1_{C(E_1,q_1)} \otimes C_0(E_2, q_2)$ und $\{x_1 \otimes x_2 \mid x_1 \in E_1,\ x_2 \in E_2\}$ erzeugt.

- Zunächst zeigen wir, dass

$$Z_D\big((C_0(E_1, q_1) \otimes 1_{C(E_2,q_2)}) \cup (1_{C(E_1,q_1)} \otimes C_0(E_2, q_2))\big) = A(E_1, q_1)\hat{\otimes}_R A(E_2, q_2)$$

gilt.

Es sei also $z \in D$ derart, dass z sowohl $C_0(E_1, q_1) \otimes 1_{C(E_2,q_2)}$ als auch $1_{C(E_1,q_1)} \otimes C_0(E_2, q_2)$ zentralisiert. Sei $\{v_1, v_2, \ldots, v_k\}$ eine Basis von $C(E_2, q_2)$ und $u_i \in C(E_1, q_1)$ $(i = 1, 2, \ldots, k)$ derart, dass $z = \sum_{i=1}^k (u_i \otimes v_i)$ (die u_i sind dadurch eindeutig festgelegt). Es gilt dann für alle $z_0 \in C_0(E_1, q_1)$:

$$\sum_{i=1}^k (u_i z_0 \otimes v_i) = z(z_0 \otimes 1_{C(E_2,q_2)}) = (z_0 \otimes 1_{C(E_2,q_2)})z = \sum_{i=1}^k (z_0 u_i \otimes v_i).$$

Da $\{v_1, v_2, \ldots, v_k\}$ eine Basis ist, folgt $u_i z_0 = z_0 u_i$ und daher $u_i \in A(E_1, q_1)$ für alle $i = 1, 2, \ldots, k$. Es gilt also $z \in A(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$. Ist nun $\{u_1, u_2, \ldots, u_k\}$ (für ein $k \in \mathbb{N}$) eine Basis von $A(E_1, q_1)$ und $z = \sum_{i=1}^k (u_i \otimes v_i)$ für geeignete (eindeutige) $v_i \in C(E_2, q_2)$, so gilt analog:

$$\sum_{i=1}^k (u_i \otimes v_i z_0) = z(1_{C(E_1,q_1)} \otimes z_0) = (1_{C(E_1,q_1)} \otimes z_0)z = \sum_{i=1}^k (u_i \otimes z_0 v_i)$$

für alle $z_0 \in C_0(E_2, q_2)$. Weil $\{u_1, u_2, \dots, u_k\}$ eine Basis ist, folgt: $v_i z_0 = z_0 v_i$ und es muss also $v_i \in A(E_2, q_2)$ für alle $i = 1, 2, \dots, k$ gelten. Wir erhalten somit: $z \in A(E_1, q_1)\hat{\otimes}_R A(E_2, q_2)$.

Umgekehrt gilt für alle $z = \sum_{i=1}^k (u_i \otimes v_i) \in A(E_1, q_1)\hat{\otimes}_R A(E_2, q_2) \subset D$ trivialerweise:

$$z(z_0 \otimes 1_{C(E_2,q_2)}) = \sum_{i=1}^k (u_i z_0 \otimes v_i) = \sum_{i=1}^k (z_0 u_i \otimes v_i) = (z_0 \otimes 1_{C(E_2,q_2)})z$$

für alle $z_0 \in C_0(E_1, q_1)$, sowie

$$z(1_{C(E_1,q_1)} \otimes z_0) = \sum_{i=1}^k (u_i \otimes v_i z_0) = \sum_{i=1}^k (u_i \otimes z_0 v_i) = (1_{C(E_1,q_1)} \otimes z_0)z$$

für alle $z_0 \in C_0(E_2, q_2)$ und wir erhalten daher auch die umgekehrte Inklusion.

- Wir zeigen nun für $z \in A(E_1, q_1)\hat{\otimes}_R A(E_2, q_2)$:

$$z(x_1 \otimes x_2) = (x_1 \otimes x_2)z \quad \forall x_1 \in E_1,\, x_2 \in E_2 \iff (\mu_1 \otimes \beta_2)(z) = (\beta_1 \otimes \mu_2)(z).$$

Sei $z = \sum_{i=1}^k (u_i \otimes v_i)$ mit $u_i = u_{i_0} + u_{i_1} \in A(E_1, q_1) = A_0(E_1, q_1) \oplus A_1(E_1, q_1)$, $v_i = v_{i_0} + v_{i_1} \in A(E_2, q_2) = A_0(E_2, q_2) \oplus A_1(E_2, q_2)$ für $i = 1, 2, \dots, k$. Für $x_1 \in E_1 \subset C_1(E_1, q_1)$, $x_2 \in E_2 \subset C_1(E_2, q_2)$ gilt dann:

$$z(x_1 \otimes x_2) = \sum_{i=1}^k \big((u_{i_0} x_1 \otimes v_{i_0} x_2) - (u_{i_0} x_1 \otimes v_{i_1} x_2) + (u_{i_1} x_1 \otimes v_{i_0} x_2) - (u_{i_1} x_1 \otimes v_{i_1} x_2)\big) =$$

$$= \sum_{i=1}^k \big((x_1 \mu_1(u_{i_0}) \otimes v_{i_0} x_2) + (x_1 \mu_1(u_{i_0}) \otimes -v_{i_1} x_2) + (x_1 \mu_1(u_{i_1}) \otimes v_{i_0} x_2) +$$
$$+ (x_1 \mu_1(u_{i_1}) \otimes -v_{i_1} x_2)\big) = (x_1 \otimes 1_{C(E_2,q_2)})(\mu_1 \otimes \beta_2)(z)(1_{C(E_1,q_1)} \otimes x_2).$$

Analog zeigt man:

$$(x_1 \otimes x_2)z = (x_1 \otimes 1_{C(E_2,q_2)})(\beta_1 \otimes \mu_2)(z)(1_{C(E_1,q_1)} \otimes x_2).$$

Gilt nun $(\mu_1 \otimes \beta_2)(z) = (\beta_1 \otimes \mu_2)(z)$, so folgt daher $z(x_1 \otimes x_2) = (x_1 \otimes x_2)z$.

Um die umgekehrte Implikation zu zeigen, sei also $z(x_1 \otimes x_2) = (x_1 \otimes x_2)z$ für alle $x_1 \in E_1$, $x_2 \in E_2$. Es gilt dann nach Obigem

$$(x_1 \otimes 1_{C(E_2,q_2)})(\mu_1 \otimes \beta_2)(z)(1_{C(E_1,q_1)} \otimes x_2) = (x_1 \otimes 1_{C(E_2,q_2)})(\beta_1 \otimes \mu_2)(z)(1_{C(E_1,q_1)} \otimes x_2)$$

für alle $x_1 \in E_1$, $x_2 \in E_2$. Sei nun $x_1 \in E_1$ beliebig fix. Da E_2 frei (also insbesondere treu) und nichtsingulär ist, gibt es nach Proposition 2.6 Elemente $x_{2,1}, x_{2,2}, \dots, x_{2,k} \in E_2$ und $r_1, r_2, \dots, r_k \in R$, sodass $r_1 q_2(x_{2,1}) + r_2 q_2(x_{2,2}) + \dots + r_k q_2(x_{2,k}) = 1_{C(E_2,q_2)}$. Es gilt dann:

$$(x_1 \otimes 1_{C(E_2,q_2)})(\mu_1 \otimes \beta_2)(z) = \sum_{i=1}^k (x_1 \otimes 1_{C(E_2,q_2)})(\mu_1 \otimes \beta_2)(z)(1_{C(E_1,q_1)} \otimes r_i q(x_{2,i})) =$$

$$= \sum_{i=1}^k r_i\big((x_1 \otimes 1_{C(E_1,q_1)})(\mu_1 \otimes \beta_2)(z)(1_{C(E_1,q_1)} \otimes x_{2,i})\big)(1_{C(E_1,q_1)} \otimes x_{2,i}) =$$

$$= \sum_{i=1}^k r_i\big((x_1 \otimes 1_{C(E_1,q_1)})(\beta_1 \otimes \mu_2)(z)(1_{C(E_1,q_1)} \otimes x_{2,i})\big)(1_{C(E_1,q_1)} \otimes x_{2,i}) =$$

$$= (x_1 \otimes 1_{C(E_1,q_1)})(\beta_1 \otimes \mu_2)(z).$$

Wendet man Proposition 2.6 auf E_1 an und wiederholt die obige Vorgehensweise, so erhält man $(\mu_1 \otimes \beta_2)(z) = (\beta_1 \otimes \mu_2)(z)$ und damit die Behauptung.

- Zuletzt haben wir noch zu zeigen, dass $(\alpha_1 \otimes id_{A(E_2,q_2)}) = (id_{A(E_1,q_1)} \otimes \alpha_2)$ gilt und dass diese Involution von $A(E_1, q_1) * A(E_2, q_2)$ der Konjugation α von $A(E, q)$ entspricht.

Wegen $(\alpha_1 \otimes \alpha_2)(z) = z$ für alle $z \in A(E_1, q_1) * A(E_2, q_2)$ folgt sofort:

$$(\alpha_1 \otimes id_{A(E_2,q_2)})(z) = (\alpha_1 \otimes id_{A(E_2,q_2)}) \circ (\alpha_1 \otimes \alpha_2)(z) = (\alpha_1^2 \otimes \alpha_2)(z) = (id_{E_1} \otimes \alpha_2)(z)$$

und die erste Identität ist damit gezeigt. Sei nun $z' \in A(E, q)$ beliebig und $z := \phi^{-1}(z') \in A(E_1, q_1) * A(E_2, q_2)$. Seien $x_{2,1}, x_{2,2}, \ldots, x_{2,k} \in E_2$ und $r_1, r_2, \ldots, r_k \in R$ wie oben. Dann gilt für alle $x_1 \in E_1$:

$$z(x_1 \otimes 1_{C(E_2,q_2)}) = \sum_{i=1}^{k} r_i\big(z(x_1 \otimes x_{2,i})\big)(1_{C(E_1,q_1)} \otimes x_{2,i}) =$$

$$= \sum_{i=1}^{k} r_i\big((x_1 \otimes 1_{C(E_1,q_1)})(\mu_1 \otimes \beta_2)(z)(1_{C(E_1,q_1)} \otimes x_{2,i})\big)(1_{C(E_1,q_1)} \otimes x_{2,i}) =$$

$$= (x_1 \otimes 1_{C(E_2,q_2)})(\mu_1 \otimes \beta_2)(z)$$

und es folgt daher:

$$(x_1 \otimes 1_{C(E_2,q_2)})z = (x_1 \otimes 1_{C(E_2,q_2)})(\mu_1 \otimes \beta_2)\big((\mu_1 \otimes \beta_2)(z)\big) = (\mu_1 \otimes \beta_2)(z)(x_1 \otimes 1_{C(E_2,q_2)}).$$

Auf analoge Weise erhält man $(1_{C(E_1,q_1)} \otimes x_2)z = (\mu_1 \otimes \beta_2)(z)(1_{C(E_1,q_1)} \otimes x_2)$ für alle $x_2 \in E_2$. Es folgt daher für alle $x_1 \in E_1$, $x_2 \in E_2$ (man beachte hierbei, dass nach Abschnitt 1.8 E_i in $C(E, q)$ eingebettet werden kann):

$$x_1 z' = \phi((x_1 \otimes 1_{C(E_2,q_2)})z) = \phi\big((\mu_1 \otimes \beta_2)(z)(x_1 \otimes 1_{C(E_2,q_2)})\big) = \big(\phi \circ (\mu_1 \otimes \beta_2) \circ \phi^{-1}\big)(z')x_1,$$

$$x_2 z' = \big(\phi \circ (\mu_1 \otimes \beta_2) \circ \phi^{-1}\big)(z')x_2.$$

Da offensichtlich auch $\big(\phi \circ (\mu_1 \otimes \beta_2) \circ \phi^{-1}|_{A(E,q)}\big)^2 = id_{A(E,q)}$ gilt, folgt wegen der Eindeutigkeit des R-Algebren-Automorphismus $\mu : A(E, q) \to A(E, q)$ mit diesen Eigenschaften die Identität: $\mu = \phi \circ (\mu_1 \otimes \beta_2) \circ \phi^{-1}|_{A(E,q)}$. Trivialerweise gilt: $\beta = \phi \circ (\beta_1 \otimes \beta_2) \circ \phi^{-1}|_{A(E,q)}$ und es folgt somit für die Konjugation α auf $A(E, q)$:

$$\alpha = \beta\mu = \phi \circ (\beta_1 \otimes \beta_2) \circ \phi^{-1} \circ \phi \circ (\mu_1 \otimes \beta_2) \circ \phi^{-1}|_{A(E,q)} = \phi \circ (\alpha_1 \otimes id_{A(E_2,q_2)}) \circ \phi^{-1}|_{A(E,q)}.$$

Wir erhalten also $\alpha \circ \Phi|_{A(E_1,q_1)*A(E_2,q_2)} = \Phi \circ (\alpha_1 \otimes id_{A(E_2,q_2)})|_{A(E_1,q_1)*A(E_2,q_2)}$ und die Behauptung ist somit bewiesen. □

Bemerkung: Obiges Resultat gilt auch, wenn E_1, E_2, $A(E_1, q_1)$, $A(E_2, q_2)$ nicht frei sind; man muss dann voraussetzen, dass E_1, E_2 treu sind. Für das Folgende wird die eingeschränkte Aussage jedoch genügen.

2.5. **Spezielle Elemente.**

Sei (E, q) ein nichtsingulärer, endlich erzeugter, projektiver, treuer quadratischer R-Modul, dessen Rang nur gerade oder ungerade Werte annimmt; es gelte also entweder $rk_{R_\mathfrak{p}}(E \otimes_R R_\mathfrak{p}) \equiv 0 \pmod 2$ für alle Primideale $\mathfrak{p} \subset R$ oder $rk_{R_\mathfrak{p}}(E \otimes_R R_\mathfrak{p}) \equiv 1 \pmod 2$ für alle Primideale $\mathfrak{p} \subset R$.

Definition 2.6. *Ein Element $z \in C(E, q)$ heißt* speziell*, wenn $\{1_{C(E,q)}, z\}$ eine Basis von $A(E, q)$ als R-Modul ist und außerdem*

- *falls der Rang von E ungerade ist, die Eigenschaften $z \in C_1(E,q)$, $\alpha(z) = -z$ und $b := z^2 \in R^*$ erfüllt sind,*
- *falls der Rang von E gerade ist, die Eigenschaften $z \in C_0(E,q)$, $\alpha(z) = a - z$ und $z^2 = az + b$ für gewisse $a, b \in R$ mit $a^2 + 4b \in R^*$ erfüllt sind.*

Das Polynom $X^2 - aX - b \in R[X]$ (mit $a = 0$ falls der Rang von E ungerade ist) heißt das Polynom von z.

Offenbar impliziert die Existenz eines speziellen Elements notwendigerweise bereits, dass $A(E,q)$ frei von Rang 2 ist. Für nichtsinguläre, endlich erzeugte, projektive quadratische R-Moduln von ungeradem Rang muss stets $2 \in R^*$ gelten. Es folgt daher, dass auch im Fall ungeraden Ranges $a^2 + 4b = 0 + 4b$ in R invertierbar ist. Wegen

$$(a - 2z)^2 = a^2 - 4az + 4z^2 = a^2 - 4az + 4(az + b) = a^2 + 4b \in R^*$$

ist $a - 2z \in A(E,q)$ invertierbar und das Inverse ist gegeben durch $(a - 2z)^{-1} = (a^2 + 4b)^{-1}(a - 2z)$. Im Fall ungeraden Ranges gilt daher $z \in A(E,q)^*$ für jedes spezielle Element $z \in A(E,q)$.

Proposition 2.9. *Sei (E,q) ein nichtsingulärer, endlich erzeugter, projektiver, treuer quadratischer R-Modul von geradem oder ungeradem Rang. Sei z ein spezielles Element von $C(E,q)$ mit Polynom $X^2 - aX - b$ und $z' \in C(E,q)$ beliebig. Dann ist z' genau dann speziell, wenn*

- *im Fall ungeraden Ranges $z' = tz$ für ein $t \in R^*$ gilt,*
- *im Fall geraden Ranges $z' = r + tz$ für ein $r \in R$ und ein $t \in R^*$ gilt.*

Beweis. Ist z' speziell, so muss $\{1_{C(E,q)}, z'\}$ eine Basis von $A(E,q)$ sein und daher $z' = r + tz$ für ein $r \in R$ und ein $t \in R^*$ gelten.

Sei nun der Rang von E ungerade. Ist $z' = tz$, so ist z' offensichtlich ein spezielles Element, da dann $z' = tz \in C_1(E,q)$, $\alpha(z') = t\alpha(z) = -tz = -z'$ und $b' := z'^2 = (tz)^2 = t^2 b \in R^*$ gilt. Das zugehörige Polynom ist dann gegeben durch $X^2 - t^2 b$. Ist umgekehrt z' ein spezielles Element, so muss $z' \in C_1(E,q)$ gelten und es folgt daher $r = 0$, also $z' = tz$.

Sei nun der Rang von E gerade. Für $z' = r + tz$ gilt $z' \in C_0(E,q)$ und

$$\alpha(z') = r + t\alpha(z) = r + t(a - z) = 2r + ta - (r + tz) = (2r + ta) - z',$$
$$z'^2 = (r + tz)^2 = r^2 + 2rtz + t^2 z^2 = r^2 + 2rtz + t^2(az + b) =$$
$$= (2r + ta)(r + tz) - (2r + ta)r + r^2 + t^2 b = (2r + ta)z' + (t^2 b - tar - r^2).$$

Setzen wir $a' := 2r + ta$, $b' := t^2 b - tar - r^2$, so gilt:

$$a'^2 + 4b' = 4r^2 + 4tar + t^2 a^2 + 4t^2 b - 4tar - 4r^2 = t^2(a^2 + 4b) \in R^*.$$

$z' = r + tz$ ist daher ein spezielles Element mit Polynom $X^2 - (2r + ta)X - (t^2 b - tar - r^2)$. □

Bemerkung: Im Beweis des Lemmas haben wir auch gesehen, dass für zwei spezielle Elemente z, z' mit zugehörigen Polynomen $X^2 - aX - b$ bzw. $X^2 - a'X - b'$ (sowohl im Fall ungeraden Ranges als auch im Fall geraden Ranges) gilt: $a'^2 + 4b' = t^2(a^2 + 4b)$ für ein $t \in R^*$. Die Restklasse von $a^2 + 4b$ in $R^*/(R^*)^2$ ist also unabhängig von der Wahl des speziellen Elements.

Lemma 2.10. *Sei (E,q) wie im vorigen Lemma. $C(E,q)$ hat genau dann ein spezielles Element mit Polynom $X^2 - aX - b$, wenn $R[X]/(X^2 - aX - b)$ separabel ist und es einen Isomorphismus $R[X]/(X^2 - aX - b) \to A(E,q)$ von graduierten R-Algebren* *mit Konjugation gibt, wobei die Graduierung von $R[X]/(X^2 - aX - b)$ gegeben sei durch $R1 \oplus Rx$ mit $x = X + (X^2 - aX - b)$, falls der Rang von E ungerade ist, bzw. durch die triviale Graduierung, falls der Rang gerade ist, und falls E ungeraden Rang hat zusätzlich $a = 0$ gilt.*

Beweis. Sei zunächst der Rang von E ungerade. Ist z ein spezielles Element mit Polynom $X^2 - b$, so ist $\{1_{C(E,q)}, z\}$ eine Basis von $A(E,q)$ und wegen $z \in C_1(E,q)$ ist die Graduierung auf $A(E,q)$ gegeben durch $A(E,q) = R1_{C(E,q)} \oplus Rz$. Die freie R-Algebra $A := R[X]/(X^2 - b)$ ist wegen $4b \in R^*$ separabel und die Zerlegung $A = R1_A \oplus Rx$ mit $x = X + (X^2 - b)$ ist eine $\mathbb{Z}/2\mathbb{Z}$-Graduierung auf A. Sei nun die Abbildung $\psi : A \to A(E,q)$ gegeben durch $1_A \mapsto 1_{C(E,q)}$, $x \mapsto z$ sowie R-lineare Fortsetzung. Wegen $\psi(x^2) = \psi(b1_A) = b1_{C(E,q)} = z^2 = \psi(x)^2$ ist ψ ein R-Algebren-Isomorphismus und erhält offensichtlich die Graduierungen. Für die Konjugationen ς und α von A bzw. $A(E,q)$ gilt wegen $\alpha(z) = -z$:

$$\begin{aligned}\psi(\varsigma(r_0 1_A + r_1 x)) &= \psi(r_0 1_A - r_1 x) = r_0 1_{C(E,q)} - r_1 z = \\ &= \alpha(r_0 1_{C(E,q)} + r_1 z) = \alpha(\psi(r_0 1_A + r_1 x))\end{aligned}$$

für alle $r_0, r_1 \in R$. Damit ist auch gezeigt, dass ψ die Konjugationen erhält. Ist nun umgekehrt $A := R[X]/(X^2 - b) = R1_A \oplus Rx$ mit $x = X + (X^2 - b)$ separabel und $\psi : A \to A(E,q)$ ein graduierter R-Algebren-Isomorphismus, der die Konjugationen erhält, so definieren wir $z := \psi(x)$. Da ψ ein Isomorphismus ist, bilden $1_{C(E,q)} = \psi(1_A)$ und $z = \psi(x)$ eine Basis von $A(E,q)$ und weil ψ graduiert ist, gilt $z \in A_1(E,q) \subset C_1(E,q)$. Weiters folgt aus $\psi \circ \varsigma = \alpha \circ \psi$ für $r_0, r_1 \in R$:

$$r_0 1_{C(E,q)} - r_1 z = \psi \circ \varsigma(r_0 1_A + r_1 x) = \alpha \circ \psi(r_0 1_A + r_1 x) = r_0 1_{C(E,q)} + r_1 \alpha(z).$$

Da $\{1_{C(E,q)}, z\}$ eine Basis ist, folgt $\alpha(z) = -z$. Weiters gilt:

$$z^2 = \psi(x)^2 = \psi(x^2) = \psi(b1_A) = b1_{C(E,q)}.$$

Da A separabel ist, muss $4b \in R^*$ gelten; wegen $2 \in R^*$ (da der Rang von E ungerade und (E,q) nichtsingulär ist) folgt $b \in R^*$ und somit ist auch $z^2 \in R^*$ erfüllt – es ist also $z = \psi(x)$ ein spezielles Element von $C(E,q)$.

