Involutionen als Erzeugende in unitären Gruppen

Dissertation

zur

Erlangung des Doktorgrades

der

Mathematisch - Naturwissenschaftlichen Fakultät

der Christian-Albrechts-Universität zu Kiel

vorgelegt von

Florian Bünger

Kiel 1997

Involutionen als Erzeugende in unitären Gruppen

Florian Bünger

*Es ist mit der üblen Laune völlig wie mit der Trägheit,
denn es ist eine Art von Trägheit. Unsere Natur hängt
sehr dahin und, wenn wir nur einmal die Kraft haben,
uns zu ermannen, geht uns die Arbeit frisch von der Hand,
und wir finden in der Tätigkeit ein wahres Vergnügen.*

(J.W. v. Goethe : Werther, Am 1. Julius)

Einleitung

Für die **Strukturanalyse** der sogenannten 'Klassischen Gruppen' [mit diesen sind hier allgemeine lineare Gruppen und orthogonale, symplektische oder unitäre Gruppen bezüglich regulärer symplektischer, symmetrischer oder hermitescher Formen auf einem endlich-dimensionalen Vektorraum über einem kommutativen Körper gemeint] hat es sich bewährt, Erzeugendensysteme mit besonderen Eigenschaften zu studieren. Dies findet in exemplarischer Weise in dem bekannten Werk 'La géométrie des groupes classiques' von J. Dieudonné [22] seine Bestätigung.
Was aber sind ausgezeichnete Erzeugendensysteme? Sicherlich bilden die **einfachen** Elemente einer klassischen Gruppe ein solches. Dies sind Abbildungen, die eine Hyperebene festlassen, oder anders formuliert: Abbildungen, die auf dem projektiven Raum eine Axial-Kollineation induzieren. Dabei unterscheidet man zwischen Transvektionen - das Zentrum der induzierten Abbildung liegt auf der Achse - und Dilatationen. Falls die betrachtete klassische Gruppe sowohl Transvektionen als auch Dilatationen enthält, werden diese beiden Erzeugendensysteme gewöhnlich getrennt untersucht. Klassische Resultate lauten:

(1) Alle einfachen Elemente einer symplektischen Gruppe sind Transvektionen, und diese erzeugen die ganze Gruppe.

(2) Alle einfachen Elemente orthogonaler Gruppen sind Symmetrien [involutorische einfache Abbildungen]. Hat der Grundkörper eine Charakteristik $\neq 2$, so sind die Symmetrien Dilatationen und andernfalls Transvektionen. Jede orthogonale Gruppe mit der einzigen Ausnahme $\mathrm{O}^+(4,2)$ wird von ihren einfachen Elementen erzeugt.

(3) Dilatationen in unitären Gruppen werden Quasi-Symmetrien genannt. Bis auf $\mathrm{U}(2,2)$ wird jede unitäre Gruppe von Quasi-Symmetrien erzeugt.

Weiterhin ist man an Erzeugendensystemen interessiert, deren Elemente keiner Einschränkung hinsichtlich der Dimension ihres Fix-Raumes unterliegen. Weil diese Produkte der unter (1) bis (3) aufgeführten einfachen Elemente sind [mit den angegebenen Ausnahmen], liegt es nahe, möglichst 'elementare' Produkte zu betrachten. Es bieten sich diejenigen an, die aus paarweise kommutierenden Faktoren bestehen. In orthogonalen Gruppen über Körpern mit Charakteristik $\neq 2$ erhält man auf diese Weise alle Involutionen. In unitären Gruppen werden diese Abbildungen E.W. Ellers [28] folgend Quasi-Involutionen genannt.
Wie üblich, geht die Analyse stets mit der **Kennzeichnung** einher, so daß der Wunsch besteht eine klassische Gruppe über die Eigenschaften eines Erzeugendensystems axiomatisch zu charaktrisie-

ren. In dem Buch von F. Bachmann [2] über den 'Aufbau der Geometrie aus dem Spiegelungsbegriff' heißt es hierzu:

> Eine Lösung des Charakterisierungsproblems wird erleichert, wenn zuvor das **Längenproblem** und das **Relationenproblem** gelöst werden. Das Längenproblem ist die Frage nach der Minimalzahl von Erzeugenden, die zur Darstellung eines bestimmten Gruppenelements notwendig sind. Das Relationenproblem ist die Frage nach einer Menge möglichst kurzer Relationen zwischen Erzeugenden mit der Eigenschaft, daß jede Relation zwischen Erzeugenden Folgerelation von Relationen dieser Menge ist.

Es sind die grundlegenden Arbeiten von E. Cartan [15], P. Scherk [65], J. Dieudonné [21] und D. Callan [13], in denen die Längenprobleme bezüglich der unter (1) bis (3) angegebenen Erzeugendensysteme gelöst werden. Das Involutionen-Längenproblem in orthogonalen Gruppen und symplektischen Gruppen über Körpern der Charakteristik 2 wird in den Arbeiten von M.J. Wonenburger [79], D.Ž. Djoković [23], R. Gow [38] und E.W. Ellers und W. Nolte [29] gelöst.

Diese Arbeit ordnet sich in den Kreis der Längenprobleme ein, und gehört daher im Sinne von Bachmann dem Bereich der Kennzeichnung klassischer Gruppen an. Gegenstand sind unitäre Gruppen, und als Erzeugendensysteme in diesen werden einerseits unitäre Symmetrien und andererseits die Menge aller unitären Involutionen betrachtet. Es werden die Längenprobleme bezüglich beider Erzeugendensysteme eingehend studiert.
Für das Involutionen-Längenproblem ist es naheliegend, ersteinmal zu fragen, wann ein unitäres Element ein Produkt von zwei unitären Involutionen ist. Diesem Problem ist das Kapitel 2 gewidmet. Der dort eingeschlagene Weg erfordert eine genaue Kenntnis der auf J. Williamson und G.E. Wall zurückgehenden Beschreibung der Konjugiertenklassen klassischer Gruppen. Eine konzentrierte Einführung in dieses Gebiet gibt das erste Kapitel. Kapitel 3 behandelt dann das Symmetrien-Längenproblem - dabei bereiten die kleinen Körper F_4 und F_9 besondere Schwierigkeiten - und Kapitel 4 das Involutionen-Längenproblem. Dieses hängt eng mit den Vermutungen von O. Ore und J.G. Thompson zusammen. Den Kapiteln 2,3 und 4 sind ausführliche Einleitungen vorangestellt, auf welche ich hier für eine genaue Beschreibung der hergeleiteten Kernresultate verweisen möchte.

Ich freue mich, an dieser Stelle all denjenigen danken zu können, die mich und diese Arbeit während der letzten Jahre begleitet haben. Besonderen Dank schulde ich Herrn Prof. Dr. F. Knüppel, auf dessen Anregung sie entstanden ist, und Herrn Dr. K. Nielsen für die vielen klärenden Diskussionen, ohne die einige Abschnitte sicherlich ärmer ausgefallen wären.

Zu außerordentlichem Dank bin ich der Friedrich-Ebert-Stiftung verpflichtet, die mich durch ein Doktoranden-Stipendium gefördert hat.

Inhaltsverzeichnis

Kapitel 1

Grundlagen

1.1 Notation

Im gesamten Text seien K ein (kommutativer) Körper, $^-$ ein involutorischer Körperautomorphismus von K ($^- = 1_K$ sei zunächst zugelassen) und V ein K-Vektorraum. Der Fixkörper $\{\mu \in K | \bar{\mu} = \mu\}$ von $^-$ sei mit F bezeichnet. Ist $^- \neq 1_K$, so ist K eine quadratische Körpererweiterung von F. Sei W ein weiterer K-Vektorraum. Die Menge der K-linearen Abbildungen von V nach W nennen wir $\mathrm{Hom}_K(V, W)$ oder auch einfachheitshalber $\mathrm{Hom}(V, W)$. Im Fall $V = W$ schreiben wir $\mathrm{Hom}_K(V)$ bzw. $\mathrm{Hom}(V)$. Ferner bezeichne $\mathrm{GL}(V)$ die Gruppe der K-linearen Bijektionen von V, und für $n \in \mathbb{N}$ sei $\mathrm{GL}_n(K)$ die Gruppe der invertierbaren $n \times n$ Matrizen mit Einträgen aus K und neutralem Element $I = I_n$. Haben V und W endliche Dimensionen n bzw. m, und ist $\mathcal{A} = (a_i)_{1 \leq i \leq n}$ eine Basis von V, $\mathcal{B} = (b_i)_{1 \leq i \leq m}$ eine Basis von W mit zugehöriger dualer Basis $\mathcal{B}^* = (b_i^*)_{1 \leq i \leq m}$, und ist $\pi \in \mathrm{Hom}_K(V, W)$, so nennen wir $\mathcal{M}_{\mathcal{B}}^{\mathcal{A}}(\pi) := ((a_i \pi) b_j^*)_{(i,j) \in \mathbb{N}_{\leq n} \times \mathbb{N}_{\leq m}} \in K^{n \times m}$ die Matrix von π bezüglich $\mathcal{A}$ und $\mathcal{B}$. Ist $\mathcal{A} = \mathcal{B}$, so schreiben wir $\mathcal{M}_{\mathcal{A}}(\pi)$ anstelle von $\mathcal{M}_{\mathcal{A}}^{\mathcal{A}}(\pi)$. Für $\pi \in \mathrm{Hom}(V)$ und $\mu \in K$ bezeichne $\mathrm{F}_\mu(\pi) := \ker(\pi - \mu)$ den μ-Eigenraum von π. Man nennt $\mathrm{F}(\pi) := F_1(\pi)$ den Fixraum, $\mathrm{B}(\pi) := V(\pi - 1)$ die Bahn und $\mathrm{B}^2(\pi) := V(\pi - 1)^2$ die zweite Bahn von π. Sind $\phi, \psi \in \mathrm{Hom}(V)$, so erhält man aus der Identität

$$(\phi - 1)(\psi - 1) = (\phi\psi - 1) - (\phi - 1) - (\psi - 1)$$

die grundlegende Beziehung

$$\mathrm{B}(\phi\psi) + \mathrm{B}(\psi) = \mathrm{B}(\phi) + \mathrm{B}(\psi).$$

Für $v \in V$ sei $\langle v \rangle_\pi := \langle v\pi^i | i \in \mathbb{N} \cup \{0\} \rangle$ der von v erzeugte π-Modul. Man nennt π zyklisch oder auch V π-zyklisch, wenn $V = \langle v \rangle_\pi$ für ein $v \in V$ gilt. Man nennt V π-zerlegbar, falls es nichttriviale π-invariante Unterräume U, W von V gibt, so daß $V = U \oplus W$ ist. Ist V endlichdimensional, so kürzen wir das charakteristische Polynom von π mit $\mathrm{char}(\pi)$, das Minimalpolynom mit $\mathrm{mip}(\pi)$ und den π-Annullator eines Vektors $v \in V$ mit $\mathrm{ann}_\pi(v)$ ab. Es gibt dann Vektoren $a_1, \ldots, a_m$, $m \in \mathbb{N}$, so daß $V = \langle a_1 \rangle_\pi \oplus \cdots \oplus \langle a_m \rangle_\pi$ ist, und die π-Moduln $\langle a_i \rangle_\pi$ π-unzerlegbar sind. Zu jedem $i \in \mathbb{N}_{\leq m}$ gibt es ein normiertes irreduzibles Polynom $p_i \in K[x]$ und ein $n_i \in \mathbb{N}$ mit $\mathrm{ann}_\pi(a_i) = p_i^{n_i}$. Das Polynom $\mathrm{ann}_\pi(a_i)$ wird ein (Weierstraß'scher) Elementarteiler von π genannt

und die Zahl $|\{j \in \mathbb{N}_{\leq m}; \mathrm{ann}_\pi(a_j) = \mathrm{ann}_\pi(a_i)\}|$ seine Vielfachheit. Die Menge $\{\mathrm{ann}_\pi(a_i); i \in \mathbb{N}_{\leq m}\}$ und die Vielfachheit jedes ihrer Elemente ist unabhängig von der Wahl der a_i. Man kann daher von '**der** Menge der Elementarteiler von π' und '**der** Vielfachheit eines Elementarteilers' sprechen. Mit 'den Elementarteilern von π' sei stets die Menge der Elementarteiler von π gemeint. Die Ähnlichkeitsklasse $\{\psi^{-1}\pi\psi; \psi \in \mathrm{GL}(V)\}$ von π ist dann eindeutig durch die Elementarteiler von π und deren Vielfachheiten festgelegt.
Sind schließlich A und B Mengen, C eine Teilmenge von A und f eine Abbildung von A nach B, so bezeichne f_C die Restriktion von f auf C.

Alle weiteren Bezeichnungen gehören entweder zum mathematischen Standardvokabular oder werden im Kontext erklärt.

1.2 Sesquilinearformen und Klassische Gruppen

Die Ausführungen dieses Abschnittes folgen im wesentlichen [8], [40] Kapitel 1, [41] 5.1A und [52] XIII, §7, und erheben keinen Anspruch auf Originalität. Sie dienen lediglich zur Einführung der im weiteren verwendeten Terminologie.

Definition 1.2.1 (Anti-Vektorraum/Anti-Dualraum/Semilinearität) *Der durch die Skalarenmultiplikation $k \bullet v := \bar{k}v$, $k \in K$ und $v \in V$, und die ursprüngliche Addition auf V definierte K-Vektorraum $\bar{V}$ heißt der Anti-Vektorraum von V (bezüglich $^-$). Bezeichnet man den Dualraum von V mit V^*, so heißt $\overline{V^*}$ der Anti-Dualraum von V.*
Ein $\pi \in \mathrm{Hom}_K(W, \bar{V})$ heißt $^-$-anti-linear oder $^-$-semi-linear.

Wir fixieren einen weiteren K-Vektorraum W.

Definition/Satz 1.2.2 (adjungierte Abbildung) *Sei $\pi \in \mathrm{Hom}_K(V, W)$. Dann wird durch $\alpha \mapsto \pi\alpha$ eine lineare Abbildung ${}^*\pi : \overline{W^*} \to \overline{V^*}$ definiert, welche man die zu π adjungierte Abbildung nennt. Im Falle $^- = 1_K$ schreibt man auch ${}^t\pi$ statt ${}^*\pi$ und nennt ${}^t\pi$ die zu π transponierte Abbildung.*
Sind V und W endlichdimensional mit Basen $\mathcal{V} = (v_i)_{i\in\mathbb{N}_{\leq n}}$ und $\mathcal{W} = (w_j)_{j\in\mathbb{N}_{\leq m}}$, und bezeichnet man mit $\mathcal{V}^* := (v_i^*)_{i\in\mathbb{N}_{\leq n}}$ und $\mathcal{W} = (w_j^*)_{j\in\mathbb{N}_{\leq m}}$ die zu $\mathcal{V}$ und $\mathcal{W}$ dualen Basen, so sind diese auch Basen von $\overline{V^*}$ bzw. $\overline{W^*}$ und es gilt

$$\mathcal{M}_{\mathcal{V}^*}^{\mathcal{W}^*}({}^*\pi) = \overline{\mathcal{M}_{\mathcal{W}}^{\mathcal{V}}(\pi)}^t.$$

Beweis. Wegen $\pi \in \mathrm{Hom}_K(V, W)$, gilt $\pi\alpha \in \mathrm{Hom}(V, K) = V^*$ für jedes $\alpha \in W^*$. Folglich ist ${}^*\pi$ eine wohldefinierte Abbildung. Für $k \in K$ und $\alpha, \beta \in W^*$ gilt $(k \bullet \alpha + \beta)^*\pi = \pi(k \bullet \alpha + \beta) = k \bullet (\pi\alpha) + \pi\beta = k \bullet (\alpha^*\pi) + \beta^*\pi$, i.e. ${}^*\pi \in \mathrm{Hom}_K(\overline{W^*}, \overline{V^*})$.
Seien V und W endlichdimensional und $\mathcal{V} = (v_i)_{i\in\mathbb{N}_{\leq n}}$, $\mathcal{W} = (w_j)_{j\in\mathbb{N}_{\leq m}}$, $\mathcal{V}^* := (v_i^*)_{i\in\mathbb{N}_{\leq n}}$ und $\mathcal{W} = (w_j^*)_{j\in\mathbb{N}_{\leq m}}$ wie oben. Die kanonische Einbettung $i_V : V \to V^{**}, \alpha(vi_V) := v\alpha$, $v \in V$, $\alpha \in V^*$, ist ein Isomorphimus, und $\{v_1 i_V, \ldots, v_n i_V\}$ ist die zu $\mathcal{V}^*$ duale Basis. Für $j \in \mathbb{N}_{\leq m}$ und $i \in \mathbb{N}_{\leq n}$ gilt $(w_j^*({}^*\pi))(v_i i_V) = (v_i\pi)w_j^*$, also $w_j^*({}^*\pi) = \sum_{i=1}^n (w_j^*({}^*\pi))(v_i i_V)v_i^* = \sum_{i=1}^n \overline{(v_i\pi)w_j^*} \bullet v_i^*$. Hieraus

folgt, daß der (j,i)-Eintrag in $\mathcal{M}_{\mathcal{V}^*}^{\mathcal{W}^*}({}^*\pi)$ gerade $\overline{(v_i\pi)w_j^*}$ ist. Weil $(v_i\pi)w_j^*$ der (i,j)-Eintrag von $\mathcal{M}_{\mathcal{W}}^{\mathcal{V}}(\pi)$ ist, folgt die Behauptung. ■

Zur Motivation der bald folgenden Definition von $^-$-Sesquilinearformen machen wir die

Beobachtung 1.2.3 *Sei $W \leq \overline{V^*}$. Dann hat die Abbildung $f : V \times W \to K, f(v,w) := vw$ folgende Eigenschaften :*

(i) $f_r : W \to \overline{V^*}, w \mapsto f(\cdot, w)$ *ist eine wohldefinierte Abbildung aus* $\mathrm{Hom}_K(W, \overline{V^*})$.

(ii) $f_l : V \to \overline{W}^*, v \mapsto f(v, \cdot)$ *ist eine wohldefinierte Abbildung aus* $\mathrm{Hom}_K(V, \overline{W}^*)$.

Beweis. (i). Es gilt $f_r = 1_W$.
(ii). Seien $k,l \in K$, $v_1, v_2 \in V$ und $w_1, w_2 \in W$. Dann gilt

$$f(v_1 + kv_2, w_1 + lw_2) = f(v_1, w_1) + kf(v_2, w_1) + lf(v_1, w_2) + klf(v_2, w_2).$$

Für $k = 0$ erhält man $(w_1 + lw_2)(v_1 f_l) = w_1(v_1 f_l) + l(w_2(v_1 f_l))$, i.e. $v_1 f_l \in \overline{W}^*$. Für $l = 0$ erhält man $(w_1)((v_1 + kv_2)f_l) = w_1(v_1 f_l) + k(w_1(v_2 f_l))$, i.e. f_l ist K-linear. ■

Definition 1.2.4 (Sesquilinearform) *Eine Abbildung $f : V \times W \to K$ heißt $^-$-Sesquilinearform auf $V \times W$ (auf V im Falle $V = W$), wenn die Bedingungen* (i) *und* (ii) *aus 1.2.3 erfüllt sind. Dies ist genau dann der Fall, wenn*

$$f(v_1 + kv_2, w_1 + lw_2) = f(v_1, w_1) + kf(v_2, w_1) + \bar{l}f(v_1, w_2) + k\bar{l}f(v_2, w_2)$$

für alle $k, l \in K$, $v_1, v_2 \in V$ und $w_1, w_2 \in W$ gilt.
*Man nennt f-*lrad $:= \ker f_l$ *das Linksradikal, f-*rrad $:= \ker f_r$ *das Rechtssradikal von f und f-*rad $:= \ker f_l \cap \ker f_r$ *das Radikal von f.*
Man nennt f :

(i) *rechtsregulär (linksregulär), falls f_r (f_l) injektiv ist;*

(ii) *regulär, falls f rechts- und linksregulär ist ;*

(iii) *rechtsreflexiv (linksreflexiv), falls f_r (f_l) surjektiv ist;*

(iv) *reflexiv, falls f rechts- und linksreflexiv ist ;*

(v) *nicht rechtssingulär (nicht linkssingulär), falls f_r (f_l) bijektiv ist;*

(vi) *nicht singulär, falls f nicht rechts- und nicht linkssingulär ist.*

*Sind $Y \leq V$ und $Z \leq W$ Unterräume, so nennt man den K-Vektorraum $Y \times Z$ bzw. Y, falls $Y = Z$ ist, f-rechtsregulär, f-linksregulär, f-regulär, f-rechtsreflexiv , f-linksreflexiv, f-reflexiv, nicht f-rechtssingulär, nicht f-linkssingulär bzw. f-singulär, falls dies auf die $^-$-Sesquilinearform $f_{Y\times Z}$ zutrifft. Ferner setzt man f-*lrad $Y \times Z := f_{Y\times Z}$-lrad, *$f$-*rrad $Y \times Z := f_{Y\times Z}$-rrad *und* f-rad $Y \times Z := f_{Y\times Z}$-rad.
Falls keine Verwechslung möglich ist, wird das Präfix 'f' in obiger Notation fortgelassen, und im Falle $Y = Z$ schreibt man stets nur Y anstelle von $Y \times Y$.

Bezeichnung 1.2.5 (kanonische Sesquilinearform)
Eine wie in 1.2.3 definierte $^-$-Sesquilinearform nennt man eine kanonische $^-$-Sesquilinearform. Ist f eine beliebige $^-$-Sesquilinearform auf $V \times W$, so stimmt f mit der kanonischen $^-$-Sesquilinearform auf $V \times f_r(W)$ überein.

Für das weitere sei eine $^-$-Sesquilinearform f auf $V \times W$ fixiert.

Bemerkung 1.2.6 (transponierte Sesquilinearform) *Die Abbildung $\tilde{f} : W \times V \to K, (v, w) \mapsto \overline{f(w, v)}$ ist eine $^-$-Sesquilinearform auf $W \times V$ und heißt die zu f transponierte $^-$-Sesquilinearform. Sie ist genau dann rechtsregulär (linksregulär, rechtsreflexiv, linksreflexiv), wenn f linksregulär (rechtsregulär, linksreflexiv, rechtsreflexiv) ist.* ∎

Lemma 1.2.7 (Regularität, Reflexivität, Singularität) *Für die in 1.2.4* (i)-(vi) *eingeführten Begriffe gelten folgende Implikationen :*

(i) *f ist nicht rechtssingulär $\Rightarrow$ f ist rechtsreflexiv $\Rightarrow$ f ist linksregulär;*
(ii) *f ist nicht linkssingulär $\Rightarrow$ f ist linksreflexiv $\Rightarrow$ f ist rechtsregulär;*
(iii) *f ist nicht singulär $\Rightarrow$ f ist reflexiv $\Rightarrow$ f ist regulär.*

Beweis. Die ersten Implikation in (i)-(iii) sind per Definition wahr.
(i). Sei f rechtsreflexiv. Dann gilt $\ker f_l \leq \cap_{w\in W} \ker f_r(w) = \cap_{\alpha \in \overline{V^*}} \ker \alpha = \{0\}$.
(ii) folgt mit 1.2.6 aus (i) angewandt auf $\tilde{f}$ und (iii) erhält man aus (i) und (ii). ∎

Als nächstes betrachten wir die endlichdimensionale Situation und klären die Zusammenhänge der in 1.2.4 (i)-(vi) eingeführten Begriffe für diesen Spezialfall.

Definition/Satz 1.2.8 (Gram'sche Matrix) *Sind V und W endlichdimensional mit Basen $\mathcal{V} = (v_i)_{i\in\mathbb{N}_{\leq n}}$ und $\mathcal{W} = (w_j)_{j\in\mathbb{N}_{\leq m}}$, so heißt $\mathcal{M}^{\mathcal{V}}_{\mathcal{W}}(f) := (f(v_i, w_j)_{(i,j)\in\mathbb{N}_{\leq n}\times\mathbb{N}_{\leq m}})$ die Gram'sche Matrix von f bezüglich $\mathcal{V}$ und $\mathcal{W}$. Falls $\mathcal{V} = \mathcal{W}$ ist, nennt man einfachheitshalber $\mathcal{M}_{\mathcal{V}}(f) := \mathcal{M}^{\mathcal{V}}_{\mathcal{V}}(f)$ die Gram'sche Matrix von f bezüglich $\mathcal{V}$. Bezeichnet man mit $\mathcal{V}^* := (v_i^*)_{i\in\mathbb{N}_{\leq n}}$ und $\mathcal{W}^* = (w_j^*)_{j\in\mathbb{N}_{\leq m}}$, die zu $\mathcal{V}$ und $\mathcal{W}$ dualen Basen, so gilt für alle $v \in V$ und $w \in W$:*

$$f(v, w) = \sum_{i=1}^{n}\sum_{j=1}^{m}(vv_i^*)f(v_i, w_j)\overline{(ww_j^*)} = (vv_1^*, \ldots, vv_n^*)\mathcal{M}^{\mathcal{V}}_{\mathcal{W}}(f)(\overline{ww_1^*}, \ldots, \overline{ww_m^*})^t.$$

Hieraus ergeben sich unmittelbar die folgenden Äquivalenzen:

(i) *f ist rechtsregulär $\Leftrightarrow$ $\mathcal{M}^{\mathcal{V}}_{\mathcal{W}}(f)$ hat vollen Spaltenrang $\Leftrightarrow$ f ist linksreflexiv;*
(ii) *f ist linkssregulär $\Leftrightarrow$ $\mathcal{M}^{\mathcal{V}}_{\mathcal{W}}(f)$ hat vollen Zeilenrang $\Leftrightarrow$ f ist rechtsreflexiv ;*
(iii) *f ist regulär $\Leftrightarrow$ $\mathcal{M}^{\mathcal{V}}_{\mathcal{W}}(f)$ ist invertierbar $\Leftrightarrow$ f ist reflexiv $\Leftrightarrow$*
f ist nicht singulär $\Leftrightarrow$ f ist nicht rechtssingulär $\Leftrightarrow$ f ist nicht linkssingulär. ∎

Definition/Satz 1.2.9 (Diskriminante) *Seien $\mathcal{N} : K \mapsto F, \alpha \mapsto \alpha\bar{\alpha}$ und $V = W$ endlichdimensional mit Basen $\mathcal{B}$ und $\mathcal{C}$. Dann gilt*

$$\mathcal{M}_{\mathcal{C}}(f) = \mathcal{M}^{\mathcal{C}}_{\mathcal{B}}(1_V)\mathcal{M}_{\mathcal{B}}(f)\overline{\mathcal{M}^{\mathcal{C}}_{\mathcal{B}}}^t.$$

Ist f regulär, so ist insbesondere

$$\mathrm{disc}(f) := \det \mathcal{M}_{\mathcal{B}}(f)\mathcal{N}(K^*) \in F^*/\mathcal{N}(K^*)$$

von der Wahl der Basis $\mathcal{B}$ unabhängig. Man nennt dann $\mathrm{disc}(f)$ *die Diskriminante von f.* ∎

Bezeichnung 1.2.10 (isotrop, anisotrop, totalisotrop) *Ein $y \in V \cap W \backslash \{0\}$ heißt isotrop, wenn $f(y,y) = 0$ ist, und anisotrop sonst. Eine Teilmenge Y von $V \cap W$ heißt anisotrop, wenn dies auf jedes $y \in Y \backslash \{0\}$ zutrifft, und totalisotrop, wenn $Y = \mathrm{lrad}\ Y$ ($\Leftrightarrow Y = \mathrm{rrad}\ Y = \mathrm{rad}\ Y$) gilt.*

Definition 1.2.11 (Orthogonalität und Senkrechtrelation) *Seien $Y \subseteq V$ und $Z \subseteq W$. Dann heißt der Unterraum $Y^{\perp_f} := \cap_{y \in Y} \ker f_l(y)$ ($^{\perp_f}Z := \cap_{z \in Z} \ker f_r(z)$) der f-Senkrechtraum oder f-Verschwindungsraum von Y (Z). Es gilt offenbar $Z \subseteq Y^{\perp_f}$ genau dann, wenn $Y \subseteq {}^{\perp}_{f} Z$. Ist eine dieser äquivalenten Bedingungen erfüllt, so schreibt man $Y \perp_f Z$. Sind Y und Z Unterräume und gilt $Y \perp_f Z$ und $Y \cap Z = \{0\}$, so bezeichnet man den K-Vektorraum $Y \oplus Z$ mit $Y \bigoplus\!\!\!\!\!\!\perp_{f} Z$. Falls keine Verwechslung möglich ist, wird der Index f in allen oben eingeführten Notationen fortgelassen.*

Bemerkung 1.2.12 *Für $Y \subseteq V$ und $Z \subseteq W$ gilt $Y \perp_f Z$ genau dann, wenn $Z \perp_{\tilde{f}} Y$, i.e. $\perp_{\tilde{f}}$ ist die zu $\perp_f$ inverse Relation.*

Lemma 1.2.13 (a) *Es gilt* $\mathrm{lrad}\ Y \times Z = Y \cap {}^{\perp}Z$ *und* $\mathrm{rrad}\ Y \times Z = Y^{\perp} \cap Z$.

(b) *Sei $Y \leq V = W$. Dann gilt*

- (i) *Y ist rechtsreflexiv $\Rightarrow V = Y + Y^{\perp}$;*
- (ii) *Y ist nicht rechtssingulär $\Rightarrow V = Y \bigoplus\!\!\!\!\!\!\perp\ Y^{\perp}$;*
- (iii) *Y ist linksreflexiv $\Rightarrow V = Y + {}^{\perp}Y$;*
- (iv) *Y ist nicht linkssingulär $\Rightarrow V = {}^{\perp}Y \bigoplus\!\!\!\!\!\!\perp\ Y$.*

Beweis. (a) ist trivial.
(b). Sei $v \in V$. Dann gilt $(vf_r)_Y \in Y^*$. Weil Y rechtsreflexiv ist, gibt es ein $y \in Y$ mit $(vf_r)_Y = (yf_r)_Y$. Es folgt $v - y \in Y^{\perp}$ und damit $v = y + (v - y) \in Y + Y^{\perp}$. Somit ist (i) bewiesen. Sei Y zusätzlich rechtsregulär und sei $y' \in Y$ mit $v - y' \in Y^{\perp}$. Dann gilt $(yf_r)_Y = (vf_r)_Y = (v'f_r)_Y$, i.e. $y - y' \in \mathrm{rrad}Y = \{0\}$, womit (ii) bewiesen wäre. Die Aussagen (iii) und (iv) ergeben sich mit 1.2.6 und 1.2.12 aus (i) und (ii) angewandt auf $\tilde{f}$. ∎

Lemma 1.2.14 (Bipolarensätze) *Seien $Y \subseteq V$ und $Z \subseteq W$. Dann gilt stets $\langle Y \rangle \leq {}^{\perp}(Y^{\perp})$ ($\langle Z \rangle \leq ({}^{\perp}Z)^{\perp}$). Ist f rechtsreflexiv (linksreflexiv), so gilt $\langle Y \rangle = {}^{\perp}(Y^{\perp})$ ($\langle Z \rangle = ({}^{\perp}Z)^{\perp}$).*

Beweis. Die erste Aussage folgt unmittelbar aus der Definition von $\perp$. Seien f rechtsreflexiv und $y' \in {}^{\perp}(Y^{\perp})$. Nimmt man $y' \notin Y$ an, so findet man ein $\alpha \in V^*$ mit $Y \leq \ker \alpha$ und $y'\alpha \neq 0$. Weil f rechtsreflexiv ist, gibt es ein $w \in W$ mit $wf_r = \alpha$. Es folgt $w \in Y^{\perp}$ und $f(y', w) = y'\alpha \neq 0$, ein Widerspruch. Die Aussagen in Klammern ergeben sich wiederum aus dem bereits Bewiesenen angewandt auf $\tilde{f}$. ∎

Lemma 1.2.15 *Seien $(V_j)_{j\in J}$ und $(W_j)_{j\in J}$ Familien von Unterräumen von V bzw. W. Es gilt*

(i) $(\sum_{j\in J} V_j)^\perp = \cap_{j\in J} V_j^\perp$ $({}^\perp(\sum_{j\in J} W_j) = \cap_{j\in J}{}^\perp W_j)$;

(ii) $(\cap_{j\in J} V_j)^\perp \supseteq \sum_{j\in J} V_j^\perp$ $({}^\perp(\cap_{j\in J} W_j) \supseteq \sum_{j\in J}{}^\perp W_j)$;

(iii) *Ist f rechtsreflexiv (linksreflexiv) und J endlich, so gilt* $(\cap_{j\in J} V_j)^\perp = \sum_{j\in J} V_j^\perp$ $({}^\perp(\cap_{j\in J} W_j) = \sum_{j\in J}{}^\perp W_j)$.

Beweis. (i) und (ii) sind trivial.
(iii). Man kann o.B.d.A. $J = \{1,2\}$ annehmen. Sei $w \in (V_1 \cap V_2)^\perp$. Wähle ein Komplement U von $V_1 \cap V_2$ in V_2. Dann gilt $V_1 + V_2 = V_1 \oplus U$. Es gibt ein $\alpha \in V^*$ mit $U \le \ker\alpha$ und $\alpha_{V_1} = (wf_r)_{V_1}$. Weil f rechtsreflexiv ist, gibt es ein $w' \in W$ mit $w'f_r = \alpha$. Wegen $V_1 \cap V_2 \le \ker(wf_r)_{V_1} \le \ker\alpha = \ker(w'f_r)$ gilt $V_2 = U \oplus (V_1 \cap V_2) \le \ker(w'f_r)$, i.e. $w' \in V_2^\perp$. Wegen $(w'f_r)_{V_1} = (wf_r)_{V_1}$ gilt $w - w' \in V_1^\perp$ und somit $w = (w-w') + w' \in V_1^\perp + V_2^\perp$. ■

Wir kommen nun zur kanonischen Verallgemeinerung des in 1.2.2 eingeführten Begriffes der adjungierten Abbildung.

Definition/Satz 1.2.16 ((f,g)-Adjungierte) *Seien Y und Z K-Vektorräume, g eine $^-$-Sesquilinearform auf $Y \times Z$ und $\pi \in \mathrm{Hom}_K(V,Y)$. Es sei f auf $V \times W$ nicht rechtssingulär. Dann ist $\pi^* := g_r({}^*\pi)f_r^{-1} \in \mathrm{Hom}_K(Z,W)$ die eindeutig bestimmte K-lineare Abbildung von Z nach W für die*

$(*)$ $g(v\pi, z) = f(v, z\pi^*)$

für alle $v \in V$ und $z \in Z$ gilt. Man nennt π^* die (f,g)-Adjungierte (im Fall $f = g$ die f-Adjungierte) von π.

Sind V, W, Y, Z endlichdimensional mit Basen $\mathcal{V}$, $\mathcal{W}$ $\mathcal{Y}$ und $\mathcal{Z}$, so gilt

$$\mathcal{M}^{\mathcal{Z}}_{\mathcal{W}}(\pi^*) = \overline{\mathcal{M}^{\mathcal{Y}}_{\mathcal{Z}}(g)}^t\, \overline{\mathcal{M}^{\mathcal{V}}_{\mathcal{Y}}(\pi)}^t\, \overline{\mathcal{M}^{\mathcal{V}}_{\mathcal{W}}(f)^{-1}}^t.$$

Beweis. Seien $v \in V$ und $z \in Z$, dann gilt $f(v, z\pi^*) = v((z\pi^*)f_r) = v((zg_r)^*\pi) = (v\pi)(zg_r) = g(v\pi, z)$. Ist ϕ eine weitere Abbildung mit der Eigenschaft $(*)$, so gilt $f(v, z(\phi - \pi^*)) = 0$ für alle $v \in V$ und $z \in Z$. Weil f rechtsregulär ist, folgt $\phi = \pi^*$.
Seien V und W endlichdimensional. Aus $(*)$ folgt $\mathcal{M}^{\mathcal{V}}_{\mathcal{Y}}(\pi)\mathcal{M}^{\mathcal{Y}}_{\mathcal{Z}}(g) = \mathcal{M}^{\mathcal{V}}_{\mathcal{W}}(f)\overline{\mathcal{M}^{\mathcal{Z}}_{\mathcal{W}}(\pi^*)}^t$. ■

Korollar 1.2.17 *Seien V endlich-dimensional, $f = g$ regulär und $\pi \in \mathrm{GL}(V)$. Dann gehört auch π^* zu $\mathrm{GL}(V)$ und bezüglich einer Basis $\mathcal{V}$ von V gilt*

$$\mathcal{M}_{\mathcal{V}}(\pi^*) = \overline{\mathcal{M}_{\mathcal{V}}(f)}^t\, \overline{\mathcal{M}_{\mathcal{V}}(\pi)}^t\, \overline{\mathcal{M}_{\mathcal{V}}(f)^{-1}}^t.$$

Setzt man für ein Polynom $p = \sum_{i=1}^m p_i x^i \in K[x]$ vom Grad $m \in \mathbb{N}$ $\bar{p} := \sum_{i=1}^m \bar{p}_i x^i$, so ist insbesondere $r \in K[x]$ genau dann ein Elementarteiler von π^*, wenn $\bar{r}$ ein Elementarteiler von π ist. Für das charakteristische Polynom und das Minimalpolynom von π^* ergeben sich weiterhin folgende Identitäten: $\mathrm{char}(\pi^*) = \overline{\mathrm{char}(\pi)}$ *und* $\mathrm{mip}(\pi^*) = \overline{\mathrm{mip}(\pi)}$. ■

Für das weitere setzen wir $V = W$ voraus. Aus 1.2.11 und 1.2.13 ergibt sich auf natürliche Weise die Frage, welche Symmetrieeigenschaften die Senkrechtrelation $\perp_f$ besitzt, i.e. wann aus $Y \perp_f Z$ auch $Z \perp_f Y$ folgt und umgekehrt.
Um dies wenigstens für nichtsinguläre Sesquilinearformen zu klären, benötigen wir die folgende

Definition 1.2.18 (Multiplikatoren) *Ist f nicht rechtssingulär, so heißt die $(f, \tilde{f})$-Adjungierte von 1_V der Rechtsmultiplikator von f und wird mit R_f bezeichnet. Ist f nicht linkssingulär, so ist $\tilde{f}$ nicht rechtssingulär. Die $(\tilde{f}, f)$-Adjungierte von 1_V heißt der Linkssmultiplikator von f und wird mit L_f bezeichnet. Ist f nicht singulär, so gilt $L_f = R_f^{-1}$, und man nennt dann $M_f := R_f = L_f^{-1}$ den Multiplikator von f.*

Lemma 1.2.19 *Seien $A, B \subseteq V$. Falls f nicht rechtssingulär (nicht linkssingulär) ist, so folgt aus $AR_f \subseteq A$ ($AL_f \subseteq A$) und $B \perp A$ ($A \perp B$) auch $A \perp B$ ($B \perp A$).*

Beweis. Seien f nicht rechtssingulär, A R_f-invariant, $B \subseteq {}^{\perp}A$, $a \in A$ und $b \in B$. Dann gilt $\overline{f(a,b)} = f(b, aR_f) = 0$, also $A \perp B$. Die zweite Aussage ergibt sich aus der ersten angewandt auf $\tilde{f}$. ∎

Lemma 1.2.20 *Seien $V \neq \{0\}$ und f nicht singulär. Folgende Aussagen sind äquivalent:*

(i) *$\perp_f$ ist symmetrisch;*

(ii) *Jeder Unterraum von V ist M_f invariant;*

(iii) *Es gibt ein $\lambda \in K^*$ mit $\lambda\bar{\lambda} = 1$ derart, $\overline{f(a,b)} = \lambda f(b,a)$ gilt.*

Beweis. (i) $\Rightarrow$ (iii). Annahme: Es gibt ein $v \in V$ mit $vM_f^{-1} \notin \langle v \rangle$. Man findet dann ein $\alpha \in V^*$ mit $v\alpha = 0 \neq (vM_f^{-1})\alpha$. Weil f rechtsreflexiv ist, gibt es ein $w \in V$, so daß $\alpha = wf_r$ gilt. Es folgt der Widerspruch

$$\begin{aligned} 0 &= f(v,w) = f(w,v) = \tilde{f}(w, vL_f) = \overline{f(vM_f^{-1}, w)} \\ &= f(vM_f^{-1}, w) = (vM_f^{-1})\alpha \neq 0. \end{aligned}$$

Somit gilt $vM_f^{-1} \in \langle v \rangle$ für alle $v \in V$. Hieraus folgt bekanntlich $M_f^{-1} = \lambda 1_V$ für ein $\lambda \in K$. Aus den Voraussetzungen leitet man unmittelbar ab, daß es $y, z \in V$ mit $f(y,z) \neq 0$ gibt. Man berechnet nun

$$f(y,z) = \tilde{f}(y, zM_f^{-1}) = \overline{f(zM_f^{-1}, y)} = f(yM_f^{-1}, zM_f^{-1}) = \lambda\bar{\lambda} f(y,z).$$

Wegen $f(y,z) \neq 0$ folgt $\lambda\bar{\lambda} = 1$ und damit $M_f = \bar{\lambda} 1_v$.
Die Implikation $(iii) \Rightarrow (ii)$ ist trivial, und $(ii) \Rightarrow (i)$ wurde in 1.2.19 bewiesen. ∎

Definition 1.2.21 (klassische Sesquilinearformen)
Eine nichtsinguläre $^-$-Sesquilinearform, welche eine der drei äquivalenten Bedingungen aus 1.2.20 erfüllt heißt eine klassische $^-$-Sesquilinearform. Ist g eine solche und λ gemäß 1.2.20 (iii) *gewählt, so nennt man g*

(i) *symmetrisch,* *falls* $^- = 1_K$ *und* $\lambda = 1$ *ist,*
(ii) *symplektisch,* *falls* $^- = 1_K$ *und* $f(v,v) = 0$ *für alle* $v \in V$ *gilt,*
(iii) *hermitesch,* *falls* $^- \neq 1_K$ *und* $\lambda = 1$ *ist,*
(iv) *schiefhermitesch,* *falls* $^- \neq 1_K$ *und* $\lambda = -1 \neq 1$ *ist.*

Im Fall $\mathrm{char}(K) \neq 2$ *ist* g *genau dann symplektisch, wenn* $\lambda = -1$ *ist. Im Fall* $\mathrm{char}(K) = 2$ *ist jede symplektische Form auch symmetrisch.*

Nachdem die klassischen Formen eingeführt wurden, betrachten wir nun ihre Automorphismengruppen. Dafür Seien f und g zunächst beliebige Sesquilinearformen über isomorphen [, nicht notwendig identischen] K-Vektorräumen V bzw. W.