Sei nun der Rang von E gerade. Ist z ein spezielles Element, so ist $\{1_{C(E,q)}, z\}$ eine Basis von $A(E,q)$ und $z \in C_0(E,q)$. Wir erhalten daher die triviale Graduierung $A(E,q) = A(E,q) \oplus \{0\}$. Wegen $a^2 + 4b \in R^*$ ist die R-Algebra $A := R[X]/(X^2 - aX - b)$ separabel und ebenfalls trivial graduiert. Sei $x = X + (X^2 - aX - b)$ und $\psi : A \to A(E,q)$ der R-Modul-Homomorphismus, der gegeben ist durch $1_A \mapsto 1_{C(E,q)}$, $x \mapsto z$. Wegen $\psi(x)^2 = z^2 = az + b1_{C(E,q)} = \psi(ax + b1_A) = \psi(x^2)$ ist ψ ein R-Algebren-Isomorphismus. ψ erhält trivialerweise die Graduierung und es gilt:

$$\begin{aligned}\psi(\varsigma(r_0 1_A + r_1 x)) &= \psi((r_0 + r_1 a)1_A - r_1 x) = (r_0 + r_1 a)1_{C(E,q)} - r_1 z = \\ &= r_0 1_{C(E,q)} + r_1(a1_{C(E,q)} - z) = \alpha(\psi(r_0 1_A + r_1 x));\end{aligned}$$

ψ erhält also die Konjugation. Ist nun umgekehrt $A := R[X]/(X^2 - aX - b)$ separabel und $\psi : A = A \oplus \{0\} \to A(E,q)$ ein graduierter R-Algebren-Isomorphismus, der die Konjugationen erhält, so definieren wir analog zum ersten Fall $z := \psi(x)$ für $x = X + (X^2 - aX - b)$. Es ist dann $\{1_{C(E,q)}, z\}$ eine Basis von $A(E,q)$ und $z \in C_0(E,q)$. Wegen

$$\begin{aligned}(r_0 + ar_1)1_{C(E,q)} - r_1 z &= \psi \circ \varsigma(r_0 1_A + r_1 x) = \\ &= \alpha \circ \psi(r_0 1_A + r_1 x) = r_0 1_{C(E,q)} + r_1 \alpha(z)\end{aligned}$$

gilt auch $\alpha(z) = a1_{C(E,q)} - z$. Es gilt $z^2 = \psi(x)^2 = \psi(x^2) = \psi(ax + b1_A) = az + b1_{C(E,q)}$ und da A separabel ist, ist auch $a^2 + 4b \in R^*$ erfüllt. $\square$

Beispiele:

(1) Ist E frei von Rang 1 und $\{x\}$ eine Basis von E, so gilt $x \in C_1(E,q)$. Es ist $C(E,q)$ kommutativ, die Arf-Algebra ist gegeben durch $A(E,q) = C(E,q)$ und $\{1_{C(E,q)}, x\}$ ist eine Basis von $A(E,q)$. In Beispiel (1) aus Abschnitt 2.4 haben wir gesehen, dass in diesem Fall $\alpha = \sigma$ gilt und erhalten daher $\alpha(x) = -x$. Da (E,q) nichtsingulär ist, muss $2 \in R^*$ sowie $b(x,x) = 2q(x) \in R^*$ gelten, also auch $x^2 = q(x) \in R^*$. Somit haben wir gezeigt, dass x ein spezielles Element mit Polynom $X^2 - q(x)$ ist.

(2) Sei nun E frei von Rang 2 und $\{x_1, x_2\}$ eine Basis. Setze $z := x_1x_2 \in C_0(E,q)$. In Beispiel (2) aus Abschnitt 2.4 haben wir gesehen, dass in diesem Fall $A(E,q) = C_0(E,q)$ gilt und die Konjugation durch die Einschränkung der kanonischen Involution auf $A(E,q)$ gegeben ist. Es ist $\{1_{C(E,q)}, z\}$ eine Basis von $A(E,q)$ und z erfüllt:

$$\alpha(z) = \overline{x_1x_2} = x_2x_1 = b(x_1,x_2) - x_1x_2$$

$$z^2 = x_1x_2x_1x_2 = x_1(b(x_1,x_2) - x_1x_2)x_2 = b(x_1,x_2)z - q(x_1)q(x_2).$$

Setzen wir nun $a := b(x_1,x_2)$ und $b := -q(x_1)q(x_2)$, so gilt, da (E,q) nichtsingulär ist: $a^2+4b = b(x_1,x_2)^2 - 4q(x_1)q(x_2) \in R^*$. Daher ist z ein spezielles Element mit Polynom $X^2 - b(x_1,x_2)X + q(x_1)q(x_2)$.

Die beiden Beispiele zeigen insbesondere:

Lemma 2.11. *Ist (E,q) nichtsingulär und frei von Rang 1 oder 2, so besitzt $C(E,q)$ ein spezielles Element.*

Lässt sich (E,q) als orthogonale Summe zweier Untermoduln schreiben, so ist folgendes Resultat nützlich:

Lemma 2.12. *Sei (E,q) nichtsingulär und es gebe eine Zerlegung $E = E_1 \perp E_2$ mit E_1, E_2 frei von Rang $n_1 \geq 1$ bzw. $n_2 \geq 1$. Weiters existiere für $i = 1, 2$ in der Clifford-Algebra $C(E_i,q_i)$ zu $(E_i, q_i = q|_{E_i})$ ein spezielles Element z_i mit Polynom $X^2 - a_iX - b_i$. Dann besitzt auch $C(E,q)$ ein spezielles Element, nämlich $a_1a_2 1_{C(E,q)} - a_1z_2 - a_2z_1 + 2z_1z_2$ und dessen Polynom $X^2 - aX - b$ ist gegeben durch $a = a_1a_2$ und $b = a_1^2b_2 + a_2^2b_1 + (-1)^{n_1n_2}4b_1b_2$.*

Beweis. Für $i = 1, 2$ gilt: Da $C(E_i,q_i)$ ein spezielles Element mit Polynom $X^2 - a_iX - b_i$ besitzt, gibt es einen Isomorphismus $\psi_i : A_i := R[X]/(X^2 - a_iX - b_i) \to A(E_i,q_i)$ von graduierten R-Algebren mit Konjugation, wobei die Graduierung von A_i im Fall $n_i \equiv 1 \pmod 2$ durch $A_i = R1_{A_i} \oplus Rx_i$ mit $x_i = X + (X^2 - a_iX - b_i)$ gegeben ist, im Fall $n_i \equiv 0 \pmod 2$ trivial ist. Dabei ist ψ_i durch $x_i \mapsto z_i$ gegeben.

Sei die Teilalgebra P von $A_1 \hat{\otimes}_R A_2$ definiert durch:

$$P := \{p \in A_1 \hat{\otimes}_R A_2 \mid (\varsigma_1 \otimes \varsigma_2)(p) = p\},$$

wobei ς_i die Konjugation von A_i sei ($i = 1, 2$). Wir definieren $z := (x_1 \otimes x_2) + (\varsigma_1(x_1) \otimes \varsigma_2(x_2))$. Man kann nun zeigen, dass $z \in P$ und $\{1_P = 1_{A_1} \otimes 1_{A_2},\ z\}$ eine Basis von P ist. Weiters gilt (wie man durch längere Berechnungen sieht): $z^2 = b1_P + az$ für die gegebenen Elemente $a, b \in R$.
Ist nun $A := R[X]/(X^2 - aX - b)$, so erhalten wir durch $1_A \mapsto 1_P,\ x = X + (X^2 - aX - b) \mapsto z$ einen R-Algebren-Isomorphismus $\theta : A \to P$. Wir definieren nun eine Graduierung und eine Konjugation auf P: Gilt $n_1 + n_2 \equiv 1 \pmod 2$, so gilt $n_1 \equiv 1 \pmod 2$ oder $n_2 \equiv 1 \pmod 2$ und es folgt $a_1 = 0$ oder $a_2 = 0$; wir erhalten also $a = 0$ und $P = R1_P \oplus Rz$ ist eine Graduierung auf P. Im Fall $n_1 + n_2 \equiv 0 \pmod 2$ ist P trivial graduiert. Für alle $p \in P$ gilt: $(\varsigma_1 \otimes id_{A_2})(p) =$

$(\varsigma_1 \otimes id_{A_2}) \circ (\varsigma_1 \otimes \varsigma_2)(p) = (id_{A_1} \otimes \varsigma_2)(p)$ und wir definieren die Konjugation auf P daher durch $\varsigma_1 \otimes id_{A_2} = id_{A_1} \otimes \varsigma_2$. Offensichtlich erhält der R-Algebren-Isomorphismus θ die Graduierungen. Ist ς die Konjugation von A, so gilt:

$$\begin{aligned}
(\theta \circ \varsigma)(r_0 1_A + r_1 x) = \theta((r_0 + ar_1)1_A - r_1 x) = (r_0 + ar_1)1_P - r_1 z = \\
= (r_0 + ar_1)(1_{A_1} \otimes 1_{A_2}) - r_1\big((x_1 \otimes x_2) + (\varsigma_1(x_1) \otimes \varsigma_2(x_2))\big) = \\
= (r_0 + a_1 a_2 r_1)(1_{A_1} \otimes 1_{A_2}) - r_1(x_1 \otimes x_2) - a_1 a_2 r_1 (1_{A_1} \otimes 1_{A_2}) + \\
+ a_1 r_1 (1_{A_1} \otimes x_2) + a_2 r_1 (x_1 \otimes 1_{A_2}) - r_1(x_1 \otimes x_2) = \\
= r_0(1_{A_1} \otimes 1_{A_2}) + a_1 r_1 (1_{A_1} \otimes x_2) + a_2 r_1 (x_1 \otimes 1_{A_2}) - 2r_1(x_1 \otimes x_2) = \\
= r_0(1_{A_1} \otimes 1_{A_2}) + r_1\big((\varsigma_1(x_1) \otimes x_2) + (x_1 \otimes \varsigma_2(x_2))\big) = \\
= (\varsigma_1 \otimes id_{A_2})\big(r_0(1_{A_1} \otimes 1_{A_2}) + r_1((x_1 \otimes x_2) + (\varsigma_1(x_1) \otimes \varsigma_2(x_2)))\big) = \\
= (\varsigma_1 \otimes id_{A_2})(r_0 1_P + r_1 z) = \big((\varsigma_1 \otimes id_{A_2}) \circ \theta\big)(r_0 1_A + r_1 x).
\end{aligned}$$

θ ist somit ein graduierter R-Algebren-Isomorphismus, der die Konjugationen erhält.

Die Isomorphismen ψ_1, ψ_2 induzieren nun einen eindeutigen R-Algebren-Homomorphismus $(\psi_1 \otimes \psi_2) : A_1 \hat{\otimes}_R A_2 \to A(E_1, q_1) \hat{\otimes}_R A(E_2, q_2)$, der sich zu einem R-Algebren-Isomorphismus $P \to A(E_1, q_1) * A(E_2, q_2) = \{z \in A(E_1, q_1) \hat{\otimes}_R A(E_2, q_2) \mid (\alpha_1 \otimes \alpha_2) z = z\}$ einschränken lässt, wobei α_1, α_2 die Konjugationen von $A(E_1, q_1)$ bzw. $A(E_2, q_2)$ seien, und verträglich mit den Graduierungen und Konjugationen ist. Es gilt:

$$\begin{aligned}
(\psi_1 \otimes \psi_2)(z) = (z_1 \otimes z_2) + ((a_1 1_{C(E_1,q_1)} - z_1) \otimes (a_2 1_{C(E_2,q_2)} - z_2)) = \\
= a_1 a_2 (1_{C(E_1,q_1)} \otimes 1_{C(E_2,q_2)}) - a_1(1_{C(E_1,q_1)} \otimes z_2) - a_2(z_1 \otimes 1_{C(E_2,q_2)}) + 2(z_1 \otimes z_2).
\end{aligned}$$

Durch Verknüpfung mit dem R-Algebren-Isomorphismus $\Phi : A(E_1, q_1) * A(E_2, q_2) \to A(E, q)$ aus Lemma 2.8 erhalten wir einen R-Algebren-Isomorphismus $P \to A(E, q)$, der z in

$$\begin{aligned}
\Phi((\psi_1 \otimes \psi_2)(z)) = \\
= \phi\big(a_1 a_2 (1_{C(E_1,q_1)} \otimes 1_{C(E_2,q_2)}) - a_1(1_{C(E_1,q_1)} \otimes z_2) - a_2(z_1 \otimes 1_{C(E_2,q_2)}) + 2(z_1 \otimes z_2)\big) = \\
= a_1 a_2 1_{C(E,q)} - a_1 z_2 - a_2 z_1 + 2 z_1 z_2
\end{aligned}$$

überführt. Da die R-Algebren-Isomorphismen θ, $(\psi_1 \otimes \psi_2)$ und $\Phi|_{A(E_1,q_1)*A(E_2,q_2)}$ mit den jeweiligen Graduierungen und Konjugationen verträglich sind, gilt dies auch für die Komposition

$$\begin{aligned}
\Phi \circ (\psi_1 \otimes \psi_2) \circ \theta : \quad A = R[X]/(X^2 - aX - b) \to A(E, q), \\
x = X + (X^2 - aX - b) \mapsto a_1 a_2 1_{C(E,q)} - a_2 z_1 - a_1 z_2 + 2 z_1 z_2.
\end{aligned}$$

Wegen

$$\begin{aligned}
a^2 + 4b = a_1^2 a_2^2 + 4(a_1^2 b_2 + a_2^2 b_1 + (-1)^{n_1 n_2} 4 b_1 b_2) = \\
= \begin{cases} (a_1^2 + 4b_1)(a_2^2 + 4b_2) \in R^* & falls \;\; n_1 n_2 \equiv 0 \pmod 2 \\ -4 b_1 b_2 \in R^* & falls \;\; n_1 \equiv n_2 \equiv 1 \pmod 2). \end{cases}
\end{aligned}$$

ist A separabel und nach Lemma 2.10 und dessen Beweis folgt, dass $a_1 a_2 1_{C(E,q)} - a_1 z_2 - a_2 z_1 + 2 z_1 z_2$ ein spezielles Element von $C(E, q)$ mit Polynom $X^2 - aX - b$ ist. □

Lemma 2.13. *Sei (E, q) ein nichtsingulärer, endlich erzeugter, projektiver quadratischer R-Modul. Ist R ein lokaler Ring und $E \neq 0$, dann hat $C(E, q)$ ein spezielles Element.*

Beweis. Da E ein endlich erzeugter, projektiver Modul über einem lokalen Ring ist, ist E frei von endlichem Rang und weil E auch nichtsingulär ist, gibt es eine orthogonale Zerlegung $E = E_1 \perp E_2 \perp \ldots \perp E_k$, wobei die Untermoduln E_i nichtsingulär und frei von Rang 1 oder 2 sind ($i = 1, 2, \ldots, k$). Mittels Induktion über die Anzahl k der orthogonalen Summanden ergibt sich die Behauptung aus den beiden vorangegangenen Lemmata. □

2.6. **Spezielle Elemente und die Struktur von Clifford-Algebren.**

Der folgende Satz stellt nun einen Zusammenhang zur Struktur von Clifford-Algebren her.

Satz 2.14. *Sei (E, q) ein nichtsingulärer, treuer, endlich erzeugter, projektiver quadratischer R-Modul. Sei z ein spezielles Element in $C(E, q)$ mit Polynom $X^2 - aX - b$.*

- *Ist der Rang von E ungerade, so gilt: a=0,*
$$Z(C(E,q)) = A(E,q) \cong R[X]/(X^2 - b) = R1 \oplus Rx$$
mit $1 = 1_R + (X^2 - b),\ x = X + (X^2 - b)$
$$\textit{und} \quad Z(C_0(E,q)) = R.$$
Hat $X^2 - b$ eine Nullstelle in R, dann gilt $Z(C(E,q)) \cong R \oplus R$.
- *Ist der Rang von E gerade, so gilt:*
$$Z(C(E,q)) = R$$
$$\textit{und} \quad Z(C_0(E,q)) = A(E,q) \cong R[X]/(X^2 - aX - b)$$
mit der trivialen Graduierung. Hat $X^2 - aX - b$ eine Nullstelle in R, dann gilt $Z(C_0(E,q)) \cong R \oplus R$.

Beweis. Sei zunächst der Rang von E ungerade. Es ist dann $z \in C_1(E,q)$ und daher $\alpha(z) = -z = \beta(z)$ für $\beta = \sigma|_{A(E,q)}$. Da $\{1_{C(E,q)}, z\}$ eine Basis von $A(E,q)$ ist, folgt $\alpha = \beta$. Die Konjugation α ist jedoch definiert durch $\alpha = \beta\mu = \mu\beta$ und es muss daher $\mu = id_{A(E,q)}$ gelten. Daraus folgt: $Z(C(E,q)) = \{z \in A(E,q) \mid \mu(z) = z\} = A(E,q)$. Weil der Rang von E ungerade ist, gilt $a = 0$ und die Isomorphie $A(E,q) \cong R[X]/(X^2 - b) = R1 \oplus Rx$ von graduierten R-Algebren folgt aus Lemma 2.10. Wegen $z \in C_1(E,q)$ gilt andererseits auch: $Z(C_0(E,q)) = C_0(E,q) \cap A(E,q) = R$.

Ist nun der Rang von E gerade, so gilt $z \in C_0(E,q)$ und da $\{1_{C(E,q)}, z\}$ eine Basis von $A(E,q)$ ist, gilt daher $A(E,q) \subset C_0(E,q)$. Es folgt $Z(C_0(E,q)) = A(E,q)$ und die Isomorphie zu $R[X]/(X^2 - aX - b)$ erhalten wir aus Lemma 2.10. Sei nun $r_0 1_{C(E,q)} + r_1 z \in Z(C(E,q)) \subset A(E,q)$. Es gilt dann $r_0 1_{C(E,q)} + r_1 z = \mu(r_0 1_{C(E,q)} + r_1 z)$. Da $z \in C_0(E,q)$ muss $\beta = id_{A(E,q)}$ gelten und somit $\alpha = \mu$. Damit folgt:
$$r_0 1_{C(E,q)} + r_1 z = \alpha(r_0 1_{C(E,q)} + r_1 z) = (r_0 + ar_1) 1_{C(E,q)} - r_1 z$$
und wegen der linearen Unabhängigkeit von $\{1_{C(E,q)},\ z\}$ erhalten wir $ar_1 = 0$, sowie $2r_1 = 0$. Es gilt daher: $r_1(a^2 + 4b) = ar_1 a + 2r_1 2b = 0$. Da $a^2 + 4b \in R^*$, folgt $r_1 = 0$ und somit $Z(C(E,q)) = R$.

Sei nun $r \in R$ eine Nullstelle von $X^2 - aX - b$. Wir wollen zeigen, dass dann $R[X]/(X^2 - aX - b) \cong R[X]/(X^2 - X)$ gilt. Seien $s_0 := (a^2 + 4b)^{-1}(ar + 2b)$ und $s_1 := (a^2 + 4b)^{-1}(a - 2r)$. Wegen

$s_1^2 = (a^2 + 4b)^{-2}(a^2 - 4ar + 4r^2) = (a^2 + 4b)^{-2}(a^2 - 4ar + 4(ar + b)) = (a^2 + 4b)^{-1}$

ist s_1 invertierbar. Daher ist $\{1, s_0+s_1x\}$ mit $1 = 1_R+(X^2-aX-b)$, $x = X+(X^2-aX-b)$ eine Basis von $R[X]/(X^2-aX-b)$. Wir definieren nun $\psi : R[X]/(X^2-X) \to R[X]/(X^2-aX-b)$ durch $1' = 1_R+(X^2-X) \mapsto 1$, $x' = X+(X^2-X) \mapsto s_0+s_1x$ und lineare Fortsetzung. Es gilt:

$$s_0^2 + bs_1^2 = (a^2+4b)^{-2}(a^2r^2+4abr+4b^2+b(a^2-4ar+4r^2)) =$$
$$= (a^2+4b)^{-2}((a^2+4b)r^2+(a^2+4b)b) = (a^2+4b)^{-1}(ar+b+b) = s_0,$$

sowie

$$a^2+4b = a^2-2ar+2ar+4b = (a^2+4b)(as_1+2s_0), \quad \textit{also } \; as_1+2s_0 = 1$$

und daher

$$\psi(x')^2 = (s_0+s_1x)^2 = s_0^2+2s_0s_1x+s_1^2(ax+b) =$$
$$= s_0^2+bs_1^2+s_1(2s_0+as_1)x = s_0+s_1x = \psi(x') = \psi(x'^2).$$

ψ ist also ein Isomorphismus von R-Algebren und es gilt somit

$$R[X]/(X^2-aX-b) \tilde{=} R[X]/(X^2-X).$$

$R \oplus R$ ist der Ring $R \times R$ mit der R-Algebrenstruktur $r(r_1, r_2) = (rr_1, rr_2)$. Es bilden $(1_R, 1_R)$, $(0_R, 1_R)$ eine Basis von $R \oplus R$ als R-Modul. Bilden wir nun $(1_R, 1_R)$ auf $1'$ und $(0_R, 1_R)$ auf x' ab, so erhalten wir durch lineare Fortsetzung einen R-Modul-Isomorphismus $R \oplus R \to R[X]/(X^2-X)$. Wegen $(0_R, 1_R)^2 = (0_R, 1_R)$ und $x'^2 = x'$ sieht man leicht, dass diese Abbildung ein Isomorphismus von R-Algebren ist. □

Wir werden das folgende Resultat verwenden:

Proposition 2.15. *Sei (E, q) ein nichtsingulärer, endlich erzeugter, projektiver quadratischer R-Modul, dessen Rangfunktion nur gerade oder ungerade Werte annimmt. Weiters sei $z \in C(E, q)$ ein spezielles Element mit Polynom $X^2 - aX - b$.*

- *Ist der Rang von E ungerade, so gilt:*
$$C_0(E, q) = zC_1(E, q) \quad \textit{und} \quad C_1(E, q) = zC_0(E, q).$$
- *Ist der Rang von E gerade, so gilt:*
$$C_0(E, q) = Z_{C(E,q)}(z) \quad \textit{und} \quad C_1(E, q) = \{c \in C(E, q) \mid cz + zc = ac\}.$$

Beweis. Sei zunächst der Rang von E ungerade. Es gilt dann $z \in C_1(E, q)$ und $z^2 = b \in R^*$ und wir erhalten daher:

$$C_0(E, q) = bC_0(E, q) = z^2C_0(E, q) \subset zC_1(E, q) \subset C_0(E, q).$$

Damit ist die erste Gleichung gezeigt. Analog ergibt sich aus

$$C_1(E, q) = bC_1(E, q) = z^2C_1(E, q) \subset zC_0(E, q) \subset C_1(E, q)$$

auch die Gleichung $C_1(E, q) = zC_0(E, q)$.

Sei nun der Rang von E gerade. Da $z \in A(E, q) = Z_{C(E,q)}C_0(E, q)$, gilt klarerweise $C_0(E, q) \subset Z_{C(E,q)}(z)$. Wir wollen zunächst die Inklusion $C_1(E, q) \subset \{c \in C(E, q) \mid cz+zc = ac\}$ zeigen. Der R-Modul $C_1(E, q)$ wird von allen Produkten $x_1x_2 \ldots x_{2k+1}$ mit $k \geq 0$ erzeugt und es genügt daher zu zeigen, dass all diese Produkte in $\{c \in C(E, q) \mid cz + zc = ac\}$ liegen. Dazu verwenden wir Induktion über k. Da $z \in C_0(E, q)$, gilt $\alpha(z) = \mu\beta(z) = \mu(z)$ und für $x \in E$ folgt daher:

$$(a - z)x = \alpha(z)x = \mu(z)x = xz$$

– damit ist die Behauptung für $k = 0$ bewiesen. Sei die Behauptung für $k - 1 \geq 0$ bereits gezeigt. Für $c_1 = c_1' x_{2k} x_{2k+1} \in C_1(E,q)$ mit $c_1' = x_1 x_2 \dots x_{2(k-1)+1}$ gilt dann:

$$ac_1 = ac_1' x_{2k} x_{2k+1} = (c_1' z + zc_1') x_{2k} x_{2k+1} = c_1'(zx_{2k}) x_{2k+1} + zc_1 =$$
$$= c_1'(ax_{2k} - x_{2k} z) x_{2k+1} + zc_1 = ac_1 - c_1' x_{2k}(zx_{2k+1}) + zc_1 =$$
$$= ac_1 - ac_1 + c_1 z + zc_1 = c_1 z + zc_1.$$

Damit haben wir $C_1(E,q) \subset \{c \in C(E,q) \mid cz + zc = ac\}$ bewiesen.
Ist $c \in Z_{C(E,q)}(z) \cap \{c \in C(E,q) \mid cz + zc = ac\}$, so gilt $(a - 2z)c = 0$. Zu Beginn von Abschnitt 2.5 haben wir gesehen, dass $a - 2z$ invertierter ist; es folgt daher $c = 0$. Wir erhalten somit:

$$Z_{C(E,q)}(z) \cap \{c \in C(E,q) \mid cz + zc = ac\} = \{0\}.$$

Da $C_1(E,q) \in \{c \in C(E,q) \mid cz + zc = ac\}$, folgt nun $Z_{C(E,q)}(z) \cap C_1(E,q) = \{0\}$ und somit die Inklusion $Z_{C(E,q)}(z) \subset C_0(E,q)$ – es gilt also $C_0(E,q) = Z_{C(E,q)}(z)$. Weiter erhalten wir wegen $C_0(E,q) \cap \{c \in C(E,q) \mid cz + zc = ac\} = \{0\}$ nun auch $\{c \in C(E,q) \mid cz + zc = ac\} \subset C_1(E,q)$ und somit die letzte Gleichung. □

Proposition 2.16. *Sei (E,q) ein endlich erzeugter, projektiver und nichtsingulärer quadratischer R-Modul, dessen Rangfunktion nur ungerade Werte annimmt. Dann gilt:*

$$C(E,q) \tilde{=} C_0(E,q) \otimes_R Z(C(E,q)).$$

Beweis. Wir betrachten zunächst den Fall, dass R ein lokaler Ring ist. Sei f die Einbettung $C_0(E,q) \hookrightarrow C(E,q)$ und g die Einbettung $Z(C(E,q)) \hookrightarrow C(E,q)$. Es gilt offenbar $f(y)g(c) = yc = cy = g(c)f(y)$ für alle $y \in C_0(E,q),\ c \in Z(C(E,q))$. Aus der universellen Eigenschaft des Tensorproduktes von Algebren folgt daher, dass f und g einen Homomorphismus $\psi : C_0(E,q) \otimes_R Z(C(E,q)) \to C(E,q)$ von R-Algebren induzieren, der $\psi(y \otimes c) = f(y)g(c) = yc$ für alle $y \in C_0(E,q),\ c \in Z(C(E,q))$ erfüllt. Wir wollen nun eine Umkehrabbildung zu ψ konstruieren.
Da R lokal ist, existiert ein spezielles Element $z \in C(E,q)$ und da der Rang von E ungerade ist, ist dieses invertierbar in $A(E,q) = Z(C(E,q))$. Wegen $C_1(E,q) = zC_0(E,q)$ gibt es daher für alle $c' \in C(E,q)$ eine eindeutige Darstellung $c' = y_1 + zy_2$ mit $y_1,\ y_2 \in C_0(E,q)$. Wir definieren nun eine Abbildung $\psi' : C(E,q) \to C_0(E,q) \otimes Z(C(E,q))$ durch $c' = y_1 + zy_2 \mapsto (y_1 \otimes 1_{C(E,q)}) + (y_2 \otimes z)$. Diese ist offensichtlich R-linear und es gilt für alle $c' = y_1 + zy_2 \in C(E,q)$:

$$\psi \circ \psi'(c') = \psi((y_1 \otimes 1_{C(E,q)}) + (y_2 \otimes z)) = y_1 + y_2 z = c',$$

sowie für alle $y \otimes c = y \otimes (r_0 1_{C(E,q)} + r_1 z) \in C_0(E,q) \otimes_R Z(C(E,q))$:

$$\psi' \circ \psi(y \otimes c) = \psi'(yc) = \psi'(cy) = \psi'((r_0 1_{C(E,q)} + r_1 z)y) = \psi'(r_0 y + zr_1 y) =$$
$$= (r_0 y \otimes 1_{C(E,q)}) + (r_1 y \otimes z) y \otimes (r_0 1_{C(E,q)} + r_1 z) = y \otimes c.$$

Es gilt daher, dass ψ' invers zu ψ ist und somit ψ ein Isomorphismus ist.

Ist nun R ein beliebiger (kommutativer) Ring (mit Eins) und $\mathfrak{p} \subset R$ ein Primideal, so gilt nach Obigem für den endlich erzeugten, freien $R_\mathfrak{p}$-Modul $E_\mathfrak{p}$ die Isomorphie

$$C(E_\mathfrak{p}, q_{R_\mathfrak{p}}) \tilde{=} C_0(E_\mathfrak{p}, q_{R_\mathfrak{p}}) \otimes_{R_\mathfrak{p}} Z(C(E_\mathfrak{p}, q_{R_\mathfrak{p}})).$$

Nach Satz 1.9 gilt daher:

$$C(E,q) \otimes_R R_\mathfrak{p} \tilde{=} \big(C_0(E,q) \otimes_R R_\mathfrak{p}\big) \otimes_{R_\mathfrak{p}} \big(A(E,q) \otimes_R R_\mathfrak{p}\big) \tilde{=} \big(C_0(E,q) \otimes_R A(E,q)\big) \otimes_R R_\mathfrak{p},$$

wobei wir die Isomorphie $A(E_\mathfrak{p}, q_{R_\mathfrak{p}}) \tilde{=} A(E,q) \otimes_R R_\mathfrak{p}$ verwendet haben. Da dies für alle Primideale $\mathfrak{p} \subset R$ gilt, folgt $C(E,q) \tilde{=} C_0(E,q) \otimes_R A(E,q)$ und somit die Behauptung. $\square$

2.7. **Skalierte quadratische Formen und das Tensorprodukt von Clifford-Algebren.**

Definition 2.7. *Sei (E,q) ein quadratischer R-Modul und sei $u \in R^*$. Die* skalierte quadratische Form ${}^u q$ *auf E ist definiert durch*

$$ {}^u q(x) := uq(x) $$

für alle $x \in E$.

Satz 2.17. *Sei (E,q) ein nichtsingulärer, endlich erzeugter, projektiver quadratischer R-Modul, für den es eine orthogonale Zerlegung $E = E_1 \perp E_2$ gebe, wobei der Rang von E_1 entweder gerade oder ungerade sei. Weiters habe $C(E_1, q_1)$ ein spezielles Element z mit Polynom $X^2 - aX - b$ und es sei $u := a^2 + 4b$.*

- *Falls der Rang von E_1 ungerade ist, so gilt:*
$$C_0(E,q) \tilde{=} \big(C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2)\big)_0 \tilde{=} C_0(E_1,q_1) \otimes_R C(E_2, {}^{-u} q_2).$$
- *Ist der Rang von E_1 gerade, so gilt:*
$$C(E,q) \tilde{=} C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2) \tilde{=} C(E_1,q_1) \otimes_R C(E_2, {}^u q_2).$$

Beweis. Die Isomorphien

$$C_0(E,q) \tilde{=} \big(C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2)\big)_0 \text{ und } C(E,q) \tilde{=} C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2)$$

haben wir bereits in Abschnitt 1.7 bewiesen. Es bleibt daher jeweils die zweite Isomorphie zu zeigen. Es sei $w := a - 2z$. Dann gilt $w^2 = a^2 + 4b \in R^*$ und $w \in A(E_1, q_1)$ (siehe Abschnitt 2.5).

- Sei nun zunächst der Rang von E_1 ungerade.

Es gilt dann wegen $z \in C_1(E_1, q_1)$ und $a = 0$ auch $w \in C_1(E_1, q_1)$. Ist

$$D := \big(R1_{C(E_1,q_1)}\hat{\otimes}_R C_0(E_2,q_2)\big) \oplus \big(Rw\hat{\otimes}_R C_1(E_2,q_2)\big),$$

so bildet D eine Teilalgebra von $\big(C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2)\big)_0$. Da $w \in A(E_1,q_1)$, kommutieren alle Elemente von D mit jenen von $C_0(E_1,q_1)\hat{\otimes}_R R1_{C(E_2,q_2)}$. Aus der universellen Eigenschaft des Tensorproduktes von Algebren, sowie der Isomorphie $C_0(E_1,q_1) \tilde{=} C_0(E_1,q_1)\hat{\otimes}_R R1_{C(E_2,q_2)}$ folgt nun, dass es einen eindeutigen Homomorphismus

$$\psi_1 : C_0(E_1,q_1) \otimes_R D \to \big(C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2)\big)_0$$

von R-Algebren gibt, sodass $\psi_1(c \otimes d) = (c \otimes 1_{C(E_2,q_2)})d$ für alle $c \in C_0(E_1,q_1),\ d \in D$ gilt. Wegen $2 \in R^*$ folgt aus Proposition 2.15:

$$wC_0(E_1,q_1) = 2zC_0(E_1,q_1) = zC_0(E_1,q_1) = C_1(E_1,q_1).$$

Das Erzeugnis von D und $C_0(E_1,q_1)\hat{\otimes}_R R1_{C(E_2,q_2)}$ ist somit gerade die R-Algebra

$$\big(C_0(E_1,q_1)\hat{\otimes}_R C_0(E_2,q_2)\big) \oplus \big(C_1(E_1,q_1)\hat{\otimes}_R C_1(E_2,q_2)\big) = \big(C(E_1,q_1)\hat{\otimes}_R C(E_2,q_2)\big)_0$$

– der Homomorphismus ψ_1 von R-Algebren ist also surjektiv. Wir wollen nun zeigen, dass ψ_1 sogar ein Isomorphismus ist. Da $\{1_{C(E_1,q_1)}, w\}$ eine Basis des freien R-Moduls $A(E_1,q_1)$ ist, ist insbesondere Rw endlich erzeugt und projektiv. Weil E_1, E_2 endlich erzeugt und projektiv sind, folgt aus 1.14, dass auch $C(E_i,q_i)$ und $C_j(E_i,q_i)$

für $i = 1, 2,\ j = 0, 1$ endlich erzeugt und projektiv sind. Da das Tensorprodukt endlich erzeugter, projektiver R-Moduln wieder endlich erzeugt und projektiv ist, sind $C_0(E_1, q_1) \otimes_R D$ und $\big(C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)\big)_0$ endlich erzeugt und projektiv. Für ein beliebiges Primideal $\mathfrak{p} \subset R$ gilt:

$$rg_{\mathfrak{p}}(C_0(E_1, q_1) \otimes_R D) = rg_{\mathfrak{p}}(C_0(E_1, q_1))\big(rg_{\mathfrak{p}}(C_0(E_2, q_2)) + rg_{\mathfrak{p}}(C_1(E_2, q_2))\big) =$$

$$= \frac{1}{2} rg_{\mathfrak{p}}(C(E_1, q_1)) rg_{\mathfrak{p}}(C(E_2, q_2)) = rg_{\mathfrak{p}}\big(\big(C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)\big)_0\big),$$

wobei wir hier für einen R-Modul A zur einfacheren Notation $rg_{R_{\mathfrak{p}}} A_{\mathfrak{p}}$ mit $rg_{\mathfrak{p}}(A)$ bezeichnen. Die jeweiligen Rangfunktionen stimmen also überein und der surjektive Homomorphismus ψ_1 zwischen den beiden endlich erzeugten, projektiven R-Algebren muss daher ein Isomorphismus sein.

Wir betrachten nun die Abbildung $\delta : E_2 \to D$, die gegeben ist durch $\delta(x) = w \otimes x$ für alle $x \in E_2$. Wegen $w^2 = u$ gilt:

$$\delta(x)^2 = (w \otimes x)^2 = -w^2 \otimes x^2 = -uq(x)(1_{C(E_1,q_1)} \otimes 1_{C(E_2,q_2)}).$$

Aus der universellen Eigenschaft der Clifford-Algebra zu $(E_2, {}^{-u} q_2)$ folgt nun die Existenz eines eindeutigen Homomorphismus $\psi_2 : C(E_2, {}^{-u} q_2) \to D$ von R-Algebren, sodass $\psi_2(x) = w \otimes x$ für alle $x \in E_2$. Da $w^2 \in R^*$ und $C(E_2, {}^{-u} q_2)$ als R-Algebra von E_2 erzeugt wird, sind $R1_{C(E_1,q_1)}\hat{\otimes}_R C_0(E_2, q_2)$ und $Rw\hat{\otimes}_R C_1(E_2, q_2)$ im Bild von ψ_2 enthalten – also ist ψ_2 ein surjektiver Homomorphismus von endlich erzeugten, projektiven R-Algebren. Offenbar gilt für alle Primideale $\mathfrak{p} \subset R$:

$$rg_{\mathfrak{p}}(C(E_2, {}^{-u} q_2)) = 2^{rg_{\mathfrak{p}} E_2} = rg_{\mathfrak{p}}(D).$$

Die Rangfunktionen stimmen also überein und es folgt, dass ψ_2 ein Isomorphismus ist.

Durch Verknüpfung erhalten wir nun einen Isomorphismus

$$\psi_1 \circ (id_{C_0(E_1,q_1)} \otimes \psi_2) : C_0(E_1, q_1) \otimes_R C(E_2, {}^{-u} q_2) \to \big(C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)\big)_0$$

von R-Algebren und die Aussage für den Fall, dass E_1 ungeraden Rang hat, ist somit bewiesen.

- Sei der Rang von E_1 gerade.