Bezeichnung 1.2.22 (Äquivalenz, Isometrie) *Die Formen* f *und* g *heißen äquivalent, wenn es einen Isomorphismus* $\pi : V \to W$ *gibt, so daß* $f(a,b) = g(a\pi, b\pi)$ *für alle* $a, b \in V$ *gilt. Ein solcher wird Isometrie (bezüglich* f *und* g*) gennant, und die Menge aller dieser mit* $\mathrm{Iso}(f,g)$ *bezeichnet. Ist* $V = W$*, so schreiben wir* $\mathrm{Aut}(f,g)$ *statt* $\mathrm{Iso}(f,g)$*. Ist* $f = g$*, so ist* $\mathrm{Aut}(f) := \mathrm{Aut}(f,f)$ *eine Gruppe, die sogenannte Automorphismen- oder Isometriegruppe (bezüglich* f*). Ist* f *eine klassische Form im Sinne von Definition 1.2.21, so nennt man, je nach dem ob* f *symmetrisch, symplektisch, oder (schief)hermitesch ist,* $\mathrm{Aut}(f)$ *auch die zu* f *gehörige orthogonale, symplektische oder unitäre Gruppe und schreibt* $\mathrm{O}(f)$, $\mathrm{Sp}(f)$ *oder* $\mathrm{U}(f)$*. Diese Gruppen werden klassische Gruppen genannt.*

Bemerkung 1.2.23 *Ist* f *eine schiefhermitesche Form, so gilt insbesondere* $^- \neq 1$ *und* $\mathrm{char}(K) \neq 2$*. Man findet dann ein* $\iota \in K^*$ *mit* $\bar{\iota} = -\iota$*. Setzt man* $f' := \iota \cdot f$*, so ist* f' *eine hermitesche Form und es gilt* $\mathrm{Aut}(f) = \mathrm{Aut}(f')$*. Dies rechtfertigt, die in Definition 1.2.22 angegebene einheitliche Bezeichnug 'unitäre Gruppe'.*

Offenbbar ist ein Isomorphismus $\pi \in \mathrm{Hom}(V,W)$ genau dann eine Isometrie bezüglich f und g, wenn π^{-1} mit der (f,g)-Adjungierten π^* von π übereinstimmt. Wir wollen einige einfache Konsequenzen für die endlich-dimensionale Situation festhalten. Hierfür hierfür benötigen wir die

Bezeichnung 1.2.24 *Für ein normiertes Polynom* $p = \sum_{i=0}^m p_i x^i \in K[x]$ *vom Grad* m *mit* $p_0 \neq 0$*, seien* $p^\times := p_0^{-1} \sum_{i=0}^m p_i x^{m-i}$ *und* $p^* := \bar{p}^\times = \overline{p_0}^{-1} \sum_{i=0}^m \overline{p_i} x^{m-i}$*. Man nennt* p *symmetrisch bzw.* $^-$*-symmetrisch, wenn* $p^\times = p$ *bzw.* $p^* = p$ *gilt.*

Bemerkung 1.2.25 *Sei* $A \in \mathrm{GL}_n(K)$*. Dann gilt* $\mathrm{char}(A^{-1}) = \mathrm{char}(A)^\times$, $\mathrm{mip}(A^{-1}) = \mathrm{mip}(A)^\times$, $\mathrm{char}(\bar{A}^{-1}) = \mathrm{char}(A)^*$ *und* $\mathrm{mip}(\bar{A}^{-1}) = \mathrm{mip}(A)^*$.

Bemerkung 1.2.26 *Sei* V *endlich-dimensional mit Basis* $\mathcal{B}$*. Ein* $\pi \in \mathrm{GL}(V)$ *ist genau dann eine Isometrie, wenn* $\mathcal{M}_\mathcal{B}(f) = \mathcal{M}_\mathcal{B}(\pi)\mathcal{M}_\mathcal{B}(f)\overline{\mathcal{M}_\mathcal{B}(\pi)}^t$ *gilt. Insbesondere ist* $\mathcal{M}_\mathcal{B}(\pi)$ *ähnlich zu* $\overline{\mathcal{M}_\mathcal{B}(\pi)^{-1}}^t$*. Nach 1.2.25 sind* $\mathrm{char}(\pi)$ *und* $\mathrm{mip}(\pi)$ $^-$*-symmetrisch.*

Abschließend halten wir eine elementare Rechenregel fest, deren Bedeutung im folgenden Abschnitt besonders deutlich wird (vgl. 1.3.9 unten).

Bemerkung 1.2.27 *Seien* $\pi \in \mathrm{Aut}(f)$ *und* $r = \sum_{i=1}^m r_i x^i \in K[x]$*. Dann gilt* $f(vr(\pi), w) = f(v, w\bar{r}(\pi^{-1}))$ *für alle* $v, w \in V$.

Beweis. Es gilt

$$f(vr(\pi), w) = \sum_{i=1}^{m} r_i f(v\pi^i, w) = \sum_{i=1}^{m} f(v, w\bar{r}_i\pi^{-i}) = f(v, w\bar{r}(\pi^{-1})). \qquad \blacksquare$$

Abschließend kommen wir zu den Sätzen von Witt. Für das folgende setzen wir voraus, daß V und W endlichdimensional und f, g klassische Formen gleichen Typs im Sinne von Definition 1.2.21 sind. Es sei $\delta = -1$, falls f symplektisch oder schiefhermitesch ist, und $\delta = 1$ andernfalls. [Für $(h, Y) \in \{(f, V), (g, W)\}$ ist dann $h(a, b) = \delta\overline{h(b, a)}$ für alle $a, b \in Y$ erfüllt.]

Definition 1.2.28 (Spur-wertig) *Die Form f heißt Spur-wertig (engl. trace-valued), falls die Bedingung*

(T) $\{f(v, v)|v \in V\} \subseteq \{\alpha + \delta\bar{\alpha}|\alpha \in K\}$

erfüllt ist.

Bemerkung 1.2.29 *Genau dann ist f Spur-wertig, wenn eine der folgenden Aussagen zutrifft:*

(i) *f ist symplektisch,*

(ii) *f ist symmetrisch und* $\mathrm{char}(K) \neq 2$,

(iii) *f ist hermitesch oder schiefhermitesch.*

Anders formuliert ist f genau dann nicht Spur-wertig, wenn $\mathrm{char}(K) = 2$ *und f symmetrisch jedoch nicht symplektisch ist.*

Beweis. $\Rightarrow$. Seien (i) und (iii) nicht erfüllt. Dann ist f symmetrisch und damit $^{-} \neq 1_K$. Weil f nicht symplektisch ist, folgt mit (T):

$$\{0\} \neq \{f(v, v)|v \in V\} \subseteq \{\alpha + \bar{\alpha}|\alpha \in K\} = \{2\alpha; \alpha \in K\},$$

also $2 \neq 0$.

$\Leftarrow$. 1.Fall: f ist symplektisch. Dann ist $^{-} = 1_K$ und $\delta = -1$. Dies bedeutet

$$\{\alpha + \delta\bar{\alpha}|\alpha \in K\} = \{0\} = \{f(v, v)|v \in V\}.$$

2.Fall: f ist symmetrisch und $\mathrm{char}(K) \neq 2$. In diesem Fall ist $^{-} = 1_K$ und $\delta = 1$. Wegen $f(v, v) = \frac{1}{2}f(v, v) + \overline{\frac{1}{2}f(v, v)}$ für alle $v \in V$ ist (T) erfüllt.
3.Fall: f ist hermitesch oder schiefhermitesch. Es ist $^{-} \neq 1_K$ und deshalb sowohl

$$U := \{\alpha \in K|\bar{\alpha} = \delta\alpha\} \text{ als auch } Y := \{\alpha + \delta\bar{\alpha}|\alpha \in K\}$$

ein von $\{0\}$ und K verschiedener F-Untervektorraum von K. Weil K ein 2-dimensionaler F-Vektorraum ist, folgt $\dim_F U = 1 = \dim_F Y$. Wegen

$$\overline{\alpha + \delta\bar{\alpha}} = \delta(\alpha + \delta\bar{\alpha})$$

für alle $\alpha \in K$ ist Y in U enthalten. Dies impliziert $\{f(v, v)|v \in V\} \subseteq U = Y$. $\blacksquare$

Definition 1.2.30 (hyperbolischer Raum, hyperbolische Ebene) *Man nennt f hyperbolisch bzw. V einen f-hyperbolischen [oder auch einfach einen hyperbolischen] Raum, falls V die direkte Summe von zwei totalisotropen Unterräumen ist. Ein 2-dimensionaler hyperbolischer Raum wird hyperbolische Ebene genannt.*

Bemerkung 1.2.31 *Folgende Aussagen sind äquivalent:*

(i) *V ist ein f-hyperbolischer Raum,*

(ii) *V ist eine direkte orthogonale Summe von f-hyperbolischen Ebenen,*

(iii) *Es gibt eine Basis $\mathcal{B}$ von V so, daß*

$$\mathcal{M}_{\mathcal{B}}(f) = \begin{bmatrix} 0 & 1 & & & \\ \delta & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & \delta & 0 \end{bmatrix}$$

(iv) *Es gibt eine Basis $\mathcal{B}$ von V so, daß*

$$\mathcal{M}_{\mathcal{B}}(f) = \begin{bmatrix} 0 & I_m \\ \delta I_m & 0 \end{bmatrix}$$

für ein $m \in \mathbb{N}$ gilt. ∎

Korollar 1.2.32 *Ein hyperbolischer Raum hat eine gerade Dimension. Sind f und g hyperbolisch, so sind f und g bereits äquivalent.* ∎

Definition 1.2.33 (Witt-Zerlegung) *Eine Zerlegung $V = H \bigoplus A$ in einen hyperbolischen Raum H und einen anisotropen Raum A heißt eine Witt-Zerlegung von V.*

Definition/Satz 1.2.34 (Witt-Index) *Es gelte* (T). *Je zwei maximale totalisotrope Unterräume von V haben dieselbe Dimension. Diese wird der Witt-Index von f bzw. V genannt und mit* $\mathrm{Ind}(f)$ *bzw.* $\mathrm{Ind}(V)$ *bezeichnet. Weiterhin gibt es zu jedem maximalen totalisotropen Unterraum U von V einen weiteren W derart, daß $H := U \oplus W$ hyperbolisch ist. Insbesondere besitzt V eine Witt-Zerlegung $V = H \bigoplus H^\perp$ mit anisotropem Unterraum $H^\perp$.*

Beweis. Siehe [8] §4, no. 2 Corollaire 1. ∎

Satz 1.2.35 (Witt'scher Fortsetzungssatz) *Seien f und g Spur-wertig, U ein Unterraum von V und $\pi : U \to W$ linear und injektiv mit $g(a\pi, b\pi) = f(a, b)$ für alle $a, b \in U$. Dann läßt sich π zu einer Isometrie $\hat{\pi} \in \mathrm{Iso}(f, g)$ fortsetzen.*

Beweis. [8] §4, no. 3 Théorème 1. ∎

Satz 1.2.36 (Witt'scher Kürzungssatz) *Seien f und g Spur-wertig, und es gelte $V = V_1 \bigoplus V_2$ und $W = W_1 \bigoplus W_2$ für Unterräume V_i von V bzw. W_i von W, $i = 1, 2$. Aus der Äquivalenz von f und g und der von f_{V_1} und g_{W_1} folgt die von f_{V_2} und g_{W_2}.*

Beweis. [8] §4, no. 3 Corollaire 1. ∎

1.3 Konjugation in Klassischen Gruppen

Von nun an setzen wir voraus, daß V endlichdimensional und f eine reguläre symmetrische, symplektische oder $^-$-hermitesche Form auf V ist.

Für die späteren Anwendungen ist eine genaue Kenntnis der Konjugiertenklassen klassischer Gruppen über endlichdimensionalen Vektorräumen erforderlich. Diese wurden ausführlich von vielen Mathematikern untersucht. Wesentliche Arbeiten stammen von J. Milnor [55], C. Riehm und M.A. Shrader-Frechette [60], [61], T.A. Springer und R. Steinberg [67] , [68], R. Scharlau [63], G.E. Wall [73] und J. Williamson [74],...,[78] und H. Zassenhaus [81], [82].
Das Konzept dieser Arbeiten besteht im wesentlichen darin, sogenannte hermitesche Invarianten $\mathrm{H}(\pi, r)$ für jeden $^-$-symmetrischen Elementarteiler $r \in K[x]$ einer Isometrie $\pi \in \mathrm{Aut}(f)$ zu definieren. Diese Invariante ist eine bestimmte reguläre hermitesche, schiefhermitesche, symmetrische oder symplektische Form auf einem endlich-dimensionalen Vektorraum über einer endlichen Körpererweiterung von K. Bis auf einige Ausnahmen bei Körpercharakteristik 2 gilt der

Satz 1.3.1 *Seien $\phi, \psi \in \mathrm{Aut}(f)$. Genau dann sind ϕ und ψ in $\mathrm{Aut}(f)$ zueinander konjugiert, wenn ϕ zu ψ ähnlich ist und $\mathrm{H}(\phi, r)$ und $\mathrm{H}(\psi, r)$ für jeden $^-$-symmetrischen Elementarteiler r von ϕ und ψ äquivalent sind.*

Im folgenden soll das eben angegebene Konzept präzisiert und der Satz 1.3.1 bewiesen werden. Die wesentlichen Beweisideen wurden den oben angegebenen Arbeiten entnommen. Es werden die zwei in der Literatur üblichen Definitionen der hermiteschen Invarianten vorgestellt (cf. 1.3.14 und 1.3.20) und ihre Äquivalenz bewiesen (cf. 1.3.21). In der gesamten Darstellung wurde Wert auf ausführliche Beweise gelegt.

Generalvoraussetzung 1.3.2 *Wir fixieren einen weiteren K-Vektorraum W mit $\dim W = \dim V$ und eine reguläre klassissche Form g auf W, die vom selben Typ wie f sei. Ferner setzen wir*

$$\varepsilon := \begin{cases} -1 & \text{, falls } f \text{ symplektisch ist,} \\ 1 & \text{sonst.} \end{cases} \tag{1.3.1}$$

Definition 1.3.3 *Für einen Endomorphismus π von V und ein $p \in K[x]$ sei $\ker p(\pi)^\infty := \cup_{i\in\mathbb{N}} \ker p(\pi)^i$. Ist p ein Primteiler von $\mathrm{mip}(\pi)$, so sei $\mathrm{I}(\pi, p) := \{i \in \mathbb{N}; p^i$ ist ein Elementarteiler von $\pi\}$. Eine Familie $\mathcal{U} = (U_i)_{i\in \mathrm{I}(\pi,p)}$ mit den Eigenschaften*

(i) *Für jedes $j \in I := \mathrm{I}(\pi, p)$ ist U_j ein π-Modul, für den p^j der einzige Elementarteiler von π_{U_j} ist; (also $U_j = Z_{j,1} \oplus \cdots \oplus Z_{j,s}$, wobei die $Z_{j,k}$ zyklische π-Moduln mit Minimalpolynom p^j sind.)*

(ii) $\ker p(\pi)^\infty = \oplus_{j\in I} U_j$;

heißt eine p-Komponentenzerlegung von $\ker p(\pi)^\infty$ und für jedes $j \in I$ heißt U_j die p^j-Komponente von $\mathcal{U}$ und eine p^j-Komponente von π.

Es sei angemerkt, daß π-Moduln mit der in 1.3.3 (i) genannten Eigenschaft auch isotypisch genannt werden, vgl. [63].

Definition 1.3.4 *Zwei Isometrien $\pi \in \mathrm{Aut}(f)$ und $\phi \in \mathrm{Aut}(g)$ heißen ähnlich, falls es einen Isomorphismus $\psi : V \to W$ gibt, so daß $\pi\psi = \psi\phi$ gilt. Ist $\psi \in \mathrm{Iso}(f,g)$, so heißen π und ψ metrisch konjugiert.*

Im folgenden soll nun bis auf einige spezielle Ausnahmen geklärt werden, wann zwei Isometrien $\pi \in \mathrm{Aut}(f)$ und $\phi \in \mathrm{Aut}(g)$ metrisch konjugiert sind. Eine notwendige Bedingung ist offensichtlich, daß π und ϕ ähnlich sind. Falls π und ϕ keine $^-$-symmetrischen Elementarteiler besitzen, ist diese Bedingung auch hinreichend, wie der Satz 1.3.7 zeigen wird. Als ein Hilfsmittel für den Beweis dieses Satzes benötigen wir die folgenden beiden Lemmata

Lemma 1.3.5 *Es gelte $V = A \oplus B$ und $W = C \oplus D$ für f-totalisotrope Unterräume A, B und g-totalisotrope Unterräume C, D. Sei $\pi : A \to C$ ein Isomorphismus. Dann gibt es genau eine Isometrie $\hat{\pi} \in \mathrm{Iso}(f,g)$ mit $\hat{\pi}_A = \pi$ und $B\hat{\pi} = D$. Im Fall $(V, A, B, f) = (W, C, D, g)$ haben alle Elementarteiler von $\hat{\pi}_B$ die Form p^*, wobei p ein Elementarteiler von π ist, und für eine p-Komponente U von π_A und eine p^*-Komponente W von $\hat{\pi}_B$ gilt $\dim U = \dim W$. Insbesondere gilt $\mathrm{mip}(\hat{\pi}_B) = \mathrm{mip}(\pi)^*$ und damit $\mathrm{mip}(\hat{\pi}) = \mathrm{lcm}(\mathrm{mip}(\pi), \mathrm{mip}(\pi)^*)$.*

Beweis. Weil V f-regulär ist und A, B f-totalisotrop sind, ist $h := f_{A\times B}$ eine reguläre $^-$-Sesquilinearform. Analog ist $l := g_{C\times D}$ eine reguläre $^-$-Sesquilinearform. Nach 1.2.2 ist die (h,l)-Adjungierte π^* von π der wohldefinierte und eindeutig bestimmte Isomorphismus $\psi : D \to B$, für den $g(a\pi, d) = f(a, d\psi)$ für alle $a \in A$ und $d \in D$ gilt. Folglich ist $\hat{\pi} := \pi \oplus \pi^{*-1}$ der eindeutig bestimmte Isomorphismus $\phi : V \to W$, für den $\phi_A = \pi$, $B\phi = D$ und $g(a\phi, b\phi) = f(a,b)$ für alle $a \in A$ und $b \in B$ gilt. Für $a, a' \in A$ und $b, b' \in B$ gilt dann

$$g((a+b)\hat{\pi}, (a'+b')\hat{\pi}) = g(a\pi, b'\pi^{*-1}) + \varepsilon\overline{g(a'\pi, b\pi^{*-1})} = f(a,b') + \varepsilon\overline{f(a',b)} = f(a+b, a'+b'),$$

i.e. $\hat{\pi} \in \mathrm{Iso}(f,g)$. Sei $(V, A, B, f) = (W, C, D, g)$. Für geeignete Basen $\mathcal{A}$ von A und $\mathcal{B}$ von B gilt dann $\mathcal{M}_{\mathcal{B}}(\pi^{*-1}) = \overline{\mathcal{M}_{\mathcal{A}}(\pi)^{-1}}^t$. Hieraus ergeben sich die restlichen Aussagen der Behauptung. ∎

Lemma 1.3.6 *Seien $p, q \in K[x]$ normierte Teiler von $\mathrm{mip}(\pi)$, so daß p zu q^* teilerfremd ist. Dann gilt $\ker p(\pi) \perp \ker q(\pi)$. Sind $(p_i)_{i\in I}$ und $(q_j)_{j\in J}$ Familien paarweise teilerfremder, normierter, irreduzibler Polynome derart, daß jedes p_i $^-$-symmetrisch, jedes q_j nicht $^-$-symmetrisch und $\mathrm{mip}(\pi) = (\prod_{i\in I} p_i^{m_i})(\prod_{j\in J} q_j^{n_j})$ für geeignete $m_i, n_j \in \mathbb{N}$ ist (cf.1.2.26), so haben wir eine Zerlegung*

$$V = (\textstyle\bigoplus\!\!\!\!\perp_{\,i\in I}(\ker p_i(\pi)^{m_i}) \bigoplus\!\!\!\!\perp\ (\bigoplus\!\!\!\!\perp_{\,j\in J}(\ker q_j(\pi)^{n_j} \oplus \ker q_j^*(\pi)^{n_j})$$

von V in reguläre π-Moduln $\ker p_i(\pi)^{m_i}$, $\ker q_j(\pi)^{n_j} \oplus \ker q_j^*(\pi)^{n_j}$. Dabei ist $\ker q_j(\pi)^{n_j} \oplus \ker q_j^*(\pi)^{n_j}$ ein hyperbolischer Raum mit totalisotropen π-invarianten Teilräumen $\ker q_j(\pi)^{n_j}$ und $\ker q_j^*(\pi)^{n_j}$.

Beweis. Man findet $r, s \in K[x]$, so daß $pr + q^*s = 1$ ist. Für $a \in \ker p(\pi)$ und $b \in \ker q(\pi)$ folgt: $f(a,b) = f(a(pr+q^*s)(\pi), b) = \overline{q(0)}^{-1} f(as(\pi), bq(\pi)\pi^{-\deg(q)}) = 0$. ∎

Satz 1.3.7 *Seien $\pi \in \mathrm{Aut}(f)$ und $\phi \in \mathrm{Aut}(g)$ derart, daß kein irreduzibler Primteiler von $\mathrm{mip}(\pi)$ und $\mathrm{mip}(\phi)$ $^-$-symmetrisch ist. Dann sind π und ϕ genau dann metrisch konjugiert, wenn π und ϕ ähnlich sind.*

Beweis. Seien $\psi : V \to W$ ein Isomorphismus mit $\pi\psi = \psi\phi$ und p ein irreduzibler Primteiler von $\mathrm{mip}(\pi) = \mathrm{mip}(\phi)$. Seien $A := \ker p(\pi)^\infty, B := \ker p^*(\pi)^\infty, C := \ker p(\phi)^\infty, D := \ker p^*(\phi)^\infty$. Dann sind $A \oplus B$, $C \oplus D$ nach 1.3.6 regulär, A, B, C, D sind totalisotrop, und es gilt $A\psi = C$ und $B\psi = D$. O.B.d.A. gelte $V = A \oplus B$ und $W = C \oplus D$. Seien $\beta := \psi_A \in \mathrm{Hom}_K(A, C)$ und $\hat{\beta} \in \mathrm{Iso}(f, g)$ die nach 1.3.5 eindeutig bestimmte Fortsetzung von β mit $B\beta = D$. Dann ist $\gamma := \hat{\beta}^{-1}\pi\hat{\beta} \in \mathrm{Aut}(g)$ eine Fortsetzung von ϕ_C mit $D\gamma = D$ und stimmt daher nach 1.3.5 mit ϕ überein. ■

Nachdem wir nun den 'Trivialfall' abgehandelt haben, soll jetzt die allgemeine Situation in Angriff genommen werden. Wie eingangs erwähnt muß zunächst zu jedem Elementarteiler p^i, $p \in K[x]$ irreduzibel und $^-$-symmetrisch, $i \in \mathbb{N}$, von π bzw. ϕ eine reguläre klassische Form, eine sogenannte hermitesche Invariante $\mathrm{H}(\pi, p^i)$ von π bzw. $\mathrm{H}(\phi, p^i)$ von ϕ definiert werden. Ziel aller weiteren Untersuchungen wird es sein, folgenden Satz zu beweisen.

Satz 1.3.8 *Seien $\pi \in \mathrm{Aut}(f)$ und $\phi \in \mathrm{Aut}(g)$. Es gelte $\mathrm{char}(K) \neq 2$ oder $^- \neq 1_K$ oder $x + 1$ sei kein Teiler von $\mathrm{mip}(\pi)$ und $\mathrm{mip}(\phi)$. Dann sind π und ϕ genau dann metrisch konjugiert, wenn π und ϕ ähnlich und für jeden $^-$-symmetrischen Elementarteiler p^i, $p \in K[x]$ irreduzibel, $i \in \mathbb{N}$, von π und ϕ die hermiteschen Invarianten $\mathrm{H}(\pi, p^i)$ und $\mathrm{H}(\phi, p^i)$ äquivalent sind.*

Für das folgende seien zwei ähnliche Isometrien $\pi \in \mathrm{Aut}(f)$ und $\phi \in \mathrm{Aut}(g)$ fixiert. Aufgrund von 1.3.7 setzen wir voraus, daß jeder irreduzible Primteiler von $\mathrm{mip}(\pi) = \mathrm{mip}(\phi)$ $^-$-symmetrisch ist. Für die Definition der hermiteschen Invarianten werden nun einige Vorbereitungen getroffen.
Es seien $p \in K[x]$ ein normiertes, irreduzibles, $^-$-symmetrisches Polynom mit $p(0) \neq 0$, $i \in \mathbb{N}$, $\zeta := x + p^iK[x] \in K[x]/p^iK[x]$ und $\xi := x + pK[x] \in K[x]/pK[x]$. Mit dieser Notation erhalten wir den folgenden leicht zu verifizierenden

Satz 1.3.9 *$K[x]/p^iK[x] = K[\zeta]$ ist ein lokaler Ring mit maximalem Ideal $p(\zeta)K[\zeta]$ und es gilt $\zeta \in K[\zeta]\backslash p(\zeta)K[\zeta] = K[\zeta]^*$. (Dabei bezeichne $K[\zeta]^*$ die Einheitengruppe von $K[\zeta]$.) Die Abbildung $K[\zeta] \to K[\zeta], q(\zeta) \mapsto \bar{q}(\zeta^{-1})$, $q \in K[x]$, ist ein wohldefinierter involutorischer Ringautomorphismus, der $k + p^iK[x]$, $k \in K$, auf $\bar{k} + p^iK[x]$ abbildet, also eine 'Fortsetzung' von $^-$ ist und deshalb ebenfalls mit $^-$ bezeichnet wird. Der von $^-$ auf dem Faktorkörper $K[\zeta]/p(\zeta)K[\zeta] \cong K[x]/pK[x] = K[\xi]$ induzierte involutorische Körperautomorphismus ist durch $q(\xi) \mapsto \bar{q}(\xi^{-1})$, $q \in K[x]$, gegeben und wird auch mit $^-$ bezeichnet.*

Beweis. Sei $m := \deg(p^i)$. Es ist $K[\zeta]$ ein m-dimensionaler K-Vektorraum, auf dem ζ durch Rechtsmultiplikation einen Endomorphismus $\alpha : K[\zeta] \to K[\zeta], r \mapsto r\zeta$ mit Minimalpolynom $\mathrm{mip}_K(\zeta) := \mathrm{mip}(\alpha) = p^i$ induziert. Es ist $\mathrm{mip}_K(\zeta)$ das eindeutig bestimmte normierte Polynom q kleinsten Grades, für das $q(\zeta) = 0$ gilt. Der Einsetzhomomorphismus $K[x] \to K[\alpha], r \mapsto r(\alpha)$ induziert dann einen Isomorphismus $K[\zeta] = K[x]/\mathrm{mip}(\alpha)K[x] \to K[\alpha], r(\zeta) \mapsto r(\alpha)$, der ζ auf α abbildet. Folglich gilt für $r \in K[x]$:

$$\begin{aligned} r(\zeta) \notin K[\zeta]^* \quad &\Leftrightarrow \quad r(\alpha) \text{ ist singulär} \Leftrightarrow \\ p \text{ teilt } r \quad &\Leftrightarrow \quad r(\zeta) \in p(\zeta)K[\zeta]. \end{aligned}$$

Hieraus folgt, daß die Menge der Nichteinheiten in $K[\zeta]$ das Ideal $p(\zeta)K[\zeta]$ ist. Dies wiederum impliziert, daß $K[\zeta]$ ein lokaler Ring mit maximalem Ideal $p(\zeta)K[\zeta]$ ist. Wegen $p(0) \neq 0$, ist p kein Teiler von x in $K[x]$. Demnach ist ζ eine Einheit in $K[\zeta]$, besitzt also ein Inverses $\zeta^{-1} \in K[\zeta]$. Der von ζ^{-1} auf dem K-Vektorraum $K[\zeta]$ durch Rechtsmultiplikation induzierte Endomorphismus $K[\zeta] \to K[\zeta], r \mapsto r\zeta^{-1}$ ist α^{-1}. Es folgt $\mathrm{mip}_K(\zeta^{-1}) = \mathrm{mip}(\alpha^{-1}) = \mathrm{mip}(\alpha)^\times = \mathrm{mip}_K(\zeta)^\times = p^{\times i} = \bar{p}^i$.

'Wohldefiniertheit und Injektivität von $^-$'. Seien $q, r \in K[x]$. Es gilt (in $K[\zeta]$):

$$\begin{aligned} q(\zeta) = r(\zeta) \quad &\Leftrightarrow \quad (q-r)(\zeta) = 0 \Leftrightarrow \\ p^i \text{ teilt } q - r \quad &\Leftrightarrow \quad p^{\times i} = \bar{p}^i \text{ teilt } \overline{q-r} \Leftrightarrow \\ \overline{(q-r)}(\zeta^{-1}) = 0 \quad &\Leftrightarrow \quad \bar{q}(\zeta^{-1}) = \bar{r}(\zeta^{-1}). \end{aligned}$$

'Homomorphieeigenschaften von $^-$'. Weil sowohl das Einsetzen von ζ und ζ^{-1} in Polynome aus $K[x]$ als auch die Abbildung $K[x] \to K[x], r \mapsto \bar{r}$ Ringhomomorphismen sind, erhält man für $q, r \in K[x]$:

$$\overline{(qr)(\zeta)} = \overline{qr}(\zeta^{-1}) = (\bar{q}\bar{r})(\zeta^{-1}) = \bar{q}(\zeta^{-1})\bar{r}(\zeta^{-1}),$$
$$\overline{(q+r)(\zeta)} = \overline{q+r}(\zeta^{-1}) = (\bar{q}+\bar{r})(\zeta^{-1}) = \bar{q}(\zeta^{-1}) + \bar{r}(\zeta^{-1}).$$

'Involutorizität und Surjektivität von $^-$'. Seien $a_0, \ldots, a_m \in K$ mit $p^i = \sum_{j=0}^m a_j x^j$. Dann gilt $a_m = 1$, $\overline{a_0} = a_0^{-1}$ und $\zeta^{-1} = -\overline{a_0} \sum_{j=1}^m a_j \zeta^{j-1}$. Es folgt:

$$\begin{aligned} \bar{\bar{\zeta}} = \overline{\zeta^{-1}} \quad &= \quad (-a_0 \sum_{j=1}^m \overline{a_j} \zeta^{1-j}) = (-a_0 \sum_{j=1}^m \overline{a_j} \zeta^{-j})\zeta = (-a_0 \sum_{j=0}^m \overline{a_j} \zeta^{-j})\zeta + \zeta \\ &= \quad -a_0 \bar{p}^i(\zeta^{-1})\zeta + \zeta = \zeta. \end{aligned}$$

Weil $^-$ wie bereits gezeigt ein Ringhomomorphismus ist, gilt für $q \in K[x]$:

$$\overline{\overline{q(\zeta)}} = \overline{\bar{q}(\zeta^{-1})} = \bar{\bar{q}}(\overline{\zeta^{-1}}) = q(\zeta).$$

Folglich ist $^-$ involutorisch und damit auch surjektiv.

Nach dem dritten Homomorphiesatz für Ringe ist

$$\beta : K[\zeta]/p(\zeta)K[\zeta] \to K[\xi], r(\zeta) + p(\zeta)K[\zeta] \mapsto r(\xi)$$

ein Ringisomorphismus (cf.[7] chapt.1, §4, no.7, Theorem 4.b)). Weil $K[\zeta]/p(\zeta)K[\zeta]$ und $K[\xi]$ Körper sind, ist β ein Körperisomorphismus, der ζ auf ξ und ζ^{-1} auf ξ^{-1} abbildet. Weil $p(\zeta)K[\zeta]$ das einzige maximale Ideal von $K[\zeta]$ ist und $^-$ als Ringautomorphismus maximale Ideale auf solche abbildet, ist $p(\zeta)K[\zeta]$ $^-$-invariant. Folglich ist

$$\gamma : K[\zeta]/p(\zeta)K[\zeta] \to K[\zeta]/p(\zeta)K[\zeta], r(\zeta) + p(\zeta)K[\zeta] \mapsto \overline{r(\zeta)} + p(\zeta)K[\zeta]$$

eine wohldefinierte Abbildung. Weil $^-$ ein involutorischer Ringendomorphismus ist, trifft dies auch auf γ zu. Weil Involutionen bijektiv sind, ist γ ein Körperautomorphismus. Folglich ist auch $\delta := \beta^{-1}\gamma\beta$ ein Körperautomorphismus. Für $q \in K[x]$ gilt

$q(\xi)\delta = (\bar{q}(\zeta^{-1}) + p(\zeta)K[\zeta])\beta = \bar{q}(\zeta^{-1}\beta) = \bar{q}(\xi^{-1}).$ ■

Das nächste Lemma liefert Erzeuger des von $p(\zeta)$ in $K[\zeta]$ erzeugten Hauptideales $p(\zeta)K[\zeta]$, die von $^-$ fixiert oder negiert werden.

Lemma 1.3.10 *Es gelte* $\mathrm{char}(K) \neq 2$ *oder* $p \neq x \pm 1$ *oder* $^-|_K \neq 1_K$. *Dann gibt es ein* $a(\zeta) \in K[\zeta]^*$, $a \in K[x]$, *so daß für* $q := ap$ *gilt:* $q(\zeta) \in \mathrm{Fix}(^-)$, *falls* $p \neq x \pm 1$ *oder* $^-|_K \neq 1_K$, $q(\zeta) \in \mathrm{Neg}(^-)$, *falls* $p = x \pm 1$ *und* $^-|_K = 1_K$. *(Dabei ist* $^-$ *durch 1.3.9 gegeben.)*

Beweis. Seien $t := \deg(p)$, $\delta \in \{\pm 1\}$ und $a(\zeta) \in K[\zeta]^*$, $a \in K[x]$. Dann gilt

$$\begin{aligned} ap(\zeta) - \delta\overline{ap(\zeta)} &= ap(\zeta) - \delta\overline{a(\zeta)}\zeta^{-t}\overline{p(0)}(\zeta^t p(0)\bar{p}(\zeta^{-1})) = ap(\zeta) - \delta\overline{a(\zeta)}\zeta^{-t}\overline{p(0)}p^*(\zeta) \\ &= (a(\zeta) - \delta\overline{a(\zeta)}\zeta^{-t}\overline{p(0)})p(\zeta) =: z(\delta). \end{aligned}$$

Falls $\zeta^{-t}\overline{p(0)} + 1$ nicht in $K[\zeta]^*$ enthalten ist, gilt auch $\zeta^t + \overline{p(0)} \notin K[\zeta]^*$. Folglich ist p ein Teiler von $x^t + \overline{p(0)}$. Weil p ein normiertes Polynom vom Grad t ist, folgt $p = x^t + p(0)$ und $p(0) = \overline{p(0)} = p(0)^{-1} \in \{\pm 1\}$. Weil p dann symmetrisch ist, ist $\deg(p)$ gerade oder $p = x \pm 1$.
Ist $p \neq x \pm 1$, so wähle $a(\zeta) := \zeta^{-t}\overline{p(0)} + 1$, falls $\zeta^{-t}\overline{p(0)} + 1$ in $K[\zeta]^*$ enthalten ist, und $a(\zeta) := \zeta^{-\frac{t}{2}} \in K[\zeta]^*$ sonst. Dann gilt $z(1) = 0$, i.e. $ap(\zeta) \in \mathrm{Fix}(^-)$. Falls $p = x \pm 1$ und $^-|_K \neq 1_K$ ist, gibt es ein $\omega \in K^*$ mit $\bar{\omega} \neq \omega$. Setze $\alpha := \bar{\omega}$ und $\beta := \omega p(0)$. Wegen $p(0) \neq \frac{\omega}{\bar{\omega}}p(0)$ ist p kein Teiler von $\alpha x + \beta = \bar{\omega}(x + \frac{\omega}{\bar{\omega}}p(0))$. Demnach gehört $a(\zeta) := \overline{\alpha\zeta + \beta}$ zu $K[\zeta]^*$. Man berechnet nun

$$a(\zeta) - \overline{a(\zeta)}\zeta^{-t}\overline{p(0)} = \bar{\alpha}\zeta^{-1} + \bar{\beta} - (\alpha\zeta + \beta)\zeta^{-1}p(0) = \omega\zeta^{-1} + \bar{\omega}p(0) - \bar{\omega}p(0) - \omega\zeta^{-1} = 0,$$

also wiederum $z(1) = 0$. Falls $p = x \pm 1$ und $^-|_K = 1_K$ ist, ist nach Voraussetzung $\mathrm{char}(K) \neq 2$. In diesem Fall gilt $a(\zeta) := \overline{\zeta - p(0)} \in K[\zeta]^*$ und $a(\zeta) + \overline{a(\zeta)}\zeta^{-t}\overline{p(0)} = (\zeta^{-1} - p(0)) + (\overline{p(0)} - \zeta^{-1}) = 0$, also $z(-1) = 0$, i.e. $ap(\zeta) \in \mathrm{Neg}(^-)$. ■

Das folgende Lemma macht in gewissem Sinne eine Reichhaltigkeitsausage über den K-Dualraum $K[\xi]^\star := \mathrm{Hom}_K(K[\xi], K)$. Zuvor sei noch bemerkt, daß durch die Multiplikationsvorschrift $(\alpha \cdot \tau)(\beta) := \tau(\alpha\beta)$, $\alpha, \beta \in K[\xi], \tau \in K[\xi]^\star$, $K[\xi]^\star$ ein $K[\xi]$-Vektorraum wird.

Lemma 1.3.11 *Es gilt* $\dim_{K[\xi]} K[\xi]^\star = 1$, *und es gibt ein* $\tau \in K[\xi]^\star \backslash \{0\}$, *das mit* $^-$ *kommutiert, i.e. für alle* $\alpha \in K[\xi]$ *gilt* $\overline{\tau(\alpha)} = \tau(\bar{\alpha})$.

Beweis. Es ist $\dim_K K[\xi]^\star = \dim_K K[\xi] = \deg(p) =: t > 0$. Insbesondere gibt es ein $\alpha \in K[\xi]^\star \backslash \{0\}$. Zeige nun, daß $(\xi^i \cdot \alpha)_{0 \leq i \leq t-1}$ eine K-Basis von $K[\xi]^\star$ ist. Seien $a_0, \ldots, a_{t-1} \in K$, so daß $0 = \sum_{i=0}^{t-1} a_i(\xi^i \cdot \alpha) = (\sum_{i=0}^{t-1} a_i\xi^i) \cdot \alpha$ gilt. Wegen $\alpha \neq 0$ gilt dann $\sum_{i=0}^{t-1} a_i\xi^i = 0$. Weil $(\xi^i)_{0 \leq i \leq t-1}$ eine K-Basis von $K[\xi]$ ist, folgt $a_i = 0$ für alle $0 \leq i \leq t-1$.
Sei nun $\beta \in K[\xi]^\star$. Nach dem Vorherigen gibt es dann $b_0, \ldots, b_{t-1} \in K$, so daß $\beta = \sum_{i=0}^{t-1} b_i(\xi^i \cdot \alpha) = (\sum_{i=0}^{t-1} b_i\xi^i) \cdot \alpha$. Folglich ist $\{\alpha\}$ eine $K[\xi]$-Basis von $K[\xi]^\star$.
Da auch $\tilde{\alpha} : K[\xi] \to K, a \mapsto \overline{\alpha(\bar{a})}$ ein Element von $K[\xi]^\star \backslash \{0\}$ ist und $\{\alpha\}$ eine $K[\xi]$-Basis von $K[\xi]^\star$ ist, gibt es genau ein $b \in K[\xi] \backslash \{0\}$, so daß $\tilde{\alpha} = b \cdot \alpha$ gilt. Sei $a \in K[\xi]$ mit $\alpha(a) \neq 0$. Dann gilt $\overline{\alpha(a)} = b \cdot \alpha(\bar{a}) = b\bar{b} \cdot \overline{\alpha(a)}$, also $b\bar{b} = 1$. Falls $^- \neq 1_{K[\xi]}$ ist, gibt es bekanntlich (nach dem Satz 90 von Hilbert) ein $c \in K[\xi]$ mit $b = c\bar{c}^{-1}$.

Setze $\tau := c\cdot\alpha \in K[\xi]^\star\backslash\{0\}$. Für $a \in K[\xi]$ gilt dann $\overline{\tau(\bar a)} = \overline{(c\cdot\alpha)(\bar a)} = b\cdot\alpha(\bar c a) = (c\cdot\alpha)(a) = \tau(a)$. Falls ${}^- = 1_{K[\xi]}$ ist, gilt insbesondere ${}^-|_K = 1_K$ und $\tau := \alpha$ hat trivialerweise die gewünschten Eigenschaften. ■

Die Bedeutung von 1.3.11 wird im nächsten Lemma deutlich. Für das weitere sei ein $\tau \in K[\xi]^\star$ gemäß 1.3.11 fest gewählt.

Lemma 1.3.12 *Sei U ein $K[\xi]$-Vektorraum. Dann ist U in natürlicher Weise auch ein K-Vektorraum. Sei $h : U\times U \to K$ eine ${}^-$-Sesquilinearform auf dem K-Vektorraum U und es gelte $h(ru, v) = h(u, \bar r v)$ für alle $u, v \in U$ und $r \in K[\xi]$. Dann gibt es genau eine ${}^-$-Sesquilinearform $H : U \times U \to K[\xi]$ auf dem $K[\xi]$-Vektorraum U, für die $\tau\circ H = h$ gilt. Ist h regulär, so ist auch H regulär. Gibt es ein $\delta \in K$, so daß $\overline{h(a, b)} = \delta h(b, a)$ für alle $a, b \in U$ gilt, so gilt auch $\overline{H(a, b)} = \delta H(b, a)$ für alle $a, b \in U$.*

Beweis. Seien $u, v \in U$. Dann ist die Abbildung $\alpha : K[\xi] \to K, a \mapsto h(au, v)$ ein Element von $K[\xi]^\star$. Es sei $H(u, v)$ das nach 1.3.11 eindeutig bestimmte Element von $K[\xi]$, für das $H(u, v)\cdot\tau = \alpha$ gilt. Zeige nun, daß $H : U \times U \to K[\xi], (a, b) \mapsto H(a, b)$ eine ${}^-$-Sesquilinearform auf dem $K[\xi]$-Vektorraum U ist. Seien $u, v, w, z \in U$ und $a, b, c \in K[\xi]$. Es gilt

$$\begin{aligned}
\tau(aH(u+bv, w+cz)) &= h(a(u+bv), w+cz) = h(au, w) + h(abv, w) + h(\bar c au, z) + h(\bar c abv, z)\\
&= \tau(aH(u, w)) + \tau(abH(v, w)) + \tau(a\bar c H(u, z)) + \tau(ab\bar c H(v, z))\\
&= \tau(a(H(u, w) + bH(v, w) + \bar c H(u, z) + b\bar c H(v, z))),
\end{aligned}$$

also $H(u + bv, w + cz) = H(u, w) + bH(v, w) + \bar c H(u, z) + b\bar c H(v, z)$. Seien h regulär und $u \in H\text{-rad } U$. Dann gilt $h(y, u) = \tau(H(y, u)) = 0 = \tau(H(u, y)) = h(u, y)$ für alle $y \in U$, also $u \in h\text{-rad } U = \{0\}$. Folglich ist H eine reguläre ${}^-$-Sesquilinearform auf dem $K[\xi]$-Vektorraum U. Es gebe ein $\delta \in K$, so daß $\overline{h(w, z)} = \delta h(w, z)$ für alle $w, z \in U$ gilt. Dann gilt $\tau(a\overline{H(u, v)}) = \overline{\tau(H(u, av))} = \overline{h(u, av)} = \delta h(av, u) = \tau(a\delta H(v, u))$ für alle $a \in K[\xi]$, also $\overline{H(u, v)} = \delta H(v, u)$. ■

Wir kommen nun zur Definition der hermiteschen Invarianten $\mathrm{H}(\pi, p^i)$ und $\mathrm{H}(\phi, p^i)$. Zu diesem Zweck sei $(\psi, h) \in \{(\pi, f), (\phi, g)\}$. Von nun an sei vorausgesetzt, daß p^i ein Elementarteiler von ψ ist (dabei ist weiterhin p wie in der Vereinbarung nach 1.3.8). In der Formulierung von Satz 1.3.8 wurde die Situation

(E) $\mathrm{char}(K) = 2$ und ${}^-|_K = 1_K$ und $p = x + 1$

ausgeschlossen. Sie soll entartet und ihre Negation

(R) $\mathrm{char}(K) \neq 2$ oder ${}^-|_K \neq 1_K$ oder $p \neq x + 1$

regulär genannt werden. (Die Bezeichnung rührt daher, daß die Spurabbildung $K[\xi] \to K[\xi], a(\xi) \mapsto a(\xi) + \overline{a(\xi)}$ von $K[\xi]$ genau dann Werte ungleich 0 annimmt, wenn die Bedingung (R) erfüllt ist.)

Notation 1.3.13 *Im Fall* (R) *seien q wie in 1.3.10 und $\eta := 1$, falls $p \neq x \pm 1$ oder ${}^-|_K \neq 1_K$ ist, bzw. $\eta := -1$, falls $p = x \pm 1$ und ${}^-|_K = 1_K$ ist. Im Fall* (E) *seien $q := p(\zeta) = \zeta + 1$ und $\eta := 1$.*

Definition/Satz 1.3.14 (hermitesche Invarianten I**)** *Seien* $A := \ker p(\psi)^i$, $B := (Ap(\psi)^{i-1})^\perp \cap A$ *und* $C := A/B$. *Wegen* $Ap(\psi) \subseteq B$ *ist* C *auf kanonische Weise ein* $K[\xi]$*-Vektorraum. Es ist*

$$l : C \times C \mapsto K,\ l(u+B, v+B) := h(uq(\psi)^{i-1}, v),$$

$u, v \in A$, *eine wohldefinierte reguläre* $^-$*-Sesquilinearform auf dem* K*-Vektorraum* C, *für die* $l(ra, b) = l(a, \bar{r}b)$ *und* $\overline{l(a,b)} = \eta^{i-1}\varepsilon l(b,a)$ *für alle* $a, b \in C, r \in K[\xi]$ *gilt. Die nach 1.3.12 eindeutig bestimmte reguläre* $^-$*-Sesquilinearform* $\mathrm{H}(\psi, p^i) : C \times C \to K[\xi]$ *auf dem* $K[\xi]$*-Vektorraum* C, *für die* $\tau \circ \mathrm{H}(\psi, p^i) = l$ *gilt, nennt man die zum Elementarteiler* p^i *gehörende hermitesche Invariante von* ψ. *Nach 1.3.12 gilt* $\overline{\mathrm{H}(\psi, p^i)(a,b)} = \eta^{i-1}\varepsilon \mathrm{H}(\psi, p^i)(b, a)$ *für alle* $a, b \in C$.

Beweis. Es ist $z := h \circ (q(\psi)^{i-1} \times id)_A$ eine $^-$-Sesquilinearform auf dem K-Vektorraum A. Weil im Fall (R) $\overline{q(\zeta)^{i-1}} = \eta^{i-1}q(\zeta)^{i-1}$ ist, gilt $\bar{q}(\psi_A^{-1})^{i-1} = \eta^{i-1}q(\psi_A)^{i-1}$. Für $a, b \in A$ gilt daher

$$\begin{aligned} z(a,b) &= h(aq(\psi)^{i-1}, b) = h(a, b\bar{q}(\psi^{-1})^{i-1}) \\ &= \eta^{i-1}h(a, bq(\psi)^{i-1}) = \varepsilon\eta^{i-1}\overline{h(bq(\psi)^{i-1}, a)} \\ &= \varepsilon\eta^{i-1}\overline{z(b,a)}. \end{aligned}$$

Im Fall (E) ist h insbesondere symmetrisch und wir haben $Aq(\psi)^{i-1} = A(\psi+1)^{i-1} \leq \mathrm{F}(\psi)$, so daß wir auch in diesem Fall

$$\begin{aligned} z(a,b) &= h(a(\psi+1)^{i-1}, b) = h(a, b(\psi+1)^{i-1}\psi^{1-i}) \\ &= h(a, b(\psi+1)^{i-1}) = h(b(\psi+1)^{i-1}, a) \\ &= z(b,a) = \eta^{i-1}\varepsilon z(b,a) \end{aligned}$$

für alle $a, b \in A$ erhalten. Weiterhin gilt $a \in z$-rad $A \Leftrightarrow h(aq(\psi)^{i-1}, b) = 0$ für alle $b \in A \Leftrightarrow a \in B$. Folglich ist l eine wohldefinierte reguläre $^-$-Sesquilinearform auf dem K-Vektorraum C und für $u, v \in C$ gilt $\overline{l(u,v)} = \varepsilon\eta^{i-1}l(v,u)$. Die restlichen Aussagen folgen aus 1.3.12. ■

Korollar 1.3.15 *Sei* $H := \mathrm{H}(\psi, p^i)$.

(i) *Ist* $^-|_K \neq 1_K$ *oder* $p \neq x \pm 1$, *so ist* H *eine hermitesche oder schiefhermitesche Form.*

(ii) *Ist* $\mathrm{char}(K) \neq 2$, $^-|_K = 1_K$, $p = x \pm 1$ *und* f *symmetrisch, so ist* H *symmetrisch, falls* i *ungerade, und symplektisch, falls* i *gerade ist.*

(iii) *Ist* $\mathrm{char}(K) \neq 2$, $^-|_K = 1_K$, $p = x \pm 1$ *und* f *symplektisch, so ist* H *symmetrisch, falls* i *gerade, und symplektisch, falls* i *ungerade ist.*

(iv) *Im Fall* (E) *ist* H *symmetrisch.*

Insbesondere ist H *eine hermitesche oder schiefhermitesche oder symmetrische oder symplektische Form.*

Beweis. Wir greifen die Bezeichnungen aus 1.3.14 auf.
(i). Es gilt $^- \neq 1_{K[\xi]}$ und $\overline{H(a,b)} = \varepsilon\eta^{i-1}H(b,a)$ für alle $a, b \in C$ (cf. 1.3.14).

(ii) und (iii). Es ist $K[\xi] = K[x]/(x \pm 1)K[x] \cong K$ und damit $^- = 1_{K[\xi]}$. Ferner gilt $\eta = -1$ (cf. 1.3.13). Für $a \in C$ folgt

$$H(a,a) = \overline{H(a,a)} = \varepsilon\eta^{i-1}H(a,a) = \varepsilon(-1)^{i-1}H(a,a),$$

so daß sich sämtliche Behauptungen aus (1.3.1) ergeben.
(iv). Es ist $^- = 1_{K[\xi]}$ und $\varepsilon = 1 = \eta$ (cf. (1.3.1) und 1.3.13). ∎

Bemerkung 1.3.16 *Die Bedingung* (R) *impliziert die Spur-Wertigkeit von* $\mathrm{H}(\psi, p^i)$.

Beweis. Aus (R) folgt, daß K und damit auch $K[\xi]$ eine von 2 verschiedene Charakteristik hat oder der Körperautomorphismus $^-$ von $K[\xi]$ nicht die Identität ist. Also ist eine der Bedingungen (i), (ii) oder (iii) von 1.2.29 für $\mathrm{H}(\psi, p^i)$ und $K[\xi]$ [anstelle von f und K] erfüllt. ∎

Es soll nun der Begriff der hermiteschen Invarianten durch eine etwas andere Betrachtungsweise zugänglich gemacht werden.

Lemma 1.3.17 *Es gibt eine p-Komponentenzerlegung von* $\ker p(\psi)^\infty$ *derart, daß* $\ker p(\psi)^\infty = \bigoplus_{j \in \mathrm{I}(\psi,p)} U_j$ *ist.*

Beweis. Seien $I := \mathrm{I}(\psi,p)$ und $(U_j)_{j\in I}$ eine p-Komponentenzerlegung von $\ker p(\psi)^\infty$.
Der Beweis wird durch Induktion über $|I| \in \mathbb{N}$ geführt, wobei der Induktionsanfang trivial ist.
Induktionsschritt: Sei $|I| > 1$. Seien $l := \max I$ und $0 \neq u \in \ker p(\psi) \cap U_l = U_l p(\psi)^{l-1}$. Sei $v \in U_l$ derart, daß $u = vp(\psi)^{l-1}$ gilt. Weil $\ker p(\psi)^\infty$ regulär ist, gibt es ein $z = \sum_{j\in I} z_j$, $z_j \in U_j$, mit $0 \neq f(u,z) = f(v, z\bar{p}(\psi^{-1})^{l-1}) = f(v, z_l\bar{p}(\psi^{-1})^{l-1}) = f(u, z_l)$. Folglich gilt $u \notin \mathrm{rad}\ U_l$ und damit $\mathrm{rad}\ U_l \cap \ker p(\psi_{U_l}) = \{0\}$. Da jeder minimale ψ-Untermodul von U_l in $\ker p(\psi_{U_l})$ enthalten und $\mathrm{rad}\ U_l$ ψ-invariant ist, folgt $\mathrm{rad}\ U_l = \{0\}$, i.e. U_l ist regulär. Es gilt demnach $\ker p(\psi)^\infty = U_l \oplus U_l^\perp$. Nach dem Satz von Krull-Remak-Schmidt ist $\mathrm{I}(\psi_{U_l^\perp}, p) = I \backslash \{l\}$, so daß sich auf $U_l^\perp$ die Induktionsvoraussetzung anwenden läßt. ∎

Wir führen nun zwei neue Begriffe ein.

Definition 1.3.18 (orthogonale p-Komponentenzerlegung)
Eine p-Komponentenzerlegung $\mathcal{U} = (U_j)_{j\in\mathrm{I}(\psi,p)}$ mit den in 1.3.17 aufgeführten Eigenschaften heißt eine orthogonale p-Komponentenzerlegung von $\ker p(\psi)^\infty$.

Bemerkung 1.3.19 *Ist R eine reguläre p^j-Komponente von ψ, $j \in \mathrm{I}(\psi,p)$, so gibt es eine orthogonale p-Komponentenzerlegung von* $\ker p(\psi)^\infty$ *mit p^j-Komponente R.*

Beweis. Sei $W := \ker p(\psi)^\infty \cap R^\perp$. Dann ist W ein regulärer π-Untermodul von $\ker p(\psi)^\infty$ und p^j ist kein Elementarteiler von ψ_W. Setze $L := \mathrm{I}(\psi_W, p) = \mathrm{I}(\psi,p)\backslash\{j\}$. Nach 1.3.17 besitzt $W = \ker p(\psi_W)^\infty$ eine orthogonale p-Komponentenzerlegung $(U_l)_{l\in L}$. Setzt man $U_j := R$, so ist $(U_i)_{i\in\mathrm{I}(\psi,p)}$ eine orthogonale p-Komponentenzerlegung von $\ker p(\psi)^\infty$ mit p^j-Komponente R. ∎

Definition/Satz 1.3.20 (hermitesche Invarianten II**)** *Sei R eine reguläre p^i-Komponente von ψ. Seien $S := Rp(\psi)$ und $T := R/S$. Dann ist T auf kanonische Weise ein $K[\xi]$-Vektorraum.*

Es ist $l : T \times T \mapsto K, l(u+S, v+S) := h(uq(\psi)^{i-1}, v)$, $u, v \in R$, eine wohldefinierte reguläre $^-$-Sesquilinearform auf dem K-Vektorraum T, für die $l(ra,b) = l(a, \bar{r}b)$ und $\overline{l(a,b)} = \eta^{i-1}\varepsilon l(b,a)$ für alle $a, b \in T, r \in K[\xi]$ gilt. Die nach 1.3.12 eindeutig bestimmte reguläre $^-$-Sesquilinearform $\mathrm{H}(\psi, R) : T \times T \to K[\xi]$ auf dem $K[\xi]$-Vektorraum T, für die $\tau \circ \mathrm{H}(\psi, R) = l$ gilt, heißt die zu R gehörende hermitesche Invariante von ψ. Nach 1.3.12 gilt $\overline{\mathrm{H}(\psi, R)(a,b)} = \eta^{i-1}\varepsilon \mathrm{H}(\psi, R)(b,a)$ für alle $a, b \in T$.

Beweis. Der Beweis verläuft vollkommen analog zu dem von 1.3.14. ■

Satz 1.3.21 *Für jede reguläre p^i-Komponente R von ψ sind $\mathrm{H}(\psi, R)$ und $\mathrm{H}(\psi, p^i)$ äquivalent. Insbesondere sind alle zu regulären p^i-Komponenten von ψ gehörenden hermiteschen Invarianten von ψ untereinander äquivalent.*

Beweis. Seien A, B, C wie in 1.3.14 und S, T wie in 1.3.20 und sei $(U_j)_{j \in \mathrm{I}(\psi,p)}$ eine orthogonale p-Komponentenzerlegung von $\ker p(\psi)^\infty$ mit p^i-Komponente R. Setze

$$N := (\bigoplus\nolimits_{j \in \mathrm{I}(\psi,p)_{<i}} U_j) \bigoplus (\bigoplus\nolimits_{j \in \mathrm{I}(\psi,p)_{>i}} U_j p(\psi)^{j-i}).$$

Dann gilt $A = R \bigoplus N$ und

$$B' := \ker p(\psi)^{i-1} + (\ker p(\psi)^{i+1})p(\psi) = Rp(\psi) \bigoplus N.$$

Es soll nun gezeigt werden, daß $B = B'$ ist. Seien $a \in \ker p(\psi)^{i-1}$, $b \in \ker p(\psi)^{i+1}$ und $c \in A$. Dann gilt $f(a, cp(\psi)^{i-1}) = f(a\bar{p}(\psi^{-1})^{i-1}, c) = 0$, weil $a\bar{p}(\psi^{-1})^{i-1} = 0$ ist, und $f(bp(\psi), cp(\psi)^{i-1}) = f(b, cp(\psi)^{i-1}\bar{p}(\psi^{-1})) = 0$, weil $ap(\psi)^{i-1}\bar{p}(\psi^{-1}) = 0$ ist. Es folgt $B' \leq (Ap(\psi)^{i-1})^\perp \cap A = B$. Sei $b \in B$. Wähle zu jedem $j \in \mathrm{I}(\psi, p)$ ein $u_j \in U_j$, so daß $b = \sum_{j \in \mathrm{I}(\psi,p)_{\leq i}} u_j + \sum_{j \in \mathrm{I}(\psi,p)_{>i}} u_j p(\psi)^{j-i}$. Es gilt dann $u_i \in (U_i p(\psi)^{i-1})^\perp \cap U_i = U_i p(\psi) = Rp(\psi)$ und somit $b \in B'$. Aus dem zweiten Homorphiesatz für Gruppen mit Operatoren (cf. [7] chapt.1, §4, no.6, Theorem 4c)) folgt, daß $C = A/B = R + (S \bigoplus N)/(S \bigoplus N)$ und $T = R/S = R/((S \bigoplus N) \cap R)$ als $K[\psi]$-Moduln isomorph sind. Genauer ist $\alpha : T \to C, r + S \mapsto r + B$, $r \in R$, ein $K[\psi]$-Isomorphismus (cf. [7] chapt.1, §4, no.6, Proposition 8). Damit ist α auch ein $K[\xi]$-Isomorphismus der $K[\xi]$- Vektorräume T und C. Es soll nun gezeigt werden, daß α zu $\mathrm{Iso}(\mathrm{H}(\psi, R), \mathrm{H}(\psi, p^i))$ gehört. Setze hierzu $H := \mathrm{H}(\psi, p^i)$ und $G := \mathrm{H}(\psi, R)$. Seien $a, b \in R$ und $r \in K[x]$. Dann gilt $\tau(r(\xi)H((a+S)\alpha, (b+S)\alpha)) = \tau(r(\xi)H(a+B, b+B)) = h(ar(\psi)q(\psi)^{i-1}, b) = \tau(r(\xi)G(a+S, b+S))$ (cf. 1.3.14 und 1.3.20). Hieraus folgt $H((a+S)\alpha, (b+S)\alpha) = G(a+S, b+S)$ (cf. 1.3.11). ■

Im folgenden wird deutlich werden, daß man in einem konkreten Fall mit **einer** zu einer regulären p^i-Komponente von ψ gehörenden hermiteschen Invariante besser 'rechnen' kann als mit **der** hermiteschen Invarianten $\mathrm{H}(\psi, p^i)$. Diese aber vielleicht aufgrund ihrer begrifflichen Eindeutigkeit besser zur **Formulierung** von strukturellen Zusammenhängen geeignet ist.

Für das weitere seien zwei orthogonale p-Komponentenzerlegungen $(U_j)_{j \in \mathrm{I}(\pi,p)}$ von $\ker p(\pi)^\infty$ und $(W_j)_{j \in \mathrm{I}(\phi,p)}$ von $\ker p(\phi)^\infty$ fixiert. Weil π und ϕ ähnlich sind gilt $I := \mathrm{I}(\pi, p) = \mathrm{I}(\phi, p)$ und $\dim U_j = \dim W_j$ für alle $j \in I$. Wir führen weiterhin folgende Abkürzungen ein:

Notation 1.3.22 *$R := U_i$, $S := Rp(\pi)$, $T := R/S$, $H := \mathrm{H}(\pi, R)$, $A := \ker p(\pi)^i$, $B := (Ap(\pi)^{i-1})^\perp \cap A$, $C := A/B$, $G := \mathrm{H}(\pi, p^i)$ und analog $\tilde{R} := W_i$, $\tilde{S} := \tilde{R}p(\phi)$, $\tilde{T} := \tilde{R}/\tilde{S}$, $\tilde{H} := \mathrm{H}(\phi, \tilde{R})$, $\tilde{A} := \ker p(\phi)^i$, $\tilde{B} := (\tilde{A}p(\phi)^{i-1})^\perp \cap \tilde{A}$, $\tilde{C} := \tilde{A}/\tilde{B}$, $\tilde{G} := \mathrm{H}(\phi, p^i)$.*

Durch die Multiplikationsvorschriften $z(\zeta)a := ar(\pi)$ und $z(\zeta)b := br(\phi)$, $z \in K[x]$, $a \in R$, $b \in \tilde{R}$, werden R und $\tilde{R}$ auf kanonische Weise zu $K[\zeta]$-Moduln. Diese sind frei und haben, weil π und ϕ ähnlich sind die gleiche endliche Länge.
Wir notieren nun noch ein Lemma der linearen Algebra, welches nicht in voller Allgemeinheit formuliert wird, sondern auf die spezielle vorliegende Situation zugeschnitten ist.

Lemma 1.3.23 *Jedes $\alpha \in \mathrm{Hom}_{K[\xi]}(T, \tilde{T})$ wird durch ein (nicht notwendig eindeutig bestimmtes) $\beta \in \mathrm{Hom}_{K[\zeta]}(R, \tilde{R})$ induziert, d.h. es gilt $(e+S)\alpha = e\beta + \tilde{S}$ für alle $e \in R$. Ist α ein Isomorphismus, so ist β ein Isomorphismus.*

Beweis. Sei $(v_j)_{1 \le j \le l}$ eine $K[\zeta]$-Basis von R, $l \in \mathbb{N}$. Wähle zu jedem $j \in \mathbb{N}_{\le l}$ ein $w_j \in \tilde{R}$ mit $(v_j + S)\alpha = w_j + \tilde{S}$. Dann wird durch $v_j\beta := w_j$ genau ein Homomorphismus $\beta \in \mathrm{Hom}_{K[\zeta]}(R, \tilde{R})$ definiert. Sei $e \in R$. Dann gibt es eindeutig bestimmte $r_1(\zeta), \ldots, r_l(\zeta) \in K[\zeta]$, $(r_1, \ldots, r_l \in K[x])$, so daß $e = \sum_{j=1}^l r_j(\zeta)v_j = \sum_{j=1}^l v_j r_j(\pi)$ gilt. Es folgt :

$$\begin{aligned}(e+S)\alpha &= (\sum_{j=1}^l r_j(\xi)(v_j + S))\alpha = \sum_{j=1}^l r_j(\xi)(w_j + \tilde{S}) \\ &= (\sum_{j=1}^l r_j(\zeta)w_j) + \tilde{S} = (\sum_{j=1}^l r_j(\zeta)v_j)\beta + \tilde{S} = e\beta + \tilde{S}.\end{aligned}$$

Sei α ein Isomorphismus. Wegen $R = \oplus_{j=1}^l \langle v_j \rangle_\pi$ und $\mathrm{ann}_\pi(v_j) = p^i$ ist $(v_j + S)_{1 \le j \le l}$ eine $K[\xi]$-Basis von T. Folglich ist $(w_j + \tilde{S})_{1 \le j \le l}$ eine $K[\xi]$-Basis von $\tilde{T}$. Seien $r_{0,1}, \ldots, r_{0,j} \in K[x]$ und es gelte $0 = \sum_{j=1}^l r_{0,j}(\zeta)w_j = \sum_{j=1}^l w_j r_{0,j}(\phi)$. Dann gilt $\sum_{j=1}^l r_{0,j}(\xi)w_j + S = 0$, also $r_{0,j} = r_{1,j}p$ für ein $r_{1,j} \in K[x]$. Es folgt $(\sum_{j=1}^l w_j r_{1,j}(\phi))p(\phi) = 0$, also $\sum_{j=1}^l w_j r_{1,j}(\phi) \in \ker p(\phi) = \tilde{R}p^{i-1}(\phi)$. Per Induktion findet man dann für $j \in \mathbb{N}_{\le l}, k \in \mathbb{N}_{\le i}$ Polynome $r_{k,j} \in K[x]$ mit $r_{k-1,j} = r_{k,j}p$ und $\sum_{j=1}^l w_j r_{k,j}(\phi) \in \ker p^k(\phi) = \tilde{R}p^{i-k}(\phi)$. Es folgt $r_{0,j} = p^i r_{i,j}$, also $r_{0,j}(\zeta) = 0$. Folglich ist $(w_j)_{1 \le j \le l}$ linear unabhängig über $K[\zeta]$. Wegen $l = \mathrm{len}_{K[\zeta]}R = \mathrm{len}_{K[\zeta]}\tilde{R}$, ist $(w_j)_{1 \le j \le l}$ eine $K[\zeta]$-Basis von $\tilde{R}$ und damit β ein Isomorphismus. ■

Abschließend beweisen wir den Hauptsatz 1.3.8. Hierfür können wir o.B.d.A. $V = \ker p(\pi)^\infty$ und $W = \ker p(\phi)^\infty$ annehmen.

$\Rightarrow$. Sei $\psi \in \mathrm{Iso}(f, g)$ mit $\pi\psi = \psi\phi$. Es gilt dann $A\psi = \tilde{A}$ und $B\psi = (Ap(\pi)^{i-1})^\perp \cap A)\psi = (A\psi p(\phi)^{i-1})^\perp \cap A\psi = \tilde{B}$. Folglich ist $\hat{\psi} : C \to \tilde{C}, u + B \mapsto u\psi + \tilde{B}$, $u \in A$, ein wohldefinierter K-Epimorphismus. Weil für alle $u \in A$ und $r \in K[x]$

$$(r(\xi)(u+B))\hat{\psi} = ur(\pi)\psi + \tilde{B} = u\psi r(\phi) + \tilde{B} = r(\xi)(u\psi + \tilde{B}) = r(\xi)((u+B)\hat{\psi})$$

gilt, ist $\hat{\psi}$ $K[\xi]$-linear. Sei $u + B \in \ker \hat{\psi}$. Dann gilt $0 = (u+B)\hat{\psi} = u\psi + \tilde{B}$, also $u\psi \in \tilde{B} = B\psi$. Weil ψ injektiv ist, folgt $u \in B$, also ist $\hat{\psi}$ injektiv und damit ein $K[\xi]$-Isomorphismus. Für $u, v \in A$

und $a \in K[x]$ gilt außerdem

$$\begin{aligned} \tau(a(\xi)\tilde{G}((u+B)\hat{\psi},(v+B)\hat{\psi})) &= g(u\psi a(\phi)q(\phi)^{i-1}, v\psi) = g(ua(\pi)q(\pi)^{i-1}\psi, v\psi) \\ &= f(ua(\pi)q(\pi)^{i-1}, v) = \tau(a(\xi)G(u+B, v+B)), \end{aligned}$$

also $\tilde{G}((u+B)\hat{\psi},(v+B)\hat{\psi}) = G(u+B,v+B)$, cf. 1.3.11. Folglich sind $\tilde{G}$ und G äquivalent.

$\Leftarrow$. Seien G und $\tilde{G}$ äquivalent. Nach 1.3.21 sind dann auch H und $\tilde{H}$ äquivalent. Sei $\alpha \in \mathrm{Hom}_{K[\xi]}(T,\tilde{T})$ ein Isomorphismus mit $\tilde{H}(a\alpha, b\alpha) = H(a,b)$ für alle $a,b \in T$. Es soll nun durch Induktion über $j \in \mathbb{N}_{\leq i}$ gezeigt werden, daß es einen Isomorphismus $\beta_j \in \mathrm{Hom}_{K[\zeta]}(R,\tilde{R})$ gibt, so daß $g(u\beta_j q^{i-j}(\phi), v\beta_j) = f(uq^{i-j}(\pi), v)$ für alle $u,v \in R$ gilt.
Induktionsanfang : j=1. Nach 1.3.23 gibt es einen Isomorphismus $\beta \in \mathrm{Hom}_{K[\zeta]}(R,\tilde{R})$ der α induziert, i.e. für den $(u+S)\alpha = u\beta + \tilde{S}$ für alle $u \in R$ gilt. Es folgt

$$g(u\beta q^{i-1}(\phi), v\beta) = \tau(\tilde{H}((u+S)\alpha,(v+S)\alpha)) = \tau(H(u+S,v+S)) = f(uq^{i-1}(\pi), v)$$

für alle $u,v \in R$. Setze $\beta_1 := \beta$.
Induktionsschritt: $j \to j+1$. Seien $j \in \mathbb{N}_{\leq i-1}$, $\beta := \beta_j$ und

$$l : \tilde{R} \times \tilde{R} \to K, (u,v) \mapsto f(u\beta^{-1}q(\pi)^{i-j-1}, v\beta^{-1}) - g(uq(\phi)^{i-j-1}, v).$$

Dann ist l eine $^-$-Sesquilinearform auf dem K-Vektorraum $\tilde{R}$ und für $u,v \in \tilde{R}$ gilt $\overline{l(u,v)} = \varepsilon\eta^{i-j-1}l(v,u)$, cf.1.3.13. Nach Induktionsannahme ist

$$\begin{aligned} l(uq(\phi),v) &= f(uq(\phi)\beta^{-1}q(\pi)^{i-j-1}, v\beta^{-1}) - g(uq(\phi)^{i-j}, v) \\ &= f(u\beta^{-1}q(\pi)^{i-j}, v\beta^{-1}) - g(uq(\phi)^{i-j}, v) = 0. \end{aligned}$$

Hieraus erhält man $\tilde{S} = \tilde{R}p(\phi) = \tilde{R}q(\phi) \leq l\text{-rad}\ \tilde{R}$. Folglich ist $L : \tilde{T} \times \tilde{T} \to K, (u+\tilde{S}, v+\tilde{S}) \mapsto l(u,v)$, $u,v \in \tilde{R}$, eine wohldefinierte $^-$-Sesquilinearform auf dem K-Vektorraum $\tilde{T}$, für die $L(ay,z) = L(y,\bar{a}z)$ und $\overline{L(y,z)} = \varepsilon\eta^{i-j-1}L(z,y)$ für alle $y,z \in \tilde{T}$ und $a \in K[\xi]$ gilt. Nach 1.3.12 gibt es eine eindeutig bestimmte $^-$-Sesquilinearform $D : \tilde{T} \times \tilde{T} \to K[\xi]$ auf dem $K[\xi]$-Vektorraum $\tilde{T}$ mit $\tau \circ D = L$ und $\overline{D(y,z)} = \varepsilon\eta^{i-j-1}D(z,y)$ für alle $y,z \in \tilde{T}$. Weil der Fall (E) ausgeschlossen wurde findet man ein $\delta \in K[\xi]$, so daß $\delta + \bar{\delta} = 1$ ist. Weil $\tilde{H}$ regulär ist, gibt es (genau) ein $\psi' \in \mathrm{End}_{K[\xi]}(\tilde{T})$ mit $\tilde{H} \circ (\psi' \times 1_{\tilde{T}}) = \delta D$. Nach 1.3.23 wird ψ' von einem $\psi \in \mathrm{End}_{K[\zeta]}(\tilde{R})$ induziert, i.e. $(e+\tilde{S})\psi' = e\psi + \tilde{S}$ für alle $e \in \tilde{R}$. Für $u,v \in \tilde{R}$ gilt dann

$$\begin{aligned} &f(u\beta^{-1}q(\pi)^{i-j-1}, v\beta^{-1}) - g(uq(\phi)^{i-j-1}, v) = l(u,v) = L(u+\tilde{S}, v+\tilde{S}) \\ &= \tau(D(u+\tilde{S}, v+\tilde{S})) = \tau(\delta D(u+\tilde{S}, v+\tilde{S}) + \varepsilon\eta^{i-j-1}\overline{\delta D(v+\tilde{S}, u+\tilde{S})}) \\ &= \tau(\tilde{H}(u\psi+\tilde{S}, v+\tilde{S})) + \varepsilon\eta^{i-j-1}\overline{\tau(\tilde{H}(v\psi+\tilde{S}, u+\tilde{S}))} \\ &= g(u\psi q(\phi)^{i-1}, v) + \varepsilon\eta^{i-j-1}\overline{g(v\psi q(\phi)^{i-1}, u)} \\ &= g(u\psi q(\phi)^{i-1}, v) + \eta^{-j}g(uq(\phi)^{i-1}, v\psi) \\ &= g(u\psi q(\phi)^{i-1}, v) + g(uq(\phi)^{i-j-1}, v\psi q(\phi)^j) \\ &= g(u\psi q(\phi)^{i-1}, v) + g(uq(\phi)^{i-j-1}, v\psi q(\phi)^j) + g(u\psi q(\phi)^{i-1}, v\psi q(\phi)^j), \end{aligned}$$

also

$f(u\beta^{-1}q(\pi)^{i-j-1}, v\beta^{-1}))$
$= g(u\psi q(\phi)^{i-1}, v) + g(uq(\phi)^{i-j-1}, v\psi q(\phi)^j) + g(u\psi q(\phi)^{i-1}, v\psi q(\phi)^j) + g(uq(\phi)^{i-j-1}, v)$
$= g(u(1+\psi q(\phi)^j)q(\phi)^{i-j-1}, v(1+\psi q(\phi)^j))$.