Es sind dann z und $w = a - 2z$ in $C_0(E_1, q_1)$. Sei die Teilalgebra D von $C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$ definiert durch $D = R1_{C(E_1,q_1)}\hat{\otimes}_R C_0(E_2, q_2) + Rw\hat{\otimes}_R C_1(E_2, q_2)$. Trivialerweise kommutiert $R1_{C(E_1,q_1)}\hat{\otimes}_R C_0(E_2, q_2)$ mit $C(E_1, q_1)\hat{\otimes}_R R1_{C(E_2,q_2)}$ sowie w mit $C_0(E_1, q_1)$. Für $c \in C_1(E_1, q_1)$ gilt nach Proposition 2.15:

$$wc = ac - 2zc = ac - 2(ac - cz) = -ac + 2cz = -cw.$$

Wir erhalten damit für $c \in C_1(E_1, q_1),\ c' \in C_1(E_2, q_2)$:

$$(w \otimes c')(c \otimes 1_{C(E_2,q_2)}) = -wc \otimes c' = cw \otimes c' = (c \otimes 1_{C(E_2,q_2)})(w \otimes c').$$

Daher kommutieren alle Elemente von D mit jenen von $C(E_1, q_1)\hat{\otimes}_R R1_{C(E_2,q_2)}$. Betten wir nun die beiden Teilalgebren D und $C(E_1, q_1)\hat{\otimes}_R R1_{C(E_2,q_2)}$ in $C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$ ein, so erhalten wir wegen der universellen Eigenschaft des Tensorproduktes von Algebren und der Isomorphie $C(E_1, q_1)\hat{\otimes}_R R1_{C(E_2,q_2)} \tilde{=} C(E_1, q_1)$ einen eindeutigen R-Algebren-Homomorphismus

$$\psi_1 : C(E_1, q_1) \otimes_R D \to C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$$

mit $\psi(c \otimes d) = (c \otimes 1_{C(E_2,q_2)})d$. Wir wollen nun zeigen, dass diese Abbildung surjektiv ist. Seien also $c_1 \in C(E_1, q_1),\ c_2 \in C(E_2, q_2)$ beliebig. Ist $c_2 \in C_0(E_2, q_2)$, so liegt

$c_1 \otimes c_2 = (c_1 \otimes 1_{C(E_2,q_2)})(1_{C(E_1,q_1)} \otimes c_2)$ wegen $c_1 \in C(E_1, q_1)$, $(1_{C(E_1,q_1)} \otimes c_2) \in D$ offenbar im Bild von ψ_1. Ist $c_2 \in C_1(E_2, q_2)$, so gilt:

$$c_1 \otimes c_2 = uc_1 \otimes u^{-1}c_2 = (c_1 w \otimes 1_{C(E_2,q_2)})(w \otimes u^{-1}c_2) = \psi_1(c_1 w \otimes (w \otimes u^{-1}c_2))$$

– es liegt also auch in diesem Fall $c_1 \otimes c_2$ im Bild von ψ_1. Da $C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$ von den Elementen $c_1 \otimes c_2$ mit $c_1 \in C(E_1, q_1)$, $c_2 \in C(E_2, q_2)$ erzeugt wird, folgt daraus die Surjektivität des Homomorphismus ψ_1 von R-Algebren. Da $C(E_1, q_1) \otimes_R D$ und $C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$ endlich erzeugt und projektiv sind und für jedes Primideal $\mathfrak{p} \subset R$

$$\begin{aligned} rg_{\mathfrak{p}}(C(E_1, q_1) \otimes_R D) &= 2^{rg_{\mathfrak{p}} E_1}(2 \cdot 2^{rg_{\mathfrak{p}} E_2 - 1}) = \\ &= 2^{rg_{\mathfrak{p}} E_1} 2^{rg_{\mathfrak{p}} E_2} = rg_{\mathfrak{p}}(C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)) \end{aligned}$$

gilt – also die jeweiligen Rangfunktionen übereinstimmen – folgt, dass ψ_1 ein Isomorphismus ist.

Sei $\delta : E_2 \to D$, $\delta(x) := w \otimes x$. Dann gilt wegen $w \in C_0(E_1, q_1)$ und $w^2 = u$:

$$\delta(x)^2 = (w \otimes x)^2 = w^2 \otimes x^2 = uq(x)(1_{C(E_1,q_1)} \otimes 1_{C(E_2,q_2)}).$$

Daher gibt es einen eindeutigen Homomorphismus $\psi_2 : C(E_2, {}^u q_2) \to D$ von R-Algebren, sodass $\psi_2(x) = w \otimes x$ für alle $x \in E_2$. Da $C_0(E_2, q_2)$ als R-Algebra von allen Produkten xx' mit $x, x' \in E_2$ erzeugt wird, folgt aus $u \in R^*$ und $\psi_2(xx') = (w \otimes x)(w \otimes x') = u(1_{C(E_1,q_1)} \otimes xx')$, dass $R1_{C(E_1,q_1)}\hat{\otimes}_R C_0(E_2, q_2)$ im Bild von ψ_2 liegt. Wegen $(w \otimes x)(1_{C(E_1,q_1)} \otimes c_2) = (w \otimes xc_2)$ für alle $x \in E_2$ und alle $c_2 \in C_0(E_2, q_2)$ liegt auch $Rw\hat{\otimes}_R C_1(E_2, q_2)$ im Bild von ψ_2 und der Homomorphismus von R-Algebren ist somit surjektiv. Da die Rangfunktionen der beiden endlich erzeugten, projektiven R-Algebren übereinstimmen, ist ψ_2 sogar ein Isomorphismus. Verknüpfen wir nun ψ_1 mit $id_{C(E_1,q_1)} \otimes \psi_2$, so erhalten wir einen Isomorphismus $C(E_1, q_1) \otimes_R C(E_2, {}^u q_2) \to C(E_1, q_1)\hat{\otimes}_R C(E_2, q_2)$, der $c_1 \otimes c_2 \mapsto (c_1 \otimes 1_{C(E_2,q_2)})(w \otimes c_2)$ für alle $c_1 \in C(E_1, q_1)$, $c_2 \in C(E_2, q_2)$ erfüllt. Offenbar respektiert dieser Isomorphismus auch die jeweiligen Graduierungen. □

2.8. Die Struktur von C(E,q) und C$_0$(E,q).

Ist (E, q) ein nichtsingulärer, endlich erzeugter, projektiver quadratischer R-Modul, so behandelt der folgende Satz den Fall, dass die Rangfunktion nur gerade, oder nur ungerade Werte annimmt.

Satz 2.18. *Sei (E, q) ein nichtsingulärer, endlich erzeugter, projektiver quadratischer R-Modul.*

- *Ist der Rang von E gerade, so ist $C(E, q)$ zentral und separabel über R.*
- *Ist der Rang von E ungerade, so ist $C_0(E, q)$ zentral und separabel über R.*

Beweis. Sei zunächst der Rang von E gerade. Wir betrachten vorerst den Spezialfall, dass R ein lokaler Ring ist. Der R-Modul E ist dann frei und von konstantem Rang; sei $rg_R E = 2m$. Wir führen den Beweis mittels Induktion über m. Ist $m = 0$, also $E = \{0\}$, so gilt $q = 0$ und $C(E, q) = R$; die Behauptung ist dann trivial. Im Fall $m = 1$ ist $C(E, q)$ eine freie Quaternionen-Algebra und wir haben die Behauptung bereits in Abschnitt 2.2 gezeigt. Sei nun $m \geq 2$. Dann gibt es eine orthogonale Zerlegung $E = E_1 \perp E_2 \perp \ldots \perp E_m$, sodass alle E_i $(1 \leq i \leq m)$ frei von Rang 2 sind. Wir setzen nun $F := E_1$ und $F' := E_2 \perp E_2 \perp \ldots \perp E_m$. Für die Clifford-Algebra zu $(E = F \perp F', q)$ gilt dann nach Satz 2.17: $C(E, q) \tilde{=} C(F, q|_F) \otimes_R C(F', {}^u q|_{F'})$ für ein

$u \in R^*$. Nach Induktionsvoraussetzung sind $C(F, q|_F)$ und $C(F', {}^u q|_{F'})$ beide zentral und separabel über R. Es folgt, dass auch $C(E, q)$ zentral und separabel ist.
Sei nun R ein beliebiger kommutativer Ring (mit Eins) und $\mathfrak{p} \subset R$ ein Primideal von R. Es sei $\varphi : C(E \otimes_R R_\mathfrak{p}, q_{R_\mathfrak{p}}) \to C(E, q) \otimes_R R_\mathfrak{p}$ der Isomorphismus von $R_\mathfrak{p}$-Algebren aus Satz 1.9. Nach Obigem ist $C(E \otimes_R R_\mathfrak{p}, q_{R_\mathfrak{p}})$ zentral und separabel über dem lokalen Ring $R_\mathfrak{p}$. Da φ ein Isomorphismus ist, muss auch $C(E, q) \otimes_R R_\mathfrak{p}$ zentral und separabel über $R_\mathfrak{p}$ sein. Da dies für alle Primideale $\mathfrak{p} \subset R$ gilt, folgt, dass $C(E, q)$ separabel über R ist (siehe Anhang). Es bleibt zu zeigen, dass $C(E, q)$ zentral ist.
Da $C(E, q)$ separabel ist und $R_\mathfrak{p}$ eine kommutative R-Algebra ist, gibt es einen Isomorphismus $\psi : Z(C(E, q)) \otimes_R R_\mathfrak{p} \to Z\big(C(E, q) \otimes_R R_\mathfrak{p}\big)$. Andererseits können wir φ einschränken zu einem $R_\mathfrak{p}$-Algebren-Isomorphismus $\varphi' : Z\big(C(E \otimes_R R_\mathfrak{p}, q_{R_\mathfrak{p}})\big) \to Z\big(C(E, q) \otimes_R R_\mathfrak{p}\big)$. Sei weiters die Abbildung $k : R_\mathfrak{p} \to Z(C(E, q)) \otimes_R R_\mathfrak{p}$ gegeben durch $a \mapsto 1_{C(E,q)} \otimes a$. Durch Komposition erhalten wir nun einen Homomorphismus

$$\Psi := \varphi'^{-1} \circ \psi \circ k : R_\mathfrak{p} \to Z\big(C(E \otimes_R R_\mathfrak{p}, q_{R_\mathfrak{p}})\big)$$

von $R_\mathfrak{p}$-Algebren. Da φ' und ψ Isomorphismen sind und k injektiv ist, ist auch Ψ injektiv. Nach Obigem ist $C(E \otimes_R R_\mathfrak{p}, q_{R_\mathfrak{p}})$ zentral über $R_\mathfrak{p}$ und es folgt daher, dass Ψ ein Isomorphismus ist. Es ist somit auch $k : R_\mathfrak{p} \to Z(C(E, q)) \otimes_R R_\mathfrak{p}$ ein Isomorphismus von $R_\mathfrak{p}$-Algebren. Dies bedeutet, dass für jedes Primideal $\mathfrak{p} \subset R$ die Lokalisierung in $\mathfrak{p}$ der Einbettung $i : R \to Z(C(E, q))$, $r \mapsto r1_{C(E,q)}$ ein Isomorphismus ist. Daher muss auch i ein Isomorphismus sein und wir haben damit gezeigt, dass $C(E, q)$ zentral ist.

Sei nun der Rang von E ungerade. Auch in diesem Fall setzen wir zunächst voraus, dass R ein lokaler Ring ist. Der R-Modul E ist dann frei; es sei der Rang von E gleich $2m + 1$ für ein $m \geq 0$. Es gibt eine orthogonale Zerlegung $E = E_0 \perp E_1 \perp \ldots \perp E_m$, wobei E_0 frei von Rang 1, E_i $(1 \leq i \leq m)$ frei von Rang 2 und alle E_i $(0 \leq i \leq m)$ nichtsingulär sind. Setzen wir nun $F := E_0$, $F' := E_1 \perp \ldots \perp E_m$, so gilt: $C_0(E, q) \tilde{=} C_0(F, q|_F) \otimes_R C(F', {}^{-u} q|_{F'})$ für ein $u \in R^*$. Wegen $C_0(F, q) \tilde{=} R$ folgt: $C_0(E, q) \tilde{=} R \otimes_R C(F', {}^{-u} q|_{F'}) \tilde{=} C(F', {}^{-u} q|_{F'})$. Da F' geraden Rang hat, folgt aus Obigem, dass $C_0(E, q)$ zentral und separabel ist.
Sie nun R ein beliebiger kommutativer Ring und $\mathfrak{p} \subset R$ ein Primideal. Wir betrachten die Einschränkung des Isomorphismus φ von $R_\mathfrak{p}$-Algebren aus Satz 1.9 zu $\varphi' : C_0(E \otimes_R R_\mathfrak{p}, q_{R_\mathfrak{p}}) \to C_0(E, q) \otimes_R R_\mathfrak{p}$. Man argumentiert nun analog zu Obigem, dass aus der Zentralität und der Separabilität von $C_0(E \otimes_R R_\mathfrak{p}, q_{R_\mathfrak{p}})$ ebendiese Eigenschaften auch für $C_0(E, q)$ folgen. □

In obigem Satz haben wir die wichtige Voraussetzung verwendet, dass der Rang von E gerade oder ungerade ist. Hahn zeigt in [4, Chap. 9.B, (9.9)] das folgende allgemeine Resultat:

Satz 2.19. *Sei (E, q) ein nichtsingulärer, endlich erzeugter, projektiver quadratischer R-Modul. Dann sind die beiden Algebren $C(E, q)$ und $C_0(E, q)$ separabel über R.*

Die Voraussetzung an die Rangfunktion von E ist also nur für die Zentralität notwendig. Der folgende Satz zeigt, dass wir den allgemeinen Fall auf die beiden Spezialfälle von geradem oder ungeradem Rang zurückführen können (siehe [4, Chap. 9.C]).

Satz 2.20. *Sei (E, q) ein nichtsingulärer, endlich erzeugter, projektiver quadratischer Modul über R. Dann gibt es eine Zerlegung $R = R_0 \times R_1$, die*

- *eine Zerlegung $(E,q) = (E_0,q_0) \times (E_1,q_1)$ induziert, für die gilt: (E_0,q_0) und (E_1,q_1) sind nichtsinguläre, endlich erzeugte, projektive Moduln über R_0 bzw. R_1 und der Rang von E_0 nimmt nur gerade, jener von E_1 nur ungerade Werte an.*
- *einen Isomorphismus $C(E,q) \tilde{=} C(E_0,q_0) \times C(E_1,q_1)$ von R-Algeb-ren induziert, der sich zu einem Isomorphismus $C_0(E,q) \tilde{=} C_0(E_0,q_0) \times C_0(E_1,q_1)$ einschränken lässt.*

Damit lässt sich das folgende zusammenfassende Resultat beweisen (siehe [4, Chap. 9.D]):

Satz 2.21. *Ist (E,q) ein treuer, nichtsingulärer, endlich erzeugter, projektiver quadratischer R-Modul, so gilt:*

(1) *$A(E,q)$ ist eine separable, endlich erzeugte, projektive R-Algebra von konstantem Rang 2,*
(2) *$C(E,q)$ ist genau dann zentral und separabel über R, wenn der Rang von E gerade ist,*
(3) *$C_0(E,q)$ ist genau dann zentral und separabel über R, wenn der Rang von E ungerade ist,*
(4) *$Z(C(E,q))$ ist genau dann eine separable, endlich erzeugte, projektive R-Algebra von Rang 2, wenn $Z(C(E,q)) = A(E,q)$ gilt. Dies ist äquivalent dazu, dass der Rang von E ungerade ist,*
(5) *$Z(C_0(E,q))$ ist genau dann eine separable, endlich erzeugte, projektive R-Algebra von Rang 2, wenn $Z(C_0(E,q)) = A(E,q)$ gilt. Dies ist genau dann der Fall, wenn der Rang von E ungerade ist.*

2.9. **Verallgemeinerung für den Fall ungeraden Ranges.**

Einen endlich erzeugten quadratischen R-Modul (E,q), der nichtsingulär ist, nennt man auch *regulär*. Ist nun der Rang von E ungerade, so kann die quadratische Form q nur dann regulär sein, wenn $2 \in R^*$ gilt. Diese sehr starke Voraussetzung lässt sich jedoch abschwächen.
Sei zunächst E ein freier R-Modul von ungeradem Rang n und $\{e_1, e_2, \dots, e_n\}$ eine R-Basis von E. Wir untersuchen nun die Diskriminante $d(e_1, e_2, \dots, e_n) := \det(b(e_i,e_j)_{i,j=1}^n)$ bezüglich der gegebenen Basis von E; b sei hierbei die zur quadratischen Form q assoziierte Bilinearform auf E. Modulo 2 gilt:

$$d(e_1,e_2,\dots,e_n) = \det \begin{pmatrix} 2q(e_1) & b(e_1,e_2) & \cdots & b(e_1,e_n) \\ b(e_1,e_2) & 2q(e_2) & \cdots & b(e_2,e_n) \\ \vdots & \cdots & \ddots & \vdots \\ b(e_1,e_n) & \cdots & b(e_{n-1},e_n) & q(e_n) \end{pmatrix} \equiv$$

$$\equiv \det \begin{pmatrix} 0 & -b(e_1,e_2) & \cdots & -b(e_1,e_n) \\ b(e_1,e_2) & 0 & \cdots & -b(e_2,e_n) \\ \vdots & \cdots & \ddots & \vdots \\ b(e_1,e_n) & \cdots & b(e_{n-1},e_n) & 0 \end{pmatrix} \pmod 2.$$

Modulo 2 ist $(b(e_i,e_j)_{i,j=1}^n)$ also kongruent zu einer schiefsymmetrischen $(n \otimes n)$-Matrix von ungeradem Rang. Es gilt daher $d(e_1,e_2,\dots,e_n) = \det(b(e_i,e_j)_{i,j=1}^n) \equiv 0$

(mod 2), es gilt also $d(e_1, e_2, \ldots, e_n) \in 2R$ und wir können daher $d(e_1, e_2, \ldots, e_n)$ schreiben als

$$d(e_1, e_2, \ldots, e_n) = 2d'(e_1, e_2, \ldots, e_n),$$

wobei $d'(e_1, e_2, \ldots, e_n)$ ein Polynom in $\mathbb{Z}[q(e_i), b(e_i, e_j) \mid i, j = 1, \ldots, n]$ ist. Kneser definiert nun in [8, Kap. I, (2.13)] den Begriff der *Semi-* oder *Halbregularität* folgendermaßen:

Definition 2.8. *Ist (E, q) ein freier quadratischer R-Modul von ungeradem Rang n und $\{e_1, e_2, \ldots, e_n\}$ eine Basis von E, so heißt (E, q) halbregulär, falls $d'(e_1, e_2, \ldots, e_n)$ in R invertierbar ist.*

Da sich die Diskriminante bei Basiswechsel gerade um ein Quadrat in R^* ändert, ist diese Definition unabhängig von der Wahl der Basis. Die Restklasse von $d'(e_1, e_2, \ldots, e_n)$ modulo $(R^*)^2$ ist also unabhängig von der Wahl der Basis und wir nennen sie die *Halbdiskriminante* von (E, q).
Ist nun (E, q) ein beliebiger endlich erzeugter, projektiver quadratischer R-Modul von ungeradem Rang, so definiert Knus in [9, Chap. IV, (3.1)] das *Halbdiskriminanten-Ideal* durch

$$d'(E, q) := < d'(x_1, x_2, \ldots, x_n) \mid x_i \in E_i,\ 1 \leq i \leq n >_R .$$

Definition 2.9. *Ein endlich erzeugter, projektiver quadratischer R-Modul von ungeradem Rang heißt* semiregulär*, falls $d'(E, q) = R$ gilt.*

Ist (E, q) frei und $\{e_1, e_2, \ldots, e_n\}$ eine beliebige Basis, so gilt genau dann $d'(E, q) = R$, wenn $d'(e_1, e_2, \ldots, e_n) \in R^*$ gilt und Definition 2.9 verallgemeinert somit Definition 2.8. Ist 2 eine Einheit in R, so ist offenbar jeder semireguläre quadratische R-Modul regulär, im allgemeinen gilt dies jedoch nicht, wie das folgende einfache Beispiel zeigt:

Beispiel: Sei (E, q) ein freier quadratischer R-Modul von Rang 1 und $\{e\}$ eine Basis von E, sodass $q(e) \in R^*$ gilt. Dann gilt $d(e) = 2q(e)$ und ist $2 \notin R^*$, so ist (E, q) semiregulär, aber nicht regulär.

Knus zeigt nun in [9, Chap. IV, Prop. (3.2.4)] das folgende Resultat über quadratische Moduln von ungeradem Rang, das Proposition 2.16 und Satz 2.18 verallgemeinert:

Satz 2.22. *Sei (E, q) ein semiregulärer quadratischer R-Modul. Dann ist $C_0(E, q)$ zentral und separabel über R. Weiters gilt für das Zentrum der Clifford-Algebra $Z(C(E, q)) = A(E, q)$ und es gibt einen Isomorphismus $C(E, q) \to C_0(E, q) \otimes_R Z(C(E, q))$ von R-Algebren.*

3. Quadratische Moduln von Rang 2

Sei in diesem Abschnitt (E,q) ein projektiver quadratischer R-Modul von konstantem Rang 2.

3.1. **Standardinvolutionen auf projektiven Algebren von Rang 2.**

Ist A eine freie R-Algebra von Rang 2, so ist A kommutativ. Mittels Lokalisierung lässt sich diese Tatsache auch auf projektive Algebren von konstantem Rang 2 verallgemeinern.