Setze $\gamma := \beta(1+\psi q(\phi)^j) \in \mathrm{Hom}_{K[\zeta]}(R, \tilde{R})$. Zeige nun, daß γ injektiv ist. Sei $u \in \ker\gamma$. Dann gilt $u\beta = -u\beta\psi q(\phi)^j$ und somit $u\beta = (-1)^k u\beta\psi^k q(\phi)^{kj}$ für alle $k \in \mathbb{N}$. Wegen $j \neq 0$ folgt $u\beta = 0$. Weil β injektiv ist, gilt $u = 0$. Wegen $\mathrm{len}_{K[\zeta]}(R) = \mathrm{len}_{K[\zeta]}(\tilde{R}) \in \mathbb{N}$ ist γ auch surjektiv, also ein Isomorphismus. Setze $\beta_{j+1} := \gamma$.
Es gilt nun $\psi(R, \tilde{R}) := \beta_i \in U(f_R, g_{\tilde{R}})$ und wegen $\psi(R, \tilde{R}) \in \mathrm{Hom}_{K[\zeta]}(R, \tilde{R})$ auch $\pi_R\psi(R, \tilde{R}) = \psi(R, \tilde{R})\phi_{\tilde{R}}$.
Durch 'Zusammensetzen' erhält man eine Isometrie $\psi := \textcircled{\perp}_{i\in I}\psi(U_i, W_i) \in \mathrm{Iso}(f, g)$, für die $\pi\psi = \psi\phi$ gilt. ■

Als eine bekannte Anwendung des Satzes 1.3.8 machen wir die folgende

Bemerkung 1.3.24 (Wall) *Seien K ein endlicher Körper, f eine reguläre $^{-}$-hermitesche Form und $\pi, \phi \in \mathrm{U}(f)$. Dann sind π und ϕ genau dann in $\mathrm{U}(f)$ konjugiert, wenn sie ähnlich sind.*

Beweis. Seien π und ϕ ähnlich, $p \in K[x]$ normiert und irreduzibel so, daß p^i ein Elemantarteiler von π und ϕ mit Vielfacheit $m \in \mathbb{N}$ ist, $i \in \mathbb{N}$. Seien R, R' reguläre p^i-Komponenten von π bzw. ϕ Nach 1.3.15 (i) sind $\mathrm{H}(\pi, R)$ und $\mathrm{H}(\phi, R')$ beides hermitesche oder beides schiefhermitesche Formen auf den m-dimensionalen $K[x]/pK[x]$-Vektorräumen R bzw. R'. Weil $K[x]/pK[x]$ ein endlicher Körper ist, sind bekanntlich $\mathrm{H}(\pi, R)$ und $\mathrm{H}(\phi, R')$ äquivalent. Nach 1.3.8 sind ϕ und ψ konjugiert in $\mathrm{U}(f)$.
■

1.4 Korrespondenzen zwischen f und H

Es seien die Annahmen und Notation des vorigen Abschnittes weiterhin gültig (cf. 1.3.1, 1.3.13, 1.3.22).

Bemerkung 1.4.1 *Seien Y, Z π-Untermoduln von R und $a, b \in R$. Dann gilt:*

(i) *$Y + S/S \perp_H Z + S/S \Leftrightarrow Yp(\pi)^{i-1} \perp_f Z$;*

(ii) *$H(a+S, b+S) = 0 \Leftrightarrow \langle ap(\pi)^{i-1}\rangle_\pi \leq \langle b\rangle_\pi^{\perp_f}$; Insbesondere ist $a+S$ ist genau dann H-isotrop, wenn $\mathrm{ann}_\pi(a) = p^i$ und $\langle a\rangle_\pi$ nicht regulär ist;*

(iii) *Y ist genau dann $f-$regulär, wenn $Y + S/S$ H-regulär ist und es einen π-Modul W mit $R = Y \oplus W$ gibt.*

Beweis. (i) Seien $y \in Y$ und $z \in Z$.
$\Rightarrow$. Es gilt $0 = \tau(H(y+S, z+S)) = f(yq(\pi)^{i-1}, z)$, also $Yp(\pi)^{i-1} = Yq(\pi)^{i-1} \perp_f Z$.
$\Leftarrow$. Für alle $a \in K[x]$ gilt $0 = f(ya(\pi)q(\pi)^{i-1}, z) = \tau(a(\xi)H(y+S, z+S))$. Nach Definition von H folgt hieraus $H(y+S, z+S) = 0$.
(ii) folgt unmittelbar aus (i) angewandt auf $Y = \langle a\rangle_\pi$ und $Z = \langle b\rangle_\pi$.

(iii) $\Rightarrow$. Sei $u + S \in H$-rad $(Y + S/S)$, $u \in Y$. Nach (i) gilt dann $up(\pi)^{i-1} \in f$-rad $Y = \{0\}$, i.e. $u \in \ker p(\pi)^{i-1} \cap R = S$. Weiterhin ist $W := Y^{\perp} \cap R$ ein π-Modul, für den $R = Y \oplus W$ gilt.
$\Leftarrow$. Sei $u \in (f\text{-rad } Y) \cap \ker p(\pi)$. Weil Y und W π-invariant sind, gilt nach dem Satz von Krull-Remak-Schmidt $\ker p(\pi_Y) = Yp(\pi)^{i-1}$, also $u = yp(\pi)^{i-1}$ für ein $y \in Y$. Aus (i) folgt dann $y + S \in H$-rad $Y + S/S = \{0\}$, i.e. $y \in S = Rp(\pi)$. Dies liefert $u \in Rp(\pi)^i = \{0\}$. ∎

Das nun folgende Lemma wurde in [48] für symmetrisches f bewiesen, der angegebene Beweis macht jedoch von der Symmetrie keinen Gebrauch. Vollständigkeitshalber wird er hier wiederholt.

Lemma 1.4.2 *Sei $r \in K[X]$ ein irreduzibler Teiler von* $\text{mip}(\pi)$. *Seien $u, w \in V$ mit $\text{ann}_\pi(u) = r^i = \text{ann}_\pi(w)^*$, $i \in \mathbb{N}$, derart, daß $\langle u\rangle_\pi$ und $\langle w\rangle_\pi$ nicht regulär sind und $\langle ur(\pi)^{i-1}\rangle_\pi \not\leq \langle w\rangle_\pi^\perp$ gilt. Dann gilt $\langle u\rangle_\pi \cap \langle w\rangle_\pi = \{0\}$ und $L := \langle u\rangle_\pi \oplus \langle w\rangle_\pi$ ist regulär.*

Beweis. Seien $a \in \langle u\rangle_\pi$ und $b \in \langle w\rangle_\pi$ mit $0 \neq f(ar(\pi)^{i-1}, b) = f(a, b\bar{r}(\pi^{-1})^{i-1})$. Demnach gilt auch $\langle wr^*(\pi)^{i-1}\rangle_\pi = \langle w\bar{r}(\pi^{-1})^{i-1}\rangle_\pi \not\leq \langle u\rangle_\pi^\perp$.

'$\langle u\rangle_\pi \cap \langle w\rangle_\pi = \{0\}$'. Dies ist trivial falls $r \neq r^*$ ist, so daß man $r = r^*$ annehmen kann. Aus $\langle u\rangle_\pi \cap \langle w\rangle_\pi \neq \{0\}$ würde dann $\langle ur(\pi)^{i-1}\rangle_\pi = \langle wr(\pi)^{i-1}\rangle_\pi \leq \text{rad } \langle w\rangle_\pi \leq \langle w\rangle_\pi^\perp$ folgen, ein Widerspruch.

'$L := \langle u\rangle_\pi \oplus \langle w\rangle_\pi$ ist regulär'. Sei $z \in (\text{rad } L) \cap (\ker r(\pi) \oplus \ker r^*(\pi)) \leq \langle ur(\pi)^{i-1}\rangle_\pi \oplus \langle wr^*(\pi)^{i-1}\rangle_\pi$. Wähle $a \in \langle ur(\pi)^{i-1}\rangle_\pi$ und $b \in \langle wr^*(\pi)^{i-1}\rangle_\pi$ so, daß $z = a + b$ ist. Dann gilt für $c, d \in K[x]$:

$$0 = f(uc(\pi), zd(\pi)) = f(uc(\pi), bd(\pi))$$

also $\langle b\rangle_\pi \leq \langle u\rangle_\pi^\perp \cap \langle wr^*(\pi)^{i-1}\rangle_\pi = \{0\}$, und analog

$$0 = f(wc(\pi), zd(\pi)) = f(wc(\pi), ad(\pi))$$

also $\langle a\rangle_\pi \leq \langle w\rangle_\pi^\perp \cap \langle ur(\pi)^{i-1}\rangle_\pi = \{0\}$. Es folgt $z = 0$ und wegen $\text{mip}(\pi_L) = \text{lcm}(r, r^*)^i$ damit auch rad $L = \{0\}$. ∎

Im Kontext der hermiteschen Invarianten bedeutet 1.4.2 folgendes:

Lemma 1.4.3 *Seien $a, b \in R$. Folgende Aussagen sind äquivalent:*

(i) *$a + S$ und $b + S$ sind H-isotrop und $L := \langle a\rangle_{K[\xi]} \oplus \langle b\rangle_{K[\xi]}$ ist eine H-hyperbolische Ebene.*

(ii) *$\text{ann}_\pi(a) = p^i = \text{ann}_\pi(b)$, $\langle a\rangle_\pi$ und $\langle b\rangle_\pi$ sind singulär und $M := \langle a\rangle_\pi \oplus \langle b\rangle_\pi$ ist regulär.*

Im Fall (R) *impliziert jede der beiden gleichwertigen Aussagen* (i) *und* (ii) *die Aussage*

(iii) *Es gibt $c, d \in \langle a\rangle_\pi \oplus \langle b\rangle_\pi$, so daß $\langle c\rangle_\pi$ und $\langle d\rangle_\pi$ totalisotrop sind und $\langle a\rangle_\pi \oplus \langle b\rangle_\pi = \langle c\rangle_\pi \oplus \langle d\rangle_\pi$ ist.*

Beweis. (i) $\Rightarrow$ (ii). Weil L eine Ebene ist, folgt $a, b \notin S$ und daher $\text{ann}_\pi(a) = p^i = \text{ann}_\pi(b)$. Nach 1.4.1 (ii) sind $\langle a\rangle_\pi$ und $\langle b\rangle_\pi$ singulär. Weil L H-regulär ist, gilt $H(a + S, b + S) \neq 0$, so daß sich

$\langle ap(\pi)^{i-1}\rangle_\pi \not\leq \langle b\rangle_\pi^{\perp_f}$ aus 1.4.1 (ii) ergibt. Nun beweist 1.4.2 die letzte Aussage von (ii).

(ii) $\Rightarrow$ (i). Wegen $\operatorname{ann}_\pi(a) = p^i = \operatorname{ann}_\pi(b)$, sind $a+S$ und $b+S$ von S verschieden. Weil $\langle a\rangle_\pi$, $\langle b\rangle_\pi$ singulär sind und M regulär ist, gilt $\langle ap(\pi)^{i-1}\rangle_\pi \leq \langle a\rangle_\pi^\perp$, $\langle bp(\pi)^{i-1}\rangle_\pi \leq \langle b\rangle_\pi^\perp$ und $\langle ap(\pi)^{i-1}\rangle_\pi \not\leq \langle b\rangle_\pi^\perp$. Nach 1.4.1 (ii) sind $a+S$ und $b+S$ H-isotrop und es gilt $H(a+S, b+S) \neq 0$. Insbesondere ist $\langle a\rangle_{K[\xi]} \neq \langle b\rangle_{K[\xi]}$ und $\langle a\rangle_{K[\xi]} \oplus \langle b\rangle_{K[\xi]}$ eine H-hyperbolische Ebene.

(ii) $\Rightarrow$ (iii). Falls i gerade ist, ist $Z := \langle ap(\pi)^{i/2}\rangle_\pi \oplus \langle bp(\pi)^{i/2}\rangle_\pi$ ein totalisotroper Unterraum mit $\dim Z = \frac{1}{2}\dim M$. Falls i ungerade ist, ist $Z := \langle ap(\pi)^{(i-1)/2}\rangle_\pi \oplus \langle bp(\pi)^{(i+1)/2}\rangle_\pi$ ein totalisotroper Unterraum mit $\dim Z = \frac{1}{2}\dim M$.
Sei Y ein weiterer totalisotroper Unterraum von M mit $M = Y \oplus Z$. Wegen $\dim Y = \frac{1}{2}\dim M = \deg p^i$ gibt es ein $\psi \in \mathrm{GL}(Y)$ mit $\mathrm{mip}(\psi) = p^i$. Sei $\hat{\psi} \in \mathrm{U}(f_M)$ die nach 1.3.5 eindeutig bestimmte Fortsetzung von ψ, für die $Z\hat{\psi} = Z$ gilt. Wegen $p = p^*$ gilt dann nach 1.3.5 $\mathrm{mip}(\hat{\psi}_Z) = p^i$. Folglich sind π_M und $\hat{\psi}$ ähnlich. Seien $D := Mp(\hat{\psi})$, $D' := Mp(\pi)$, $E := M/D$, $E' := M/D'$, $G := \mathrm{H}(\hat{\psi}, p^i) = \mathrm{H}(\hat{\psi}, M)$, $G' := \mathrm{H}(\pi_M, p^i) = \mathrm{H}(\pi_M, M)$ und $y \in Y, z \in Z$ mit $Y = \langle y\rangle_{\hat{\psi}}$ und $Z = \langle z\rangle_{\hat{\psi}}$.
Nach (ii) $\Rightarrow$ (i) [mit ψ, y und z anstelle von π, a und b] ist E eine G-hyperbolische Ebene. Weil aus dem gleichen Grund auch E' eine G'-hyperbolische Ebene ist, sind G und G' äquivalent.
Dann sind E und E' auf kanonische Weise $K[\xi]$-Vektorräume und $E = \langle y + D\rangle_{K[\xi]} \oplus \langle z + D\rangle_{K[\xi]}$ ist ein 2-dimensionaler $K[\xi]$-Vektorraum mit G-isotropen Basisvektoren $y + D$, $z + D$, i.e. E ist eine G-hyperbolische Ebene. Nach obigem ist auch $E' = \langle u + D'\rangle_{K[\xi]} \oplus \langle w + D'\rangle_{K[\xi]}$ eine G'-hyperbolische Ebene mit G'-isotropen Basisvektoren $u + D'$, $w + D'$. Folglich sind G und G' äquivalent. Nach 1.3.8 sind π_M und ψ metrisch konjugiert. ■

Wir kommen nun zur Verallgemeinerung von 1.4.3 auf hyperbolische Räume, deren Beweis jedoch auf dem Spezialfall 1.4.3 beruht.

Lemma 1.4.4 *Es gelte* (R). *Sei L ein π-invarianter Unterraum von R. Dann sind folgende Aussagen äquivalent:*

(i) *$L + S/S$ ist ein H-regulärer, H-hyperbolischer Raum.*

(ii) *L enthält einen f-regulären, f-hyperbolischen π-Modul M, für den $L + S/S = M + S/S$ gilt, und es gibt totalisotrope π-Moduln $Y, Z \leq M$ mit $M = Y \oplus Z$.*

Beweis. (i) $\Rightarrow$ (ii). Seien $Y, Z \leq L$ f-totalisotrope π-Moduln derart, daß $Y \oplus Z$ ein regulärer π-Modul ist. Es seien Y, Z so gewählt, daß $M := Y \oplus Z$ maximal ist. Sei $U := M^{\perp_f} \cap L$. Dann gilt $L = M \bigoplus_f U$. Nach 1.4.1 (i) und (iii) gilt $L + S/S = (Y + S/S \oplus Z + S/S) \bigoplus_H U + S/S$ und $Y + S/S \oplus Z + S/S = (Y + Z) + S/S$ ist ein H-regulärer, H-hyperbolischer Raum mit H-totalisotropen $K[\xi]$-Unterräumen $Y + S/S, Z + S/S$.

Annahme: $U + S/S \neq \{0\}$. Weil $L + S/S$ ein H-regulärer, H-hyperbolischer Raum ist, ist nach dem Witt'schen Kürzungssatz auch $U + S/S$ ein H-regulärer, H-hyperbolischer Raum.

Wähle $a, b \in U$, so daß $a+S, b+S$ H-isotrop sind und $\langle a+S\rangle_{K[\xi]} \oplus \langle b+S\rangle_{K[\xi]}$ eine H-hyperbolische Ebene ist. Nach 1.4.3 kann man a, b so wählen, daß daß $\langle a\rangle_\pi$ und $\langle b\rangle_\pi$ totalisotrope π-Moduln sind und $N := \langle a\rangle_\pi \oplus \langle b\rangle_\pi \leq U$ regulär ist.
Setze $Y' := Y \oplus \langle a\rangle_\pi$ und $Z' := Z \oplus \langle b\rangle_\pi$. Dann sind Y', Z' totalisotrope π-Moduln und $Y' \oplus Z' = M \mathbin{\bigcirc\!\!\!\!\perp} N$ ist ein regulärer, hyperbolischer π-Modul mit der M echt umfaßt, ein Widerspruch zur Wahl von M. Es folgt $U \leq S$ und damit $L + S/S = M + S/S$.

(ii) $\Rightarrow$ (i). Nach 1.4.1 sind $Y + S/S$ und $Z + S/S$ H-totalisotrop und $L + S/S = M + S/S$ ist H-regulär. Also ist $L + S/S = Y + S/S \oplus Z + S/S$ ein H-regulärer, H-hyperbolischer Raum. ∎

1.5 Normalformen von Isometrien

Wir benötigen einige Fakten über Normalformen von orthogonalen, symplektischen und unitären Isometrien, wie man sie zum Beispiel in dem Buch 'Angewandte Lineare Algebra' von B. Huppert [43] nachschlagen kann. Weil diese sich jedoch im wesentlichen unmittelbar mit den bereitgestellten Hilfsmitteln der letzten beiden Abschnitte herleiten lassen, haben wir uns entschlossen, kurze Beweise anzugeben.

Definition 1.5.1 *Sei $\pi \in \mathrm{Aut}(f)$. Nenne $V \neq \{0\}$ einen orthogonal unzerlegbaren π-Modul, falls aus $V = U \mathbin{\bigcirc\!\!\!\!\perp} W$ für π-Moduln U und W entweder $U = \{0\}$ oder $W = \{0\}$ folgt.*

Lemma 1.5.2 (orthogonale Zerlegung in π-Moduln) *Sei $\pi \in \mathrm{Aut}(f)$. Dann besitzt V eine Zerlegung $V = V_1 \mathbin{\bigcirc\!\!\!\!\perp} \ldots \mathbin{\bigcirc\!\!\!\!\perp} V_k$ in orthogonal unzerlegbare π-Moduln V_i.* ∎

Satz 1.5.3 (orthogonal unzerlegbare π-Moduln) *Seien $\pi \in \mathrm{Aut}(f)$ und $V \neq \{0\}$ ein orthogonal unzerlegbarer π-Modul. Dann gehört V zu genau einem der folgenden Typen:*

(I) *Es gilt $\mathrm{mip}(\pi) = p^i p^{*i}$ für ein $i \in \mathbb{N}$ und ein $p \in K[x]$, das irreduzibel und teilerfremd zu p^* ist. Ferner ist $V = \ker p^i(\pi) \oplus \ker p^{*i}(\pi)$, wobei die π-Moduln $\ker p^i(\pi)$ und $\ker p^{*i}(\pi)$ π-unzerlegbar (also π-zyklisch) und totalisotrop sind. Insbesondere ist V ein hyperbolischer Raum und ein zyklischer π-Modul.*

(II) *Es ist $^- = 1_K$, $\mathrm{mip}(\pi) = (x \pm 1)^i$ für ein $i \in \mathbb{N}$ und es gilt $V = U \oplus W$ für zwei π-unzerlegbare (also π-zyklische) π-Moduln U, W. Dabei stimmen die Minimalpoynome von π_U und π_W mit dem von π überein.*

Ist $\mathrm{char}(K) \neq 2$, so ist i gerade (bzw. ungerade), falls f symmetrisch (bzw. symplektisch) ist. Ferner gibt es in diesem Fall totalisotrope π-Moduln U', W' mit $V = U' \oplus W'$.

(III) *Der π-Modul V ist π-unzerlegbar. Dann gilt $\mathrm{mip}(\pi) = p^i$ für ein irreduzibles $^-$-symmetrisches Polynom $p \in K[x]$ und ein $i \in \mathbb{N}$, und V ist π-zyklisch.*

Ist $^- = 1_K$ und $p = x \pm 1$ und $\mathrm{char}(K) \neq 2$, so ist i ungerade (bzw. gerade), falls f symmetrisch (bzw. symplektisch) ist.

Ist $^- = 1_K$ und $p = x \pm 1$ und $\mathrm{char}(K) = 2$, so ist $i = 1$ oder i ist gerade.

Beweis. Zunächst bemerken wir, daß V keine echten, nichttrivialen, regulären π-Untermoduln U enthalten kann, da sonst auch $U^\perp$ π-invariant und damit $V = U \bigcirc\!\!\!\!\perp\, U^\perp$ eine nichttriviale Zerlegung von V in π-Moduln wäre.
Nach 1.3.6 gilt $\operatorname{mip}(\pi) = \gcd(p, p^*)^i$ für ein irreduzibles normiertes Polynom $p \in K[x]$ und ein $i \in \mathbb{N}$.

Fall A: $p \neq p^*$. Dann ist $V = \ker p(\pi)^i \oplus \ker p^*(\pi)^i$. Nach 1.3.6 sind $\ker p(\pi)^i$ und $\ker p^*(\pi)^i$ totalisotrop. Sei $v \in \ker p(\pi)^i$ mit $\operatorname{ann}_\pi(v) = p^i$. Weil dann $vp(\pi)^{i-1} \in \ker p(\pi)^i \backslash \{0\}$ liegt, findet man aufgrund der Regularität von f ein $w \in \ker p^*(\pi)^i$ mit $0 \neq f(vp(\pi)^{i-1}, w) = p(0)f(v, wp^*(\pi)^{i-1}\pi^{\deg(p)(1-i)})$. Damit ist insbesondere $wp^*(\pi)^{i-1} \neq 0$, i.e. $\operatorname{ann}_\pi(w) = p^{*i}$. Nach 1.4.2 ist $\langle v\rangle_\pi \oplus \langle w\rangle_\pi$ ein regulärer π-Modul, so daß aus der Vorbemerkung $V = \langle v\rangle_\pi \oplus \langle w\rangle_\pi$ folgt. Demnach ist V vom Typ I.

Fall B: $p = p^*$. Nach 1.3.17 ist V bereits eine p^i-Komponente. Seien $H := \mathrm{H}(\pi, p^i)$ und $S := Vp(\pi)$. Ferner seien ε wie in (1.3.1) und q, η wie unter 1.3.13 aus Abschnitt 1.3 definiert.

B1: H ist nicht symplektisch. Dann gibt es ein $a \in V$, so daß $a + S$ ein H-anisotroper Vektor ist. Nach 1.4.1 (ii) ist $\operatorname{ann}_\pi(a) = p^i$ und $\langle a\rangle_\pi$ ein regulärer π-Modul. Somit ist $V = \langle a\rangle_\pi$ und V vom Typ III. Seien $^- = 1_K$ und $p \in \{x+1, x-1\}$. Ist $\operatorname{char}(K) \neq 2$, so haben wir in 1.3.15 (ii) gesehen, daß i ungerade (gerade) sein muß, wenn f symmetrisch (symplektisch) ist. Sei schließlich $\operatorname{char}(K) = 2$. Beachte, daß dann das Quadrieren ein Körpermonomorphismus ist. Annahme: $i = 2j + 1$ für ein $j \in \mathbb{N}$. Wir berechnen

$$\begin{aligned}
f(v(\pi+1)^{2j-1}\pi, v) &= f(v\pi^{2j}, v(\pi+1)^{2j-1}) = f(v\pi^{2j} + 1, v(\pi+1)^{2j-1}) + f(v, v(\pi+1)^{2j-1}) \\
&= f(v(\pi^j + 1)^2, v(\pi+1)^{2j-1}) + f(v, v(\pi+1)^{2j-1}) \\
&= f(v(\pi+1)^2(\sum_{k=0}^{j-1} \pi^k)^2, v(\pi+1)^{2j-1}) + f(v, v(\pi+1)^{2j-1}) \\
&= f(v, v(\pi+1)^{2j-1}).
\end{aligned}$$

Dies impliziert

$$f(v(\pi+1)^{2j}, v) = f(v(\pi+1)^{2j-1}\pi, v) + f(v(\pi+1)^{2j-1}, v) = f(v, v(\pi+1)^{2j-1}) + f(v(\pi+1)^{2j-1}, v) = 0.$$

Hieraus folgt bereits $v(\pi+1)^{2j} \in \operatorname{rad} V$, ein Widerspruch.
B2: H ist symplektisch. Nach 1.3.15 ist dann $^- = 1_K$ und im Fall $\operatorname{char}(K) \neq 2$ ist i gerade (ungerade), falls f symmetrisch (symplektisch) ist. Wähle $a, b \in V$, so daß $a + S$ und $b + S$ H-isotrop sind und eine H-hyperbolische Ebene aufspannen. Nach 1.4.3 ist $\operatorname{ann}_\pi(a) = p^i = \operatorname{ann}_\pi(b)$, $\langle a\rangle_\pi$ und $\langle b\rangle_\pi$ sind singulär und $\langle a\rangle_\pi \oplus \langle b\rangle_\pi$ ist regulär. Demnach ist $V = \langle a\rangle_\pi \oplus \langle b\rangle_\pi$ vom Typ II. Für $\operatorname{char}(K) \neq 2$ haben wir in 1.4.3 (iii) die letzte unter (II) aufgeführte Aussage bewiesen. ■

Es sei angemerkt, daß alle in Satz 1.5.3 aufgeführten Fälle auch tatsächlich vorkommen können. (Für Beweise verweisen wir auf das bereits oben zitierte Werk von B. Huppert.)
Ist f symplektisch, $\pi \in \mathrm{Sp}(f)$ und V ein orthogonal unzerlegbarer π-Modul vom Typ II, so haben wir gesehen, daß V stets eine Zerlegung $V = U \oplus W$ in totalisotrope π-Moduln U und W gestattet,

vorausgesetzt die Charakteristik von K ist ungleich 2. Diese Tatsache werden wir später benötigen um zu klären, wann eine unipotente unitäre Isometrie ein Produkt von zwei unitären Involutionen ist.
Für $\mathrm{char}(K) = 2$ ist die Sachlage anders. In [43] (Kapitel V, §8, S.588,589, Aufgabe A8.2) wird ein Beispiel angegeben, bei dem $\mathrm{mip}(\pi) = (x+1)^3$ ist und es keine Zerlegung der oben genannten Art gibt. (Weitere solche Beispiele mit beliebigem ungeraden Exponenten $t > 1$ werden wir im nächsten Abschnitt sehen, cf. 2.2.4 (iii).)
Wir wollen nun auf elementare Weise zeigen, daß es für gerade Exponenten $i \in \mathbb{N}$ und $\mathrm{mip}(\pi) = (x+1)^i$, auch bei Charakteristik 2 stets totalisotrope π-Moduln gibt, die V zerlegen.
Hierfür benötigen wir zunächst eine in [43] (Kapitel V, §8, S.588,589, Aufgabe A8.1) als Übungsaufgabe gestellte

Bemerkung 1.5.4 *Seien* $\mathrm{char}(K) = 2$, f *symmetrisch und* $\pi \in \mathrm{Aut}(f)$. *Es gelte* $V = \langle u\rangle_\pi \oplus \langle v\rangle_\pi$ *für singuläre* π*-Moduln* $\langle u\rangle_\pi$, $\langle v\rangle_\pi$ *und* $\mathrm{ann}_\pi(u) = (x+1)^i = \mathrm{ann}_\pi(v)$, $i \in \mathbb{N}$. *Dann ist* V *ein orthogonal unzerlegbarer* π*-Modul vom Typ II.*

Beweis. Sei $H := \mathrm{H}(\pi, V)$. Nach 1.3.15 (iv) ist H eine symmetrische Form. Nach 1.4.3 (ii) $\Rightarrow$ (i) ist $V/\mathrm{B}(\pi)$ eine H-hyperbolische Ebene. Wegen $\mathrm{char}(K[\xi]) = 2$ folgt dann bereits, daß H symplektisch ist. Wäre V orthogonal zerlegbar, so gäbe es ein $c \in V$ mit $\mathrm{ann}_\pi(c) = (x+1)^i$, so daß $\langle c\rangle_\pi$ regulär ist. Nach 1.4.1 wäre dann $c + \mathrm{B}(\pi)$ ein H-anisotroper Vektor, ein Widerspruch. ∎

Satz 1.5.5 *Seien* $\mathrm{char}(K) = 2$, f *symplektisch und* $\pi \in \mathrm{Sp}(f)$ *mit* $\mathrm{mip}(\pi) = (x+1)^{2t}$, $t \in \mathbb{N}$, *derart, daß* V *ein orthogonal unzerlegbarer* π*-Modul vom Typ II ist. Dann gibt es* $u, v \in V$, *so daß* $\langle u\rangle_\pi, \langle v\rangle_\pi$ *totalisotrop sind und* $V = \langle u\rangle_\pi \oplus \langle v\rangle_\pi$ *ist.*

Beweis. Der Beweis erfolgt durch Induktion über $t \in \mathbb{N}$. Wir beweisen:

(∗) Sind $a, b \in V$ mit $V = \langle a\rangle_\pi \oplus \langle b\rangle_\pi$, so gibt es $a', b' \in \mathrm{B}(\pi)$, so daß $\langle a + a'\rangle_\pi$ und $\langle b + b'\rangle_\pi$ totalisotrop sind und $V = \langle a + a'\rangle_\pi \oplus \langle b + b'\rangle_\pi$ gilt.

Seien $a, b \in V$, so daß $V = \langle a\rangle_\pi \oplus \langle b\rangle_\pi$ ist. Weil V orthogonal unzerlegbar ist, sind $\langle a\rangle_\pi$ und $\langle b\rangle_\pi$ singulär. Weil $\langle a(\pi+1)^{2t-1}\rangle_\pi$ ($\langle b(\pi+1)^{2t-1}\rangle_\pi$) der kleinste π-Untermodul von $\langle a\rangle_\pi$ ($\langle b\rangle_\pi$) und $\mathrm{rad}\ \langle a\rangle_\pi$ ($\mathrm{rad}\ \langle b\rangle_\pi$) π-invariant ist, folgt

(1) $\langle a(\pi+1)^{2t-1}\rangle_\pi \leq \mathrm{rad}\ \langle a\rangle_\pi$ ($\langle b(\pi+1)^{2t-1}\rangle_\pi \leq \mathrm{rad}\ \langle b\rangle_\pi$).

Induktionsanfang: $t = 1$. Weil f symplektisch ist, folgt mit dem eben gezeigten, daß $\langle a\rangle_\pi$ und $\langle b\rangle_\pi$ bereits totalisotrop sind. (Wähle $a' = 0 = b'$.)

Induktionsschritt: Sei $t \geq 2$. Seien $B := \mathrm{B}(\pi)$ und $R := \mathrm{F}(\pi) = \mathrm{B}(\pi) \cap \mathrm{F}(\pi) = \mathrm{rad}\mathrm{B}(\pi)$ und $\tilde{} : B \to B/R, a \mapsto a + R$. Dann induziert f auf B/R eine wohldefinierte, reguläre, symplektische Form

$$\tilde{f} : B/R \times B/R, (\tilde{a}, \tilde{b}) \mapsto f(a, b)$$

und π eine wohldefinierte Isometrie

$$\tilde{\pi} : B/R \to B/R, \tilde{a} \mapsto \widetilde{a\pi}$$

von $\tilde{f}$. Setze $c := a(\pi+1)$ und $d := b(\pi+1)$. Dann gilt $B/R = \langle\tilde{c}\rangle_{\tilde{\pi}} \oplus \langle\tilde{d}\rangle_{\tilde{\pi}}$ und $\mathrm{ann}_{\tilde{\pi}(\tilde{c})} = (x+1)^{2(t-1)} = \mathrm{ann}_{\tilde{\pi}}(\tilde{d})$. Unter Ausnutzung von (1) berechnet man leicht, daß $\langle\tilde{c}\rangle_{\tilde{\pi}}$ und $\langle\tilde{d}\rangle_{\tilde{\pi}}$ $\tilde{f}$-singulär sind. Nach 1.5.4 ist B/R ein orthogonal unzerlegbarer $\tilde{\pi}$-Modul vom Typ II. Wir können daher die Induktionsannahme $(*)$ auf B/S, $\tilde{f}$, $\tilde{\pi}$, $\langle\tilde{c}\rangle_{\tilde{\pi}}$ und $\langle\tilde{d}\rangle_{\tilde{\pi}}$ anwenden. Wegen $\mathrm{B}(\tilde{\pi}) = \widetilde{\mathrm{B}^2(\pi)}$ findet man deshalb $a', b' \in \mathrm{B}(\pi)$, so daß für $u := a + a'$, $v := u(\pi+1)$, $y := b + b'$ und $z := y(\pi+1)$ die $\tilde{\pi}$-Moduln $\langle\tilde{v}\rangle_{\tilde{\pi}}$ und $\langle\tilde{z}\rangle_{\tilde{\pi}}$ $\tilde{f}$-totalisotrop sind und $B/R = \langle\tilde{v}\rangle_{\tilde{\pi}} \oplus \langle\tilde{z}\rangle_{\tilde{\pi}}$ gilt.

Wegen $2t \geq 4 > 3$ liegt $b_3 := b(\pi+1)^{2t-3}$ in $\mathrm{B}(\pi)\backslash\{0\}$. Ziel ist es, einen Faktor $\lambda \in K$ so zu bestimmen, daß $w := u + \lambda b_3$ einen totalisotropen π-Modul $\langle w\rangle_\pi = \langle w, w(\pi+1), \ldots, w(\pi+1)^{2t-1}\rangle$ erzeugt. Weil $\langle w\rangle_\pi$ für jedes $\lambda \in K$ singulär ist mit $w(\pi+1)^{2t-1} \in \mathrm{rad}\ \langle w\rangle_\pi$, und weil f symplektisch ist, ist dies genau dann der Fall, wenn $f(w(\pi+1)^j, w(\pi+1)^k) = 0$ für alle $j, k \in \{0, \ldots, 2(t-1)\}$ mit $j > k$ gilt.

Seien $j, k \in \mathbb{N}$ mit diesen Eigenschaften gewählt, $b_2 := b_3(\pi+1) = b(\pi+1)^{2(t-1)}$ und $b_1 := b_2(\pi+1) = b(\pi+1)^{2t-1} \in \mathrm{F}(\pi) = R$. Wir betrachten zunächst den Fall $j + k \geq 3$. Man berechnet

$$\begin{aligned}
f(w(\pi+1)^j, w(\pi+1)^k) &= f((v+\lambda b_2)(\pi+1)^{j-1}, w(\pi+1)^k) \\
&= f((v+\lambda b_2)\pi^{j-1}, (v+\lambda b_2)(\pi+1)^{k+j-2}) \\
&= f((v+\lambda b_2)\pi^{j-1}, v(\pi+1)^{k+j-2} + \lambda b_1(\pi+1)^{k+j-3}) \\
&= \tilde{f}((\tilde{v}+\lambda\tilde{b_2})\tilde{\pi}^{j-1}, \tilde{v}(\tilde{\pi}+1)^{k+j-2}) \\
&= \lambda\tilde{f}(\tilde{b_2}\tilde{\pi}^{j-1}, \tilde{v}(\tilde{\pi}+1)^{k+j-2}) \\
&= \lambda\tilde{f}(\tilde{b_1}(\tilde{\pi}+1)^{k+j-3}\tilde{\pi}^{j-1}, \tilde{v}\tilde{\pi}^{k+j-2}) = 0.
\end{aligned}$$

Ferner gilt

$$\begin{aligned}
f(w(\pi+1)^2, w) &= f(w(\pi+1)\pi, w(\pi+1)) = f((v+\lambda b_2)\pi, v+\lambda b_2) \\
&= f(v\pi + \lambda b_2 + \lambda b_1, v + \lambda b_2) = \tilde{f}(\tilde{v}\tilde{\pi}, \lambda\tilde{b_2}) + \tilde{f}(\lambda\tilde{b_2}, \tilde{v}) \\
&= \tilde{f}(\tilde{v}(\tilde{\pi}+1), \lambda\tilde{b_2}) = \tilde{f}(\tilde{v}\tilde{\pi}, \lambda\tilde{b_2}(\tilde{\pi}+1)) \\
&= \tilde{f}(\tilde{v}\tilde{\pi}, \lambda\tilde{b_1}) = 0.
\end{aligned}$$

Wegen $4t - 5 \geq 2t - 1$ folgt aus (1):

$$f(b_2, b_3) = f(b(\pi+1)^{2(t-1)}, b(\pi+1)^{2t-3}) = f(b(\pi+1)^{4t-5}, b\pi^{2t-3}) = 0,$$

also

$$\begin{aligned}
f(w(\pi+1), w) &= f(u(\pi+1) + \lambda b_2, u + \lambda b_3) = f(u(\pi+1), u) + f(u(\pi+1), \lambda b_3) + f(\lambda b_2, u) \\
&= f(u(\pi+1), u) + f(u\pi, \lambda b_2) + f(\lambda b_2, u) = f(u(\pi+1), u) + f(u(\pi+1), \lambda b_2) \\
&= f(u(\pi+1), u) + f(u, \lambda b_2(\pi+1)\pi^{-1}) = f(u(\pi+1), u) + \lambda f(u, b_1).
\end{aligned}$$

Wegen $b_1^\perp = (b(\pi+1)^{2t-1})^\perp = \langle a\rangle_\pi(\pi+1) \oplus \langle b\rangle_\pi$, gilt

$$f(u, b_1) = f(a + a', b(\pi+1)^{2t-1}) = f(a, b(\pi+1)^{2t-1}) \neq 0.$$

Wählt man $\lambda := f(u(\pi+1), u) f(u, b_1)^{-1}$, so hat w die gewünschten Eigenschaften. Analog findet man ein $\delta \in K$, so daß $e := y + \delta a(\pi+1)^{2t-3}$ einen totalisotropen π-Modul erzeugt. Offenbar ist $\operatorname{ann}_\pi(w) = (x+1)^{2t-1} = \operatorname{ann}_\pi(e)$. Wegen $w(\pi+1)^{2t-1} = a(\pi+1)^{2t-1}$ und $e(\pi+1)^{2t-1} = b(\pi+1)^{2t-1}$ gilt $\langle w(\pi+1)^{2t-1}\rangle_\pi \neq \langle e(\pi+1)^{2t-1}\rangle_\pi$ und daher bekanntlich $\langle w\rangle_\pi \cap \langle e\rangle_\pi = \{0\}$. Wir erhalten somit eine Zerlegung $V = \langle w\rangle_\pi \oplus \langle e\rangle_\pi$ der gewünschten Art und w, e haben die unter $(*)$ geforderte Gestalt. (Wähle $a'' := a' + \lambda b_3 \in \mathrm{B}(\pi)$ und $b'' := b' + \delta a(\pi+1)^{2t-3} \in \mathrm{B}(\pi)$. Dann gilt $w = a + a''$ und $e = b + b''$.) $\blacksquare$

Kapitel 2

Eine Kennzeichnung der Produkte von zwei unitären Involutionen

Wir betrachten folgendes Problem:

(P) Gibt es eine einfache algebraische Beschreibung der Produkte von zwei unitären Involutionen?

Wir listen zunächst in knapper Form Beispiele klassischer Gruppen auf, für die eine befriedigende algebraische Beschreibung der Produkte von zwei Involutionen vorliegt.

1. Allgemeine lineare Gruppen (D.Ž. Djoković [24], M.J. Wonenburger [79]):

   Ein $\pi \in \mathrm{GL}(V)$ ist genau dann ein Produkt von zwei Involutionen aus $\mathrm{GL}(V)$, wenn π ähnlich zu π^{-1} ist.

2. Orthogonale Gruppen (D.Ž. Djoković [23], E.W. Ellers und W. Nolte [29], R. Gow [38], M.J. Wonenburger [79]):

   Jede Isometrie einer orthogonalen Gruppe ist ein Produkt von zwei Involutionen.

3. Symplektische Gruppen.

   Charakteristik $= 2$ (E.W. Ellers und W. Nolte [29], R. Gow [38]):

   Jede Isometrie einer symplektischen Gruppe über einem Körper der Charakteristik 2 ist ein Produkt von zwei Involutionen.

   Charakteristik $\neq 2$ (K. Nielsen [56]):

   Seien f eine symplektische Form, $\mathrm{char}(K) \neq 2$ und $n := \dim V$. Dann ist $\pi \in \mathrm{Sp}(f)$ genau dann ein Produkt von zwei Involutionen, wenn es eine Darstellung

$$\mathcal{M}_{\mathcal{B}}(\pi) = \begin{bmatrix} P & 0 \\ 0 & (P^{-1})^t \end{bmatrix} \text{ und } \mathcal{M}_{\mathcal{B}}(f) = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$$

   gibt, wobei $P \in \mathrm{GL}_{n/2}(K)$ ähnlich zu P^{-1} ist ($\mathcal{B}$ eine Basis von V).

Ist nun f eine reguläre $^-$-hermitesche Form und $\pi \in \mathrm{U}(f)$ ein Produkt von zwei Involutionen $\rho, \sigma \in \mathrm{U}(f)$, so ist π, wie es für Produkte von zwei Involutionen in beliebigen Gruppen stets der Fall ist, konjugiert zu $\pi^{-1} = \pi^\rho = \pi^\sigma$. Dies ist also in Hinblick auf das Problem (P) stets eine notwendige Bedingung. Wie man sich aber am Beispiel einer unitären Transvektion über einem endlichen Körper der Charakteristik $\neq 2$ klarmachen kann, ist sie aber nicht hinreichend.
Unser Ansatz ist der folgende: Mit π ist auch jedes Element der Konjugiertenklasse $\Omega := \pi^{\mathrm{U}(f)}$ von π ein Produkt von zwei unitären Involutionen. Diese ist nach Satz 1.3.8 (bis auf einige Ausnahmen bei Körpercharakteristik 2) eindeutig durch die Äquivalenzklassen der f-hermiteschen Invarianten von π festgelegt. Das Problem lautet daher:

(P') Zu welchen Äquivalenzklassen gehören die f-hermiteschen Invarianten von π ?

Dieses Problem ist eng mit einem anderen verknüpft, zu dessen Formulierung wir bemerken, daß für ein $\iota \in K^*$ mit $\bar{\iota} = -\iota$ die Abbildung

$$s_f : V \times V \to F, s_f(a, b) := \iota(f(a, b) - f(b, a))$$

eine wohldefinierte reguläre symplektische Form auf dem F-Vektorraum V ist. Es ist $\mathrm{Sp}(s_f)$ von der Wahl von ι unabhängig und $\mathrm{U}(f) \leq \mathrm{Sp}(s_f)$ (cf. 2.1.2 unten).

(P") Zu welchen Äquivalenzklassen gehören die s_f-hermiteschen Invarianten von π ?

Bis auf oben angesprochene Ausnahmen bei Körpercharakteristik 2 lautet eine Antwort auf das Problem (P):
$\pi \in \mathrm{U}(f)$ ist genau dann ein Produkt von zwei unitären Involutionen, wenn π ähnlich zu π^{-1} ist, und alle s_f-hermiteschen Invarianten von π hyperbolische Formen sind (cf. 2.3.1 unten).

2.1 Symplektisierung und Symmetrisierung

Von nun an setzen wir $^- \neq 1_K$ voraus. Damit ist f eine reguläre $^-$-hermitesche Form. Außerdem sei $\iota \in K^*$ mit $\bar{\iota} = -\iota$ und im Fall $\mathrm{char}(K) = 2$ $\omega \in K^*$ mit $\bar{\omega} = \omega + 1$ fest gewählt. (Beachte, daß ι in dem Fixkörper F von $^-$ liegt, falls K die Charakteristik 2 hat.)

Bemerkung 2.1.1 *Jeder K-Vektorraum W ist auf natürliche Weise auch ein F-Vektorraum. Dieser sei mit W_F bezeichnet. Ist $\mathcal{B}$ eine K-Basis von W, so ist $\mathcal{B} \stackrel{\bullet}{\cup} \{\nu b | b \in \mathcal{B}\}$ für jedes $\nu \in K \backslash F$ eine F-Basis von W_F. Ist W endlich-dimensional, so gilt insbesondere $\dim W_F = 2 \dim W$. Ferner gehört jedes $\pi \in \mathrm{Hom}(W)$ auch zu $\mathrm{Hom}(W_F)$ und wir schreiben oft deutlichkeitshalber π_F, wenn π ausdrücklich als F-Endomorphismus aufgefaßt werden soll. Mit dieser Notation ergeben sich folgende Zusammenhänge:*

(i) $\det \pi_F = \det \pi \overline{\det \pi}$;

(ii) $\mathrm{char}(\pi_F) = \mathrm{char}(\pi)\overline{\mathrm{char}(\pi)}$;

(iii) $\mathrm{mip}(\pi_F) = \mathrm{lcm}(\mathrm{mip}(\pi), \overline{\mathrm{mip}(\pi)})$;

(iv) $\mathrm{ann}_{\pi_F}(v) = \mathrm{lcm}(\mathrm{ann}_\pi(v), \overline{\mathrm{ann}_\pi(v)})$ *für alle $v \in V$;*

(v) *Ein Polynom* $r' \in F[x]$ *ist genau dann ein Elementarteiler von* π_F, *wenn es einen Elementarteiler* $r \in K[x]$ *von* π *mit* $r' = \mathrm{lcm}(r, \bar{r})$ *gibt.*

(vi) *Ist* $v \in V$, *so gilt* $\langle v \rangle_\pi = \langle v \rangle_{\pi_F} + \langle \nu v \rangle_{\pi_F}$. *Ist* $\mathrm{ann}_\pi(v)$ *teilerfremd zu* $\overline{\mathrm{ann}_\pi(v)}$, *so ist* $\langle v \rangle_\pi = \langle v \rangle_{\pi_F}$. *Liegt* $\mathrm{ann}_\pi(v)$ *in* $F[x]$, *so gilt* $\langle v \rangle_\pi = \langle v \rangle_{\pi_F} \oplus_F \langle \nu v \rangle_{\pi_F}$.

(vii) *Seien* r *ein Elementarteiler von* π, R *eine* r*-Komponente und* $\bar{R}$ *eine* $\bar{r}$*-Kompnente, falls* $\bar{r}$ *ein Elementarteiler von* π *ist, bzw.* $\bar{R} = \{0\}$ *andernfalls. Im Fall* $r = \bar{r} \in F[x]$ *gelte* $R = \bar{R}$. *Für* $r' := \mathrm{lcm}(r, \bar{r})$ *ist dann* $R' := (R + \bar{R})_F$ *eine* r'*-Komponente. Die Vielfachheit des Elementarteilers* r' *von* π_F *ist die Summe der Vielfachheiten von* r *und* $\bar{r}$ *als Elementarteiler von* π. *Insbesondere hat* r' *eine gerade Vielfachheit, wenn* $r = \bar{r}$ *ist.* ■

Definition/Satz 2.1.2 (i) *Die Abbildung*

$$s_f := \iota(f - \bar{f}) : V_F \times V_F \to F, (a, b) \mapsto \iota(f(a, b) - f(b, a))$$

ist eine reguläre symplektische Form auf V_F *und heißt eine Symplektisierung von* f. *Weil es zu jedem* $\kappa \in K^*$ *mit* $\bar{\kappa} = -\kappa$ *ein* $\lambda \in F^*$ *mit* $\lambda\iota = \kappa$ *gibt, gilt* $h := \kappa(f - \bar{f}) = \lambda s_f$ *und damit* $\mathrm{Sp}(h) = \mathrm{Sp}(s_f)$. *In diesem Sinne kann man von* s_f *als* **der** *Symplektisierung von* f *sprechen.*

(ii) *Die Abbildung*

$$o_f := f + \bar{f} : V_F \times V_F \to F, (a, b) \mapsto f(a, b) + f(b, a)$$

ist eine reguläre symmetrische Form auf V_F *und soll Symmetrisierung von* f *genannt werden.*

(iii) *Ist* $\mathrm{char}(K) \neq 2$, *so gilt* $s_f = o_f \circ (\iota 1_V \times 1_V)$ $[o_f = s_f \circ (\iota^{-1} 1_V \times 1_V)]$ *und damit*

$$f = \iota^{-1} s_f + o_f = \iota^{-1} o_f \circ (\iota 1_V \times 1_V) + o_f = \iota^{-1} s_f + s_f \circ (\iota^{-1} 1_V \times 1_V).$$

Ist $\mathrm{char}(K) = 2$, *so gilt* $s_f = \iota o_f$ *und* $f = o_f \circ (1_V \times \omega 1_V) + \omega o_f$.

(iii) *Es gilt stets*

$$\mathrm{U}(f) = \mathrm{Sp}(s_f) \cap \mathrm{GL}_K(V) = \mathrm{O}(o_f) \cap \mathrm{GL}_K(V) \leq \mathrm{Sp}(s_f) \cap \mathrm{O}(o_f).$$

Im Fall $\mathrm{char}(K) \neq 2$ *ist* $\mathrm{U}(f) = \mathrm{Sp}(s_f) \cap \mathrm{O}(o_f)$.

(iv) *Für Teilmengen* U, W *von* V *mit* $K \cdot U \subseteq U$ *und* $g \in \{o_f, s_f\}$ *gilt* $U \perp_f W$ *genau dann, wenn* $U \perp_g W$. *Insbesondere ist ein* K*-Untervektorraum von* V *genau dann* f*-regulär, wenn er* s_f*-regulär (*o_f*-regulär) ist.* ■

Bemerkung 2.1.3 *Sei* $\pi \in \mathrm{U}(f)$ *und* r *ein* $^-$*-symmetrischer Elementarteiler von* π. *Seien weiterhin* R *eine reguläre* r*-Komponente und* $\tilde{R}$ *eine reguläre* $\bar{r}$*-Komponente von* π, *falls* $\bar{r}$ *ein Elementarteiler von* π *ist, bzw.* $\bar{R} = \{0\}$ *andernfalls. Der* π_F*-Modul* $R' := (R + \tilde{R})_F$ *ist dann eine* s_f*-reguläre (*o_f*-reguläre)* r'*-Komponente von* π_F.

Beweis. Nach 2.1.1 (vii) ist R' eine r'-Komponente von π_F. Nach 2.1.2 (iv) ist R' s_f-regulär (o_f-regulär). ■

Ist nun $\pi \in \mathrm{U}(f)$ ein Produkt von zwei unitären Involutionen ρ und σ, so sind ρ_F und σ_F Involutionen aus $\mathrm{Sp}(s_f)$, also ist π ähnlich zu π^{-1} und π_F ein Produkt von zwei s_f-symplektischen Involutionen.
Ein Ziel ist es, für $\mathrm{char}(K) \neq 2$ die Umkehrung dieser Aussage zu etablieren (cf. 2.3.5 unten).

2.2 Unitäre Darstellungen von Diedergruppen

Als eine triviale Folgerung aus 1.3.5 notieren wir zunächst das

Lemma 2.2.1 *Es seien die Voraussetzungen von 1.3.5 erfüllt und es gelte* $(V, A, B, f) = (W, C, D, g)$. *Ist dann* π *ein Produkt von zwei Involutionen* ρ, σ, *so sind* $\hat{\rho}, \hat{\sigma} \in \mathrm{U}(f)$ *Involutionen, und es gilt* $\hat{\pi} = \hat{\rho}\hat{\sigma}$. ■

Das nun folgende einfache aber nützliche Lemma charakterisiert im Fall $\mathrm{char}(K) \neq 2$ die Zweierprodukte π von Involutionen in $\mathrm{U}(f)$, für die V π-unzerlegbar ist.

Lemma 2.2.2 *Sei* $\pi \in \mathrm{U}(f)$ *und* V *sei* π*-zyklisch.*

(i) *Ist* $\mathrm{mip}(\pi)$ *symmetrisch und gibt es ein* $v \in V$ *mit* $V = \langle v \rangle_\pi$ *und* $f(v\pi^i, v\pi^j) = f(v\pi^j, v\pi^i)$ *für alle* $i, j \in \mathbb{N}_0$, *so ist* π *ein Produkt von zwei Involutionen aus* $\mathrm{U}(f)$.

(ii) *Ist* π *ein Produkt von zwei unitären Involutionen,* V π*-unzerlegbar und gilt [*$\mathrm{char}(K) \neq 2$ *oder* $\mathrm{mip}(\pi) \notin \{(x+1)^{2t}; t \in \mathbb{N}\}$*], so gibt es ein* $v \in V$ *mit* $V = \langle v \rangle_\pi$ *und* $f(v\pi^i, v\pi^j) = f(v\pi^j, v\pi^i) \in F$ *für alle* $i, j \in \mathbb{N}_0$.

Beweis. (i). Sei $n := \dim V$. Definiere $\rho, \sigma \in \mathrm{GL}(V)$ durch $v\pi^i\rho := v\pi^{n-i-1}$ und $v\pi^i\sigma := v\pi^{n-i}$ für $i \in \{0, \ldots, n-1\}$. Dann gilt $\pi = \rho\sigma$, $\rho^2 = 1$ und $v\pi^i\sigma^2 = v\pi^i$ für alle $i \in \{1, \ldots, n-1\}$. Weil $\mathrm{mip}(\pi) = \sum_i^n p_i x^i$, $p_n = 1$, symmetrisch ist, gilt auch $v\sigma^2 = v\pi^n\sigma = -v\sum_{i=0}^{n-1} p_i\pi^{n-i} - v + v = -v\pi^n\mathrm{mip}(\pi)(\pi^{-1}) + v = v$, also $\sigma^2 = 1$. Für $i, j \in \{0, \ldots, n-1\}$ gilt $f(v\pi^i\sigma, v\pi^j\sigma) = f(v\pi^{n-i}, v\pi^{n-j}) = f(v\pi^j, v\pi^i) = f(v\pi^i, v\pi^j)$, also $\sigma \in \mathrm{U}(f)$. Weil $\mathrm{U}(f)$ eine Gruppe ist, gehört auch $\rho = \pi\sigma$ zu $\mathrm{U}(f)$.

(ii). Seien $\rho, \sigma \in \mathrm{U}(f)$ Involutionen, für die $\pi = \rho\sigma$ gilt. Weil V π-unzerlegbar ist, ist $\mathrm{mip}(\pi) = p^i$ für ein normiertes, irreduzibles Polynom $p \in K[x]$ und ein $i \in \mathbb{N}$.
Annahme: $\mathrm{F}(\rho) + \mathrm{F}(\sigma) \neq V \neq \mathrm{F}(\rho) + \mathrm{B}(\rho)$. Dann gilt insbesondere $\mathrm{char}(K) = 2$, $\mathrm{B}(\rho) \subseteq \mathrm{F}(\rho)$ und $\mathrm{B}(\sigma) \subseteq \mathrm{F}(\sigma)$ und damit

$$\mathrm{B}(\pi) \subseteq \mathrm{B}(\rho) + \mathrm{B}(\sigma) \subsetneq V.$$

Dies impliziert $p = x + 1$. Nach Voraussetzung ist dann $i = \dim V$ ungerade. Wegen $\dim \mathrm{B}(\pi) = \dim V - 1$ folgt $\mathrm{B}(\pi) = \mathrm{B}(\rho) + \mathrm{B}(\sigma) = \mathrm{F}(\rho) + \mathrm{F}(\sigma)$ und damit $\mathrm{F}(\pi) = \mathrm{B}(\pi)^\perp = \mathrm{F}(\rho)^\perp \cap \mathrm{F}(\sigma)^\perp =$

$\mathrm{B}(\rho) \cap \mathrm{B}(\sigma)$. Insbesondere gilt $\dim \mathrm{B}(\rho) \cap \mathrm{B}(\sigma) = 1$. Es folgt :

$$\begin{aligned}
\dim V &= \dim(\mathrm{B}(\rho) + \mathrm{B}(\sigma)) + \dim \mathrm{F}(\pi) \\
&= \dim \mathrm{B}(\rho) + \dim \mathrm{B}(\sigma) - \dim \mathrm{B}(\rho) \cap \mathrm{B}(\sigma) + \dim \mathrm{F}(\pi) \\
&= \dim \mathrm{B}(\rho) + \dim \mathrm{B}(\sigma)
\end{aligned}$$

und

$$\begin{aligned}
\dim \mathrm{B}(\rho) &= \dim V - \dim \mathrm{F}(\rho) = \dim \mathrm{B}(\rho) + \dim \mathrm{B}(\sigma) - \dim \mathrm{F}(\rho) \\
&= \dim \mathrm{B}(\sigma) - (\dim \mathrm{F}(\rho) - \dim \mathrm{B}(\rho)) \geq \dim \mathrm{B}(\sigma)
\end{aligned}$$

und analog $\dim \mathrm{B}(\sigma) \geq \dim \mathrm{B}(\rho)$, also $\dim \mathrm{B}(\sigma) = \dim \mathrm{B}(\rho)$ und $\dim V = 2 \dim \mathrm{B}(\sigma)$ ist gerade, ein Widerspruch.

Es gibt daher ein $\eta \in \{\rho, \sigma\}$ und ein $v \in \mathrm{F}(\eta) \cup \mathrm{B}(\eta)$ mit $\mathrm{ann}_\pi(v) = p^i$. Dann gilt $V = \langle v \rangle_\pi$ und

$$\begin{aligned}
f(v\pi^j, v\pi^l) &= f(v\pi^j\eta, v\pi^l\eta) = f(v\eta\pi^{-j}, v\eta\pi^{-l}) \\
&= f(v\pi^{-j}, v\pi^{-l}) = f(v\pi^l, v\pi^j)
\end{aligned}$$

für alle $j, l \in \mathbb{N}_0$. ■

Korollar 2.2.3 *Seien $\pi \in \mathrm{U}(f)$ mit $\mathrm{mip}(\pi) = (x \pm 1)^t$ und V ein orthogonal unzerlegbarer π-Modul.*

(i) *Ist $\mathrm{char}(K) \neq 2$, so ist π genau dann ein Produkt von zwei unitären Involutionen, wenn t ungerade ist.*

(ii) *Ist $\mathrm{char}(K) = 2$, so ist π genau dann ein Produkt von zwei unitären Involutionen, wenn t gerade oder $= 1$ ist.*

Zum Beweis benötigen wir einige für sich interessante Tatsachen, welche in der folgenden Zwischenbemerkung festgehalten werden sollen.

Bemerkung 2.2.4 *Es seien die Voraussetzungen von 2.2.3 erfüllt.*

(i) *Ist $\mathrm{char}(K) \neq 2$, so ist V_F genau dann ein s_f-orthogonal (o_f-orthogonal) unzerlegbarer π_F-Modul, wenn t ungerade (gerade) ist.*

(ii) *Ist $\mathrm{char}(K) = 2$ und $v \in V$ mit $\mathrm{ann}_\pi(v) = (x+1)^t$, so gilt $f(v, v(\pi+1)^{t-1}) \in F^*$. Ist $t > 1$ ungerade, so gilt zusätzlich $f(v, v(\pi+1)^{t-2}) \notin F$.*

(iii) *Ist $\mathrm{char}(K) = 2$, so ist V_F ein s_f-orthogonal unzerlegbarer π_F-Modul, und es gibt genau dann ein $u \in V$ mit der Eigenschaft*

(∗) $\mathrm{ann}_\pi(u) = (x+1)^t$ *und* $\langle u \rangle_{\pi_F}$ *ist* s_f*-totalisotrop,*

wenn t gerade oder $= 1$ ist.

Beweis. Sei $p := \mathrm{mip}(\pi)$. Es ist π ähnlich zu π^{-1} und V eine reguläre p-Komponente. Nach 2.1.3 ist auch V_F eine reguläre p-Komponente. Aus $\dim V_F = 2\dim V$ folgt bereits, daß p als Elementarteiler von π_F die Vielfachheit 2 besitzt. Behauptung (i) folgt nun aus 1.5.3 (II) und (III). Sei $\mathrm{char}(K) = 2$ (ii). Wegen $\langle v(\pi+1)^{t-1}\rangle = \mathrm{F}(\pi) = \mathrm{B}(\pi)^{\perp}$ gilt

$$0 \neq \delta := f(v, v(\pi+1)^{t-1}) = f(v(\pi+1)^{t-1}\pi^{1-t}, v) = f(v(\pi+1)^{t-1}, v) \in F^*.$$

Seien $t > 1$ ungerade und $i := (t-1)/2 \in \mathbb{N}$. Man berechnet

$$f(v(\pi+1)^{2i-1}, v(\pi^{2i}+1)) = f(v(\pi+1)^{2i-1}, v(\pi^i+1)^2) = f(v(\pi+1)^{2i-1}, v(\pi+1)^2(\sum_{j=0}^{i-1}\pi^j)^2) = 0,$$

somit

$$\begin{aligned}
\delta &= f(v, v(\pi+1)^{2i}) = f(v, v(\pi+1)^{2i-1}\pi) + f(v, v(\pi+1)^{2i-1}) \\
&= f(v(\pi+1)^{2i-1}, v\pi^{2i}) + f(v, v(\pi+1)^{2i-1}) \\
&= f(v(\pi+1)^{2i-1}, v(\pi^{2i}+1)) + f(v(\pi+1)^{2i-1}, v) + f(v, v(\pi+1)^{2i-1}) \\
&= f(v(\pi+1)^{2i-1}, v) + f(v, v(\pi+1)^{2i-1}).
\end{aligned}$$

Also liegt $f(v(\pi+1)^{2i-1}, v)$ nicht in F.
(iii). Es gilt $V_F = \langle v\rangle_{\pi_F} \oplus \langle \omega v\rangle_{\pi_F}$ (cf. 2.1.1 (vi)). Aus (ii) folgt $s_f(v, v(\pi+1)^{t-1}) = 0 = s_f(\omega v, \omega v(\pi+1)^{t-1})$. und hieraus $v(\pi+1)^{t-1} \in s_f$-rad $\langle v\rangle_{\pi_F}$ und $\omega v(\pi+1)^{t-1} \in s_f$-rad $\langle \omega v\rangle_{\pi_F}$. Nach 1.5.4 ist V_f ein s_f-orthogonal unzerlegbarer π_F-Modul. Ist t gerade, so gibt es nach 1.5.5 ein $u \in V$ mit der Eigenschaft $(*)$. Ist $t = 1$, so ist $\langle v\rangle_{\pi_F}$ eindimensional und trivialerweise s_f-totalisotrop. Ist $t > 1$ ungerade, so kann es wegen der zweiten Aussage unter (ii) keinen Vektor u mit der Eigenschaft $(*)$ geben. ■

Wir kommen nun zum Beweis von 2.2.3.
Sei $p := \mathrm{mip}(\pi)$.
(i) $\Rightarrow$. Nach 2.2.2 gibt es ein $v \in V$ mit $V = \langle v\rangle_\pi$ und $f(v\pi^i, v\pi^j) = f(v\pi^j, v\pi^i) \in F$ für alle $i, j \in \mathbb{N}_0$. Seien $U := \langle v\rangle_{\pi_F}$, G die Gramsche Matrix von f und H die von $(o_f)_U$ bezüglich der Basis $(v, \ldots, v\pi^{t-1})$. Dann gilt $H = 2G$. Wegen $\mathrm{char}(K) \neq 2$ ist H invertierbar, also U ein von V_F verschiedener o_f-regulärer, o_f-orthogonal unzerlegbarer π_F-Modul. Nach 2.2.4 (i) ist t ungerade.
$\Leftarrow$. Nach 2.2.4 (i) ist V_f ein s_f-orthogonal unzerlegbarer π_F-Modul vom Typ II. Nach 1.5.3 (II) gibt es ein $v \in V$ mit $\mathrm{ann}_{\pi_F}(v) = p$, so daß $\langle v\rangle_{\pi_F}$ s_f-totalisotrop ist. Dies bedeutet $f(v\pi^i, v\pi^j) \in F$ für alle $i, j \in \mathbb{N}$. Nach 2.2.2 ist π ein Produkt von zwei unitären Involutionen.

(ii) $\Rightarrow$. Seien $t = 2i+1$, $i \in \mathbb{N}$. Nach 2.2.4 (ii) und 2.2.2 (ii) kann π kein Produkt von zwei unitären Involutionen sein.
$\Leftarrow$. Sei t gerade. Nach 2.2.4 (iii) gibt es ein ein Vektor $u \in V$ der die dortige Bedingung $(*)$ erfüllt, so daß die Behauptung wiederum mit 2.2.2 (i) (angewandt auf u) folgt. ■

Der nun folgende Satz zeigt, wie sich beliebige Zweierprodukte von unitären Involutionen in direkte orthogonale Summen von 'elementaren' Zweierprodukten unitärer Involutionen zerlegen lassen. Es handelt sich hierbei um das unitäre Analogon der Ergebnisse aus [48] von F. Knüppel und K. Nielsen und [56] (Satz 7.1) von K. Nielsen für orthogonale bzw. symplektische Gruppen über Körpern der Charakteristik $\neq 2$. Für eine allgemeine Klassifikation endlich-dimensionaler Darstellungen von Diedergruppen sei auf die Arbeiten von S.D. Berman und K. Buzaši [4], D.Ž. Djoković [25], V.M. Bondarenko [5] und C.M. Ringel [62] hingewiesen.

Satz 2.2.5 *Sei $\pi \in \mathrm{U}(f)$ ein Produkt von zwei unitären Involutionen ρ und σ. Es gelte* $\mathrm{char}(K) \neq 2$ *oder $x+1$ sei kein Teiler von* $\mathrm{mip}(\pi)$. *Dann gibt es eine orthogonale Zerlegung $V = \bigoplus_{l \in L} V_l$ in π-, ρ- und σ-invariante Unterräume V_l, so daß für jedes $l \in L$ $\;A := V_l$ einer der folgenden Bedingungen genügt :*

(i) *$A = U \oplus W$ ist ein orthogonal unzerlegbarer π-Modul vom Typ I mit totalisotropen, π-unzerlegbaren, ρ-invarianten π-Moduln U und W.*

(ii) *$A = U \oplus W$ ist ein orthogonal unzerlegbarer π-Modul vom Typ I mit totalisotropen π-unzerlegbaren π-Moduln U und $W = U\rho$.*

(iii) *$A = (U \oplus W) \bigoplus (Y \oplus Z)$, sowohl $U \oplus W$ als auch $Y \oplus Z$ ist ein orthogonal unzerlegbarer π-Modul vom Typ I mit totalisotropen π-unzerlegbaren π-Moduln U, W, $Y = U\rho$ und $Z = W\rho$.*

(iv) *$A = U \bigoplus W$, U und $W = U\rho$ sind orthogonal unzerlegbare π-Moduln vom Typ III und* $\mathrm{mip}(\pi_U)$ *ist nicht symmetrisch.*

(v) *$A = U \oplus W$, $U = U\rho$ und $W = W\rho$ sind π-unzerlegbare nichtreguläre π-Moduln mit* $\mathrm{mip}(\pi_U) = \mathrm{mip}(\pi_W) = (x \pm 1)^{2t}$ *für ein $t \in \mathbb{N}$.*

(vi) *A ist ein orthogonal unzerlegbarer π-Modul vom Typ III mit Minimalpolynom* $\mathrm{mip}(\pi_A) = p^t$ *für ein irreduzibles, symmetrisches $p \in F[x]$ und ein $t \in \mathbb{N}$. Ist $p = x \pm 1$, so ist t ungerade.*

Beweis. Weil π als Produkt von zwei Involutionen zu π^{-1} ähnlich ist, ist $\mathrm{mip}(\pi)$ sowohl symmetrisch als auch $^-$-symmetrisch. Demnach ist $r \in K[x]$ genau dann ein Teiler von $\mathrm{mip}(\pi)$, wenn r^*, $r^\times$ und $\bar{r}$ ein Teiler von $\mathrm{mip}(\pi)$ ist. Ist p ein irreduzibler Teiler von $\mathrm{mip}(\pi)$, so haben $p, p^*, p^\times, \bar{p}$ denselben Exponenten j in der Primfaktorzerlegung von $\mathrm{mip}(\pi)$ in $K[x]$. Setze $C := \ker p(\pi)^j$, $C^* := \ker p^*(\pi)^j$, $C^\times := \ker p^\times(\pi)^j$ und $\tilde{C} := \ker \bar{p}(\pi)^j$. Wegen $\pi^\rho = \pi^{-1}$ haben wir $C\rho = C^\times$ und $C^*\rho = \tilde{C}$. Weil $B := C + C^* + C^\times + \tilde{C}$ ein regulärer π-Modul ist, kann man o.B.d.A. $V = B$ annehmen. Offenbar genügt es zu zeigen, daß es einen regulären π-Modul A gibt, der eine der Bedingungen (i)-(vi) erfüllt, weil nämlich in diesem Fall $V = A \bigoplus A^\perp$ und $A^\perp = A^\perp\rho = A^\perp\pi$ gilt, so daß die Behauptung per Induktion über $\dim V$ folgt.

1.Fall: $p^* \neq p = p^\times$. Dann gilt $V = C \oplus C^*$, und $C = C^\times$ und $C^* = \tilde{C}$ sind totalisotrope, ρ- und σ-invariante Unterräume. Wegen $p \neq x-1$ gilt $C = \mathrm{B}(\pi_C) = \mathrm{B}(\rho_C) + \mathrm{B}(\sigma_C)$ und $C^* = \mathrm{B}(\pi_{C^*}) = \mathrm{B}(\rho_{C^*}) + \mathrm{B}(\sigma_{C^*})$. Es gibt demnach ein $\eta \in \{\rho, \sigma\}$ und ein $a \in \mathrm{B}(\eta_C)$ mit $ap(\pi)^{j-1} \neq 0$. Weil V regulär ist, gibt es ein $\kappa \in \{\rho, \sigma\}$ und ein $b \in \mathrm{B}(\kappa_{C^*})$ mit $\langle ap(\pi)^{j-1}\rangle_\pi \not\leq \langle b\rangle_\pi^\perp$. Insbesondere gilt $\mathrm{ann}_\pi(b) = p^{*j}$. Es sind $\langle a\rangle_\pi$ und $\langle b\rangle_\pi$ totalisotrop und damit insbesondere nicht regulär und ρ- und σ-invariant. Nach 1.4.2 gilt $\langle a\rangle_\pi \cap \langle b\rangle_\pi = \{0\}$ und $A := \langle a\rangle_\pi \oplus \langle b\rangle_\pi$ ist ein regulärer, orthogonal unzerlegbarer π-Modul. Folglich erfüllt A die Bedingung (i).

2.Fall: $p^* \neq p = \bar{p}$. Dann gilt $V = C \oplus C^*$, und $C = C^*\rho$ ist totalisotrop. Annahme: Für alle $a \in C$ ist $f(ap(\pi)^{j-1}, a\rho) = 0$. Seien $a, b \in C$ und $\lambda \in K^*$ mit $\bar{\lambda} \neq -\lambda$. Dann gilt

$$0 = f((\lambda a + b)p(\pi)^{j-1}, (\lambda a + b)\rho) = f(\lambda ap(\pi)^{j-1}, b\rho) + f(bp(\pi)^{j-1}, \lambda a\rho).$$

Wegen $p = \bar{p}$ folgt

$$\begin{aligned}\lambda f(ap(\pi)^{j-1}, b\rho) &= -f(bp(\pi)^{j-1}, \lambda a\rho) = -f(b, \lambda a\rho p(\pi^{-1})^{j-1}) \\ &= -f(b\rho, \lambda ap(\pi)^{j-1}) = -\bar{\lambda}\overline{f(ap(\pi)^{j-1}, b\rho)}.\end{aligned}$$

Dies impliziert $f(ap(\pi)^{j-1}, b\rho) = 0$, also $Cp(\pi)^{j-1} \leq (C\rho)^\perp = C^{*\perp}$, ein Widerspruch.
Es gibt also ein $a \in C$ mit $\langle ap(\pi)^{j-1})\rangle_\pi \not\leq \langle a\rho\rangle_\pi^\perp$. Weil dann insbesondere $\mathrm{ann}_\pi(a) = p^j = \mathrm{ann}_\pi(a\rho)^*$ gilt, und weil $\langle a\rangle_\pi$ und $\langle a\rho\rangle_\pi$ totalisotrop sind, folgt aus 1.4.2, daß $\langle a\rangle_\pi \cap \langle a\rho\rangle_\pi = \{0\}$ und $A := \langle a\rangle_\pi \oplus \langle a\rho\rangle_\pi$ ein regulärer, orthogonal unzerlegbarer π-Modul ist. Er erfüllt also die Bedingung (ii).

3.Fall: $p^* \neq p \neq p^\times \neq p^*$. Dann gilt $V = (C \oplus C^*) \bigoplus\!\!\!\!\!\!\perp\; (C^\times \oplus \tilde{C})$ und $C, C^*, C^\times$ und $\tilde{C}$ sind totalisotrop. Wähle $a \in C$, $b \in C^*$ mit $\langle ap(\pi^{i-1})\rangle_\pi \not\leq \langle b\rangle_\pi^\perp$. Dann gilt auch $\langle a\rho p(\pi)^{i-1}\rangle_\pi \not\leq \langle b\rho\rangle_\pi^\perp$. Weil dann $p^j = \mathrm{ann}_\pi(a) = \mathrm{ann}_\pi(a\rho)^\times = \mathrm{ann}_\pi(b)^* = \overline{\mathrm{ann}_\pi(b\rho)}$ ist und $U := \langle a\rangle_\pi$, $W := \langle b\rangle_\pi$, $Y := \langle a\rho\rangle_\pi$, $Z := \langle b\rho\rangle_\pi$ totalisotrop sind, erhält man aus 1.4.2, daß $U \cap W = \{0\} = Y \cap Z$ ist, und $U \oplus W$, $Y \oplus Z$ reguläre, orthogonal unzerlegbare π-Moduln sind. Folglich erfüllt $A := (U \oplus W) \bigoplus\!\!\!\!\!\!\perp\; (Y \oplus Z)$ die Bedingung (iii).

4.Fall: $p^* = p \neq p^\times$. Dann gilt $V = C \bigoplus\!\!\!\!\!\!\perp\; C^\times$. Wähle $a \in C$ derart, daß $\langle a\rangle_\pi$ ein regulärer π-Modul ist. Dann ist auch $\langle a\rho\rangle_\pi \leq C^\times$ regulär. Also erfüllt $A := \langle a\rangle_\pi \bigoplus\!\!\!\!\!\!\perp\; \langle a\rho\rangle_\pi$ die Bedingung(iv).

5.Fall: $p^* = p = p^\times$. Dann gilt $V = C = C^* = C^\times = \tilde{C}$. Wegen $\mathrm{char}(K) \neq 2$ oder $p \neq x + 1$ gilt $V = \mathrm{F}(\rho) + \mathrm{B}(\rho) + \mathrm{F}(\sigma) + \mathrm{B}(\sigma)$. Es gibt demnach ein $\eta \in \{\rho, \sigma\}$ und ein $a \in \mathrm{B}(\eta) \cup \mathrm{F}(\eta)$ mit $ap(\pi)^{j-1} \neq 0$. Ist der π-Modul $\langle a\rangle_\pi$ regulär, so muß im Fall $\mathrm{char}(K) = 2$ und $p = x \pm 1$ j nach 2.2.3 (i) ungerade sein, womit (vi) zutreffen würde. Man kann daher o.B.d.A. annehmen :

(1) $\langle c\rangle_\pi$ ist für kein $c \in \mathrm{B}(\rho) \cup \mathrm{F}(\rho) \cup \mathrm{B}(\sigma) \cup \mathrm{F}(\sigma)$ mit $\mathrm{ann}_\pi(c) = p^j$ regulär.

Weil V regulär ist, gibt es ein $\kappa \in \{\rho, \sigma\}$ und ein $b \in \mathrm{B}(\kappa) \cup \mathrm{F}(\kappa)$ mit $\langle ap(\pi)^{j-1}\rangle_\pi \not\leq \langle b\rangle_\pi^\perp$. Weil dann auch $\mathrm{ann}_\pi(b) = p^j$ folgt und weil $\langle a\rangle_\pi$ und $\langle b\rangle_\pi$ nach (1) nicht regulär sind, gilt nach 1.4.2 $\langle a\rangle_\pi \cap \langle b\rangle_\pi = \{0\}$ und $A := \langle a\rangle_\pi \oplus \langle b\rangle_\pi$ ist ein regulärer ρ-invarianter π-Modul und wir können $V = A$ annehmen. Falls $p = x \pm 1$ und j gerade ist, erfüllt er die Bedingung (v), so daß man weiterhin $p \neq x \pm 1$ oder j ungerade annehmen kann. Wir unterscheiden diese beiden Fälle.