Proposition 3.1. *Die Clifford-Algebra $C(E,q)$ zu einem projektiven quadratischen R-Modul (E,q) von konstantem Rang 2 ist projektiv und hat konstanten Rang 4. Die kanonische Involution $\gamma = \sigma \circ \tau$ (siehe Abschnitt 2.2) auf $C(E,q)$ ist eine Standard-Involution und die Einschränkung $\gamma_0 := \gamma|_{C_0(E,q)}$ macht $C_0(E,q)$ zu einer Algebra mit Standard-Involution.*

Beweis. Da E projektiv ist, ist nach Satz 1.14 auch $C(E,q)$ projektiv. Weil für jedes Primideal $\mathfrak{p} \subset R$ die Lokalisierung $E_\mathfrak{p} = E \otimes_R R_\mathfrak{p}$ frei von Rang 2 über $R_\mathfrak{p}$ ist, hat wegen $C(E,q)_\mathfrak{p} = C(E,q) \otimes_R R_\mathfrak{p} \tilde{=} C(E_\mathfrak{p}, q_\mathfrak{p} := q_{R_\mathfrak{p}})$ die Clifford-Algebra $C(E,q)$ offenbar konstanten Rang 4. Nach Proposition 2.2 ist die kanonische Involution $\gamma_\mathfrak{p}$ auf $C(E_\mathfrak{p}, q_\mathfrak{p})$ eine Standardinvolution; es gilt also für alle $z_\mathfrak{p} \in C(E_\mathfrak{p}, q_\mathfrak{p})$, dass $n_\mathfrak{p}(z_\mathfrak{p}) := z_\mathfrak{p}\gamma_\mathfrak{p}(z_\mathfrak{p}) \in R_\mathfrak{p}$. Wir haben nun zu zeigen, dass $n(z) \in R$ für alle $z \in C(E,q)$ gilt. Man betrachte das folgende kommutative Diagramm:

$$\begin{tikzcd} C(E_\mathfrak{p}, q_\mathfrak{p}) \arrow[r, "n_\mathfrak{p}"] \arrow[d, "\varphi"'] & C(E_\mathfrak{p}, q_\mathfrak{p}) \arrow[d, "\varphi"] \\ C(E,q) \otimes R_\mathfrak{p} \arrow[r, "n \otimes id_{R_\mathfrak{p}}"'] & C(E,q) \otimes R_\mathfrak{p} \end{tikzcd}$$

wobei φ der $R_\mathfrak{p}$-Algebren-Isomorphismus $C(E_\mathfrak{p}, q_\mathfrak{p}) \to C(E,q) \otimes_R R_\mathfrak{p}$ aus Satz 1.9 sei. Es gilt also für alle $x \in E$:

$$R_\mathfrak{p} \ni n_\mathfrak{p} \circ \varphi^{-1}(x \otimes 1_{R_\mathfrak{p}}) = \varphi^{-1} \circ (n \otimes id_{R_\mathfrak{p}})(x \otimes 1_{R_\mathfrak{p}}) = \varphi^{-1}(n(x) \otimes 1_{R_\mathfrak{p}}).$$

Da φ ein $R_\mathfrak{p}$-Algebren-Isomorphismus ist und dies für alle Primideale $\mathfrak{p} \subset R$ gilt, folgt, dass $n(x) \in R$ gelten muss. Weil $C(E,q)$ als R-Algebra von E erzeugt wird und γ ein Antiautomorphismus von R-Algebren ist, erhalten wir daher $n(z) \in R$ für alle $z \in C(E,q)$. Die letzte Aussage folgt, weil γ die Graduierung erhält. □

Wir werden zeigen, dass es auf jeder Algebra, die (als Modul) projektiv und von konstantem Rang 2 ist, eine Standardinvolution gibt. Das folgende Lemma zeigt uns, dass, falls auf einer Algebra eine Standardinvolution existiert, diese eindeutig ist (siehe [9, Chap. I, Prop. (1.3.4)]).

Lemma 3.2. *Sei A eine (als R-Modul) endlich erzeugte, projektive R-Algebra. Dann gibt es höchstens eine Standardinvolution auf A.*

Beweis. Sei zunächst R ein lokaler Ring. Dann ist A frei von endlichem Rang und insbesondere 1_A R-linear unabhängig. Daher lässt sich $e_1 := 1_A$ zu einer Basis $\{e_1, e_2, \ldots, e_n\}$ von A ergänzen. Seien nun ρ_1 und ρ_2 zwei Standardinvolutionen auf A und s_1, s_2 die entsprechenden Spurfunktionen, n_1, n_2 die jeweiligen Normen. In Abschnitt 2.1 haben wir gesehen, dass jedes $z \in A$ die quadratische Gleichung $z^2 - s(z)z + n(z) = 0$ erfüllt. Es folgt daher für alle $i = 2, \ldots, n$:

$$s_1(e_i)e_i - n_1(e_i)1_A = e_i^2 = s_2(e_i)e_i - n_2(e_i)1_A$$

und da 1_A und e_i $(2 \leq i \leq n)$ R-linear unabhängig sind, erhalten wir somit $s_1(e_i) = s_2(e_i)$, sowie $n_1(e_i) = n_2(e_i)$ für $i = 2, \ldots, n$. Andererseits gilt offensichtlich $s_1(1_A) = 2 \cdot 1_A = s_2(1_A)$. Es gilt also $e_i + \rho_1(e_i) = s_1(e_i) = s_2(e_i) = e_i + \rho_2(e_i)$ für alle $i = 1, 2, \ldots, n$, und somit $\rho_1(e_i) = \rho_2(e_i)$. Da $\{e_1, e_2, \ldots, e_n\}$ eine Basis von A (als R-Modul) bildet, folgt $\rho_1 = \rho_2$.

Seien nun R ein beliebiger kommutativer Ring (mit Eins) und ρ_1, ρ_2 zwei Standardinvolutionen auf A. Dann erhalten wir durch Lokalisierung in einem beliebigen Primideal $\mathfrak{p} \subset R$ einen freien $R_\mathfrak{p}$-Modul $A_\mathfrak{p} = A \otimes_R R_\mathfrak{p}$. Nach Obigem stimmen die Standardinvolutionen $\rho_1 \otimes id_{R_\mathfrak{p}}$ und $\rho_2 \otimes id_{R_\mathfrak{p}}$ überein. Da dies für alle Primideale $\mathfrak{p} \subset R$ gilt, folgt $\rho_1 = \rho_2$. □

Lemma 3.3. *Sei A eine R-Algebra, die ein projektiver R-Modul von konstantem Rang 2 ist. Dann gibt es eine Standardinvolution auf A.*

Beweis. Ist $\mathfrak{p} \subset R$ ein Primideal, so ist $A_\mathfrak{p}$ als $R_\mathfrak{p}$-Modul frei von Rang 2 und wir haben in Beispiel (2) in Abschnitt 2.1 bereits gezeigt, dass die Konjugation $\zeta_\mathfrak{p}$ auf $A_\mathfrak{p}$ eine Standardinvolution ist. Wegen der Eindeutigkeit von Standardinvolutionen lassen sich diese lokalen Involutionen zu einer wohldefinierten Abbildung auf A „verkleben“ und wir erhalten dadurch eine Standardinvolution auf A. □

Proposition 3.4. *Seien A und B zwei R-Algebren, die als R-Modul projektiv und von konstantem Rang 2 sind. Dann sind A und B genau dann isomorph, wenn (A, n_A) und (B, n_B) (als quadratische R-Moduln) isometrisch sind.*

Beweis. Seien ρ_A und ρ_B die n_A bzw. n_B definierenden Standardinvolutionen auf A bzw. B und sei $\psi : A \to B$ ein R-Algebren-Isomorphismus. Dann gilt für $\psi \circ \rho_A \circ \psi^{-1}$ offenbar $(\psi \circ \rho_A \circ \psi^{-1})^2 = id_B$ und

$$b(\psi \circ \rho_A \circ \psi^{-1})(b) = \psi(a)(\psi \circ \rho_A \circ \psi^{-1})(\psi(a)) = \psi(a)\psi(\rho_A(a)) =$$
$$= \psi(a\rho_A(a)) = \psi(n_A(a)) = n_A(a) \in R$$

für alle $b = \psi(a) \in B$. Es definiert daher $\psi \circ \rho_A \circ \psi^{-1}$ eine Standardinvolution auf B und wegen der Eindeutigkeit der Standardinvolution folgt $\rho_B = \psi \circ \rho_A \circ \psi^{-1}$. Somit gilt für alle $a \in A$:

$$n_B(\psi(a)) = \psi(a)\rho_B(\psi(a)) = n_A(a)$$

– die quadratischen R-Moduln (A, n_A) und (B, n_B) sind also isometrisch.

Umgekehrt erhalten wir klarerweise durch die Isometrie von (A, n_A) und (B, n_B) einen Isomorphismus $\psi : A \to B$ von R-Moduln. Es bleibt zu zeigen, dass ψ auch mit den jeweiligen Algebren-Multiplikationen in A bzw. B verträglich ist. Ist R lokal, so sind A und B freie quadratische R-Moduln von Rang 2. Sei $\{1_A, a\}$ eine Basis von A (als R-Modul). Dann ist $\{1_B, \psi(a)\}$ eine Basis von B und es gilt wegen $z^2 - s(z)z + n(z) = 0$ für alle z in einer beliebigen Algebra mit Standardinvolution (siehe Abschnitt 2.1):

$$\psi(a^2) = \psi\big(s_A(a)a - n_A(a)\big) = \psi\big(s_B(\psi(a))a - n_B(\psi(a))\big) =$$

$$= s_B(\psi(a))\psi(a) - n_B(\psi(a)) = (\psi(a))^2.$$

Für den Fall, dass R ein lokaler Ring ist, ist somit ψ ein Isomorphismus von R-Algebren und die Behauptung ist gezeigt. Der allgemeine Fall folgt nun sofort mittels Lokalisierung. □

3.2. **Formen von Typ** A.

Ist (E, q) ein freier quadratischer R-Modul von Rang 2, so gilt $C_1(E, q) = E$. Dies lässt sich auf den Fall projektiver quadratischer R-Moduln von konstantem Rang 2 verallgemeinern: Sei $\mathfrak{p} \subset R$ ein beliebiges Primideal, so gilt $C_1(E, q) \otimes_R R_\mathfrak{p} \tilde{=} C_1(E_\mathfrak{p}, q_\mathfrak{p}) = E_\mathfrak{p} = E \otimes_R R_\mathfrak{p}$ und es folgt daher auch in diesem Fall $C_1(E, q) \tilde{=} E$. Wegen

$$C_0(E, q)E = C_0(E, q)C_1(E, q) \subset C_1(E, q) = E$$

erhalten wir somit durch die Multiplikation in $C(E, q)$ die Struktur eines $C_0(E, q)$-Moduls auf E.

Sei nun E frei von Rang 2 über R und $\{e, f\}$ eine Basis von E. Dann ist $\{1_{C(E,q)}, ef\}$ eine Basis von $C_0(E, q)$. Für $x = re + sf \in E,\ y = r'1_{C(E,q)} + s'ef \in C_0(E, q)$ gilt:

$$\gamma_0(y)x = \big((r' + s'b(e, f))1_{C(E,q)} - s'ef\big)(re + sf) =$$

$$= rr'e + rs'b(e, f)e - rs'e(b(e, f) - ef) + sr'f + ss'b(e, f)f - ss'eq(f) =$$

$$= (re + sf)(r'1_{C(E,q)} + s'ef) = xy.$$

Wir erhalten also für alle $x \in E,\ y \in C_0(E, q)$:

$$xy = \gamma_0(y)x.$$

Durch Lokalisierung können wir dieses Resultat auf den Fall projektiver quadratischer R-Moduln (E, q) verallgemeinern.

Es folgt nun weiter:

$$q(yx) = y(xy)x = y\gamma_0(y)xx = n_0(y)q(x)$$

für $x \in E,\ y \in C_0(E, q)$, wobei $n_0 = n|_{C_0(E,q)}$ die durch γ_0 definierte Normfunktion auf der R-Algebra $C_0(E, q)$ sei.

Der folgende Begriff geht auf Kneser zurück (siehe [7, Chap. 4], sowie [9, Chap. III, (7.2)]):

Definition 3.1. *Sei (E, q) ein endlich erzeugter quadratischer R-Modul und A eine R-Algebra, die als R-Modul projektiv und treu ist und konstanten Rang 2 hat. Weiters sei ρ eine Standardinvolution auf A und n die entsprechende Normfunktion. Dann heißt E* von Typ A, *falls E ein projektiver A-Modul von Rang 1 ist und für alle $x \in E,\ y \in A$*

$$q(yx) = n(y)q(x)$$

gilt.

Beispiele:

(1) Seien A und A' zwei (als R-Moduln) projektive, treue R-Algebren von konstantem Rang 2 und $\eta : A \to A'$ ein Homomorphismus von R-Algebren mit Standardinvolution. Via η wird A' zu einer A-Algebra und ist als solche projektiv und hat konstanten Rang 1. Sind ρ, ρ' die Standardinvolutionen auf

A bzw. A', so gilt (weil η die Standardinvolutionen respektiert) auch für die entsprechenden Normen n und n':

$$n(a) = \eta(n(a)) = \eta(a\rho(a)) = \eta(a)\eta(\rho(a)) = \eta(a)\rho'(\eta(a)) = n'(\eta(a))$$

für alle $a \in A$. Es folgt daher:

$$n'(a \cdot a') = n('\eta(a)a') = n'(\eta(a))n'(a') = n(a)n'(a')$$

für alle $a \in A$, $a' \in A'$. Somit ist A' von Typ A.

(2) Da $C_0(E,q)$ eine projektive R-Algebra von konstantem Rang 2 ist und E als $C_0(E,q)$-Modul projektiv von konstantem Rang 1 ist, ist nach Obigem der quadratische R-Modul (E,q) offenbar von Typ $C_0(E,q)$.

Betrachten wir weiterhin $E = C_1(E,q)$ als $C_0(E,q)$-Modul, so definiert die Multiplikation in $C(E,q)$ bezüglich der Standardinvolution γ_0 auf $C_0(E,q)$ eine hermitesche Form $h : E \times E \to C_0(E,q)$ mit $h(y_1x_1, y_2x_2) = y_1\gamma_0(y_2)h(x_1,x_2)$ und $h(x_1,x_2) = \gamma_0(h(x_1,x_2))$ für $x_1, x_2 \in E,\ y_1, y_2 \in C_0(E,q)$; für diese gilt offensichtlich $h(x,x) = q(x)$ (für alle $x \in E$).

Sei nun $z = x + y \in C(E,q)$ mit $x \in E = C_1(E,q),\ y \in C_0(E,q)$. Dann gilt: $\gamma(z) = \gamma(x)+\gamma(y) = -x+\gamma_0(y)$. Für die durch die kanonische Involution γ definierte Norm n gilt daher:

$$\begin{aligned} n(z) = z\gamma(z) = (x+y)(-x+\gamma_0(y)) &= -x^2 + x\gamma_0(y) - yx + y\gamma_0(y) = \\ &= -q(x) + x\gamma_0(y) - \gamma_0(\gamma_0(y))x + n_0(y) = -q(x) + n_0(y). \end{aligned}$$

Ist f die der quadratischen Form n auf $C(E,q)$ entsprechende Bilinearform (siehe Abschnitt 2.1), so gilt für alle $x \in E,\ y \in C_0(E,q)$:

$$f(x,y) = n(x+y) - n(x) - n(y) = -q(x) + n_0(y) + q(x) - n_0(y) = 0$$

und wir erhalten daher eine orthogonale Zerlegung

$$\big(C(E,q), n\big) \tilde{=} (E, -q) \perp \big(C_0(E,q), n_0\big).$$

Proposition 3.5. *Sei A eine R-Algebra mit Standardinvolution, die als R-Modul projektiv, treu und von konstantem Rang 2 ist; (E,q) sei ein quadratischer R-Modul von Typ A. Gilt $\operatorname{Ann} q(E) := \{r \in R \mid r\,q(E) = 0\} = 0$, dann gibt es einen eindeutigen Homomorphismus $\delta : C_0(E,q) \to A$ von R-Algebren mit Standardinvolution, der für alle $x \in E,\ y \in C_0(E,q)$*

$$\delta(y)x = yx$$

erfüllt. δ ist genau dann ein Isomorphismus, wenn (E,q) primitiv ist, also wenn $Rq(E) = R$ gilt.

Beweis. Wir zeigen zunächst die Eindeutigkeit. Ist $\mathfrak{p} \subset A$ ein Primideal, so ist $(E_\mathfrak{p}, q_{A_\mathfrak{p}})$ ein freier quadratischer $A_\mathfrak{p}$-Modul von Rang 1; sei $\{x_\mathfrak{p}\}$ eine Basis von $E_\mathfrak{p}$. Dann folgt wegen der $A_\mathfrak{p}$-linearen Unabhängigkeit von $x_\mathfrak{p}$, dass $\delta_\mathfrak{p} : C_0(E,q) \to A_\mathfrak{p}$ durch $\delta_\mathfrak{p}(y)x_\mathfrak{p} = (yx)_\mathfrak{p}$ $(y \in C_0(E,q))$ eindeutig bestimmt ist. Da also die Abbildung $\delta_\mathfrak{p}$ für jedes Primideal $\mathfrak{p} \subset A$ eindeutig ist, folgt die Eindeutigkeit von δ.

Um die Existenz zu zeigen, sei zunächst R ein lokaler Ring. Dann sind A, E und $C_0(E,q)$ (als R-Moduln) frei und von Rang 2. Wir setzen voraus, dass E über A frei von Rang 1 ist. Sei $\{e\}$ eine Basis von E als A-Modul und $\{1_{C(E,q)}, c\}$ eine R-Basis von $C_0(E,q)$. Da e A-linear unabhängig ist, ist die Abbildung δ durch die Gleichung $\delta(y)e = ye$ eindeutig bestimmt. Offenbar ist δ R-linear. Für die Norm-Abbildungen n_0 und n_A von $C_0(E,q)$ bzw. A gilt:

$$n_0(y)q(e) = q(ye) = q(\delta(y)e) = n_A(\delta(y))q(e).$$

Da $\{e\}$ eine A-Basis von E ist (also $E = Ae$), kann $q(e)$ wegen $Ann\, q(E) = 0$ kein Nullteiler in R sein. Es folgt daher $n_0(y) = n_A(\delta(y))$ für alle $y \in C_0(E, q)$. Für die jeweiligen Spurfunktionen muss wegen

$$1 + s_0(y) + n_0(y) = 1 + y + \gamma_0(y) + y\gamma_0(y) = (1 + y)(1 + \gamma_0(y)) = n_0(1 + y) =$$
$$= n_A(1 + \delta(y)) = 1 + s_A(\delta(y)) + n_A(\delta(y))$$

für alle $y \in C_0(E, q)$ die Gleichheit $s_0(y) = s_A(\delta(y))$ gelten. Verwenden wir die quadratischen Gleichungen $y^2 - s_0(y)y + n(y) = 0$ für $y \in C_0(E, q)$ und $a^2 - s_A(a)a + n(a) = 0$ für $a \in A$, so erhalten wir:

$$\delta(c^2) = \delta(s_0(c)c - n_0(c)) = \delta\big(s_A(\delta(c))c - n_A(\delta(c))\big) = s_A(\delta(c))\delta(c) - n_A(\delta(c)) = \delta(c)^2.$$

Daher ist δ ein R-Algebren-Homomorphismus.
Die A-Modul-Struktur auf E lässt sich in natürlicher Weise auf Produkte $x_1x_2 \in C_0(E, q)$ fortsetzen, indem wir $a \cdot x_1x_2 := (ax_1)x_2$ für $x_1,\ x_2 \in E,\ a \in A$ definieren. Ist nun $x \in E$ beliebig, so gilt $x = ae$ für ein eindeutiges $a \in A$ und wegen der Kommutativität von A erfüllt δ für alle $y \in C_0(E, q)$:

$$\delta(y)x = (\delta(y)a)e = (a\delta(y))e = a(\delta(y)e) = a(ye) =$$
$$= a(e\gamma_0(y)) = (ae)\gamma_0(y) = y(ae) = yx.$$

Der Homomorphismus δ ist genau dann bijektiv, wenn $\{e\}$ auch eine Basis von E als $C_0(E, q)$-Modul ist. Dies ist wiederum äquivalent dazu, dass $q(e) \in R^*$ gilt: Ist nämlich $\{e\}$ eine $C_0(E, q)$-Basis von E und $\{e, f\}$ eine R-Basis von E (beachte, dass e insbesondere R-linear unabhängig ist), so gibt es eindeutige Elemente $r, s \in R$, sodass $f = (r1_{C(E,q)} + s(fe))e = re + sfq(e)$ gilt. Es folgt nun wegen der R-linearen Unabhängigkeit von e und f, dass $r = 0$ und $s = q(e)^{-1}$ gelten muss – insbesondere erhalten wir also $q(e) \in R^*$. Ist umgekehrt $q(e) \in R^*$, so ist die Abbildung $C_0(E, q) \to E,\ y \mapsto ye$ bijektiv; es besitzt also jedes Element $x \in E$ eine eindeutige Darstellung $x = ye$ mit $y \in C_0(E, q)$ und $\{e\}$ ist somit eine $C_0(E, q)$-Basis von E.
Da $\{e\}$ eine A-Basis von E ist, gilt:

$$Rq(E) = Rq(Ae) = Rn(A)q(e) = Rq(e);$$

es ist daher E genau dann primitiv, wenn es ein $e \in E$ mit $q(e) \in R^*$ gibt und die Behauptung ist somit für den Fall, dass R ein lokaler Ring und E über A frei ist, bewiesen.
Sei R weiterhin lokal und E als A-Modul projektiv und von Rang 1. Ist $\mathfrak{p} \subset A$ ein Primideal, so ist $E_\mathfrak{p} = E \otimes_A A_\mathfrak{p}$ ein freier $A_\mathfrak{p}$-Modul von Rang 1. Nach Obigem gibt es einen eindeutigen Homomorphismus $\delta_\mathfrak{p} : C_0(E, q) \to A_\mathfrak{p}$ von R-Algebren, sodass

$$\delta_\mathfrak{p}(y)x_\mathfrak{p} = (yx)_\mathfrak{p}$$

für alle $y \in C_0(E, q),\ x_\mathfrak{p} \in E_\mathfrak{p}$ gilt. Es folgt daher durch „verkleben" der Abbildungen $\delta_\mathfrak{p}$ die Existenz eines Homomorphismus $\delta : C_0(E, q) \to A$ von R-Algebren, der für alle $x \in E$ die Gleichung $\delta(y)x = yx$ erfüllt.
Ist nun R ein beliebiger kommutativer Ring (mit Eins) und $\mathfrak{q} \subset R$ ein Primideal in R, dann gibt es nach Obigem einen eindeutigen Homomorphismus $\delta_\mathfrak{q} : C_0(E_\mathfrak{q}, q_{R_\mathfrak{q}}) \to A_\mathfrak{q}$ von $R_\mathfrak{q}$-Algebren, der $\delta_\mathfrak{q}(y_\mathfrak{q})x_\mathfrak{q} = y_\mathfrak{q}x_\mathfrak{q}$ (für alle $y_\mathfrak{q} \in C_0(E_\mathfrak{q}, q_R),\ x_\mathfrak{q} \in E_\mathfrak{q}$) erfüllt. Wegen der Eindeutigkeitsaussage lassen sich diese lokalen Algebren-Homomorphismen nun zu einem Homomorphismus $\delta : C_0(E, q) \to A$ „verkleben", der die geforderte Eigenschaft besitzt. □

3.3. **Verschränkte Produkte.**

Sei A eine R-Algebra, die als R-Modul projektiv und von konstantem Rang 2 – also insbesondere kommutativ – ist. Weiters sei ρ_A eine Standardinvolution auf A. Wir betrachten nun den freien A-Modul $B := A \oplus Au$, wobei u ein abstrakter Erzeuger sei. Definieren wir eine Multiplikation auf B durch

$$a_1 \cdot a_2 := a_1 a_2 \in A, \quad u \cdot a := \rho_A(a)u, \quad u \cdot u := \lambda \in R$$

für a_1, a_2, $a \in A$, sowie R-lineare Fortsetzung, so erhalten wir auf B die Struktur einer R-Algebra, welche projektiv von konstantem Rang 4 ist. Man überprüft leicht, dass die durch

$$\rho_B : \ a_1 + a_2 u \mapsto \rho_A(a_1) - a_2 u \quad (a_1,\, a_2 \in A)$$

definierte Abbildung eine Involution auf B ist: Die R-Linearität ist klar; für $a_1 + a_2 u$, $a_1' + a_2' u \in B$ gilt:

$$(a_1 + a_2 u)(a_1' + a_2' u) = a_1 a_1' + a_1 a_2' u + a_2 u a_1' + a_2 u a_2' u =$$
$$= a_1 a_1' + a_2 \rho_A(a_2')\lambda + (a_1 a_2' + a_2 \rho_A(a_1'))u,$$

sowie

$$\rho_B(a_1' + a_2' u)\rho_B(a_1 + a_2 u) = (\rho_A(a_1') - a_2' u)(\rho_A(a_1) - a_2 u) =$$
$$= \rho_A(a_1 a_1') + a_2' \rho_A(a_2)\lambda - (\rho_A(a_1')a_2 + a_2' a_1)u$$

und wir erhalten somit wegen der Kommutativität von A:

$$\rho_B\big((a_1 + a_2 u)(a_1' + a_2' u)\big) = \rho_A(a_1 a_1' + a_2 \rho_A(a_2')\lambda) - (a_1 a_2' + a_2 \rho_A(a_1'))u =$$
$$= \rho_A(a_1 a_1') + \rho_A(a_2)a_2'\lambda - (a_1 a_2' + a_2 \rho_A(a_1'))u = \rho_B(a_1' + a_2' u)\rho_B(a_1 + a_2 u).$$

Offenbar erfüllt ρ_B für alle a_1, $a_2 \in A$:

$$s_B(a_1 + a_2 u) := (a_1 + a_2 u) + \rho_B(a_1 + a_2 u) = a_1 + a_2 u + \rho_A(a_1) - a_2 u =$$
$$= a_1 + \rho_A(a_1) = s_A(a_1),$$
$$n_B(a_1 + a_2 u) := (a_1 + a_2 u)\rho_B(a_1 + a_2 u) = (a_1 + a_2 u)(\rho_A(a_1) - a_2 u) =$$
$$= n_A(a_1) - a_1 a_2 u + a_2 a_1 u - n_A(a_2)\lambda = n_A(a_1) - \lambda n_A(a_2),$$

wobei s_A die durch ρ_A definierte Spur, n_A die Norm auf A sei. Es nehmen also insbesondere s_B und n_B nur Werte in R an – ρ_B definiert somit eine Standardinvolution auf B.

Definition 3.2. *Das oben konstruierte verschränkte Produkt B mit Standardinvolution bezeichnen wir mit $(\lambda, A/R]$.*

Beispiel: Die Algebra $(-1, \mathbb{C}/\mathbb{R}]$ entspricht gerade den Hamiltonschen Quaternionen: Die Standardinvolution auf $\mathbb{C}$ ist die durch $x + iy \mapsto x - iy$ $(x, y \in \mathbb{C})$ gegebene Konjugation. Setzen wir $e_0 := 1,\ e_1 := i,\ e_2 := u,\ e_3 = -ui$, so bildet $\{e_0,\, e_1,\, e_2,\, e_3\}$ eine Basis und die Multiplikation in $(-1, \mathbb{C}/\mathbb{R}]$ ist gegeben durch $\mathbb{R}$-lineare Fortsetzung von $e_1^2 = -e_0,\ e_2^2 = -e_0,\ e_1 e_2 = -e_2 e_1 = e_3$.

Lemma 3.6. *Sei (E, q) ein projektiver quadratischer R-Modul von konstantem Rang 2. Weiters existiere ein Element $e \in E$ derart, dass $q(e) \in R^*$. Dann gilt:*

$$(E, q) \tilde{=} \big(C_0(E, q), q(e)n_0\big) \quad \text{und} \quad C(E, q) \tilde{=} \big(q(e), C_0(E, q)/R\big],$$

wobei n_0 die durch die Standardinvolution γ_0 auf $C_0(E, q)$ definierte Norm sei.

Beweis. Wegen $q(e) \in R^*$ ist e invertierbar in $C(E,q)$ mit Inversem $e^{-1} = q(e)^{-1}e$. Die Abbildung $\psi : C_0(E,q) \to E = C_1(E,q),\ y \mapsto ye$ ist daher ein Isomorphismus von $C_0(E,q)$-Moduln und da für alle $y \in C_0(E,q)$ die Gleichung $q(\psi(y)) = q(ye) = n_0(y)q(e)$ gilt, ist ψ offenbar eine Isometrie $(C_0(E,q), q(e)n_0) \to (E,q)$. Wenden wir die obige Konstruktion nun auf den $C_0(E,q)$-Modul $C(E,q) = C_0(E,q) \oplus C_0(E,q)e$ an, so entspricht die Multiplikation in $(q(e), C_0(E,q)/R]$ gerade der Multiplikation in $C(E,q)$ und wir haben somit auch die Isomorphie $C(E,q) \tilde{=} (q(e), C_0(E,q)/R]$ gezeigt. □

Sei A eine projektive R-Algebra von Rang 2 und $\lambda \in R^*$. Wir definieren nun eine Graduierung auf $(\lambda, A/R] = A \oplus Au$ durch

$$(\lambda, A/R]_0 := A \quad und \quad (\lambda, A/R]_1 := Au.$$

Proposition 3.7. *Sei A eine projektive R-Algebra von konstantem Rang 2 (als R-Modul) und n_A eine Normfunktion auf A. Dann sind für beliebiges $\lambda \in R^*$ die graduierten R-Algebren $C(A, \lambda n_A)$ und $(\lambda, A/R]$ isomorph. Insbesondere gilt: $C_0(A, \lambda n_A) \tilde{=} A$.*

Beweis. Sei γ_A die (eindeutige) Standardinvolution auf A. Für 1_A gilt offenbar $\lambda n_A(1_A) = \lambda 1_A \gamma_A(1_A) = \lambda$. Daher folgt aus dem vorangegangenen Lemma die Isomorphie

$$C(A, \lambda n_A) \tilde{=} \big(\lambda, C_0(A, \lambda n_A)/R\big].$$

Andererseits erhalten wir ebenfalls aus obigem Lemma: $(A, \lambda n_A) \tilde{=} (C_0(A, \lambda n_A), \lambda n_0)$, also insbesondere $A \tilde{=} C_0(A, \lambda n_A)$. Somit gilt:

$$C(A, \lambda n_A) \tilde{=} (\lambda, A/R].$$

Offensichtlich ist die Isomorphie auch mit den jeweiligen Graduierungen verträglich. □

3.4. **Similaritäten, Radikal und Kern.**

In diesem Abschnitt werden wir zunächst ein paar allgemeine Begriffe definieren, die wir im darauffolgenden Abschnitt benötigen werden, um ein grundlegendes Resultat über Kompositionsabbildungen auf projektiven quadratischen Räumen von konstantem Rang 2 zu beweisen (siehe [7, Chap. 1]).

Definition 3.3. *Eine* Similarität *von (E,q) in einen weiteren quadratischen R-Modul (E',q')* mit Multiplikator *$a \in R$ ist ein Homomorphismus $\chi : E \to E'$ von R-Moduln, sodass für alle $x \in E$ gilt:*

$$q'(\chi(x)) = aq(x).$$

Die bijektiven Similaritäten mit Multiplikator 1 sind offenbar gerade die Isometrien von (E,q) nach (E',q').
Ist $a \in R^*$, so gilt: $q(x) = a^{-1}q'(\chi(x))$. Versehen wir nun E' mit der quadratischen Form $a^{-1}q'$, so ist $\chi : (E,q) \to (E', a^{-1}q')$ ein R-Modul-Homomorphismus, der die quadratischen Formen respektiert. Es gibt daher einen eindeutigen Homomorphismus $C(\chi) : C(E,q) \to C(E', a^{-1}q')$ von R-Algebren, der $C(\chi) \circ \iota = \iota' \circ \chi$ erfüllt,

wobei $\iota : E \to C(E,q)$, $\iota' : E' \to C(E', a^{-1}q')$ die jeweiligen Strukturabbildungen seien (siehe Abschnitt 1.3).

$$\begin{tikzcd}
(E,q) \arrow[r, "\iota"] \arrow[d, "\chi"'] & C(E,q) \arrow[d, "C(\chi)"] \\
(E', a^{-1}q') \arrow[r, "\iota'"'] & C(E', a^{-1}q')
\end{tikzcd}$$

Da $C(\chi)$ die jeweiligen Graduierungen erhält, lässt sich $C(\chi)$ zu einem Homomorphismus $C_0(\chi) : C_0(E,q) \to C_0(E', a^{-1}q')$ von R-Algebren, sowie zu einem Homomorphismus $C_1(\chi) : C_1(E,q) \to C_1(E', a^{-1}q')$ von R-Moduln einschränken. Es gilt offenbar:

$$C_0(\chi)(\iota(x)\iota(x')) = \iota'(\chi(x))\iota'(\chi(x')), \quad \textit{sowie} \quad C_1(\chi)(y\iota(x)) = C_0(\chi)(y)\iota'(\chi(x))$$

für alle $x, x' \in E,\ y \in C_0(E,q)$.
Sind (E,q), (E',q') endlich erzeugte, projektive quadratische R-Moduln, so sind die Strukturabbildungen $\iota,\ \iota'$ injektiv und wir werden in diesem Fall wie üblich die Einbettungen von E und E' in die jeweiligen Clifford-Algebren notationell unterdrücken (siehe Abschnitt 1.8). Gilt außerdem $yx \in E$ für alle $y \in C_0(E,q),\ x \in E = \iota(E)$, so folgt:

$$\chi(yx) = C_0(\chi)(y)\chi(x).$$

Wir wollen nun zu beliebigen Similaritäten zwischen endlich erzeugten, projektiven quadratischen R-Moduln einen Homomorphismus $C(E,q) \to C(E',q')$ von R-Algebren mit ähnlichen Eigenschaften konstruieren. Dazu benötigen wir das folgende Resultat über skalierte Formen:

Proposition 3.8. *Ist (E,q) ein endlich erzeugter, projektiver quadratischer R-Modul und $u \in R^*$, so gibt es einen eindeutig bestimmten Isomorphismus $h : C_0(E, {}^u q) \to C_0(E,q)$ von R-Algebren, der ${}^u x\, {}^u x' = \iota'(x)\iota'(x') \mapsto u\iota(x)\iota(x') = uxx'$ erfüllt, wobei ι' und ι die jeweiligen Struktur-Abbildungen von $(E, {}^u q)$ bzw. (E,q) in die entsprechenden Clifford-Algebren sind.*

Beweis. Sei $\bar{E} := E \oplus Re$ und sei $\bar{q}$ die quadratische Form auf $\bar{E}$, die gegeben ist durch $\bar{q}|_E = q$, $\bar{q}(e) = -u$ sowie die Vorgabe, dass für die assoziierte symmetrische Bilinearform $\bar{b}$ die Gleichung $\bar{b}(x,e) = 0$ für alle $x \in E$ erfüllt sei. Wir definieren nun eine Abbildung $\alpha : E \to C_0(\bar{E}, \bar{q})$ durch $x \mapsto xe$. Wegen der Orthogonalität von E und Re erfüllt α offenbar:

$$(\alpha(x))^2 = (xe)^2 = -x^2e^2 = uq(x)1_{C(\bar{E},\bar{q})}$$

und da α R-linear ist, folgt aus der universellen Eigenschaft von Clifford-Algebren, dass es einen eindeutig bestimmten Homomorphismus $\bar{\alpha} : C(E, {}^u q) \to C_0(\bar{E}, \bar{q})$ von R-Algebren gibt, der α fortsetzt. Dabei werden die Erzeugenden ${}^u x\, {}^u x'$ $(x,\, x' \in E)$ von $C_0(E, {}^u q)$ auf $xex'e = -q(e)xx' = uxx' \in C_0(E,q) \subset C_0(\bar{E}, \bar{q})$ abgebildet. (Man beachte hierbei, dass $C(E,q)$ nach Abschnitt 1.8 in $C(\bar{E}, \bar{q})$ eingebettet werden kann.) Wir können $\bar{\alpha}$ daher zu einem Homomorphismus $h : C_0(E, {}^u q) \to C_0(E,q)$ einschränken.
Auf analoge Weise lässt sich eine Umkehrfunktion $C_0(E,q) \to C_0(E, {}^u q)$ konstruieren: Definiert man nämlich die quadratische Form $\bar{q}$ auf $\bar{E} = E \oplus Re$ durch $\bar{q}|_E = {}^u q$, $\bar{q}(e) = -u^{-1}$ sowie die Vorschrift, dass E und Re zueinander orthogonal sind, so erhält man einen eindeutig bestimmten Homomorphismus $C_0(E,q) = C_0(E, {}^{u^{-1}}\, {}^u q) \to C_0(E, {}^u q)$, der offenbar zu h invers ist. $\square$

Ist nun χ eine Similarität mit Multiplikator $a \in R^*$ zwischen endlich erzeugten, projektiven quadratischen R-Moduln, so gibt es nach Obigem einen eindeutigen Homomorphismus $h \circ C_0(\chi) : C_0(E,q) \to C_0(E',q')$ von R-Algebren (mit $h : C_0(E', {}^{a^{-1}}q') \to C_0(E',q')$ wie in der vorangegangenen Proposition), der für alle $x,\ x' \in E$

$$h \circ C_0(\chi)(xx') = a^{-1}\chi(x)\chi(x')$$

erfüllt.
Wir wollen nun den Isomorphismus $h : C_0(E', {}^{a^{-1}}q') \to C_0(E',q')$ zu einer Isomorphie $H : C(E', {}^{a^{-1}}q') \to C(E',q')$ fortsetzen. Sei $z = z_0 + z_1 \in C(E', {}^{a^{-1}}q') = C_0(E', {}^{a^{-1}}q') \oplus C_1(E', {}^{a^{-1}}q')$. Unter Verwendung der Bezeichnungen aus dem Beweis von Proposition 3.8 bildet der Homomorphismus $\bar\alpha : C(E', {}^{u^{-1}}q') \to C_0(\bar E, \bar q)$ (mit $\bar E = E' \perp Re$) von R-Algebren z_0 gerade auf $h(z_0)$ ab. Wegen $C_1(E', {}^{a^{-1}}q') = C_0(E', {}^{a^{-1}}q')E'$ wird der R-Modul $C_1(E', {}^{a^{-1}}q')$ von Elementen der Form z_0x mit $z_0 \in C_0(E', {}^{a^{-1}}),\ x \in E$ aufgespannt. Diese Erzeugenden werden durch den Homomorphismus $\bar\alpha$ auf $h(z_0)\alpha(x) = h(z_0)xe \in C_1(E',q')e$ abgebildet. Da h ein Isomorphismus ist und e (wegen $q'(e) = -a^{-1} \in R^*$) invertierbar ist, erhalten wir durch Einschränkung von $\bar\alpha$ einen Isomorphismus $C_1(E', {}^{a^{-1}}q') \to C_1(E',q')e$, und wegen der Invertierbarkeit von e einen Isomorphismus $h' : C_1(E', {}^{a^{-1}}q') \to C_1(E',q')$, der $h'(z_0x) = h(z_0)x$ für alle $z_0x \in C_0(E,q)E = C_1(E,q)$ erfüllt. Sei H der R-Modul-Isomorphismus $h \oplus h' : C(E', {}^{a^{-1}}q') = C_0(E', {}^{a^{-1}}q') \oplus C_1(E', {}^{a^{-1}}q') \to C(E',q')$.
Fassen wir nun E' als Teilmenge von $C(E',q')$ auf, so gilt für alle $z_0x \in C_0(E,q)E = C_1(E,q)$:

$$(H \circ C(\chi))_1(z_0x) = h'(C_0(\chi)(z_0)\chi(x)) = (H \circ C(\chi))_0(z_0)\chi(x).$$

Gilt nun $z_0x \in E$ für alle $z_0 \in C_0(E,q),\ x \in E$, so ist $(H \circ C(\chi))_0$ der eindeutige Homomorphismus von R-Algebren $C_0(E,q) \to C_0(E',q')$, sodass

$$\chi(z_0x) = (H \circ C(\chi))_0(z_0)\chi(x)$$

für alle $z_0x \in E = C_1(E,q)$ gilt.
Um die Notation zu vereinfachen, werden wir im folgenden den R-Modul-Isomorphismus H unterdrücken und schreiben $C_0(\chi)$ anstelle von $(H \circ C(\chi))_0 = h \circ C_0(\chi)$.

Wir benötigen noch die folgenden beiden Begriffe:

Definition 3.4. Radikal *und* Kern *eines quadratischen R-Moduls (E,q) sind definiert durch*

$$rad\,E := \{x \in E \mid b(x,E) = 0\}, \quad \textit{sowie} \quad \ker E := \{x \in rad\,E \mid q(x) = 0\}.$$

Ist b_E der durch $x \mapsto b(x,\,.\,)$ gegebene Homomorphismus vom R-Modul E in dessen Dualraum $Hom_R(E)$, so ist $rad\,E$ gerade der Kern von b_E. Ist 2 kein Nullteiler in R, so folgt wegen $b(x,x) = 2q(x)$ sofort $\ker E = rad\,E$.