5.1. $p = x \pm 1$. Nach Voraussetzung ist dann $\mathrm{char}(K) \neq 2$. Weil j ungerade ist, gibt es ein

$c \in V$ mit $\mathrm{ann}_\pi(c) = p^j$, so daß $\langle c\rangle_\pi$ regulär ist (cf. 1.5.3). Nach 2.2.3 (i) und 2.2.2 (ii) kann man c so wählen, daß

(2) $f(c\pi^k, cp(\pi)^{j-1}) \in F^*$ für ein $k \in \mathbb{Z}$

gilt. Wegen $V = \mathrm{F}(\rho) \bigcirc\!\!\!\!\perp \mathrm{F}_{-1}(\rho)$, findet man $y \in \mathrm{F}(\rho)$ und $z \in \mathrm{F}_{-1}(\rho)$ so, daß $c = y + z$ ist. Wegen (1) gilt dann $\langle yp(\pi)^{j-1}\rangle_\pi \leq \mathrm{rad}\ \langle y\rangle_\pi$ und $\langle zp(\pi)^{j-1}\rangle_\pi \leq \mathrm{rad}\ \langle z\rangle_\pi$. Wegen $\mathrm{char}(K) \neq 2$ folgt nun ein Widerspruch zu (2):

$$\begin{aligned}
f(c\pi^k, cp(\pi)^{j-1}) &= f(y\pi^k, zp(\pi)^{j-1}) + f(z\pi^k, yp(\pi)^{j-1}) \\
&= f(y\pi^k, zp(\pi)^{j-1}) + f(z\pi^k\rho, yp(\pi)^{j-1}\rho) \\
&= f(y\pi^k, zp(\pi)^{j-1}) + f(z\rho\pi^{-k}, y\rho p(\pi^{-1})^{j-1}) \\
&= f(y\pi^k, zp(\pi)^{j-1}) - f(z\pi^{-k}, yp(\pi^{-1})^{j-1}) \\
&= f(y\pi^k, zp(\pi)^{j-1}) - f(zp(\pi)^{j-1}, y\pi^k) \\
&= f(y\pi^k, zp(\pi)^{j-1}) - \overline{f(y\pi^k, zp(\pi)^{j-1})} \notin F^*.
\end{aligned}$$

5.2. $p \neq x \pm 1$. Weil p symmetrisch ist, ist dann $p(0) = 1$ und $\deg(p) = 2l$ gerade, $l \in \mathbb{N}$. Setze $\psi := \pi^{l(1-j)}p(\pi)^{j-1}$ (vgl. 1.3.10). Dann gilt

(3) $\pi^{l(j-1)}p(\pi^{-1})^{j-1} = \pi^{l(j-1)}\pi^{-2l(j-1)}p^\times(\pi)^{j-1} = \psi$

Für $\kappa \in \{\rho, \sigma\}$ ergibt sich hieraus

(4) $\psi\kappa = \kappa\psi$.

Es ist

$$g := f \circ (\psi \times 1_V) : V \times V \to K, (u, v) \mapsto f(u\psi, v)$$

eine $^-$-Sesquilinearform, die wegen (3) $^-$-symmetrisch ist, und das Radikal $R := Vp(\pi)$ besitzt (vgl. 1.3.14). Für $\kappa \in \{\rho, \sigma, \pi\}$ ist $R\kappa = R$, und damit die Abbildung

$$\tilde{\kappa} : V/R \to V/R, v + R \mapsto v\kappa + R$$

wohldefiniert und eine Isometrie der von g auf V/R induzierten regulären $^-$-hermiteschen Form

$$\tilde{g} : V/R \times V/R \to K, (u + R, v + R) \mapsto g(u, v)$$

(cf. (4)). Es ist $\mathrm{mip}(\tilde{\pi}) = p \neq x \pm 1$. Also ist $\tilde{\pi} = \tilde{\rho}\tilde{\sigma}$ insbesondere keine Involution und damit $\tilde{\rho} \neq \pm 1_{V/R}$. Man findet daher ein $v \in V$ mit $\tilde{g}(v + R, (v + R)(\tilde{\rho} + 1))$ [Dies ist möglich, denn im Fall $\mathrm{char}(K) \neq 2$ ist $\mathrm{F}(\tilde{\rho}) \neq \{0\}$ $\tilde{g}$-regulär, enthält also einen $\tilde{g}$-anisotropen Vektor $v + R$. Für $\mathrm{char}(K) = 2$ folgt dies unmittelbar, indem man zum Beispiel eine Normalform von $\tilde{\rho}$ betrachtet (cf. 1.5.3 (III)).] Wegen $V = \mathrm{B}(\pi) = B(\rho) \oplus \mathrm{B}(\sigma) = \mathrm{F}_{-1}(\rho) \oplus \mathrm{F}_{-1}(\sigma)$, gibt es $u \in \mathrm{F}_{-1}(\rho)$ und

$w \in \mathrm{F}_{-1}(\sigma)$ mit $v = u + w$. Man berechnet nun:

$$\begin{aligned} 0 &\neq \tilde{g}(v+R,(v+R)(\tilde{\rho}+1) = g(v, v(\rho+1)) \\ &= g(u, w(\rho+1)) + g(w, w(\rho+1)) = g(w, w(\rho+1)) \\ &= -g(w, w\pi) + g(w,w) = g(w, w(1-\pi)) \\ &= f(w\pi^{l(1-j)}p(\pi)^{j-1}, w(1-\pi)). \end{aligned}$$

Hieraus folgt $\langle wp(\pi)^{j-1}\rangle_\pi \not\leq \operatorname{rad}\langle w\rangle_\pi^\perp$ und $\operatorname{ann}_\pi(w) = p^j$. Damit ist $\langle w\rangle_\pi$ regulär, ein Widerspruch zu (1). ■

Korollar 2.2.6 *Sei* $\operatorname{char}(K) \neq 2$ *und* π *ein Produkt von zwei unitären Involutionen; dann hat jeder Elementarteiler der Form* $(x+1)^{2t}$, $t \in \mathbb{N}$, *von* π *eine gerade Vielfachheit.* ■

Ist π ähnlich zu π^{-1} und K ein endlicher Körper mit $\operatorname{char}(K) \neq 2$, so wird sich herausstellen, daß auch die Umkehrung von 2.2.6 gilt (cf. 2.3.6 unten).

2.3 Der Charakterisierungssatz

Wir kommen nun zu der eingangs motivierten Kennzeichnung der Produkte von zwei unitären Involutionen.

Satz 2.3.1 (Charakterisierungssatz) *Sei* $\pi \in \mathrm{U}(f)$. *Es gelte* $\operatorname{char}(K) \neq 2$, *oder* $x+1$ *sei kein Teiler von* $\operatorname{mip}(\pi)$. *Folgende Aussagen sind äquivalent :*

(i) *π ist ein Produkt von zwei unitären Involutionen.*

(ii) *π ist ähnlich zu π^{-1}, und für jeden irreduziblen, $^-$-symmetrischen Teiler p von* $\operatorname{mip}(\pi)$ *besitzt* $E := \ker p(\pi)^\infty + \ker p^\times(\pi)^\infty$ *eine Zerlegung* $E = \bigoplus_{j\in J}(\langle u_j\rangle_\pi \oplus \langle w_j\rangle_\pi) \bigoplus_{l\in L}\langle v_l\rangle_\pi$ *mit folgenden Eigenschaften:*

   (a) *$\langle u_j\rangle_\pi, \langle w_j\rangle_\pi$ sind totalisotrop und es gilt* $\operatorname{ann}_\pi(u_j) = \operatorname{lcm}(p, p^\times)^{k_j} = \operatorname{ann}_\pi(w_j)$ *für ein* $k_j \in \mathbb{N}$.

   (b) *$f(v_l\pi^a, v_l\pi^b) = f(v_l\pi^b, v_l\pi^a) \in F$ für alle $a, b \in \mathbb{N}_0$ und* $\operatorname{ann}_\pi(v_l) = \operatorname{lcm}(p, p^\times)^{k_l}$ *für ein* $k_l \in \mathbb{N}$.

(iii) *Es gibt eine Zerlegung $V = \bigoplus_{j\in J}(\langle u_j\rangle_\pi \oplus \langle w_j\rangle_\pi) \bigoplus_{l\in L}\langle v_l\rangle_\pi$ mit folgenden Eigenschaften:*

   (a) *$\langle u_j\rangle_\pi, \langle w_j\rangle_\pi$ sind totalisotrop und es gilt* $\operatorname{ann}_\pi(u_j) = \operatorname{lcm}(r, r^\times) = \operatorname{ann}_\pi(w_j)^*$ *für einen Elementarteiler r von π.*

   (b) *$f(v_l\pi^a, v_l\pi^b) = f(v_l\pi^b, v_l\pi^a) \in F$ für alle $a, b \in \mathbb{N}_0$ und* $\operatorname{ann}_\pi(v_l) = \operatorname{lcm}(r, r^\times)$ *für einen Elementarteiler r von π.*

(iv) *Es gibt eine Basis $\mathcal{B}$ von V derart, daß*

$$\mathcal{M}_{\mathcal{B}}(\pi) = \begin{bmatrix} A & & \\ & \overline{A^{-1}}^t & \\ & & B \end{bmatrix}, \ \mathcal{M}_{\mathcal{B}}(f) = \begin{bmatrix} 0 & I & \\ I & 0 & \\ & & L \end{bmatrix}$$

gilt, wobei A ähnlich zu A^{-1} ist und $B, L \in F^{j\times j}$ für ein $j \in \mathbb{N}_0$.

(v) *π ist ähnlich zu π^{-1} und alle s_f-hermiteschen Invarianten von π sind hyperbolische Formen.*

Beweis. (i) $\Rightarrow$ (ii). Seien $\rho, \sigma \in \mathrm{U}(f)$ Involutionen, für die $\pi = \rho\sigma$ gilt. Als Produkt von zwei Involutionen ist π ähnlich zu π^{-1}. Seien p ein irreduzibler, $^{-}$-symmetrischer Teiler von $\mathrm{mip}(\pi)$, $p' := \mathrm{lcm}(p, p^{\times})$ und $E := \ker p'(\pi)^{\infty}$. Weil E ein regulärer ρ- und σ-invarianter π-Modul ist, gibt es eine orthogonale Zerlegung $V = \bigoplus_{l\in L} V_l$ in π-, ρ- und σ-invariante Unterräume V_l, so daß für jedes $l \in L$ der Raum V_l einer der Bedingungen (iv)-(vi) aus 2.2.5 genügt. Seien $l \in L$ und $A := V_l$.
1.Fall: $p \neq p^{\times}$. Dann hat A die Eigenschaft 2.2.5 (iv). Es gibt demnach ein $a \in A$, so daß $\mathrm{ann}_\pi(a) = p^k$ für ein $k \in \mathbb{N}$ und $A = \langle a\rangle_\pi \bigoplus \langle a\rho\rangle_\pi$ gilt. Für $w := a + a\rho$ ist dann $\mathrm{ann}_\pi(w) = pp^{\times}$ und $A = \langle w\rangle_\pi$. Wegen $w \in F(\rho)$ gilt

$$f(w\pi^j, w\pi^k) = f(w\pi^j\rho, w\pi^k\rho) = f(w\rho\pi^{-j}, w\rho\pi^{-k}) = f(w\pi^k, w\pi^j) \in F$$

für alle $j, k \in \mathbb{N}$. Folglich erfüllt A die Bedingung (b) aus (ii).

2.Fall: $p = p^{\times}$. Dann hat A entweder die Eigenschaft (v) oder (vi) aus 2.2.5. Falls A die Eigenschaft (vi) aus 2.2.5 besitzt, so erfüllt A nach 2.2.2 (ii) die Bedingung (b) aus (ii). Falls A die Eigenschaft (v) aus 2.2.5 besitzt, so gibt es nach 1.4.3 $a, b \in A$, so daß $\langle a\rangle_\pi$ und $\langle b\rangle_\pi$ totalisotrop sind und $A = \langle a\rangle_\pi \oplus \langle b\rangle_\pi$ gilt. Dabei ist $\mathrm{ann}_\pi(a) = \mathrm{ann}_\pi(b) = p^k$ für ein geeignetes $k \in \mathbb{N}$. Folglich erfüllt A die Bedingung (a) aus (ii).

(ii) $\Rightarrow$ (iii). Seien T die Menge der normierten Primteiler von $\mathrm{mip}(\pi)$ und $S := \{s \in T; s^* = s\}$ die Teilmenge der $^{-}$-symmetrischen. Sei $R \subseteq T\backslash S$ derart, daß $R^* := \{r^*; r \in R\} = T\backslash(R \cup S)$ ist. Dann gilt $T = R \dot\cup R^* \dot\cup S$ und

$$V = \bigoplus_{r\in R}(\ker r(\pi)^{\infty} \oplus \ker r^*(\pi)^{\infty}) \bigoplus_{s\in S} \ker s(\pi)^{\infty}.$$

Weil π ähnlich zu π^{-1} ist, kann man o.B.d.A. annehmen, daß

$$V = \ker r(\pi)^{\infty} + \ker r^*(\pi)^{\infty} + \ker r^{\times}(\pi)^{\infty} + \ker \bar{r}(\pi)^{\infty}$$

für ein $r \in T$ gilt. Falls $r = r^*$ ist, folgt die Behauptung sofort aus (ii), so daß man $r \neq r^*$ annehmen kann.

Fall A: $r^* \neq r^{\times} \neq r$. Dann gilt $V = \bigoplus_{j\in J}(\langle a_j\rangle_\pi \oplus \langle b_j\rangle_\pi) \bigoplus_{l\in L}(\langle c_l\rangle_\pi \oplus \langle d_l\rangle_\pi)$ für totalisotrope π-Moduln $\langle a_j\rangle_\pi, \langle b_j\rangle_\pi, \langle c_l\rangle_\pi, \langle d_l\rangle_\pi$ mit $\mathrm{ann}_\pi(a_j) = \mathrm{ann}_\pi(b_j)^*, \mathrm{ann}_\pi(c_l)^{\times} = \overline{\mathrm{ann}_\pi(d_l)} \in \{r^k; k \in \mathbb{N}\}$. Weil π ähnlich zu π^{-1} ist, kann man $J = L$ und $\mathrm{ann}_\pi(a_j) = \mathrm{ann}_\pi(b_j)^* = \mathrm{ann}_\pi(c_j)^{\times} = \overline{\mathrm{ann}_\pi(d_j)}$ für alle $j \in J$ annehmen. Setze $u_j := a_j + c_j$ und $w_j := b_j + d_j$. Dann haben u_j und w_j die in (iii) (a) geforderten Eigenschaften.

Fall B: $r^* \neq r^{\times} = r$. Dann gilt $V = \bigoplus_{j\in J}(\langle u_j\rangle_\pi \oplus \langle w_j\rangle_\pi)$ für totalisotrope π-Moduln $\langle u_j\rangle_\pi, \langle w_j\rangle_\pi$ mit $\mathrm{ann}_\pi(u_j) = \mathrm{ann}_\pi(w_j)^* \in \{r^k; k \in \mathbb{N}\}$, also genügen die u_j und w_j der Bedingung (a) aus (iii).

Fall C: $r^* = r^\times$. Dann gilt $V = \bigoplus_{j\in J}(\langle u_j\rangle_\pi \oplus \langle w_j\rangle_\pi)$ für totalisotrope π-Moduln $\langle u_j\rangle_\pi, \langle w_j\rangle_\pi$ mit $\mathrm{ann}_\pi(u_j) = \mathrm{ann}_\pi(w_j)^* = \mathrm{ann}_\pi(w_j)^\times \in \{r^k; k \in \mathbb{N}\}$. Man kann daher $|J| = 1$ annehmen und die Indizies in obiger Notation weglassen. Wegen $r = \bar{r}, r^* = r^\times \in F[x]$ gilt $\mathrm{ann}_{\pi_F}(u) = r^k = \mathrm{ann}_{\pi_F}(w)^\times$ für ein $k \in \mathbb{N}$ und $V_F = \langle u\rangle_{\pi_F} \oplus \langle \nu u\rangle_{\pi_F} \oplus \langle w\rangle_{\pi_F} \oplus \langle \nu w\rangle_{\pi_F}$ für ein $\nu \in K\backslash F$ (cf. 2.1.1 (vi)). Mit dem Normalformensatz 1.5.3 (I) und dem Satz von Krull-Remak-Schmidt folgt $V_F = (\langle a\rangle_{\pi_F} \oplus \langle b\rangle_{\pi_F}) \bigoplus_{s_f} (\langle c\rangle_{\pi_F} \oplus \langle d\rangle_{\pi_F})$ für s_f-totalisotrope π_F-Moduln $\langle a\rangle_{\pi_F}, \langle b\rangle_{\pi_F}, \langle c\rangle_{\pi_F}, \langle d\rangle_{\pi_F}$ mit $r^k = \mathrm{ann}_{\pi_F}(a) = \mathrm{ann}_\pi(a) = \mathrm{ann}_{\pi_F}(c) = \mathrm{ann}_\pi(c)$ und $r^{\times k} = \mathrm{ann}_{\pi_F}(b) = \mathrm{ann}_\pi(b) = \mathrm{ann}_{\pi_F}(d) = \mathrm{ann}_\pi(d)$ (cf. 2.1.1 (iii)). Setze $v := a + d$. Dann gilt $\mathrm{ann}_\pi(v) = (rr^*)^k$, i.e. $V = \langle v\rangle_\pi$, und $f(v\pi^i, v\pi^j) = f(v\pi^j, v\pi^i) \in F$ für alle $i, j \in \mathbb{N}_0$.
Die Implikation (iii) $\Rightarrow$ (iv) ist trivial.
(iv) $\Rightarrow$ (v). Sei $V = (U \oplus W) \bigoplus Z$ eine Zerlegung von V in π-Moduln U, W, Z derart, daß U, W totalisotrop sind, $\pi_{U\oplus W}$ ähnlich zu $\pi^{-1}_{U\oplus W}$ ist, und es eine Basis $\mathcal{Z} = (z_1, \ldots, z_n)$ von Z gibt, so daß alle Einträge von $\mathcal{M}_\mathcal{Z}(\pi_Z) = B$ und $\mathcal{M}_\mathcal{Z}(f_Z) = L$ aus F sind. Wegen $L = BL\bar{B}^t = BLB^t$ ist auch B ähnlich zu B^{-1}, so daß π ähnlich zu π^{-1} ist. Setze $\phi := \pi_F$. Sei $\nu \in K\backslash F$. Dann sind

$$R := U_F \oplus \langle z_1, \ldots, z_n\rangle_\phi \text{ und } S := W_F \oplus \langle \nu z_1, \ldots, \nu z_n\rangle_\phi$$

s_f-totalisotrope ϕ-Moduln, für die $V_F = R \oplus S$ gilt. Seien p ein in $F[x]$ irreduzibler, symmetrischer Teiler von $\mathrm{mip}(\phi)$. Es ist $E := \ker p(\phi)^\infty = \ker p(\phi_R)^\infty \oplus \ker p(\phi_S)^\infty$ ein s_f-regulärer ϕ-Modul mit s_f-totalisotropen ϕ-Untermoduln $C := \ker p(\phi_R)^\infty$ und $D := \ker p(\phi_S)^\infty$. Seien $I := \mathrm{I}(\phi, p)$, $i := \max I$, $c \in C$ mit $\mathrm{ann}_\phi(c) = p^i$ und $d \in D\backslash cp^{i-1}(\phi)^\perp$. Weil hieraus insbesondere $\mathrm{ann}_\phi(d) = p^i$ folgt, gilt nach 1.4.2 $\langle c\rangle_\phi \cap \langle d\rangle_\phi = \{0\}$ und $\langle c\rangle_\phi \oplus \langle d\rangle_\phi$ ist ein s_f-regulärer ϕ-Modul. Weil dann $E = (\langle c\rangle_\phi \oplus \langle d\rangle_\phi) \bigoplus_{s_f} (\langle d\rangle_\phi^\perp \cap C) \oplus (\langle c\rangle_\phi^\perp \cap D)$ gilt und $(\langle d\rangle_\phi^\perp \cap C) \oplus (\langle c\rangle_\phi^\perp \cap D)$ ein s_f-regulärer ϕ-Modul mit s_f-totalisotropen ϕ-Untermoduln $\langle d\rangle_\phi^\perp \cap C$, $\langle c\rangle_\phi^\perp \cap D$ ist, erhält man per Induktion eine s_f-orthogonale p-Komponentenzerlegung $(U_l)_{l\in I}$ von E derart, daß für jedes $l \in I$ $U_l = \bigoplus_{j\in J} \langle c_j\rangle_\phi \oplus \langle d_j\rangle_\phi$ für s_f-totalisotrope ϕ-Moduln $\langle c_j\rangle_\phi, \langle d_j\rangle_\phi$ gilt. Nach 1.4.4 ist U_l dann ein $\mathrm{H}(\phi, U_l)$-hyperbolischer Raum, also $\mathrm{H}(\phi, p^l)$ eine hyperbolische Form.

(v) $\Rightarrow$ (ii). Seien $p \in K[x]$ ein irreduzibler, $^-$-symmetrischer Teiler von $\mathrm{mip}(\pi)$ und $i \in \mathbb{N}$ derart, daß $r = p^i$ ein Elementarteiler von π ist. Seien R eine reguläre r-Komponente von π und $R^\times$ eine reguläre $r^\times$-Komponente von π. Im Fall $r = r^\times$ gelte $R = R^\times$. Wir führen nun folgende Abkürzungen ein :

$$\begin{array}{lllllllll}
S & := & Rp(\pi), & T & := & R/S, & H & := & \mathrm{H}(\pi, R),\\
S^\times & := & R^\times p^\times(\pi), & T^\times & := & R^\times/S^\times, & H^\times & := & \mathrm{H}(\pi, R^\times),\\
E & := & R + R^\times & p' & := & \mathrm{lcm}(p, p^\times) \in F[x], & r' & := & \mathrm{lcm}(r, r^\times) = p'^i,\\
R' & := & E_F, & S' & := & R'p'(\pi_F), & T' & := & R'/S'.
\end{array}$$

Nach 2.1.3 ist R' eine s_f-reguläre r'-Komponente von π_F. Sei $H' := \mathrm{H}(\pi_F, R')$ die zu R' gehörende s_f-hermitesche Invariante von π_F. Nach Voraussetzung (v) ist T' ein H'-hyperbolischer Raum.
Sei $D \leq E$ ein regulärer π-Modul derart, daß es eine Zerlegung

$$D = \bigoplus_{j\in J} (\langle u_j\rangle_\pi \oplus \langle w_j\rangle_\pi) \bigoplus_{l\in L} \langle v_l\rangle_\pi$$

mit folgenden Eigenschaften gibt:

(a) $\langle u_j\rangle_\pi, \langle w_j\rangle_\pi$ sind totalisotrop und es gilt $\mathrm{ann}_\pi(u_j) = \mathrm{ann}_\pi(w_j) \in \{r, r^\times\}$.

(b) $f(v_l\pi^a, v_l\pi^b) = f(v_l\pi^b, v_l\pi^a) \in F$ für alle $a, b \in \mathbb{N}_0$ und $\mathrm{ann}_\pi(v_l) = r'$.

Sei D maximal bezüglich der oben angegebenen Eigenschaften gewählt. Sei $M := D^\perp \cap E$. Dann ist M ein regulärer π-Modul, und es gilt $E = D \operp M$. Mithin sind D_F und M_F s_f-reguläre π_F-Moduln und es gilt $R' = E_F = D_F \operp_{s_f} M_F$.

Annahme: $M \neq \{0\}$. Nach dem Satz von Krull-Remak-Schmidt gilt dann $\mathrm{mip}((\pi_F)_{M_F}) = r'$, also $M_F + S'/S' \neq \{0\}$. Wähle $\nu \in K \backslash F$ und setze

$$Y := (\operp_{s_f})_{j\in J}(\langle u_j\rangle_\pi)_F (\operp_{s_f})_{l\in L}\langle v_l\rangle_{\pi_F} \text{ und } Z := (\operp_{s_f})_{j\in J}(\langle w_j\rangle_\pi)_F (\operp_{s_f})_{l\in L}\langle \nu v_l\rangle_{\pi_F}.$$

Dann sind Y und Z s_f-totalisotrope π_F-Moduln und es gilt $D_F = Y \oplus Z$ (cf. 2.1.1 (vi)). Nach 1.4.4 (ii) $\Rightarrow$ (i) ist $D_F + S'/S'$ ein H'-regulärer, H'-hyperbolischer Raum. Mit 1.4.1 folgt

$$T' = D_F + S'/S' \operp_{H'} M_F + S'/S'.$$

Weil T' ein H'-hyperbolischer Raum ist, ist nach dem Kürzungssatz von Witt auch $M_F + S'/S'$ ein H'-hyperbolischer Raum. Nach 1.4.3 (iii) gibt es ein $v \in M$ mit $\mathrm{ann}_{\pi_F}(v) = r'$ und $\langle v\rangle_{\pi_F}$ ist s_f-totalisotrop, i.e. $f(v\pi^a, v\pi^b) = f(v\pi^b, v\pi^a) \in F$ für alle $a, b \in \mathbb{N}_0$. [Beachte, daß an dieser Stelle die Voraussetzung $\mathrm{char}(K) \neq 2$ oder $p \neq x + 1$ eingeht.]

Fall A. $\langle v\rangle_\pi$ ist regulär. Dann gilt insbesondere $E = \langle v\rangle_\pi \oplus (\langle v\rangle_\pi^\perp \cap E)$ und $\langle v\rangle_\pi^\perp \cap E$ ist π-invariant. Aus dem Satz von Krull-Remak-Schmidt folgt dann $\mathrm{ann}_\pi(v) \in \{r, r^\times, r'\}$. Aus $\mathrm{ann}_\pi(v) \neq r'$ erhält man aus 2.1.1 (vi) bereits $\langle v\rangle_{\pi_F} = \langle v\rangle_\pi$. Nach 2.1.2 (iv) ist $\langle v\rangle_\pi$ totalisotrop insbesondere nicht regulär, ein Widerspruch.
Setze $D' := D \operp \langle v\rangle_\pi$. Dann gilt $D < D'$ und D' hat die für D geforderten Eigenschaften, ein Widerspruch zur Wahl von D.

Fall B: $\langle v\rangle_\pi$ ist nicht regulär.
Sei $(\hat{R}, \hat{S}, \hat{T}, \hat{H}, \hat{p}, \hat{r}) \in \{(R, S, T, H, p, r), (R^\times, S^\times, T^\times, H^\times, p^\times, r^\times)\}$.

Fall B1. $v \in \hat{R}$. Dann gilt $\mathrm{ann}_\pi(v) = \hat{r}$ und $v + \hat{S} \in \hat{R} \cap M + \hat{S}/\hat{S}$ ist nach 1.4.1 (ii) ein $\hat{H}$-isotroper Vektor. Weil $\hat{R} \cap M (= \ker \hat{r}(\pi_M))$ ein regulärer π-Modul ist, ist $\hat{R} \cap M + \hat{S}/\hat{S}$ nach 1.4.1 (iii) $\hat{H}$-regulär, enthält mithin eine $\hat{H}$-hyperbolische Ebene. Nach 1.4.3 bedeutet dies, daß es $u, w \in M \cap \hat{R}$ mit $\mathrm{ann}_\pi(u) = \mathrm{ann}_\pi(w) = \hat{r}$ gibt, so daß $\langle u\rangle_\pi \oplus \langle w\rangle_\pi$ ein regulärer hyperbolischer Raum mit totalisotropen π-Moduln $\langle u\rangle_\pi$, $\langle w\rangle_\pi$ ist. Dann hat $D' := D \operp (\langle u\rangle_\pi \oplus \langle w\rangle_\pi)$ die für D geforderten Eigenschaften und es gilt $D < D'$, ein Widerspruch zur Wahl von D.

Fall B2. $v \notin R \cup R^\times$. Insbsondere ist dann $r' = rr^\times$ und $E = R \operp R^\times$. Nach 2.1.1 (iv) gilt $\mathrm{ann}_\pi(v) = p^k p^{\times l}$ für geeignete $k, l \in \mathbb{N}$ mit $\max(k, l) = i$. Sei $j := \min(k, l)$. Sei $\hat{p}$ so gewählt, daß $\mathrm{ann}_\pi(v) = \hat{p}^i \hat{p}^{\times j}$ ist. Seien $u := v\hat{p}^{\times j}(\pi) \in R$ und $w := v\hat{p}^i(\pi) \in R^\times$. Dann ist $\mathrm{ann}_\pi(u) = \hat{p}^i$,

$\mathrm{ann}_\pi(w) = \hat{p}^{\times j}$, $\langle v\rangle_\pi = \langle u\rangle_\pi \bigoplus \langle w\rangle_\pi$ und somit rad $\langle v\rangle_\pi =$ rad $\langle u\rangle_\pi \bigoplus$ rad $\langle w\rangle_\pi$. Es gibt demnach ein $z \in \{u, w\}$ mit rad $\langle z\rangle_\pi \neq \{0\}$. Falls $z = u$ oder $i = j$ gilt, folgt ein Widerspruch wie im Fall B1 mit z anstelle v. Folglich kann man annehmen, daß $\langle u\rangle_\pi$ regulär ist, $z = w$ und $j < i$ gilt. Dann ist $y := v(\hat{p}\hat{p}^\times)^j(\pi) = u\hat{p}^j(\pi) \in (\langle v\rangle_{\pi_F} \cap \langle u\rangle_\pi)\backslash\{0\}$, und es gilt $\mathrm{ann}_\pi(y) = \hat{p}^{i-j}$. Nach 2.1.1 (vi) haben wir $\langle y\rangle_\pi = \langle y\rangle_{\pi_F} \leq \langle v\rangle_{\pi_F}$. Aus 2.1.2 (iii) folgert man $\langle y\rangle_\pi \leq \langle y\rangle_\pi^\perp$, also $\langle y\rangle_\pi \leq$ rad $\langle u\rangle_\pi = \{0\}$, ein Widerspruch.

Weil sowohl der Fall A als auch der Fall B zu einem Widerspruch führt, ist die Annahme falsch und es gilt $E = D$. Im Falle $r = r^\times$ folgt hieraus die Behauptung, so daß man $r \neq r'$ annehmen kann. Weil dann für jedes $l \in L$ der π-Modul $\langle v_l\rangle_\pi$ die direkte Summe der π-unzerlegbaren π-Moduln $\langle v_l r(\pi)\rangle_\pi \leq R^\times$ und $\langle v_l r^\times(\pi)\rangle_\pi \leq R$ ist und π ähnlich zu π^{-1} ist, liefert der Satz von Krull-Remak-Schmidt, daß die Mengen $S := \{j \in J; \mathrm{ann}_\pi(u_j) = \mathrm{ann}_\pi(w_j) = r\}$ und $T := \{j \in J; \mathrm{ann}_\pi(u_j) = \mathrm{ann}_\pi(w_j) = r^\times\}$ gleichmächtig sind. Sei $\alpha \in T^S$ bijektiv. Dann ist $E = \bigoplus_{s\in S}(\langle u_s + u_{s\alpha}\rangle_\pi \oplus \langle w_s + w_{s\alpha}\rangle_\pi) \bigoplus_{l\in L}\langle v_l\rangle_\pi$ eine Zerlegung mit den gewünschten Eigenschaften.

(iii) $\Rightarrow$ (i). Für jedes $j \in J$ ist $\pi_{\langle u_j\rangle_\pi}$ zu seinem Inversen ähnlich und damit ein Produkt von zwei Involutionen aus $\mathrm{GL}(\langle u_j\rangle_\pi)$. Nach 2.2.1 ist $\pi_{\langle u_j\rangle_\pi \oplus \langle w_j\rangle_\pi}$ ein Produkt von zwei unitären Involutionen $\kappa_j, \eta_j \in \mathrm{U}(f_{\langle u_j\rangle_\pi \oplus \langle w_j\rangle_\pi})$. Nach 2.2.2 (i) ist $\pi_{\langle v_l\rangle_\pi}$ für jedes $l \in L$ ein Produkt von zwei unitären Involutionen $\rho_l, \sigma_l \in \mathrm{U}(f_{\langle v_l\rangle_\pi})$. Setze $\rho := \bigoplus_{j\in J}\kappa_j \bigoplus_{l\in L}\rho_l$ und $\sigma := \bigoplus_{j\in J}\eta_j \bigoplus_{l\in L}\sigma_l$. Dann sind ρ, σ Involutionen aus $\mathrm{U}(f)$ und es gilt $\pi = \rho\sigma$. ■

Als eine erste Folgerung aus 2.3.1 notieren wir einen Satz von Djoković ([23]).

Korollar 2.3.2 (Djoković) *Sei $\pi \in \mathrm{U}(f)$ derart, daß kein Primteiler von* $\mathrm{mip}(\pi)$ *$^-$-symmetrisch ist. Genau dann ist π ein Produkt von zwei unitären Involutionen, wenn π ähnlich zu π^{-1} ist.*

Beweis. Dies folgt sofort aus der der Äquivalenz der Aussagen (i) und (ii) von 2.3.1. ■

Bemerkung 2.3.3 *Die Bedingung (v) aus 2.3.1 ist äquivalent zu der Bedingung*

(v') *π ist ähnlich zu π^{-1}, und für jeden $^-$-symmetrischen Elementarteiler r von π ist die s_f-hermitesche Invariante* $\mathrm{H}(\pi_F, \mathrm{lcm}(r, \bar{r}))$ *eine hyperbolische Form.*

Beweis. Die Implikation (v) $\Rightarrow$ (v') ist trivial.
(v') $\Rightarrow$ (v). Sei r' ein symmetrischer Elementarteiler von π_F nach 2.1.1 (v) gibt es einen Elementarteiler r von π so, daß $r' = \mathrm{lcm}(r, \bar{r})$ gilt. Ist r $^-$-symmetrisch, so ist die zu r' gehörige s_f-hermitesche Invariante von π_F nach (v) eine hyperbolische Form. Man kann daher $r \neq r^*$ annehmen. Weil r symmetrisch ist, folgt hieraus bereits $r = r^\times$, i.e. r ist symmetrisch. Es ist $W := \ker rr*(\pi)^\infty$ ein regulärer π-Modul, und ist ψ ein Isomorphismus von V der π invertiert, so ist W ψ-invariant. Folglich ist π_W ähnlich zu π_W^{-1}. Nach 2.3.2 ist π_W ein Produkt von zwei unitären Involutinen aus $\mathrm{U}(f_W)$. Nach 2.3.1 (i) $\Rightarrow$ (v) ist die s_f-hermitesche Invariante $\mathrm{H}((\pi_W)_F, r') = \mathrm{H}(\pi_F, r')$ eine hyperbolische Form. ■

Als nächstes gehen wir auf den zu Beginn des Abschnittes angesprochenen Zusammenhang zwischen unitärer und symplektischer Zweispiegeligkeit im Fall $\mathrm{char}(K) \neq 2$ ein. In diesem Fall wurde von K. Nielsen [56] (7.1) folgender Invarianzsatz bewiesen:

Lemma 2.3.4 *Sei g eine reguläre symplektische Form auf einem endlich-dimensionalen Vektorraum Z über einem Körper der Charakteristik $\neq 2$. Sei $\phi \in \mathrm{Sp}(g)$ ein Produkt von zwei symplektischen Involutionen $\rho, \sigma \in \mathrm{Sp}(g)$. Dann gibt es eine orthogonale Zerlegung $Z = \bigoplus_{i \in I} Z_i$ mit den folgenden Eigenschaften:*

(i) *$Z_i = U_i \oplus W_i$ für totalisotrope, zyklische π-Moduln U_i, W_i mit $U_i\rho = U_i$ und $W_i\rho = W_i$.*

(ii) *Z_i ist entweder ein orthogonal unzerlegbar π-Modul vom Typ II oder es gilt $Z_i = X_i \bigoplus X_i\rho$ für orthogonal unzerlegbare π-Moduln vom Typ I oder III.* ■

Satz 2.3.5 *Seien $\mathrm{char}(K) \neq 2$ und $\pi \in \mathrm{U}(f)$. Genau dann ist π ein Produkt von zwei unitären Involutionen, wenn π ähnlich zu π^{-1} und $\pi_F \in \mathrm{Sp}(s_f)$ ein Produkt von zwei symplektischen Involutionen ist.*

Beweis. Sei π ähnlich zu π^{-1} und π_F ein Produkt von zwei Involutionen aus $\mathrm{Sp}(s_f)$. Mit dem Satz von Djoković 2.3.2 reduziert man die allgemeine Situation auf den Fall, daß jeder Primteiler von $\mathrm{mip}(\pi)$ $^-$-symmetrisch ist. Dann ist jeder Primteiler von $\mathrm{mip}(\pi_F)$ symmetrisch (cf. 2.1.1 (iii)). Nach 2.3.4 gibt es eine Zerlegung $V_F = (\bigoplus_{s_f})_{s \in S} Y_s \oplus Z_s$ für s_f-totalisotrope, π_F-unzerlegbare π_F-Moduln Y_s, Z_s. Sei $r \in F[x]$ ein symmetrischer Elementarteiler von π_F und R die aus der angegebenen Zerlegung resultierende s_f-reguläre r-Komponente. Nach 1.4.4 ist die zu R gehörige s_f-hermitesche Invariante $\mathrm{H}(\pi_F, R)$ eine hyperbolische Form. Die Implikation 2.3.1 (v) $\Rightarrow$ (i) besagt nun, daß π auch ein Produkt von zwei unitären Involutionen ist. ■

Korollar 2.3.6 *Sei K ein endlicher Körper und $\pi \in \mathrm{U}(f)$. Im Fall $\mathrm{char}(K) = 2$ sei $x+1$ kein Teiler von $\mathrm{mip}(\pi)$. Genau dann ist π ein Produkt von zwei unitären Involutionen, wenn π ähnlich zu π^{-1} ist und jeder Elementarteiler der Form $(x \pm 1)^{2t}$, $t \in \mathbb{N}$, eine gerade Vielfachheit hat.*

Beweis. $\Rightarrow$. Klar nach 2.2.6.
$\Leftarrow$. Nach 2.3.1 und 2.3.3 genügt es zu zeigen, daß für jeden $^-$-symmetrischen Elementarteiler r von π die s_f-hermitessche Invariante $\mathrm{H}(\pi_F, r')$, $r' := \mathrm{lcm}(r, \bar{r})$, eine hyperbolische Form ist.
Seien $p \in K[x]$ irreduzibel und $i \in \mathbb{N}$ so, daß $r = p^i$ ist. Seien $p' := \mathrm{lcm}(p, \bar{p})$, $\xi := x + pK[x] \in K[x]/pK[x]$, $\xi' := x + p'F[x] \in F[x]/p'F[x]$, R eine reguläre r-Komponente von π und $\tilde{R}$ eine reguläre $\bar{r}$-Komponente von π. Im Falle $r = \bar{r}$ gelte $R = \tilde{R}$. Nach 2.1.3 ist $R' := (R + \tilde{R})_F$ eine reguläre r'-Komponente von ϕ. Im Fall $p \neq x \pm 1$ ist $H(\phi, R')$ eine hermitesche oder schiefhermitesche Form (cf. 1.3.15 (i)) auf dem Vektorraum $R'/R'p'(\phi)$ über dem endlichen Körper $F[\xi']$. Wegen $\bar{r} = r^{\times}$ und weil π ähnlich zu π^{-1} ist, haben r und $\bar{r}$ dieselbe Vielfachheit. Nach 2.1.1 (vii) hat r' eine gerade Vielfachheit als Elementarteiler von π_F. Dies bedeutet, daß $\dim_{F[\xi']} R'/R'p'(\phi)$ gerade ist. Also ist $\mathrm{H}(\phi, R')$ in diesem Fall eine hyperbolische Form. Man kann daher $p = x \pm 1$ annehmen. Nach Voraussetzung gilt dann $\mathrm{char}(K) \neq 2$. Ist i ungerade, so ist $\mathrm{H}(\phi, R')$ eine symplektische Form (cf. 1.3.15 (iii)) und damit insbesondere hyperbolisch. Man kann daher weiterhin annehmen, daß i gerade ist. Wegen $^- \neq 1_K$ ist $\mathrm{H}(\pi, R)$ eine hermitesche Form

auf dem Vektorraum $R/Rp(\pi)$ über dem endlichen Körper $K[\xi] \cong K$. Nach Voraussetzung ist $\dim_{K[\xi]} R/Rp(\pi)$, die Vielfachheit des Elementarteilers $(x+1)^i$, gerade. Folglich ist $\mathrm{H}(\pi, R)$ eine hyperbolische Form. Nach 1.4.4 gibt es totalisotrope π-Moduln A und B derart, daß $M := A \oplus B$ regulär ist und $M + Rp(\pi) = R = M \bigcirc\!\!\!\!\perp (M^\perp \cap R)$ gilt. Hieraus folgt $M^\perp \cap R \leq Rp(\pi)$. [Denn ist $a \in (M^\perp \cap R)$, $S := Rp(\pi)$ und $H := \mathrm{H}(\pi, R)$, so folgt aus 1.4.1 (ii), daß $H(a+S, b+S) = 0$ für alle $b \in M$ gilt und wegen $R = M + S$ bereits $a + S \in H\text{-rad}R/S = \{0\}$, i.e. $a \in S$.] Weil r der einzige Elementarteiler von π_R ist, jedoch $(M^\perp \cap R)p^{i-1}(\pi) \leq Rp^i(\pi) = \{0\}$ gilt, folgt aus dem Satz von Krull-Remak-Schmidt, daß $M^\perp \cap R = \{0\}$ ist, i.e. $R = M$. Weil dann auch $R' = R_F = A_F \oplus B_F$ die direkte Summe der s_f-totalisotropen ϕ-Moduln A_F und B_F ist, ist wiederum nach 1.4.4 $\mathrm{H}(\phi, R')$ eine hyperbolische Form. ■

Abschließend geben wir noch eine Beschreibung solcher Isometrien an, für die kein $^-$-symmetrischer Elementarteiler in $F[x]$ liegt. Der Beweis läßt sich zwar auch mit Hilfe des Charakterisierungssatzes 2.3.1 relativ leicht führen, aufgrund der Einfachkeit der Aussage scheint aber ein direkter Beweis der lediglich den Satz von Djoković (cf. 2.3.2) ausnutzt, welcher als elementar angesehen werden kann, angemessener zu sein.

Lemma 2.3.7 *Sei $\pi \in \mathrm{U}(f)$ derart, daß kein $^-$-symmetrischer Primteiler von* $\mathrm{mip}(\pi)$ *in $F[x]$ liegt. Genau dann ist π ein Produkt von zwei unitären Involutionen, wenn π in $\mathrm{U}(f)$ konjugiert zu π^{-1} ist.*

Beweis. Die Implikation '$\Rightarrow$' ist trivial.
$\Leftarrow$. Sei $\psi \in \mathrm{U}(f)$ so, daß $\pi^\psi = \pi^{-1}$ ist. Sei $V = A \bigcirc\!\!\!\!\perp\, B$ eine Zerlegung von V in π-Moduln A und B so, daß kein (bzw. jeder) Primteiler von $\mathrm{mip}(\pi_A)$ (bzw. $\mathrm{mip}(\pi_B)$) $^-$-symmetrisch ist. Dann sind A und B auch ψ invariant, und es gilt $\psi_A^{-1}\pi_A\psi_A = \pi_A^{-1}$. Nach dem Satz von Djoković ist π_A ein Produkt von zwei unitären Involutionen aus $\mathrm{U}(f_A)$. Wir können daher o.B.d.A. $A = \{0\}$ annehmen. Seien p ein $^-$-symmetrischer Primteiler von $\mathrm{mip}(\pi)$, $C := \ker p(\pi)^\infty$ und $D := \ker p^\times(\pi)^\infty = C\psi$. Die Voraussetzung $p \neq \bar{p} = p^\times$ liefert $C \perp C^\times$. Also ist $E := C \bigcirc\!\!\!\!\perp\, D$ ein regulärer ψ- und π-invarianter Unterraum, und man kann o.B.d.A. $V = E$ annehmen. Setze $\rho := \psi_C \oplus (\psi^{-1})_D$. Dann ist $\rho \in \mathrm{GL}(V)$ eine Involution. Für $c, c' \in C$ und $d, d' \in D$ berechnet man

$$f((c+d)\rho, (c'+d')\rho) = f(c\psi, c'\psi) + f(d\psi^{-1}, d'\psi^{-1}) = f(c, c') + f(d, d') = f(c+d, c+d').$$

und

$$(c+d)\rho\pi = (c\psi + d\psi^{-1})\pi = c\pi^{-1}\psi + d\pi^{-1}\psi^{-1} = (c+d)\pi^{-1}\rho.$$

Damit ist ρ eine Involution aus $\mathrm{U}(f)$, die π invertiert. Folglich ist $\sigma := \rho\pi \in \mathrm{U}(f)$ ebenfalls eine Involution, und es gilt $\pi = \rho\sigma$. ■

2.4 Offene Fragen

(1) Man versuche auch für den Fall $\mathrm{char}(K) = 2$ und unipotentes π einen ähnlichen Zerlegungssatz wie 2.2.5 herzuleiten. Kann man in diesem Fall in Analogie zu 2.2.6 wenigstens zeigen, daß jeder Elementarteiler der Form $(x+1)^{2t+1}$, $t \in \mathbb{N}$, von π eine gerade Vielfachheit hat? Wäre

dies der Fall, so könnte man jedenfalls für endliche Körper mit analogen Schlüssen wie in 2.3.6 und unter Beachtung von 2.2.3 (ii) folgenden Satz herleiten:

Sei $\mathrm{char}(K) = 2$. Genau dann ist $\pi \in \mathrm{U}(f)$ ein Produkt von zwei unitären Involutionen, wenn jeder Elementarteiler $(x+1)^{2t+1}$, $t \in \mathbb{N}$, von π eine gerade Vielfachheit hat.

(2) Man versuche, die eingangs gemachte Voraussetzung $^{-} \neq 1_K$ fallen zu lassen, i.e. f sei eine reguläre symmetrische, symplektische oder hermitesche Form, und versuche, alle Schlüsse einheitlich zu führen. Beachte, daß dann s_f für symmetrisches f trivial wird, und für $\mathrm{char}(K) \neq 2$ und symplektisches f ist $s_f = 2f$. Ein verallgemeinerter Charakterisierungssatz 2.3.1 für Involutionen in klassischen Gruppen würde dann über die Implikation (v) $\Rightarrow$ (i) die in der Einleitung angegebenen klassischen Sätze über die Zweispiegeligkeit der orthogonalen Gruppen und symplektischen Gruppen über Körpern mit Charakteristik 2 einschließen.

Kapitel 3

Produkte von Symmetrien in unitären Gruppen

Wir nennen eine unitäre Involution mit eindimensionaler Bahn eine (unitäre) Symmetrie. Ist $\mathrm{char}(K) \neq 2$, so hat jede Symmetrie die Form

$$\sigma_a : V \to V, v \mapsto v - 2\frac{f(v,a)}{f(a,a)}a,$$

wobei $a \in V \backslash \{0\}$ ein anisotroper Vektor ist. Ist $\mathrm{char}(K) = 2$, so hat jede Symmetrie die Form

$$\sigma_{\alpha,b} : V \to V, v \mapsto v + \alpha f(v,b)b,$$

wobei $b \in V \backslash \{0\}$ ein isotroper Vektor und $\alpha \in F^*$ ist. (Falls $|F| = 2$ ist, muß $\alpha = 1$ sein. In diesem Fall schreiben wir einfachheitshalber σ_a statt $\sigma_{1,a}$.) Wir haben stets $\mathrm{B}(\sigma_a) = \langle a \rangle$ und $\mathrm{B}(\sigma_{\alpha,b}) = \langle b \rangle$. Im Fall $\mathrm{char}(K) = 2$ ist jede unitäre Symmetrie eine Transvektion und hat eine totalisotrope Bahn. Bekanntlich stimmt die von der Menge S aller unitärer Symmetrien erzeugte Gruppe mit der von allen unitären Involutionen erzeugten Gruppe überein und ist in der Untergruppe $\mathrm{U}^{\pm}(f)$ der unitären Transformationen mit Determinante ± 1 enthalten. Wir wollen die Elemente jener Gruppe beschreiben; und falls π ein Element dieser Gruppe ist, i.e. π ist ein Produkt von Symmetrien, dann wollen wir die kleinste Zahl $\mathrm{l}(\pi)$ von Symmetrien bestimmen, die in solch einem Produkt benötigt wird. Die Zahl $\mathrm{l}(\pi)$ heißt die Länge von π. Für beliebige Körper ist das Symmetrien-Längenproblem ungelöst. Der Fall $K = \mathbb{C}$ wurde von D.Ž. Djoković und J. Malzan in [54] untersucht. Der Fall, daß K ein endlicher Körper $\neq \mathrm{F}_9$ mit Charakteristik $\neq 2$ ist, wurde von Ellers [31] gelöst. Die folgenden Untersuchungen wurden von der letztgenannten Arbeit angeregt. Wir wollen allgemeine und und einfache Methoden finden, die auf beliebige Körper anwendbar sind. Vollständig gelöst wird das Symmetrien-Längenproblem für die Klasse der Körper K, in denen die Normabbildung

$$K \to F, k \mapsto k\bar{k}$$

surjektiv ist. Diese Klasse umfaßt alle endlichen Körper F_{q^2}, q eine Primzahlpotenz, aber zum Beispiel auch die perfekten Abschlüsse $K := (\mathrm{F}_{2^{j+1}}(x))^{2^{-\infty}}$ der rationalen Funktionenkörper $\mathrm{F}_{2^{j+1}}(x)$

in einer Variablen x, $j \in \mathbb{N}$. Diese sind quadratische Körpererweiterungen der perfekten Körper $F := (\mathrm{F}_{2^j}(x))^{2^{-\infty}}$, und die von dem nichttrivialen involutorischen Element $^-$ der Galoisgruppe induzierte Normabbildung ist wegen $F = F^2 \subseteq \mathcal{N}(K)$ trivialerweise surjektiv. Die Ergebnisse sind in den Sätzen 3.4.5 ($\mathrm{char}(K) \neq 2, |F| > 3$), 3.4.21 ($|F| = 3$), 3.5.5 ($\mathrm{char}(K) = 2, |F| > 2$) und 3.5.8 ($|F| = 2$) formuliert.

3.1 Äquivalenz hermitescher Formen

Bemerkung 3.1.1 *Eine hyperbolische Ebene von V ist ein 2-dimensionaler regulärer Unterraum U von V, der einen isotropen Vektor $\neq 0$ enthält. Dann besitzt U bereits eine Basis bestehend aus isotropen Vektoren, und es gilt $\{f(u,u)|u \in U\} = F$. Die Anzahl singulärer eindimensionaler Unterräume (i.e. $\langle v\rangle$, wobei $v \in V\backslash\{0\}$ isotrop ist) in einer hyperbolischen Ebene beträgt $|F|+1$. Ist allgemein $W \leq V$ ein regulärer m-dimensionaler Teilraum und $|F| = q$, q eine Primzahlpotenz, so enthält W genau $(q^{m-1}-(-1)^{m-1})(q^m-(-1)^m)/(q^2-1)$ eindimensionale singuläre Teilräume.*

Beweis. Einen Beweis für die zuletzt angegebene Formel findet man z.B. in [69] Kapitel 10, Lemma 10.4, S.117. ∎

Lemma 3.1.2 (Geometrische Äquivalenz hermitescher Formen.) *Seien d und $s : V \times V \to K$ $^-$-hermitesche Formen. (Wir setzen nicht voraus, daß d oder s regulär ist.) Es gelte*

(1) *$d(v,v) = 0$ impliziert $s(v,v) = 0$ für alle $v \in V$*

und

(2) *V enthält eine d-hyperbolische Ebene.*

Dann ist $s = \lambda d$ für ein $\lambda \in F$.

Beweis.

(i) Zu jeder d-hyperbolischen Ebene U von V gibt es genau ein $\lambda_U \in F$, so daß $s_U = \lambda_U d_U$ gilt (wobei s_U, d_U die Restriktionen auf $U \times U$ bezeichne).

Beweis. Wähle eine Basis a, b von U, so daß $d(a,a) = 0 = d(b,b)$ und $d(a,b) = 1$ ist. Sei $\lambda_U := s(a,b)$. Wähle ein $\beta \in K$, so daß $\bar{\beta} = -\beta \neq 0$ ist. Dann ist $a + \beta b$ d-isotrop, also nach (1) auch s-isotrop. Das bedeutet $\bar{\beta}\lambda_U + \beta\overline{\lambda_U} = 0$, also $\overline{\lambda_U} = \lambda_U$. ∎

(ii) Sind $a, b \in V$ d-isotrop, so folgt aus $d(a,b) = 0$ bereits $s(a,b) = 0$.

Beweis. Wir können annehmen, daß a, b linear unabhängig sind. Folglich ist $\langle a, b\rangle$ d-totalisotrop, also nach (1) auch s-totalisotrop. Insbesondere ist $s(a,b) = 0$. ∎

(iii) Sei U eine d-hyperbolische Ebene von V und seien $a, b \in V$, so daß $d(a,U) = 0 = d(b,U)$ ist. Dann gilt $s(a,b) = \lambda_U \cdot d(a,b)$.

Beweis. Wir beweisen zunächst den Spezialfall $a = b$. Wegen (1) können wir $d(a, a) \neq 0$ annehmen. Wähle ein $u \in U$ mit $d(u, u) = -d(a, a)$. Dann ist $Z := \langle a, u\rangle$ eine d-hyperbolische Ebene und $s_Z = \lambda_Z d_Z$. Wegen $u \in U \cap Z$ und $d(u, u) \neq 0$ und $s_U = \lambda_U \cdot d_U$ folgt $\lambda_U = \lambda_Z$.

Wir beweisen nun den allgemeinen Fall. Man kann o.B.d.A. $d(a, b) \in F$ annehmen. Für $\omega \in K$ gilt nach dem zuerst bewiesenen Spezialfall:

$$\begin{aligned} \lambda_U(d(a,a) + (\omega+\bar\omega)d(a,b) + \omega\bar\omega d(b,b) &= \lambda_U d(a+\omega b, a+\omega b) = s(a+\omega b, a+\omega b) \\ &= s(a,a) + \omega s(b,a) + \bar\omega s(a,b) + \omega\bar\omega s(b,b) \\ &= \lambda_U d(a,a) + \omega s(b,a) + \bar\omega s(a,b) + \omega\bar\omega\lambda_U d(b,b), \end{aligned}$$

i.e.
(3) $\lambda_U(\omega + \bar\omega)d(a, b) = \omega s(b, a) + \bar\omega s(a, b)$.

Für $\omega \in K^*$ mit $\bar\omega = -\omega$ liefert (3), daß $s(a, b) = s(b, a) \in F$ ist. Für $\omega \in K$ mit $\bar\omega \neq -\omega$ liefert (3) nun das gewünschte Resultat. ■

(iv) Sei U eine d-hyperbolische Ebene von V.
Dann folgt aus $d(a, U) = 0$ auch $s(a, U) = 0$ für jedes $a \in V$.

Beweis. Sei $d(a, U) = 0$. Ist a d-isotrop, so folgt die Behauptung aus (ii). Wir können deshalb $d(a, a) \neq 0$ annehmen. Wähle linear unabhängige Vektoren $b, c \in U$, so daß $Z_1 := \langle a, b\rangle$ und $Z_2 := \langle a, c\rangle$ d-hyperbolische Ebenen sind. Dies ist möglich:
Wähle $u, w \in U$ derart, daß $\langle u\rangle \neq \langle w\rangle$, $d(u, u) = 0 = d(w, w)$ und $d(u, w) = 1$ ist. Weil die Spurabbildung $K \to F, \mu \mapsto \mu + \bar\mu$ surjektiv ist, gibt es ein $\mu \in K$, so daß $\mu + \bar\mu = -d(a, a)$ ist. Für $\iota \in K^*$ mit $\bar\iota = -\iota$ hat $\nu := \mu + \iota$ ebenfalls die Spur $-d(a, a)$. Die Vektoren $b := u + \mu w$, $c := u + \nu w$ sind linear unabhängig und erfüllen $d(b, b) = d(c, c) = -d(a, a)$. Folglich sind $Z_1 := \langle a, b\rangle$ und $Z_2 := \langle a, c\rangle$ hyperbolische Ebenen.
Es gilt nun $s_{Z_i} = \lambda_{Z_i} \cdot d_{Z_i}$ und deshalb $s(a, b) = 0 = s(a, c)$, also $s(a, U) = 0$. ■

Wähle eine d-hyperbolische Ebene U von V. Dann gilt $V = U \bigoplus_d W$, wobei $W := U^{\perp_d}$ sei. Nun folgt aus (iv), daß $V = U \bigoplus_s W$ ist. Aus (iii) erhält man für $u_i \in U$ und $w_i \in W$

$$s(u_1+w_1, u_2+w_2) = s(u_1, u_2)+s(w_1, w_2) = \lambda_U \cdot d(u_1, u_1)+\lambda_U \cdot d(w_1, w_2) = \lambda_U \cdot d(u_1+w_1, u_2+w_2). ■$$

Lemma 3.1.3 *Seien d und $s : V \times V \to K$ $^-$-hermitesche Formen. (Wir nehmen nicht an, daß d oder s regulär ist.) Sei W ein echter Unterraum von V. Im Fall $|F| = 2$ sei $\dim W \leq \dim V - 2$. Weiterhin gelte*

(1_W) *$d(v, v) = 0$ impliziert $s(v, v) = 0$ für alle $v \in V \backslash W$,*
und
(2) *V enthält eine d-hyperbolische Ebene.*

Dann ist $s = \lambda d$ für ein $\lambda \in F$.

Beweis. Nach 3.1.2 genügt es zu zeigen:

($*$) Ist $v \in W$ und $d(v,v) = 0$, so ist auch $s(v,v) = 0$.

Sei $v \in W$ und $d(v,v) = 0$. Wegen (2) wird V von d-isotropen Vektoren erzeugt. Es gibt daher ein d-isotropes $w \in V \backslash W$. Ist $Z := \langle v, w \rangle$ nicht d-regulär, so ist Z d-totalisotrop (dim d-rad $Z = 1$ liefert, daß d-rad Z der einzige d-isotrope, eindimensionale Unterraum von Z; es gibt jedoch mindestens zwei solche, nämlich $\langle v \rangle$ und $\langle w \rangle$). Nach (1_W) sind alle eindimensionalen Unterräume von Z mit der einzig möglichen Ausnahme $\langle v \rangle$ auch s-singular. Dies ergibt bekanntlich, daß Z s-totalisotrop ist. Insbesondere ist v s-isotrop. Wir können daher folgendes annehmen:

(3) Für jedes d-isotrope $u \in V \backslash W$ ist $\langle u, v \rangle$ eine d-hyperbolische Ebene.

Insbesondere ist Z eine d-hyperbolische Ebene. Wir betrachten zunächst den Fall $|F| > 2$. Dann enthält Z mindestens vier d-singuläre 1-dimensionale Unterräume (cf. 3.1.1). Wähle $r \in Z \backslash W$, so daß $\langle r \rangle$ d-singulär und $\langle r \rangle \neq \langle w \rangle$ ist. Dann sind $\langle w \rangle$ und $\langle r \rangle$ nach (1_W) auch s-singuläre Unterräume von $Z = \langle w, r \rangle$. Wir können $d(w,r) = 1$ annehmen. Sei $\lambda := s(w,r)$. Wir behaupten, daß $s(z,z) = \lambda d(z,z)$ für jedes $z \in Z$ gilt, insbesondere folgt hieraus $s(v,v) = 0$. Es gibt einen weiteren 1-dimensionalen, d-singulären Unterraum $\langle w + \eta r \rangle \not\subseteq W, \langle w + \eta r \rangle \neq \langle w \rangle, \langle r \rangle, (\eta \in K)$. Dann gilt $\bar{\eta} = -\eta$ und $\langle w + \eta r \rangle$ ist s-singulär. Dies ergibt $\bar{\eta}\lambda + \eta\bar{\lambda} = 0$, also $\lambda = \bar{\lambda}$. Hieraus folgert man $s(z,z) = \lambda(\alpha\bar{\beta} + \bar{\alpha}\beta) = \lambda d(z,z)$ für alle $z = \alpha w + \beta r \in Z$.

Nun behandeln wir den Fall $|F| = 2$, i.e. $F = \mathrm{F}_2$ und $K = \mathrm{F}_4$. Annahme: $s(w,w) \neq 0$. Dann gilt $s(w,w) \in F^* = \{1\}$. Wegen $\dim W \leq \dim V - 2$, gibt es mindestens zwei weitere d-isotrope Vektoren $u, y \in V \backslash W$, so daß u, y, w paarweise linear unabhängig sind und

(4) $\quad \langle u, y, w \rangle \cap W = \{0\}$

ist. (Wähle zum Beispiel ein d-isotropes $y \in V \backslash W + (\langle w \rangle)$ mit $f(y,w) \in F$ und setze $u := y + w$.) Wegen (3) können wir $d(u,v) = d(w,v) = d(y,v) = 1$ annehmen. Ist $s(z,v) \in F$ für ein $z \in \{u, w, y\}$, so folgt die Behauptung wie im zuerst betrachteten Fall $|F| > 2$. (Es ist $r := z + v \notin W$ d- und s-isotrop. Es gilt $d(z,r) = d(z,v) = 1$ und $\lambda := s(z,r) = s(z,v) \in F$, somit $s_H = \lambda d_H$, wobei $H = \langle z, r \rangle$ sei. Wegen $v = r + z \in H$ folgt insbesondere $s(v,v) = 0$.)
Wir können daher $s(u,v), s(w,v), s(y,v) \in K \backslash F$ annehmen. Wegen $|K \backslash F| = 2$, können wir weiterhin $l := s(u,v) = s(w,v)$ annehmen. Es gilt $K = \{0, 1, l, l+1\}$ und $\bar{l} = l + 1 = l^{-1}$. Setze $U := \langle u, w, v \rangle$, $\mathcal{B} := (u, w, v)$, $\alpha := d(u,w)$ und $\beta := s(u,w)$. Dann gilt

$$\mathcal{M}_{\mathcal{B}}(d_U) = \begin{bmatrix} 0 & \alpha & 1 \\ \bar{\alpha} & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \text{ und } \mathcal{M}_{\mathcal{B}}(s_U) = \begin{bmatrix} 0 & \beta & l \\ \bar{\beta} & 0 & l \\ \bar{l} & \bar{l} & 1 \end{bmatrix}.$$

Man berechnet $\det \mathcal{M}_{\mathcal{B}}(d_U) = \alpha + \bar{\alpha}$. Demnach liefert $\alpha \in F$ ein $a \in d$-rad $U \backslash \{0\}$. Offensichtlich ist $\langle a \rangle \neq \langle v \rangle$, da $d(u,v) = 1 \neq 0 = d(u,a)$ ist. Nach (3) ist jedoch $d(a,v) \neq 0$, ein Widerspruch. Folglich ist $\alpha \notin F$. Seien $y := u + \bar{\alpha} w + v$ und $z := \alpha u + w + v$. Dann sind $y, z \in U \backslash W$ (cf. (4)) d-isotrop, und demnach auch s-isotrop (cf. (1_W)). Hieraus berechnen wir:

$$\bar{\alpha}\bar{\beta} + \alpha\beta + \alpha\bar{l} + \bar{\alpha}l + 1 = s(y,y) = 0 = s(z,z) = \bar{\alpha}\bar{\beta} + \alpha\beta + \bar{\alpha}\bar{l} + \alpha l + 1.$$

Es folgt der Widerspruch $\alpha = \alpha(l+\bar{l}) = \bar{\alpha}(l+\bar{l}) = \bar{\alpha}$. ■

Will man in 3.1.3 auch im Fall $|F| = 2$ Hyperebenen W zulassen, so muß man weitere Regularitätseigenschaften von den beteiligten hermiteschen Formen d und s fordern. In den späteren Anwendungen wird die Form d im Fall $|F| = 2$ besser handhabbar sein als die Form s, so daß es aus rein praktischen Gründen der Nachweisbarkeit sinnvoll erscheint, weitere Regularitätseigenschaften von d zu fordern. Wie dies aussehen kann, zeigt das

Lemma 3.1.4 *Seien $|F| = 2$ und d, s wie in 3.1.3. Sei W eine Hyperebene von V. und es gelte (1_W) von 3.1.3. Weiterhin gelte*

(2') $\dim V/d\text{-rad } V \geq 4$.

Dann ist $s = \lambda d$ für ein $\lambda \in F$.

Beweis. Nach 3.1.2 genügt es wiederum zu zeigen, daß jeder d-isotrope Vektor aus W auch s-isotrop ist.
Sei $v \in W$ d-isotrop. Annahme: v ist nicht s-isotrop. Gäbe es einen d-isotropen Vektor $a \in v^{\perp_d} \backslash W$, so wäre $H := \langle a, v \rangle$ d-totalisotrop. Wegen $H \cap W = \langle v \rangle$ gäbe es nach (1_W) vier s-singuläre eindimensionale Unterräume von H und H wäre demnach bekanntlich s-totalisotrop, ein Widerspruch. Es gilt daher:

(3) Jeder d-isotrope Vektor aus $v^{\perp_d}$ ist in W enthalten.

Insbesondere ist $v \notin d\text{-rad } V$, da V nach (2') von d-isotropen Vektoren erzeugt wird. Aus (2') erhält man weiterhin $\dim d\text{-rad } v^{\perp_d} \leq \dim d\text{-rad } V + 1 \leq \dim V - 3$, also $\dim v^{\perp_d}/d\text{-rad } v^{\perp_d} \geq 2$. Folglich wird $v^{\perp_d}$ von d-isotropen Vektoren erzeugt. Aus (3) folgt nun

(4) $v^{\perp_d} = W$.

Weil V von d-isotropen Vektoren erzeugt wird, gibt es ein d-isotropes $a \in V \backslash W$ mit $d(a, v) = 1$. Dann ist $a + v \in V \backslash W$ d-isotrop. Nach (1_W) gilt $0 = s(a+v, a+v) = s(a, v) + s(v, a) + 1$, also $\nu := s(a, v) \in K \backslash F$.
Seien $H := \langle a, v \rangle$ und $Z := H^{\perp_d}$. Weil H eine d-hyperbolische Ebene ist, gilt $V = H \bigoplus_d Z$. Aus (2') folgt, daß Z nicht d-totalisotrop ist. Sei $z \in Z$ d-anisotrop. Seien $\alpha \in K \backslash F$, $\beta \in K^*$. Es sind $a + \alpha v + \beta z, a + \bar{\alpha} v + \beta z \notin v^{\perp_d} = W$ d-isotrop, also nach (1_W) auch s-isotrop. Es folgt

$$\begin{aligned}
1 &= s(v,v) = s((a+\alpha v+\beta z)+(a+\bar{\alpha}v+\beta z),(a+\alpha v+\beta z)+(a+\bar{\alpha}v+\beta z)) \\
&= s(a+\alpha v+\beta z, a+\bar{\alpha}v+\beta z) + s(a+\bar{\alpha}v+\beta z, a+\alpha v+\beta z) \\
&= s(a+\alpha v+\beta z, v) + s(v, a+\alpha v+\beta z) \qquad \text{(Verwende } \bar{\alpha} = \alpha+1!) \\
&= (\nu+\bar{\nu}) + (\alpha+\bar{\alpha}) + \beta s(z,v) + \bar{\beta} s(v,z) \\
&= \beta s(z,v) + \bar{\beta} s(v,z).
\end{aligned}$$

Für $\beta = 1$ folgt $\delta := s(v, z) \in K \backslash F$. Für $\beta = \delta$ erhalten wir nun den Widerspruch $1 = \delta\bar{\delta} + \bar{\delta}\delta = 0$. ■

Daß die Bedingung (2') aus 3.1.4 in gewissem Sinne optimal ist, zeigt das

Beispiel 3.1.5 *Es sei $|F| = 2$, $\dim V = 3$ und $\mathcal{B} = (a, b, c)$ eine geordnete Basis von V. Weiterhin seien $d, s : V \times V \to K$ die durch*

$$\mathcal{M}_{\mathcal{B}}(d) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \mathcal{M}_{\mathcal{B}}(s) = \begin{bmatrix} 0 & \lambda & \lambda \\ \bar{\lambda} & 1 & \lambda \\ \bar{\lambda} & \bar{\lambda} & 0 \end{bmatrix}$$

definierten $^{-}$-hermiteschen Formen, wobei $\lambda \in K \backslash F$ sei. Dann gilt $\dim V/d\text{-rad } V = 3$ und es ist (1_W) aus 3.1.4 für $W := \langle b, c\rangle$ erfüllt. Jedoch ist $d(b, b) = 0$ und $s(b, b) = 1$.

Beweis. Weil $\mathcal{M}_{\mathcal{B}}(d)$ regulär ist, ist d-rad $V = \{0\}$. Die d-singulären eindimensionalen Teilräume von V, die nicht in W liegen, sind:

$$\langle a\rangle, \langle a + b\rangle, \langle a + b + \nu c\rangle, \langle a + \nu b + \nu c\rangle, \nu \in K\backslash F.$$

Man berechnet:

- $s(a, a) = 0$,
- $s(a + b, a + b) = \lambda + \bar{\lambda} + 1 = 1 + 1 = 0$,
- $s(a + b + \nu c, a + b + \nu c) = s(a + b, a + b) + s(a + b, \nu c) + s(\nu c, a + b) = 0$,
- $s(a + \nu b + \nu c, a + \nu b + \nu c) = s(a + \nu b, a + \nu b) + s(a + \nu b, \nu c) + s(\nu c, a + \nu b)$
  $= (\bar{\nu}\lambda + \nu\bar{\lambda} + 1) + (\bar{nu}\lambda + \lambda) + (\nu\bar{\lambda} + \bar{\lambda}) = 0$,

wobei $\nu \in K\backslash F$ sei. ■

Abschließend zeigen wir noch, daß man im Fall $|F| > 3$ den in 3.1.4 auftretenden Unterraum W auch durch die Menge der isotropen Vektoren einer weiteren $^{-}$-hermiteschen Form $t \notin F \cdot d$ ersetzen kann.

Lemma 3.1.6 *Sei $|F| > 3$. Seien $d, s, t : V \times V \to K$ $^{-}$-hermitesche Formen, so daß*

(∗) *$d(z, z) = 0$ impliziert $s(z, z) = 0$ oder $t(z, z) = 0$ für alle $z \in V$.*

Dann gilt: $d(z, z) = 0$ impliziert $s(z, z) = 0$ für alle $z \in V$ oder $d(z, z) = 0$ impliziert $t(z, z) = 0$ für alle $z \in V$.

Beweis. Angenommen, es gibt $u, v \in V$ so, daß $d(u, u) = 0 \neq s(u, u)$ und $d(v, v) = 0 \neq t(v, v)$ gilt. Wir können $d(u, v) \in F$ annehmen. Setze $\mu := s(u, v)$ und $\nu := t(u, v)$.
(a) Für $\beta \in K$ und $z_\beta := u + \beta v$ gilt :
$d(z_\beta, z_\beta) = (\beta + \bar{\beta})d(u, v)$, $s(z_\beta, z_\beta) = s(u, u) + \bar{\beta}\mu + \beta\bar{\mu}$ und $t(z_\beta, z_\beta) = \beta\bar{\beta}t(v, v) + \bar{\beta}\nu + \beta\bar{\nu}$.
(b) Sei $\beta \in K^*$ mit $\bar{\beta} = -\beta$. Nach (a) gilt $d(z_\beta, z_\beta) = 0$. Folglich ist $s(z_\beta, z_\beta) = 0$ oder $t(z_\beta, z_\beta) = 0$, i.e. $\beta(\mu - \bar{\mu}) = s(u, u)$ oder $\beta t(v, v) + \nu - \bar{\nu} = 0$. Wegen $s(u, u) \neq 0 \neq t(v, v)$ ist $\beta \in \{s(u, u)/(\mu - \bar{\mu}), (\bar{\nu} - \nu)/t(v, v)\}$. Insbesondere folgt $|F^*| \leq 2$, ein Widerspruch. ■

3.2 Die Wall-Form

Definition 3.2.1 *Sei $\pi \in \mathrm{U}(f)$. Definiere*

$$f_\pi : \mathrm{B}(\pi) \times \mathrm{B}(\pi) \to K, \;\; f_\pi(a,b) := f(v,b)$$

wobei $a = v(\pi - 1)$ sei. Wir nennen f_π die zu π gehörige Wall-Form (cf. [73]).

Man sieht leicht, daß f_π nicht symmetrisch zu sein braucht. Jedoch ist f_π rechts- und linksregulär und additiv in beiden Argumenten. Es gilt $f_\pi(\mu a, b) = \mu \cdot f_\pi(a,b)$ und $f_\pi(a, \mu b) = \bar{\mu} \cdot f_\pi(a,b)$, i.e. f_π ist eine nichtentartete $^-$-Sesquilinearfom. Wir schreiben $q_\pi(a) := f_\pi(a,a)$. Das folgende zentrale und wohlbekannte Lemma ist einfach zu beweisen und zeigt, wie sich die Bahn-Dimension einer unitären Transformation durch Heranmultiplizieren einer unitären Symmetrie verringern läßt.

Lemma 3.2.2 *Sei $\pi \in \mathrm{U}(f)$.*

(a) *Erfüllt $a \in \mathrm{B}(\pi)$ die Bedingung $\alpha := q_\pi(a) \in F^*$, so ist die Symmetrie*

$$\sigma := \begin{cases} \sigma_a & , falls \; \mathrm{char}(K) \neq 2 \; ist, \\ \sigma_{\alpha^{-1},a} & , falls \; \mathrm{char}(K) = 2 \; ist, \end{cases}$$

wohldefiniert und erfüllt $\mathrm{F}(\pi\sigma_a) = \mathrm{F}(\pi) \oplus \langle y \rangle$, wobei $a = y(\pi - 1)$ ist. Insbesondere ist dann $\dim \mathrm{F}(\pi\sigma) = \dim \mathrm{F}(\pi) + 1$ *und* $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) - 1$.

(b) *Ist σ eine Symmetrie mit* $\dim \mathrm{F}(\pi\sigma) = \dim \mathrm{F}(\pi) + 1$*, so ist* $\mathrm{B}(\sigma) \leq \mathrm{B}(\pi)$ *und* $q_\pi(a) \in F^*$ *für* $a \in \mathrm{B}(\sigma)\backslash\{0\}$. ■

Eine wesentliche Idee zur Lösung der Frage, wann es zu einer unitären Isometrie π ein $a \in \mathrm{B}(\pi)$ mit $q_\pi(a) \in F^*$ gibt, stammt von E.W. Ellers [31] Abschnitt 4.. Sie besteht darin, zwei hermitesche Formen s und d zu definieren, die den Real- bzw. den Imaginärteil der Wall-Form f_π darstellen.

Definition 3.2.3 (Der Real- and Imaginär-Teil von q_π) *Sei $\pi \in \mathrm{U}(f)$. Wähle $i \in K^*$, so daß*

$$\bar{i} = \begin{cases} -i & , \text{falls char}(K) \neq 2 \text{ ist}, \\ i+1 & , \text{falls char}(K) = 2 \text{ ist}. \end{cases}$$

Definiere

$$d : \mathrm{B}(\pi) \times \mathrm{B}(\pi) \to K, \;\; d(a,b) := i \cdot f_\pi(a,b) + \overline{i \cdot f_\pi(b,a)}) = f(v\pi, b(\bar{i}\pi - i))$$

und

$$s : \mathrm{B}(\pi) \times \mathrm{B}(\pi) \to K, \;\; s(a,b) := (f_\pi(a,b) + \overline{f_\pi(b,a)}) = -f(a,b),$$

wobei $a = v(\pi - 1)$ sei.

Aus der Definition liest man ab, daß d und s wohldefinierte $^-$-hermitesche Formen auf $\mathrm{B}(\pi)$ sind. Es ist s-rad $\mathrm{B}(\pi) = f$-rad $\mathrm{B}(\pi) = \mathrm{F}(\pi) \cap B(\pi)$ und d-rad $\mathrm{B}(\pi) = \ker(\pi + i\bar{i}^{-1})$, i.e. d-rad $\mathrm{B}(\pi) = \mathrm{F}_{-1}(\pi)$, falls $\mathrm{char}(K) \neq 2$. Ferner gilt

$$f_\pi(a,b) = \begin{cases} \frac{1}{2}(s(a,b) + i^{-1}d(a,b)), & \text{,falls char}(K) \neq 2 \text{ ist}, \\ d(a,b) + \bar{i}s(a,b), & \text{,falls char}(K) = 2 \text{ ist}, \end{cases}$$

für alle $a, b \in \mathrm{B}(\pi)$. Folglich liefern s und d eine Zerlegung von q_π in Real- und Imaginärteil.

Lemma 3.2.4 *Sei* $\pi \in \mathrm{U}(f)\backslash\{1_V\}$ *und seien* s, d *wie in 3.2.3 definiert. Im Fall* $\mathrm{char}(K) = 2$ *sei* $\pi^2 \neq 1$. *Ist* $s = \lambda d$ *für ein* $\lambda \in F$, *so induziert* π *auf* $\mathrm{B}(\pi)$ *eine* μ*-homothetie für ein* $\mu \in K\backslash\{-1\}$ *mit* $\mu\bar{\mu} = 1$.