3.5. **Kompositionsabbildungen.**

Definition 3.5. *Seien (E_1,q_1), (E_2,q_2) und (E,q) quadratische R-Moduln. Eine* Kompositionsabbildung *ist eine bilineare Abbildung $\nu : E_1 \times E_2 \to E$, sodass für alle $x_1 \in E_1,\ x_2 \in E_2$ gilt:*

$$q(\nu(x_1,x_2)) = q_1(x_1)q_2(x_2).$$

Satz 3.9. *Es seien* (E_1, q_1), (E_2, q_2) *und* (E, q) *primitive, projektive quadratische* R*-Moduln von konstantem Rang 2 und es gelte* $\ker E_i = \{0\}$ *für* $i = 1, 2$. *Ist* $\nu : E_1 \times E_2 \to E$ *eine Kompositionsabbildung, so gibt es eindeutig bestimmte Homomorphismen* $\eta_i : C_0(E_i, q_i) \to C_0(E, q)$ $(i = 1,\, 2)$ *von* R*-Algebren, sodass*

$$\nu(y_1 x_1, y_2 x_2) = \eta_1(y_1)\eta_2(y_2)\nu(x_1, x_2)$$

für alle $y_i \in C_0(E_i, q_i)$, $x_i \in E_i$ $(i = 1,\, 2)$ *gilt.*

Beweis. Wir zeigen die Aussage für den Fall, dass R ein lokaler Ring ist und E_i über $C_0(E_i, q_i)$ frei ist $(i = 1, 2)$. Der allgemeine Fall folgt dann mittels Lokalisierung, ähnlich wie im Beweis von Proposition 3.5.
Unter den obigen Voraussetzungen sind E_1, E_2, E, sowie $C_0(E_1, q_1)$, $C_0(E_2, q_2)$, $C_0(E, q)$ frei und von Rang 2 über R. Sei $\{e_i, f_i\}$ eine Basis von E_i über R, sodass $\{e_i\}$ eine Basis von E_i über $C_0(E_i, q_i)$ ist $(i = 1, 2)$. Es folgt dann wie im Beweis von Proposition 3.5, dass $q(e_i) \in R^*$ für $i = 1,\, 2$.

Wir zeigen zunächst die Eindeutigkeit. Seien $\eta_i : C_0(E_i, q_i) \to C(E, q)$ $(i = 1,\, 2)$ Homomorphismen von R-Algebren mit obiger Eigenschaft. Wir definieren für $x_i \in E_i$ $(i = 1,\, 2)$:

$$\kappa_1(x_1) := \nu(x_1, e_2), \quad \kappa_2(x_2) := \nu(e_1, x_2).$$

Da ν R-bilinear ist, ist (für $i = 1,\, 2$) κ_i offenbar ein R-Modul-Homomorphismus und erfüllt für alle $x_i \in E_i$:

$$q(\kappa_1(x_1)) = q(\nu(x_1, e_2)) = q_2(e_2)q_1(x_1)$$

$$\textit{sowie} \quad q(\kappa_2(x_2)) = q(\nu(e_1, x_2)) = q_1(e_1)q_2(x_2).$$

Es sind somit κ_1 und κ_2 Similaritäten von (E_1, q_1) bzw. (E_2, q_2) nach (E, q) mit Multiplikator $q_2(e_2)$ bzw. $q_1(e_1) \in R^*$. Es gibt daher nach Abschnitt 3.4 eindeutige Homomorphismen $C_0(\kappa_1) : C_0(E_1, q_1) \to C_0(E, q)$ und $C_0(\kappa_2) : C_0(E_2, q_2) \to C_0(E, q)$ von R-Algebren, die $\kappa_i(y_i x_i) = C_0(\kappa_i)(y_i)\kappa_i(x_i)$ für alle $y_i \in C_0(E_i, q_i)$, $x_i \in E_i$ $(i = 1,\, 2)$ erfüllen. Andererseits gilt auch für η_1, η_2:

$$\kappa_1(y_1 x_1) = \nu(y_1 x_1, e_2) = \eta_1(y_1)\eta_2(1_{C(E_2,q_2)})\nu(x_1, e_2) = \eta_1(y_1)\kappa_1(x_1)$$

$$\kappa_2(y_2 x_2) = \nu(e_1, y_2 x_2) = \eta_1(1_{C(E_1,q_1)})\eta_2(y_2)\nu(e_1, x_2) = \eta_2(y_2)\kappa_2(x_2)$$

und wegen der Eindeutigkeit des R-Algebren-Homomorphismus mit dieser Eigenschaft folgt

$$\eta_i = C_0(\kappa_i) \quad (i = 1,\, 2).$$

Es bleibt zu zeigen, dass (für $i = 1,\, 2$) η_i unabhängig von der Wahl der $C_0(E_i, q_i)$-Basis $\{e_i\}$ (mit $q(e_i) \in R^*$) von E_i ist. Sei also (für $i = 1,\, 2$) $\{e'_i\}$ eine weitere Basis von E_i über $C_0(E_i, q_i)$ und κ'_i der entsprechende Homomorphismus. Dann gilt:

$$C_0(\kappa_1)(y_1)C_0(\kappa_2)(y_2)\nu(x_1, x_2) = \nu(y_1 x_1, y_2 x_2) = C_0(\kappa'_1)(y_1)C_0(\kappa'_2)(y_2)\nu(x_1, x_2).$$

Setzen wir $y_2 = 1_{C(E_2,q_2)}$, $x_1 = e_1$, $x_2 = e_2$, so erhalten wir

$$C_0(\kappa_1)(y_1)\nu(e_1, e_2) = C_0(\kappa'_1)(y_1)\nu(e_1, e_2).$$

Wegen $q(\nu(e_1, e_2)) = q_1(e_1)q_2(e_2) \in R^*$ ist $\nu(e_1, e_2)$ in $C(E, q)$ invertierbar und es folgt daher die Gleichheit von $C_0(\kappa_1)$ und $C_0(\kappa'_1)$. Analog zeigt man, dass auch $C_0(\kappa_2) = C_0(\kappa'_2)$ gilt.

Nun zur Existenz: Der R-Modul-Homomorphismus κ_i sei für $i = 1,\, 2$ definiert wie oben. Wir setzen nun $\eta_i := C_0(\kappa_i)$. Weiters definieren wir eine R-bilineare Abbildung $\nu' : E_1 \times E_2 \to E$ durch

$$\nu'(y_1 e_1, y_2 e_2) := \eta_1(y_1)\eta_2(y_2)\nu(e_1, e_2)$$

und ein Element $g \in E$ durch

$$\nu'(f_1, f_2) = \nu(f_1, f_2) + g.$$

Unser Ziel ist es nun, zu zeigen, dass $g = 0$ gilt und also ν' mit der Kompositionsabbildung ν übereinstimmt.
Für beliebige $x_1 = y_1 e_1 \in E_1,\ x_2 = y_2 e_2 \in E_2$ gilt:

$$\begin{aligned} q(\nu'(x_1, x_2)) &= q(\eta_1(y_1)\eta_2(y_2)\nu(e_1, e_2)) = q(\eta_1(y_1)\nu(e_1, e_2)\nu(e_1, e_2)^{-1}\eta_2(y_2)\nu(e_1, e_2)) = \\ &= q(C_0(\kappa_1)(y_1)\kappa_1(e_1)\nu(e_1, e_2)^{-1}C_0(\kappa_2)(y_2)\kappa_2(e_2)) = \\ &= q(\kappa_1(x_1)q_1(e_1)^{-1}q_2(e_2)^{-1}\nu(e_1, e_2)\kappa_2(x_2)) = \\ &= q_1(e_1)^{-2}q_2(e_2)^{-2}n_0(\kappa_1(x_1)\nu(e_1, e_2))q(\kappa_2(x_2)) = \\ &= q_1(e_1)^{-2}q_2(e_2)^{-2}n_0(\nu(x_1, e_2)\nu(e_1, e_2))q_1(e_1)q_2(x_2) = \\ &= q_1(e_1)^{-1}q_2(e_2)^{-2}q_2(x_2)q(\nu(x_1, e_2))q(\nu(e_1, e_2)) = \\ &= q_1(e_1)^{-1}q_2(e_2)^{-2}q_2(x_2)q_1(x_1)q_2(e_2)q_1(e_1)q_2(e_2) = q_1(x_1)q_2(x_2) = q(\nu(x_1, x_2)), \end{aligned}$$

wobei n_0 die durch die Standardinvolution γ_0 definierte Norm auf $C_0(E, q)$ sei. Weiters gilt offenbar:

$$\nu'(e_1, x_2) = \nu'(e_1, y_2 e_2) = \eta_2(y_2)\nu(e_1, e_2) = C_0(\kappa_2)(y_2)\kappa_2(e_2) = \kappa_2(y_2 e_2) = \nu(e_1, x_2),$$

$$\nu'(x_1, e_2) = \nu'(y_1 e_1, e_2) = \eta_1(y_1)\nu(e_1, e_2) = C_0(\kappa_1)(y_1)\kappa_1(e_1) = \kappa_1(y_1 e_1) = \nu(x_1, e_2);$$

falls $x_1 = e_1$ oder $x_2 = e_2$ gilt, gilt also $\nu'(x_1, x_2) = \nu(x_1, x_2)$.
Setzen wir $x_1 = f_1,\ x_2 = f_2$, so erhalten wir:

$$q(\nu(f_1, f_2)) = q(\nu'(f_1, f_2)) = q(\nu(f_1, f_2) + g) = q(\nu(f_1, f_2)) + q(g) + b(\nu(f_1, f_2), g)$$

und es folgt daher

$$q(g) + b(\nu(f_1, f_2), g) = 0. \tag{4}$$

Setzen wir $x_1 = e_1 + f_1,\ x_2 = f_2$, so erhalten wir:

$$\begin{aligned} &q(\nu(e_1, f_2)) + q(\nu(f_1, f_2)) + b(\nu(e_1, f_2), \nu(f_1, f_2)) = q(\nu(e_1 + f_1, f_2)) = q(\nu'(e_1 + f_1, f_2)) = \\ &= q(\nu'(e_1, f_2) + \nu'(f_1, f_2)) = q(\nu(e_1, f_2) + \nu(f_1, f_2) + g) = \\ &= q(\nu(e_1, f_2)) + q(\nu(f_1, f_2)) + q(g) + b(\nu(e_1, f_2), \nu(f_1, f_2)) + b(\nu(e_1, f_2), g) + b(\nu(f_1, f_2), g) = \\ &= q(\nu(e_1, f_2)) + q(\nu(f_1, f_2)) + b(\nu(e_1, f_2), \nu(f_1, f_2)) + b(\nu(e_1, f_2), g) \end{aligned}$$

und es folgt daher

$$b(\nu(e_1, f_2), g) = 0. \tag{5}$$

Setzen wir $x_1 = f_1,\ x_2 = e_2 + f_2$, so erhalten wir analog zum vorangegangenen Fall

$$b(\nu(f_1, e_2), g) = 0. \tag{6}$$

Setzen wir nun zuletzt $x_1 = e_1 + f_1,\ x_2 = e_2 + f_2$, so erhalten wir:

$$\begin{aligned} q(\nu(e_1 + f_1, e_2 + f_2)) &= q(\nu'(e_1 + f_1, e_2 + f_2)) = \\ &= q(\nu'(e_1, e_2) + \nu'(f_1, e_2) + \nu'(e_1, f_2) + \nu'(f_1, f_2)) = \\ &= q(\nu(e_1, e_2) + \nu(f_1, e_2) + \nu(e_1, f_2) + \nu(f_1, f_2) + g) = \\ &= q(\nu(e_1 + f_1, e_2 + f_2) + g) = q(\nu(e_1 + f_1, e_2 + f_2)) + q(g) + b(\nu(e_1 + f_1, e_2 + f_2), g) = \\ &= q(\nu(e_1 + f_1, e_2 + f_2)) + q(g) + b(\nu(e_1, e_2), g) + b(\nu(f_1, e_2), g) + b(\nu(e_1, f_2), g) + b(\nu(f_1, f_2), g) = \\ &= q(\nu(e_1 + f_1, e_2 + f_2)) + b(\nu(e_1, e_2), g) \end{aligned}$$

und es folgt daher

$$b(\nu(e_1, e_2), g) = 0. \tag{7}$$

Nach Voraussetzung gilt $\ker E_i = \{x_i \in rad\, E_i \mid q_i(x_i) = 0\} = \{0\}$ für $i = 1, 2$. Wir zeigen nun, dass κ_1 daher injektiv ist: Sei $x_1 \in \ker \kappa_1$. Es gilt für beliebiges $x_1' \in E_1$:

$$\begin{aligned} q_2(e_2)b_1(x_1, x_1') &= q_2(e_2)q_1(x_1 + x_1') - q_2(e_2)q_1(x_1) - q_2(e_2)q_1(x_1') = \\ &= q(\nu(x_1 + x_1', e_2)) - q(\nu(x_1, e_2)) - q(\nu(x_1', e_2)) = \\ &= q(\kappa_1(x_1) + \kappa_1(x_1')) - q(\kappa_1(x_1)) - q(\kappa_1(x_1')) = b(\kappa_1(x_1), \kappa_1(x_1')) = 0. \end{aligned}$$

Da $q_2(e_2) \in R^*$, erhalten wir daher $b_1(x_1, x_1') = 0$ für alle $x_1' \in E_1$. Weiters folgt aus

$$0 = q(\kappa_1(x_1)) = q(\nu(x_1, e_2)) = q_1(x_1)q_2(e_2),$$

dass (wegen $q_2(e_2) \in R^*$) auch $q_1(x_1) = 0$ gelten muss. Es gilt also $\ker \kappa_1 \subset \ker E_1 = \{0\}$ und es folgt somit die Injektivität von κ_1.
Sei K_1 die Matrix zu κ_1 bezüglich der Basen $\{e_1, f_1\}$ von E_1 und $\{e, f\}$ von E. Aus der Injektivität von κ_1 folgt, dass die Determinante von K_1 kein Nullteiler ist. Sei nun K_1° die Adjungierte zu K_1. Es gilt dann $K_1 K_1^\circ = \det(K_1) \cdot Id$ und wir erhalten daher

$$\det(K_1) \cdot E = K_1 K_1^\circ E \subset K_1 E_1 = \kappa_1(E_1).$$

Wir wollen nun zeigen, dass $\ker E = \{0\}$ gilt. Sei $d_1 := \det(K_1)$ und $x \in \ker E$. Nach Obigem gibt es ein eindeutiges $x_1 \in E_1$, sodass $d_1 x = \kappa_1(x_1)$. Wegen $b(x, x') = 0$ für alle $x' \in E$ gilt für beliebiges $x_1' \in E_1$:

$$\begin{aligned} q_2(e_2)d_1 b_1(x_1, x_1') &= q_2(e_2)\big(q_1(x_1 + d_1 x_1') - q_1(x_1) - q_1(d_1 x_1')\big) = \\ &= q(\kappa_1(x_1 + d_1 x_1')) - q(\kappa_1(x_1)) - q(\kappa_1(d_1 x_1')) = \\ &= b(\kappa_1(x_1), \kappa_1(d_1 x_1')) = d_1 b(x, \kappa_1(d_1 x_1')) = 0. \end{aligned}$$

Da $q_2(e_2) \in R^*$ und d_1 kein Nullteiler ist, erhalten wir also $b_1(x_1, x_1') = 0$ für alle $x_1' \in E_1$. Aus $q(x) = 0$ folgt wegen

$$0 = d_1^2 q(x) = q(d_1 x) = q(\kappa_1(x_1)) = q_1(x_1)q_2(e_2),$$

dass auch $q_1(x_1) = 0$ gelten muss. Wir erhalten daher $x_1 \in \ker E_1 = \{0\}$, also $d_1 x = \kappa_1(x_1) = 0$, und da d_1 kein Nullteiler ist, folgt $x = 0$.
Wegen der Gleichungen (6) und (7) gilt $0 = b(\nu(E_1, e_2), g) = b(\kappa_1(E_1), g)$ und aus $d_1 E \subset \kappa_1(E_1)$ folgt $0 = b(d_1 E, g) = d_1 b(E, g)$. Da d_1 kein Nullteiler ist, muss somit $b(E, g) = 0$ gelten. Insbesondere gilt auch $b(\nu(f_1, f_2), g) = 0$ und aus Gleichung (4) erhalten wir daher $q(g) = 0$. Es folgt $g \in \ker E = \{0\}$, also $g = 0$ und damit die Gleichheit $\nu' = \nu$. □

3.6. **Existenz und Eindeutigkeit der Komposition.**

Seien A und A' zwei (als R-Moduln) projektive, treue R-Algebren von konstantem Rang 2, (E, q) ein quadratischer R-Modul von Typ A und $\eta : A \to A'$ ein Homomorphismus von R-Algebren mit Standardinvolution. Via η können wir nun A' als projektive A-Algebra von konstantem Rang 1 auffassen. Wir betrachten den A-Modul

$$E^\eta := A' \otimes_A E.$$

Da A' und E als A-Moduln projektiv sind und konstanten Rang 1 haben, ist E^η ein projektiver A'-Modul von Rang 1. Ist n' die Norm auf A', so sei q^η die eindeutige quadratische Form auf E^η (über R), die

$$q^\eta(a' \otimes x) = n'(a')q(x)$$

für alle $a' \in A'$, $x \in E$ erfüllt. Der quadratische R-Modul (E^η, q^η) ist somit von Typ A'.

Sind nun (E_1, q_1) und (E_2, q_2) quadratische R-Moduln von Typ A, so ist $E_1 \otimes_A E_2$ ein projektiver A-Modul von Rang 1. Versehen wir $E_1 \otimes_A E_2$ mit der eindeutigen quadratischen Form q, die $q(x_1 \otimes x_2) = q_1(x_1)q_2(x_2)$ für alle $x_1 \in E_1$, $x_2 \in E_2$ erfüllt, so gilt offenbar:

$$q(a \cdot (x_1 \otimes x_2)) = q((ax_1) \otimes x_2) = n(a)q_1(x_1)q_2(x_2) = n(a)q(x_1 \otimes x_2),$$

wobei n die Norm auf A sei, und der quadratische R-Modul $(E_1 \otimes_A E_2, q)$ ist daher von Typ A.

Definition 3.6. *Sind E_1, E_2, E drei R-Moduln vom Typ A_1, A_2, bzw. A und $\eta_i : A_i \to A$ $(i = 1, 2)$ Homomorphismen von R-Algebren mit Standardinvolution, so ist eine Kompositionsabbildung $\nu : E_1 \times E_2 \to E$* vom Typ (η_1, η_2), *falls für alle $a_i \in A_i,\ x_i \in E_i$ $(i = 1, 2)$*

$$\nu(a_1x_1, a_2x_2) = \eta_1(a_1)\eta_2(a_2)\nu(x_1, x_2)$$

gilt und zudem $E = A\nu(E_1, E_2)$ erfüllt ist, also E als A-Modul vom Bild von ν erzeugt wird.

Bemerkung: Sind E_1 und E_2 primitiv, so gibt es Elemente $e_1 \in E_1$ und $e_2 \in E_2$ mit $q_i(e_i) \in R^*$ für $i = 1, 2$. Wegen $q(\nu(e_1, e_2)) = q_1(e_1)q_2(e_2) \in R^*$ folgt, dass dann auch E primitiv ist. Nach 3.5 gilt daher $C_0(E, q) \tilde{=} A$. Andererseits folgt aus $q(\nu(e_1, e_2)) \in R^*$, dass $\nu(e_1, e_2)$ in $C(E, q)$ invertierbar ist. Daher ist die durch $y \mapsto y\nu(e_1, e_2)$ gegebene Abbildung $C_0(E, q) \to E$ bijektiv und wir erhalten somit die Isomorphie $E \tilde{=} A\nu(e_1, e_2)$. Die zweite Bedingung in obiger Definition ist für primitive quadratische Moduln also automatisch erfüllt.

Satz 3.10. *Seien A_1, A_2 und A drei R-Algebren, die (als R-Moduln) projektiv und treu sind und konstanten Rang 2 haben. Weiters seien (E_1, q_1) und (E_2, q_2) quadratische R-Moduln vom Typ A_1 bzw. A_2 und sei $\eta_i : A_i \to A$ für $i = 1, 2$ ein Homomorphismus von R-Algebren mit Standardinvolution. Dann gibt es einen quadratischen R-Modul (E, q) vom Typ A und eine Kompositionsabbildung $\nu : (E_1, q_1) \times (E_2, q_2) \to (E, q)$ vom Typ (η_1, η_2); diese sind eindeutig bis auf Isomorphie.*

Beweis. Wir definieren $E := E_1^{\eta_1} \otimes_A E_2^{\eta_2}$ und $q = q_1^{\eta_1} \otimes q_2^{\eta_2}$ (mit $E_i^{\eta_i} = A \otimes_{A_i} E_i$ und $q_i^{\eta_i}$ für $i = 1, 2$ wie oben) und die Abbildung ν durch

$$\nu(x_1, x_2) = (1_A \otimes x_1) \otimes (1_A \otimes x_2)$$

für $x_1 \in E_1,\ x_2 \in E_2$. Nach Obigem ist $(E_i^{\eta_i}, q_i^{\eta_i})$ für $i = 1, 2$ von Typ A und es ist daher auch (E, q) von Typ A. Die Abbildung ν ist offensichtlich R-bilinear und für alle $x_i \in E_i$ $(i = 1, 2)$ gilt:

$$q(\nu(x_1, x_2)) = q_1^{\eta_1}(1_A \otimes x_1)q_2^{\eta_2}(1_A \otimes x_2) = q_1(x_1)q_2(x_2);$$

somit ist ν eine Kompositionsabbildung. Weiters gilt für alle $a_i \in A_i,\ x_i \in E_i$ $(i = 1, 2)$:

$$\nu(a_1x_1, a_2x_2) = (1_A \otimes (a_1x_1)) \otimes (1_A \otimes (a_2x_2)) = (\eta_1(a_1) \otimes x_1) \otimes (\eta_2(a_2) \otimes x_2) =$$
$$= \eta_1(a_1)(1_A \otimes x_1) \otimes \eta_2(a_2)(1_A \otimes x_2) = \eta_1(a_1)\eta_2(a_2)\nu(x_1, x_2).$$

Trivialerweise ist auch $E = A\nu(E_1, E_2)$ erfüllt und die Kompositionsabbildung ν ist somit von Typ (η_1, η_2).

Es bleibt die Eindeutigkeitsaussage zu beweisen. Sei also $((E', q'), \nu')$ ein weiteres Paar, das die gewünschten Eigenschaften besitzt. Wir betrachten zunächst den Fall, dass A als Ring lokal und somit $E_i^{\eta_i}$ frei über A_i ist $(i = 1, 2)$. Sind $\{1_A \otimes e_1\}$, $\{1_A \otimes e_2\}$ Basen von $E_1^{\eta_1}$ bzw. $E_2^{\eta_2}$, so erzeugen nach Voraussetzung $\nu(e_1, e_2)$ und $\nu'(e_1, e_2)$ die A-Moduln E bzw. E'. Wir definieren nun einen A-Modul-Isomorphismus $\psi : E \to E'$ durch $\psi(\nu(e_1, e_2)) = \nu'(e_1, e_2)$. Es sind somit E und E' isomorph und für alle $x_1 = a_1 e_1 \in E_1,\ x_2 = a_2 e_2 \in E_2$ gilt:

$$(\psi \circ \nu)(x_1, x_2) = \psi\big(\eta_1(a_1)\eta_2(a_2)\nu(e_1, e_2)\big) = \eta_1(a_1)\eta_2(a_2)(\psi \circ \nu)(e_1, e_2) =$$

$$= \eta_1(a_1)\eta_2(a_2)\nu'(e_1, e_2) = \nu'(x_1, x_2).$$

Das Paar $((E, q), \nu)$ ist also bis auf Isomorphie eindeutig bestimmt.
Für den allgemeinen Fall folgt die Aussage mittels Lokalisierung: Für jedes Primideal $\mathfrak{p} \subset A$ erhalten wir wie oben einen Isomorphismus $\psi : E_{\mathfrak{p}} \to E'_{\mathfrak{p}}$ von freien $A_{\mathfrak{p}}$-Moduln; diese lokalen Isomorphismen lassen sich zu einem Isomorphismus $\psi : E \to E'$ „verkleben“, der $\psi \circ \nu = \nu'$ erfüllt. □

3.7. Die Gruppe G(A).

Im vorangegangenen Abschnitt haben wir gesehen, dass es zu zwei quadratischen R-Moduln (E_1, q_1), (E_2, q_2) von Typ A_1 bzw. A_2, einer treuen R-Algebra A von Rang 2 und vorgegebenen Homomorphismen $\eta_i : A_i \to A$ $(i = 1, 2)$ eine bis auf Isomorphie eindeutige Komposition $((E, q), \nu)$ von (E_1, q_1) und (E_2, q_2) gibt, sodass (E, q) von Typ A ist und ν von Typ (η_1, η_2). Wir wollen nun den Fall betrachten, dass A_1, A_2 und A übereinstimmen und die Homomorphismen η_i gerade die identische Abbildung sind.

Definition 3.7. *Sind (E_1, q_1), (E_2, q_2) quadratische R-Moduln von Typ A, so nennen wir eine Kompositionsabbildung $\nu : (E_1, q_1) \times (E_2, q_2) \to (E, q)$* von Typ A, *falls (E, q) ein quadratischer R-Modul von Typ A ist, und ν von Typ (id_A, id_A) ist.*

Satz 3.11. *Die Isomorphieklassen primitiver, projektiver quadratischer R-Moduln mit konstantem Rang 2, die von Typ A sind, bilden bezüglich der Komposition von Typ A eine abelsche Gruppe, die mit $G(A)$ bezeichnet wird.*

Beweis. Nach dem Beweis von Satz 3.10 ist die Komposition zweier Isomorphieklassen $[E_1, q_1]$, $[E_2, q_2]$ eindeutig durch $[E_1 \otimes_A E_2, q_1 \otimes q_2]$ zusammen mit der Kompositionsabbildung ν, welche durch $\nu(x_1, x_2) = x_1 \otimes x_2$ (für $x_1 \in E_1,\ x_2 \in E_2$) gegeben ist, bestimmt. Assoziativität und Kommutativität folgen daher sofort aus den entsprechenden Gesetzen für Tensorprodukte von Algebren. Ist n die Norm auf der R-Algebra A, so ist das neutrale Element offenbar gegeben durch $[A, n]$. Es bleibt zu einer beliebigen Isomorphieklasse $[E, q]$ ein Inverses bezüglich der Komposition zu finden. Sei (E, q) ein Repräsentant von $[E, q]$. Wir definieren nun auf dem quadratischen R-Modul (E, q) eine neue A-Modul-Struktur durch $a \cdot x := \rho(a)x$, wobei ρ die Standardinvolution auf A sei. Den resultierenden quadratischen R-Modul von Typ A bezeichnen wir mit $\overline{(E, q)}$. Da (E, q) primitiv ist, ist die Abbildung $\delta : C_0(E, q) \to A$ aus Satz 3.5 ein Isomorphismus von R-Algebren. Definieren wir nun $\psi : E \otimes_A \bar{E} \to A$ durch $\psi(x_1 \otimes x_2) = \delta(x_1 x_2)$ für $x_1,\ x_2 \in E$, so ist ψ ein A-Modul-Isomorphismus:
Sei zunächst A ein lokaler Ring. Dann ist E frei von Rang 1 über A. Da (E, q) primitiv ist, gibt es eine A-Basis $\{e\}$ von E mit $q(e) \in R^*$ (siehe Beweis von Proposition 3.5). Wir haben bereits früher bemerkt, dass sich die A-Modulstruktur von E auf Produkte in $C_0(E, q)$ fortsetzen lässt. Es folgt nun aus der Eindeutigkeit der

Standardinvolution ρ auf $A \tilde{=} Aee^{-1} = A1_{C(E,q)}$, dass $\gamma_0(a \cdot 1_{C(E,q)}) = \rho(a)1_{C(E,q)}$ gelten muss. Damit erhalten wir

$$\psi((ax_1) \otimes x_2) = \delta((ax_1)x_2) = \delta((a1_{C(E,q)})x_1x_2) = \delta(x_1\gamma_0(a1_{C(E,q)})x_2) = \\ = \delta(x_1(\rho(a)x_2)) = \psi(x_1 \otimes (a \cdot x_2))$$

für alle $a \in A,\ x_1, x_2 \in E$ und ψ ist daher bezüglich der A-Modul-Struktur auf $E \otimes_A \bar{E}$ wohldefiniert. Aus Proposition 3.5 folgt weiters:

$$(a\psi(x_1 \otimes x_2))e = (a\delta(x_1x_2))e = a(\delta(x_1x_2)e) = a(x_1x_2e) = \\ = (ax_1)x_2e = \delta((ax_1)x_2)e = \psi(a \cdot (x_1 \otimes x_2))e$$

für alle $a \in A,\ x_1, x_2 \in E$ und da $\{e\}$ eine A-Basis von E ist, erhalten wir $(a\psi(x_1 \otimes x_2)) = \psi(a \cdot (x_1 \otimes x_2))$ – also die A-Linearität der Abbildung ψ. Es gilt:

$$\psi(q(e)^{-1}e \otimes e) = q(e)^{-1}\delta(e^2) = q(e)^{-1}q(e)1_A = 1_A$$

und da ψ A-linear ist, folgt die Surjektivität von ψ. Da $E \otimes_A \bar{E}$ und A endlich erzeugte, projektive A-Moduln von konstantem Rang 1 sind, folgt aus der Surjektivität von ψ schon, dass ψ ein Isomorphismus ist (siehe Anhang). Den allgemeinen Fall zeigt man mittels Lokalisierung: Ist $\mathfrak{p} \subset A$ ein Primideal, so ist $\psi_{\mathfrak{p}} : E_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \bar{E}_{\mathfrak{p}} \to A_{\mathfrak{p}}$ ein $A_{\mathfrak{p}}$-Modul-Isomorphismus. Wegen der Isomorphie $E_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \bar{E}_{\mathfrak{p}} \tilde{=} (E \otimes_A \bar{E}) \otimes_A A_{\mathfrak{p}}$ sieht man nun leicht, dass ψ ein A-Modul-Isomorphismus ist. $\square$

ANHANG

Quadratische Moduln über lokalen Ringen.

Die folgenden Resultate findet man in [4, Kap. 4]. Ein Beweis zu Satz 1 kann etwa in [1, Chap.II, §3, Cor.2 zu Prop.5] nachgelesen werden. Es sei im folgenden R ein kommutativer Ring mit Eins, $\mathfrak{p} \subset R$ ein Primideal und (E, q) ein quadratischer R-Modul.

Die *Lokalisierung* $R_\mathfrak{p} := \{r/s \mid r \in R,\ s \in R \setminus \mathfrak{p}\}$ von R in $\mathfrak{p}$ ist ein lokaler Ring mit (einzigem) maximalem Ideal $\mathfrak{p}R_\mathfrak{p}$.

Wir bezeichnen $r/1 \in R_\mathfrak{p}$ mit $r_\mathfrak{p}$. Es gilt: $r \in R \setminus \mathfrak{p} \Rightarrow r_\mathfrak{p} \in R_\mathfrak{p}^*$.

Lemma 1. *Gilt $r_\mathfrak{p} = 0$ für alle Primideale $\mathfrak{p} \subset R$, so folgt: $r = 0$.*

$R_\mathfrak{p}$ ist eine kommutative R-Algebra und wir betrachten nun den $R_\mathfrak{p}$-Modul $E \otimes_R R_\mathfrak{p}$. Es gibt einen $R_\mathfrak{p}$-Modul-Isomorphismus von $E \otimes_R R_\mathfrak{p}$ auf den $R_\mathfrak{p}$-Modul $E_\mathfrak{p}$, den man durch Lokalisierung von E in $\mathfrak{p}$ erhält, mit $x \otimes (1/s) \mapsto x/s$ für alle $x \in E,\ s \in R \setminus \mathfrak{p}$. Wir identifizieren daher $E \otimes_R R_\mathfrak{p}$ mit $E_\mathfrak{p}$.

Da $R \neq 0$ kommutativ ist, haben zwei Basen eines freien R-Moduls stets dieselbe Kardinalität – diese bezeichnet man als den *Rang* $rk_R E$ des freien Moduls E über R (siehe etwa [6, Kap.VII, Satz 4.3]).

Satz 1. *Ist E ein endlich erzeugter, projektiver Modul über einem lokalen Ring R, so ist E frei von endlichem Rang.*

Ist E endlich erzeugt und projektiv, so ist also $E_\mathfrak{p}$ ein freier $R_\mathfrak{p}$-Modul von endlichem Rang.

Definition 1. *Sei $Spec(R)$ die Menge aller Primideale in R. Der* Rang *eines endlich erzeugten, projektiven R-Moduls E ist definiert als die Abbildung*

$$rg_E : Spec(R) \to \mathbb{N} \cup \{0\},$$

die gegeben ist durch $rg_E(\mathfrak{p}) = rg_{R_\mathfrak{p}} E_\mathfrak{p}$, wobei $rg_{R_\mathfrak{p}} E_\mathfrak{p}$ der Rang des freien $R_\mathfrak{p}$-Moduls $E_\mathfrak{p}$ ist.

Lemma 2. *Sei E endlich erzeugt und projektiv. Dann gilt: E ist genau dann treu, also $Ann_R(E) := \{r \in R \mid rx = 0\ \forall x \in E\} = \{0\}$, wenn für jedes Primideal $\mathfrak{p} \subset R$ gilt, dass $rg_{R_\mathfrak{p}} E_\mathfrak{p} \geq 1$.*

Proposition 1. *Seien E_1 und E_2 endlich erzeugte, projektive R-Moduln. Weiters gelte $rg_{E_1} = rg_{E_2}$. Ist $\varphi : E_1 \to E_2$ ein surjektiver Homomorphismus von R-Moduln, so ist φ ein Isomorphismus.*

Lemma 3. *Sei E endlich erzeugt und projektiv. Dann ist E genau dann nichtsingulär, wenn für alle Primideale $\mathfrak{p} \subset R$ der $R_\mathfrak{p}$-Modul $E_\mathfrak{p}$ nichtsingulär ist.*

Satz 2. *Sei R ein lokaler Ring und $E \neq 0$ frei von endlichem Rang und nichtsingulär. Dann existiert eine orthogonale Zerlegung $E = E_1 \perp E_2 \perp \ldots \perp E_k$ derart, dass E_i frei von Rang 1 oder 2 und nichtsingulär ist für alle $i = 1, \ldots, k$.*

Separabilität.

Die folgenden Resultate über separable Algebren sind [4, Kap. 2 und 9A] entnommen. Sei R ein kommutativer Ring (mit Eins) und A eine R-Algebra.

Wir betrachten die R-Algebra $A^e := A \otimes_R A^{op}$. Durch

$$(a \otimes b^{op})c = acb$$

für alle a, b, $c \in A$ erhalten wir eine A^e-Modul-Struktur auf A. Es gibt nun einen eindeutigen A^e-Modul-Homomorphismus $\phi : A^e \to A$ mit $\phi(a \otimes b^{op}) = ab$. Wegen $\phi(a \otimes 1^{op}) = a$, ist ϕ offensichtlich surjektiv. Die Sequenz

$$0 \longrightarrow ker\phi \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0 \tag{8}$$

ist also exakt.

Definition 2. *Eine R-Algebra A heißt* separabel*, falls die exakte Sequenz (8)* spaltet*, also falls ein Homomorphismus $\theta : A \to A^e$ von A^e-Moduln existiert, sodass $\phi \circ \theta = id_A$.*

Bemerkung:

(1) Ist A separabel, so gilt: $A^e = A \otimes_R A^{op} = ker\phi \oplus \theta(A)$.
(2) Im Spezialfall $A = R$ gilt $R = R^{op}$ und $\phi : R \otimes_R R^{op} \to R$ ist ein Isomorphismus mit Inverser $\theta := \phi^{-1} : r \mapsto r \otimes 1$. Es ist R daher eine separable R-Algebra.

Definition 3. *Ist A eine R-Algebra und $\phi : A^e \to A$ der eindeutige Homomorphismus von A^e-Moduln mit $\phi(a \otimes b^{op}) = ab$, so nennt man ein Element $e \in A^e = A \otimes_R A^{op}$* separabilitäts-idempotent für A, *falls*

$$\phi(e) = 1_A \quad \textit{und} \quad (1 \otimes a^{op})e = (a \otimes 1^{op})e$$

für alle $a \in A$ gilt.

Lemma 4. *Eine R-Algebra A ist genau denn separabel, wenn sie ein separabilitäts-idempotentes Element besitzt.*

Proposition 2. *Die freie R-Algebra $R[X]/(X^2 - aX - b)$ ist genau dann separabel, wenn $a^2 + 4b \in R^*$ gilt.*

Lemma 5. *Sind A und B separable Algebren über R, so ist auch $A \otimes_R B$ separabel über R und es gilt: $Z(A \otimes_R B) \tilde{=} Z(A) \otimes_R Z(B)$. Weiters ist für $n \in \mathbb{N}$ die R-Algebra $M_n(A)$ separabel und es gilt: $Z(M_n(A)) \tilde{=} Z(A)$.*

Lemma 6. *Sei A eine separable R-Algebra und S eine kommutative R-Algebra. Dann ist die S-Algebra $A \otimes_R S$ separabel und die natürliche Abbildung $Z(A) \otimes_R S \to Z(A \otimes_R S)$ ist ein Isomorphismus.*

Satz 3. *Sei A eine endlich erzeugte R-Algebra. Dann sind äquivalent:*

(1) *A ist separabel über R,*
(2) *$A \otimes_R R_{\mathfrak{m}}$ ist separabel über dem lokalen Ring $R_{\mathfrak{m}}$ für alle maximalen Ideale $\mathfrak{m} \subset R$,*
(3) *$A \otimes_R R/\mathfrak{m}$ ist separabel über dem Körper $R/\mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m} \subset R$.*

Satz 4. *Ist R ein Körper und A eine endlichdimensionale R-Algebra, so sind äquivalent:*

(1) *A ist zentral und separabel über R*
(2) *A ist zentral und einfach über R*
(3) *Es gibt eine endlichdimensionale zentrale Divisions-Algebra D über R, sodass $A \tilde{=} M_k(D)$ für ein $k \in \mathbb{N}$.*

Literatur

[1] N. Bourbaki, *Elements of Mathematics, Commutative Algebra, Chapters 1-7*, Springer-Verlag, Berlin-Heidelberg-New York, 1989.

[2] D.D. Fenster, J. Schwermer, *Composition of Quadratic Forms: An Algebraic Perspective*, in: C. Goldstein, N. Schappacher, J. Schwermer (Hg.), *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*, Springer, Berlin-Heidelberg-New York, 145-158 (2007).

[3] C.F. Gauss, H. Maser (Hg.), *Untersuchungen über höhere Arithmetik*, Chelsey Publishing Company, New York, 1981.

[4] A.J. Hahn, *Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups*, Springer-Verlag, New York, 1994.

[5] T.W. Hungerford, *Algebra*, Springer-Verlag, New York-Heidelberg-Berlin, 1974.

[6] J.C. Jantzen, J. Schwermer, *Algebra*, 2. Auflage, Springer, Berlin-Heidelberg, 2014.

[7] M. Kneser, *Composition of Binary Quadratic Forms*, Journal of Number Theory **15**, 406-413 (1982).

[8] M. Kneser, R. Scharlau (Mitarb.), *Quadratische Formen*, Springer, Berlin-Heidelberg, 2002.

[9] M.-A. Knus, *Quadratic and Hermitian Forms over Rings*, Grundlehren der mathematischen Wissenschaften 294, Springer-Verlag, Berlin-Heidelberg, 1991.

Zusammenfassung

Motiviert durch Martin Knesers Erkenntnisse über die Komposition binärer quadratischer Formen gibt diese Arbeit einen Überblick über die Theorie der Clifford-Algebren zu quadratischen Moduln über kommutativen Ringen. Der formale Aufbau umfasst drei Teile: Um den Leser in die Materie einzuführen, werden im ersten Kapitel zunächst grundlegende Resultate erläutert. Das zweite Kapitel behandelt die Struktur von Clifford-Algebren und deren gerader Teilalgebren. Im dritten Kapitel wird – auf den zuvor ausgearbeiteten Grundlagen aufbauend – Knesers Arbeit diskutiert: Indem man einen quadratischen Modul als Modul über der geraden Teilalgebra seiner Clifford-Algebra auffasst, lässt sich auf sehr elegante Weise eine allgemeine Theorie für die Komposition binärer quadratischer Formen aufbauen.

Abstract

Motivated by Kneser's work about composition of binary quadratic forms this thesis outlines the theory of Clifford algebras to quadratic modules over commutative rings. It comprises three parts: In the first chapter there are basic results shown to introduce the reader to Clifford algebras in this general setting. The second chapter treats the structure of Clifford algebras and their even subalgebras. The third chapter discusses Kneser's new and very efficient way of dealing with composition of projective quadratic modules of rank two by considering the quadratic module as a module over the even subalgebra of its Clifford algebra.

Curriculum Vitae

Karen Klein

Geburtsdatum:	25. August 1989
Geburtsort:	Karlsruhe
Staatsbürgerschaft:	Österreich

Bildungsweg

seit September 2011	Masterstudium Mathematik an der Universität Wien
November 2014	Abschluss des Diplomstudiums Instrumentalstudium, Studienzweig Violine an der Universität für Musik und darstellende Kunst Wien
September 2011	Abschluss des Bachelorstudiums Mathematik an der Universität Wien
August/September 2010:	einmonatiges Praktikum am Institut für Demographie (VID) der Österreichischen Akademie der Wissenschaften (ÖAW)
Juni 2007:	Matura mit ausgezeichnetem Erfolg am Gymnasium Stubenbastei, Wien