Beweis. Seien $y \in V$ und $a \in \mathrm{B}(\pi)$. Es gilt

$$\begin{aligned} f(y\pi, a(\pi - 1)) &= s(y(\pi - 1), a) = \lambda d(y(\pi - 1), a) \\ &= \lambda f(y\pi, a(\bar{i}\pi - i)), \end{aligned}$$

i.e. $f(y\pi, a((\lambda\bar{i} - 1)\pi - (\lambda i - 1)) = 0$.
Ist $\mathrm{char}(K) = 2$, so ist s-rad $\mathrm{B}(\pi) = \mathrm{rad}\ \mathrm{B}(\pi) \neq \mathrm{B}(\pi)$, da $\pi^2 \neq 1$, i.e. $s \neq 0$. Dies impliziert $\lambda \neq 0$ in diesem Fall. Wegen $\lambda \in F$ und $i \notin F$ schließen wir in jedem Fall $\nu := \lambda\bar{i} - 1 \notin \{k \in K, \bar{k} = -k\}$. Weil f regulär ist, folgt $\mathrm{B}(\pi) \leq \ker(\pi + \mu)$, wobei $\mu := \nu\bar{\nu}^{-1} \neq -1$. Wegen $\mathrm{B}(\pi) \neq \{0\}$ muß $\mu\bar{\mu} = 1$ sein. ∎

3.3 Grundlagen und triviale untere Schranken

Lemma 3.3.1 *Seien* π *und* σ_i *lineare Abbildungen von* V, *so daß* $\pi = \sigma_1 \cdots \sigma_k$. *Dann gilt* $\mathrm{B}(\pi) \leq \mathrm{B}(\sigma_1) + \cdots + \mathrm{B}(\sigma_k)$. *Sind zusätzlich alle* σ_i *einfach, so folgt* $\dim \mathrm{B}(\pi) \leq k$ *und Gleichheit herrscht genau dann, wenn* $\mathrm{B}(\pi) = \mathrm{B}(\sigma_1) \oplus \cdots \oplus \mathrm{B}(\sigma_k)$ *ist.* ∎

Aus 3.3.1 und wegen $\det \sigma = -1$ für jede unitäre Symmetrie σ erhalten wir unmittelbar untere Schranken für $l(\pi)$, $\pi \in \mathrm{U}^{\pm}(f)$.

Lemma 3.3.2 (Triviale untere Schranken.) *Seien* $\pi \in \mathrm{U}^{\pm}(f)$ *und* $m := \dim \mathrm{B}(\pi)$. *Ist* $(-1)^m = \det \pi$, *so ist* $\mathrm{l}(\pi) \geq m$. *Ist* $(-1)^m \neq \det \pi$, *so ist* $\mathrm{l}(\pi) \geq m + 1$. ∎

Lemma 3.3.3 *Seien* $\alpha, \beta \in \mathrm{U}(f)$. *Ist* $\mathrm{B}(\alpha) \cap \mathrm{B}(\beta) = \{0\}$, *so gilt* $\mathrm{B}(\alpha\beta) = \mathrm{B}(\alpha) \oplus \mathrm{B}(\beta)$. *Ist* α *eine Symmetrie und* $\mathrm{B}(\alpha) \nsubseteq \mathrm{B}(\beta)$, *so ist* $\mathrm{B}(\alpha\beta) = \mathrm{B}(\alpha) \oplus \mathrm{B}(\beta)$, *also* $\dim \mathrm{F}(\alpha\beta) = \dim \mathrm{F}(\beta) - 1$.

Beweis. Lineare Abbildungen $\alpha, \beta : V \to V$ erfüllen

$$\dim \mathrm{F}(\alpha\beta) \leq \dim \mathrm{F}(\alpha) \cap \mathrm{F}(\beta) + \dim \mathrm{B}(\alpha) \cap \mathrm{B}(\beta).$$

Nach Voraussetzung erhält man $\dim \mathrm{F}(\alpha\beta) \leq \dim \mathrm{F}(\alpha) \cap \mathrm{F}(\beta)$. Die Betrachtung der orthogonalen Komplemente liefert die erste Behauptung. Die zweite ist ein Spezialfall. ∎

Bemerkung 3.3.4 *Seien* $\mu \in K, \pi \in \mathrm{GL}(V)$ *und* $\sigma \in \mathrm{GL}(V)$ *eine einfache Abbildung. Dann gilt*

$$\dim \mathrm{F}_\mu(\pi\sigma) - 1 \leq \dim \mathrm{F}_\mu(\pi) \leq \dim \mathrm{F}_\mu(\pi\sigma) + 1.$$

Ist $\dim \mathrm{F}_\mu(\pi\sigma) + 1 = \dim \mathrm{F}_\mu(\pi)$, *so gilt* $\mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi) \cap \mathrm{F}(\sigma)$; *ist* $\dim \mathrm{F}_\mu(\pi\sigma) - 1 = \dim \mathrm{F}_\mu(\pi)$, *so gilt* $\mathrm{F}_\mu(\pi) = \mathrm{F}_\mu(\pi\sigma) \cap \mathrm{F}(\sigma)$. ∎

Bemerkung 3.3.5 *Seien* $\pi \in \mathrm{U}(f)$, σ *eine Symmetrie und* $\mu \in K^*$ *mit* $\mu\bar{\mu} = 1$. *Dann gilt:*

(a) $\dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi)$ *impliziert* $\mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi)$,

(b) $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) - 1 \leq \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) \leq \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) + 1$.

Beweis: (a). Aus $\dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi)$ folgt $\dim \mathrm{B}(\bar{\mu}\pi\sigma) = \dim \mathrm{B}(\bar{\mu}\pi)$, so daß wir $\mathrm{B}(\sigma) \leq \mathrm{B}(\bar{\mu}\pi)$ aus 3.3.3 schließen. Dies hat wiederum $\mathrm{B}(\bar{\mu}\pi\sigma) \leq \mathrm{B}(\bar{\mu}\pi) + \mathrm{B}(\sigma) = \mathrm{B}(\bar{\mu}\pi)$ zur Folge und die Gleichheit der Dimensionen erzwingt die Gleichheit der Räume. Wegen $\mu\bar{\mu} = 1$ ist $\bar{\mu}\pi$ in $\mathrm{U}(f)$ enthalten, und wir erhalten das gewünschte Ergebnis

$$\mathrm{F}_\mu(\pi\sigma) = \mathrm{B}(\bar{\mu}\pi\sigma)^\perp = \mathrm{B}(\bar{\mu}\pi)^\perp = \mathrm{F}_\mu(\pi).$$

(b). Ist $\dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi)$, so folgt aus (a) bereits $\mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi\sigma)$ und (b) ist in diesem Fall trivial. Ist $\dim \mathrm{F}_\mu(\pi\sigma) < \dim \mathrm{F}_\mu(\pi)$, so ist $H := \mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi) \cap \mathrm{F}(\sigma)$ eine Hyperebene von $\mathrm{F}_\mu(\pi)$. Sei $v \in \mathrm{F}_\mu(\pi) \backslash H$. Offenbar ist $H \cap \mathrm{rad}\ \mathrm{F}_\mu(\pi) \leq \mathrm{rad}\ H$, also $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) - 1 \leq \dim H \cap \mathrm{rad}\ \mathrm{F}_\mu(\pi) \leq \dim \mathrm{rad}\ H$, und $v^\perp \cap \mathrm{rad}\ H \leq \mathrm{rad}\ \mathrm{F}_\mu(\pi)$, also $\dim \mathrm{rad}\ H - 1 \leq \dim v^\perp \cap \mathrm{rad}\ H \leq \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi)$. Ist $\dim \mathrm{F}_\mu(\pi\sigma) > \dim \mathrm{F}_\mu(\pi) = \mathrm{F}_\mu((\pi\sigma)\sigma)$, so folgt die Behauptung aus Obigem mit π und $\pi\sigma$ in vertauschten Rollen. ■

Lemma 3.3.6 (a) *Seien $\pi \in \mathrm{U}(f), a \in \mathrm{B}(\pi) \backslash B^2(\pi)$ und $\alpha := q_\pi(a) \in F^*$, dann erfüllt*

$$\sigma := \begin{cases} \sigma_a & , falls\ \mathrm{char}(K) \neq 2\ ist, \\ \sigma_{\alpha^{-1},a} & , falls\ \mathrm{char}(K) = 2\ ist, \end{cases}$$

$\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ *und* $\dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) = \dim \mathrm{rad}\ \mathrm{B}(\pi) - 1$, *also* $\dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi)$.

(b) *Seien $\pi \in \mathrm{U}(f)$ and $\mu \in K \backslash \{1\}$, so daß $\mu\bar{\mu} = 1$ ist. Ist $a \in \mathrm{B}(\pi) \backslash \mathrm{B}(\pi)(\pi - \mu)$ mit $q_\pi(a) \in F^*$, so erfüllt die wie in* (a) *definierte Symmetrie σ* $\dim \mathrm{F}(\pi\sigma) > \dim \mathrm{F}(\pi)$ *und* $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi)$. *Falls $a \notin \mathrm{B}(\pi)(\pi - \mu) + F_\mu(\pi)$ ist, gilt zusätzlich* $\dim \mathrm{F}_\mu(\pi\sigma)/\mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi)/\mathrm{rad}\ \mathrm{F}_\mu(\pi)$.

Beweis. Für (a) siehe [47] ; Der Beweis in [47] wird für orthogonale Gruppen über Körpern der Charakteristik $\neq 2$ geführt, er läßt sich für unitäre Gruppen über Körpern mit beliebiger Charakteristik übertragen.

(b) Es gilt $\bar{\mu}\pi \in \mathrm{U}(V, f)$ und $\mathrm{F}_\mu(\pi) = \mathrm{F}(\bar{\mu}\pi)$. Weiterhin ist $\mathrm{B}(\bar{\mu}\pi) = V(\pi - \mu)$ und $\mathrm{B}(\pi) \cap V(\pi - \mu) = \mathrm{B}(\pi)(\pi - \mu)$, da $x - 1$ teilerfremd zu $x - \mu$ ist. Die Voraussetzung $\mathrm{B}(\sigma) \nsubseteq \mathrm{B}(\bar{\mu}\pi)$ und 3.3.3 zeigen, daß $\dim \mathrm{B}(\bar{\mu}\pi\sigma) = \dim \mathrm{B}(\bar{\mu}\pi) + 1$ ist. Folglich gilt $\dim \mathrm{F}(\bar{\mu}\pi\sigma) = \dim \mathrm{F}(\bar{\mu}\pi) - 1$, oder anders ausgedrückt: $\dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi) - 1$.

Sei schließlich

$$(*) \quad a \notin \mathrm{B}(\pi)(\pi - \mu) + F_\mu(\pi) = (\mathrm{B}(\bar{\mu}\pi) + \mathrm{F}_\mu(\pi)) \cap B(\pi) = \mathrm{rad}\mathrm{F}_\mu(\pi)^\perp \cap \mathrm{B}(\pi)$$

angenommen. Dann gilt $\mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi) \cap a^\perp$ und $\mathrm{B}(\bar{\mu}\pi\sigma) = \mathrm{B}(\bar{\mu}\pi) \oplus \langle a \rangle$. Dies ergibt

$$\begin{aligned} \mathrm{rad}\mathrm{F}_\mu(\pi\sigma) &= \mathrm{F}_\mu(\pi\sigma) \cap \mathrm{B}(\bar{\mu}\pi\sigma) = \mathrm{F}_\mu(\pi) \cap a^\perp \cap (\mathrm{B}(\bar{\mu}\pi) \oplus \langle a \rangle) \\ &\supseteq \mathrm{F}_\mu(\pi) \cap \mathrm{B}(\bar{\mu}\pi) \cap a^\perp = \mathrm{rad}\ \mathrm{F}_\mu(\pi) \cap a^\perp. \end{aligned}$$

Nimmt man an, daß die obige Inklusion echt ist, so findet man ein $b \in \mathrm{B}(\bar{\mu}\pi)$, so daß $b + a \in \mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) \subseteq \mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) \subseteq \mathrm{F}_\mu(\pi)$, i.e. $a \in (\mathrm{B}(\bar{\mu}\pi) + \mathrm{F}_\mu(\pi)) \cap \mathrm{B}(\pi)$, ein Widerspruch zu $(*)$. Folglich ist $\mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) = \mathrm{rad}\ \mathrm{F}_\mu(\pi) \cap a^\perp$. Wegen $(*)$ ist $\mathrm{rad}\ \mathrm{F}_\mu(\pi) \nsubseteq a^\perp$, also $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) \cap a^\perp = \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) - 1$. ■

Lemma 3.3.7

(a) *Sei $\mathcal{N}(K) = F$. Dann ist jeder reguläre* 2*-dimensionale Unterraum U von V eine hyperbolische Ebene.*

(b) *Ist die* u*-Invariante von $F \leq 2$, so gilt $\mathcal{N}(K) = F$.*

Beweis. Behauptung (a) erhält man durch einfaches Rechnen (cf. [69] Lemma 10.2, Seite 116) und (b) gilt, da die Norm-Abbildung eine reguläre quadratische Form auf dem 2-dimensionalen F-Vektorraum K ist. ■

3.4 $\mathrm{char}(K) \neq 2$

In diesem Abschnitt nehmen wir an, daß K ein Körper mit Charakteristik $\neq 2$ ist und verlangen, daß die Normabbildung von K surjektiv auf F ist.

Definition 3.4.1 *Sei $\pi \in \mathrm{U}^{\pm}(f)$. Nenne π lang, wenn π eine der folgenden Eigenschaften* (H) *oder* (T) *oder* (N) *hat. Andernfalls nenne π kurz.*

(H) $\pi \neq 1$ *und* $\pi|_{\mathrm{B}(\pi)}$ *ist eine μ-Homothetie, wobei $\mu \in K \backslash \{\pm 1\}$ ist;*

(T) $\pi \neq 1$ *und* $\mathrm{B}(\pi) \leq \mathrm{F}(\pi)$*;*

(N) $\dim \mathrm{B}(\pi)/\mathrm{F}_{-1}(\pi) = 1$ *und* $\mathrm{B}(\pi) \cap \mathrm{F}(\pi) = \{0\}$.

Dann hat π eine der folgenden Formen.

(H) $V = U \bigoplus X$, $\pi_U = \mu \cdot 1_U$ *für ein* $\mu \in K\backslash\{\pm 1\}$ *und* $\pi_X = 1_X$
(i.e. π induziert auf U eine Homothetie $\neq \pm 1$).

(T) $V = U_1 \bigoplus \ldots \bigoplus U_k \bigoplus X$, $k \geq 1$, $\dim U_i = 2$, π_{U_i} *ist eine Transvektion und* $\pi_X = 1_X$ *(, i.e. $\mathrm{B}(\pi) \neq \{0\}$ ist totalisotrop).*

(N) $V = U \bigoplus W \bigoplus X$, $\dim U = 2$, $-\pi_U$ *ist eine Transvektion,* $\pi_W = -1_W$ *und* $\pi_X = 1_X$.

Es tritt ein weiterer Typ auf, der eng mit dem Typ (N) verwandt ist. Er wird jedoch nicht zur Formulierung unserer Ergebnisse benötigt.
(N*) $\dim \mathrm{B}(\pi)/\mathrm{F}_{-1}(\pi) = 1$ und $\mathrm{B}(\pi) \cap \mathrm{F}(\pi) \neq \{0\} \neq \mathrm{F}_{-1}(\pi)$.
Eine andere Beschreibung lautet:
(N*) $V = U \bigoplus W \bigoplus X$, $\dim U = 2$, π_U ist eine Transvektion, $\dim W \geq 1$, $\pi_W = -1_W$ und $\pi_X = 1_X$.

Lemma 3.4.2 *Sei $\pi \in \mathrm{U}(f)$. Sei weiterhin W ein Teilraum von $\mathrm{B}(\pi)$, $W \neq \mathrm{B}(\pi)$. $\mathrm{B}(\pi)$ enthalte eine d-hyperbolische Ebene. Dann gibt es ein $a \in \mathrm{B}(\pi)\backslash W$, so daß $q_\pi(a) \in F^*$ ist, außer wenn π vom Typ* (H) *oder* (T) *ist.*

Beweis. Für $a \in \mathrm{B}(\pi)$ sind folgende Aussagen äquivalent:

(i) $q_\pi(a) \in F^*$;

(ii) $d(a, a) = 0$ und $s(a, a) \neq 0$.

Angenommen es gibt kein $a \in \mathrm{B}(\pi)\backslash W$ mit diesen Eigenschaften. Dann gilt: $d(a,a)=0$ impliziert s(a,a)=0 für alle $a \in \mathrm{B}(\pi)\backslash W$. Aus 3.1.3 folgt $s = \lambda d$ für ein $\lambda \in F$. Nun liefert 3.2.4 ein $\mu \in K^*\backslash\{-1\}$ mit $\mu\bar{\mu} = 1$ und $b\pi = \mu b$ für alle $b \in \mathrm{B}(\pi)$. Folglich ist π vom Typ (H) oder (T). ■

Lemma 3.4.3 *Sei $\pi \in \mathrm{U}^{\pm}(f)$ und $\pi^2 \neq 1$. Sei W ein Unterraum von* $\mathrm{B}(\pi)$, *$W \neq B(\pi)$. Dann gibt es ein $a \in \mathrm{B}(\pi)\backslash W$ mit $q_\pi(a) \in F^*$, außer wenn π vom Typ* (H) *oder* (T) *oder* (N) *oder* (N*) *ist.*

Beweis. Enthält $\mathrm{B}(\pi)$ eine d-hyperbolische Ebene, so folgt die Behauptung aus 3.4.2. Angenommen $\mathrm{B}(\pi)$ enthält keine d-hyperbolische Ebene. Dann ist $\dim \mathrm{B}(\pi)/d\text{-rad } \mathrm{B}(\pi) \leq 1$, da $\mathcal{N}(K) = F$ ist, cf. 3.3.7 . Weil π keine Involution ist, folgt $\dim \mathrm{B}(\pi)/\mathrm{F}_{-1}(\pi) = 1$. Wegen $\det \pi \in \{\pm 1\}$ hat die von π auf $\mathrm{B}(\pi)/\mathrm{F}_{-1}(\pi)$ induzierte Abbildung ebenfalls die Determinante ± 1. Deshalb muß π vom Typ (T) oder (N) oder (N*) sein. ■

Lemma 3.4.4 (Untere Schranken für lange Abbildungen) *Seien $\pi \in \mathrm{U}^{\pm}(f)$ lang und $m :=$* $\dim \mathrm{B}(\pi)$. *Dann gilt*

$$\mathrm{l}(\pi) \geq \begin{cases} m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{H})\ und\ \det \pi = (-1)^m\ ist, \\ m+1 & , falls\ \pi\ vom\ Typ\ (\mathrm{H})\ und\ \det \pi \neq (-1)^m\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{T})\ und\ \det \pi = (-1)^m\ ist, \\ m+3 & , falls\ \pi\ vom\ Typ\ (\mathrm{T})\ und\ \det \pi \neq (-1)^m\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{N})\ ist. \end{cases}$$

Beweis. Ist π vom Typ (H) und σ eine beliebige Symmetrie, so ist $\dim \mathrm{B}(\pi\sigma) = m$, falls $\mathrm{B}(\sigma) \leq \mathrm{B}(\pi)$ ist. Andernfalls ist $\dim \mathrm{B}(\pi\sigma) = m+1$ nach 3.3.3. Aus 3.3.2 angewandt auf $\pi\sigma$ folgt nun $\mathrm{l}(\pi\sigma) \geq m$, falls $-\det \pi = \det \pi\sigma = (-1)^m$ ist, und $\mathrm{l}(\pi\sigma) \geq m+1$, falls $-\det \pi = \det \pi\sigma \neq (-1)^m$ ist.

Ist π vom Typ (T), so ist $\mathrm{B}(\pi)$ totalisotrop, also gilt $\mathrm{B}(\sigma) \not\subseteq \mathrm{B}(\pi)$ für jede Symmetrie σ und demnach $\dim \mathrm{B}(\pi\sigma) = m+1$. Aus 3.3.2 folgt nun $\mathrm{l}(\pi\sigma) \geq m+1$, falls $m+1$ ungerade ist, und $\mathrm{l}(\pi\sigma) \geq m+2$, falls $m+1$ gerade ist.

Sei π vom Typ (N). Dann gilt $(-1)^m = \det \pi$, also ist $\mathrm{l}(\pi) = m+1$ nicht möglich und wir müssen nur zeigen, daß $\mathrm{l}(\pi) > m$ ist. Angenommen $\mathrm{l}(\pi) = m$, i.e. $\pi = \sigma_1 \cdots \sigma_m$ für Symmetrien σ_i. Dann ist $\mathrm{F}(\pi) = \mathrm{F}(\sigma_1) \cap \cdots \cap \mathrm{F}(\sigma_m)$. Weil $\mathrm{F}(\pi)$ regulär ist, können wir einfachheitshalber $F(\pi) = \{0\}$ annehmen. Dann gilt für mindestens eine Symmetrie $\sigma := \sigma_i$, $i \in \mathbb{N}_{\leq m}$, $\mathrm{B}(-\pi) \not\subseteq \mathrm{F}(\sigma)$. Da $\dim \mathrm{B}(-\pi) = 1$ ist, folgt $\mathrm{B}(-\pi) \cap \mathrm{F}(\sigma) = \mathrm{B}(-\pi) \cap \mathrm{B}(-\sigma) = \{0\}$. Nun impliziert 3.3.3 , daß $\mathrm{B}(\pi\sigma) = \mathrm{B}((-\pi)(-\sigma)) = \mathrm{B}(-\pi) \oplus \mathrm{B}(-\sigma) = \mathrm{B}(-\pi) \oplus \mathrm{F}(\sigma) = V = \mathrm{B}(\pi)$ ist. ■

3.4.1 $|F| > 3$

Satz 3.4.5 *Seien $|F| > 3$, $\pi \in \mathrm{U}(f)$ und $m := \dim \mathrm{B}(\pi)$. Dann ist π ein Produkt von Symmetrien.*
(a) *Ist π kurz, so gilt*

$$\mathrm{l}(\pi) = \begin{cases} m & , falls\ \det \pi = (-1)^m\ ist, \\ m+1 & , falls \det \pi \neq (-1)^m\ ist. \end{cases}$$

(b) *Ist π lang, so gilt*

$$\mathrm{l}(\pi) = \begin{cases} m+1 & , \textit{falls } \pi \textit{ vom Typ } (\mathrm{H}) \textit{ und } \det\pi \neq (-1)^m \textit{ ist,} \\ m+2 & , \textit{falls } \pi \textit{ vom Typ } (\mathrm{H}) \textit{ und } \det\pi = (-1)^m \textit{ ist,} \\ m+2 & , \textit{falls } \pi \textit{ vom Typ } (\mathrm{T}) \textit{ und } (-1)^m = 1 \textit{ ist,} \\ m+3 & , \textit{falls } \pi \textit{ vom Typ } (\mathrm{T}) \textit{ und } (-1)^m \neq 1 \textit{ ist,} \\ m+2 & , \textit{falls } \pi \textit{ vom Typ } (\mathrm{N}) \textit{ ist.} \end{cases}$$

$|F| > 3$**; Induktion**

Lemma 3.4.6 (Induktions-Lemma.) *Sei $\pi \in \mathrm{U}^{\pm}(f)$ und $\pi^2 \neq 1$.*

(a) *Ist π kurz, so gilt $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ für eine Symmetrie σ.*

(b) *Ist π kurz und $\dim \mathrm{B}(\pi) \geq 4$, so gibt es eine Symmetrie σ derart, daß $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma$ kurz ist.*

Beweis. (a) Sei π kurz. Falls π nicht vom Typ (N*) ist, liefern 3.4.3 (mit $W = \{0\}$) und 3.2.2 (a) eine Symmetrie σ' mit $\mathrm{F}(\pi\sigma') > \mathrm{F}(\pi)$. Ist π vom Typ vom (N*), so gilt $V = U \bigoplus W \bigoplus X$ für π-Moduln U, W, X, wobei $\dim U = 2, \pi_U$ eine Transvektion, $\pi_W = -1_W$, $\dim W \geq 1$ und $\pi_X = 1_X$ ist. Wir können daher eine Symmetrie σ' mit $\mathrm{B}(\sigma') \leq W$ wählen und erhalten $\mathrm{F}(\pi\sigma') > \mathrm{F}(\pi)$. Ist $\dim \mathrm{B}(\pi) \geq 3$, so ist $\pi\sigma'$ wiederum vom Typ (N*), also insbesondere kurz. Dies beweist (a).
Für den Beweis von (b) nehmen wir an, daß $\dim \mathrm{B}(\pi) \geq 4$ ist. Ist $\pi\sigma'$ kurz, so sind wir fertig. Wir können deshalb annehmen, daß $\pi\sigma'$ lang ist, i.e. zu einem der Typen (H), (T), (N) gehört. Insbesondere ist π nicht vom Typ (N*). Entsprechend dieser drei Fälle werden wir in unserem Beweis vorgehen. In (i), (ii) und (iii) sei σ eine beliebige Symmetrie mit $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$.
(i) Ist $\pi\sigma'$ vom Typ (H), so ist $\pi\sigma$ kurz oder vom Typ (H).
Beweis. Nach Voraussetzung gilt $\mathrm{F}_\mu(\pi\sigma') = \mathrm{B}(\pi\sigma')$ für ein $\mu \in K\backslash\{\pm 1\}$. Hieraus folgt $\dim \mathrm{F}_\mu(\pi) \geq \dim \mathrm{B}(\pi\sigma') - 1 = \dim \mathrm{B}(\pi) - 2 \geq 2$, also $\dim \mathrm{F}_\mu(\pi\sigma) \geq 1$. Folglich ist $\pi\sigma$ kurz oder vom Typ (H). ∎

Ist $\pi\sigma'$ vom Typ (H), so ist $\dim \mathrm{F}_\mu(\pi) \geq 2$ für ein $\mu \in K\backslash\{1, -1\}$. Insbesondere ist $\mathrm{B}(\pi)(\pi - \mu) \neq \mathrm{B}(\pi)$. Nach 3.4.3 gibt es ein $a \in \mathrm{B}(\pi)\backslash\mathrm{B}(\pi)(\pi - \mu)$, so daß $q_\pi(a) \in F^*$ ist. Dann erfüllt $\sigma := \sigma_a$ $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und nach 3.3.6 (b) auch $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) \neq 0$ (,da π nicht vom Typ (H) ist). Demnach ist $\pi\sigma$ nicht vom Typ (H) und (i) liefert, daß $\pi\sigma$ kurz ist.

(ii) Ist $\pi\sigma'$ vom Typ (T), so ist $\pi\sigma$ kurz oder vom Typ (T) .
Beweis. Aus 3.3.5 (b) erhalten wir $\dim\ \mathrm{radB}(\pi) \geq \dim \mathrm{B}(\pi\sigma') - 1 \geq 2$, also $\mathrm{radB}(\pi\sigma) \neq 0$. Somit ist $\pi\sigma$ kurz oder vom Typ (T). ∎

Ist $\pi\sigma'$ vom Typ (T) , so ist $\mathrm{B}(\pi\sigma')$ totalisotrop und $\mathrm{radB}(\pi) \neq \{0\}$. Insbesondere ist $\mathrm{B}^2(\pi) \neq \mathrm{B}(\pi)$. Nach und 3.4.3 gibt es ein $a \in \mathrm{B}(\pi)\backslash\mathrm{B}^2(\pi)$, so daß $q_\pi(a) \in F^*$ ist. Nach 3.3.6 (a) gilt $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \neq 0$ (,da π nicht vom Typ (T) ist). Demnach ist $\pi\sigma$ nicht vom Typ (T). Aus (ii) folgt, daß $\pi\sigma$ kurz ist.

(iii) Ist $\pi\sigma'$ vom Typ (N), so ist $\pi\sigma$ kurz oder vom Typ (N).
Dies folgt aus (i) und (ii) mit σ und σ' in vertauschten Rollen.

Betrachte nun den Fall, daß $\pi\sigma'$ vom Typ (N) ist. Analog zum ersten Fall finden wir eine Symmetrie σ mit $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_{-1}(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{F}_{-1}(\pi) > 1$ (,da π keine Involution und nicht vom Typ (N) oder (N*) ist). Somit ist $\pi\sigma$ nicht vom Typ (N) und (iii) zeigt, daß $\pi\sigma$ kurz ist. ■

Bahndimension ≤ 2 **außer Typ** (T)

Bemerkung 3.4.7 *Es sei* $\dim V = 2$.

(a) *Ist* $\tau \in \mathrm{U}(f)$ *eine Transvektion, so besitzt* V *eine Basis* $\{v, v(\pi-1)\}$ *derart, daß* v *und* $v(\pi-1)$ *isotrop sind und* $f(v, v(\pi-1)) = -\overline{f(v, v(\pi-1))}$ *ist.*
(b) *Ist* $\pi \in \mathrm{U}(f)$ *zyklisch mit* $\mathrm{mip}(\pi) = x^2 + \alpha x - 1$, *so besitzt* V *eine Basis* $\{v, v\pi\}$ *derart, daß* v *und* $v\pi$ *isotrop sind und* $f(v, v\pi) = \overline{f(v, v\pi)}$ *ist. Weiterhin gilt* $\alpha = -\bar{\alpha}$.

Beweis. Die Behauptung folgt unmittelbar aus der Tatsache, daß V von isotropen Vektoren erzeugt wird und das Minimalpolynom von π $^{-}$-symmetrisch ist. ■

Lemma 3.4.8 *Sei* $\pi \in \mathrm{U}(f)$ *vom Typ* (N*). *Dann ist* $\mathrm{l}(\pi) = \dim \mathrm{B}(\pi) + 1$.

Beweis. Betrachte zunächst den Fall $\dim \mathrm{B}(\pi) = 2$. Wir können dann annehmen, daß $\dim V = 3$ und π zyklisch mit $\mathrm{mip}(\pi) = (x-1)^2(x+1)$ ist. Nach 3.4.7 gibt es eine Basis $\mathcal{B}$ von V, so daß

$$\mathcal{M}_{\mathcal{B}}(\pi) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \text{ and } \mathcal{M}_{\mathcal{B}}(f) = \begin{bmatrix} 0 & \beta & 0 \\ \bar{\beta} & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

für ein β mit $\bar{\beta} = -\beta$ gilt. Wähle $a := (0,1,1) \in V$ und $\sigma := \sigma_a$. Man berechnet dann $\mathrm{mip}(\pi\sigma) = (x-1)^3$, und 3.4.6 (a) zeigt, daß $\mathrm{l}(\pi\sigma) = 2$ ist. Folglich ist $\mathrm{l}(\pi) = 3$.
Der allgemeine Fall läßt sich leicht auf den gerade behandelten reduzieren. ■

Lemma 3.4.9 *Ist* $\pi \in \mathrm{U}^{\pm}(f)$ *lang und* $\dim V = 2$, *so ist* $\pi\sigma$ *kurz für jede Symmetrie* σ.

Beweis. Sei σ eine Symmetrie. Falls π vom Typ (T) oder (N) ist, so gilt $\det \pi\sigma = -1$ und $\mathrm{F}_{\mu}(\pi) = \{0\}$ für alle $\mu \in K\backslash\{\pm 1\}$, also ist $\pi\sigma$ kurz. Ist π vom Typ (H), so ist $\det \pi\sigma = 1$ und $\dim \mathrm{F}_{\mu}(\pi\sigma) = 1$ für ein $\mu \in K\backslash\{\pm 1\}$. Hieraus folgt, daß $\pi\sigma$ kurz ist. ■

Lemma 3.4.10 *Seien* $\pi \in \mathrm{U}(f)$, $\dim V = 2$ *und* $\det \pi = -1$. *Falls* $|F| > 3$ *ist, ist* $\pi\sigma$ *kurz für eine Symmetrie* σ.

Beweis. Wir können annehmen, daß π keine Symmetrie und auch keine Homothetie ist. Dann ist π zyklisch und hat ein Minimalpolynom $x^2+\alpha x-1$, wobei $\bar{\alpha} = -\alpha \neq 0$ ist. Sei $\epsilon \in \{\pm 1\}$. Beachte, daß

$\epsilon\pi - 1$ zu $\mathrm{GL}(V)$ gehört. Es gibt eine Basis $\{v, v\pi\}$ von V, so daß v isotrop und $\beta := f(v, v\pi) \in F^*$ ist; cf. 3.4.7 (b). Wir erhalten $q_{\epsilon\pi}(w) = -\alpha^{-1}\beta(\delta+\epsilon)(\bar{\delta}+\epsilon) - \bar{\delta}\beta$ für $w = v + \delta v\pi$. Ist $|F| > 3$, so wähle ein $\delta \in F^*\backslash\{\pm 1\}$. Dann gilt $q_{\epsilon\pi}(w) \in K\backslash F$ und $f(w,w) \neq 0$; somit ist $\sigma := \sigma_w$ wohldefiniert und $\mathrm{F}_\epsilon(\pi\sigma) = \{0\}$; cf. 3.2.2 (b) . Weiterhin ist $\det \pi\sigma = 1$ und $\pi\sigma$ damit kurz. ■

Bemerkung 3.4.11 *Seien* $\pi \in \mathrm{U}(f), \dim V = 2$ *und* $\det \pi = -1$*. Falls* $|F| = 3$ *und* π *weder eine Symmetrie noch eine Homothetie ist, ist* $\pi\sigma$ *oder* $-\pi\sigma$ *eine Transvektion für jede Symmetrie* σ*. Ferner ist* π *kein Produkt von Symmetrien.*

Beweis. Wir setzen den obigen Beweis an der Stelle fort, wo $|F| > 3$ benutzt wurde. Jeder reguläre 1-dimensionale Vektorraum von V wird von einem Vektor $w = v + \delta v\pi$ mit $\delta + \bar{\delta} \in F^*$ erzeugt. Für eine beliebige Symmetrie $\sigma = \sigma_w$, zeigt die obige Formel für $q_{\epsilon\pi}(w)$, daß $q_{\epsilon\pi}(w) \in F^*$ für $\epsilon = 1$ oder $\epsilon = -1$ gilt [Wegen $\alpha^3 = \bar{\alpha} = -\alpha$ ist $-\alpha^{-1} = \alpha$ und es gibt $\mu, \nu \in F$, so daß $\delta = \mu + \nu\alpha$ ist. Dann ist $\mu = \frac{\delta+\bar{\delta}}{2} \in \mathrm{F}^* = \{1, -1\}$. Man berechnet nun $q_{\epsilon\pi}(w) = \mu\beta + ((\mu+\epsilon)^2 + \nu^2 + \nu)\alpha\beta$. Ist $\nu \in \{0, -1\}$, so wähle $\epsilon := -\mu$. Ist $\nu = 1$, wähle $\epsilon := \mu$.] Folglich ist $\mathrm{F}_\epsilon(\pi\sigma) \neq 0$ für $\epsilon = 1$ oder $\epsilon = -1$; cf. 3.2.2 (a). Wegen $\det \pi\sigma = 1$ folgt hieraus der erste Teil der Behauptung. Sei ρ eine weitere Symmetrie. Aus 3.4.9 erhalten wir, daß $\psi := \pi\sigma\rho$ kurz ist. Wegen $\mathrm{l}(\pi\sigma) \neq 2$ (cf. 3.4.4), ist ψ keine Symmetrie. Demnach hat auch ψ die von π geforderten Eigenschaften. Dies beweist den zweiten Teil der Behauptung. ■

Proposition 3.4.12 *Sei* $\pi \in \mathrm{U}^{\pm}(f)$ *kurz mit* $\dim \mathrm{B}(\pi) = 2$*. Ist* $\det \pi = 1$*, so ist* $\mathrm{l}(\pi) = 2$*. Ist* $|F| > 3$ *und* $\det(\pi) = -1$*, so gilt* $\mathrm{l}(\pi) = 3$*.*

Beweis. Die Länge kann nicht kleiner als angegeben sein, cf. 3.3.2. Sei $\det \pi = 1$. Lemma 3.4.6 (a) liefert eine Symmetrie σ, so daß $\dim \mathrm{B}(\pi\sigma) = 1$ ist. Wegen $\det \pi\sigma = -1$ ist $\pi\sigma$ eine Symmetrie. Sei nun $|F| > 3$ und $\det \pi = -1$ angenommen. Wir behaupten:

(+) $\dim \mathrm{B}(\pi\rho) = 2$ und $\pi\rho$ kurz ist für eine geeignete Symmetrie ρ.

Aus (+) folgt dann die Behauptung, da $\pi\rho$ nach dem vorherigen ein Produkt von zwei Symmetrien ist. Falls $\mathrm{B}(\pi)$ regulär ist, kann man $V = \mathrm{B}(\pi)$ annehmen und 3.4.10 beweist (+). Ist $\mathrm{B}(\pi)$ nicht regulär, so ist π vom Typ (N^*) und 3.4.8 liefert (+). ■

Wir betrachten nun die Situation, daß $\dim \mathrm{B}(\pi) = 2$ und π lang ist.

Lemma 3.4.13 *Seien* $|F| > 3$ *und* $\pi \in \mathrm{U}^{\pm}(f)$ *mit* $\dim \mathrm{B}(\pi) = 2$*.*
Ist π *vom Typ* (H)*, so ist* $\mathrm{l}(\pi) = 3$*.*
Ist π *vom Typ* (N)*, so ist* $\mathrm{l}(\pi) = 4$*.*

Beweis. Falls π vom Typ (H) oder (N) ist, liefert 3.4.9 eine Symmetrie σ, so daß $\pi\sigma$ kurz und $\dim \mathrm{B}(\pi) = 2$ ist. Die Behauptung folgt dann aus 3.4.12 und 3.4.4. ■

Für $\dim \mathrm{B}(\pi) = 2$ haben wir $l(\pi)$ bestimmt, außer wenn π vom Typ (T) ist. Diesen Fall werden wir in Abschnitt 3.4.1 behandeln.

Bahndimension 3 außer lange Abbildungen

Lemma 3.4.14 *Sei* $\pi \in \mathrm{U}^{\pm}(f)$ *kurz und* $\dim \mathrm{B}(\pi) = 3$. *Ist* $\det \pi = -1$ *und* $\mathrm{F}_{-1}(\pi) \neq \{0\}$, *so gilt* $\mathrm{l}\,(\pi) = 3$.

Beweis. Ist $\mathrm{F}_{-1}(\pi) = \mathrm{B}(\pi)$, i.e. π eine Involution, so ist π ein Produkt von drei Symmetrien, deren Bahnen paarweise orthogonal in $\mathrm{B}(\pi)$ sind. Der Fall $\dim \mathrm{F}_{-1}(\pi) = 2$ ist nicht möglich, da $\det \pi = -1$ ist und π nicht zum Typ (N) gehört. Sei also $\dim \mathrm{F}_{-1}(\pi) = 1$ angenommen.
Fall 1: $\mathrm{F}_{-1}(\pi)$ ist regulär. Dann gilt $V = U \bigoplus W \bigoplus X$ für π-Moduln U, W und X, wobei $U = \mathrm{F}_{-1}(\pi)$, $\dim \mathrm{B}(\pi_W) = 2, \det(\pi_W) = 1, \mathrm{F}_{-1}(\pi_W) = \{0\}$ und $\pi_X = 1_X$ ist. Ist π_W kurz, wähle $\sigma := -1_U \bigoplus 1_{W \oplus X}$. Dann ist $\pi\sigma$ kurz, $\dim \mathrm{B}(\pi\sigma) = 2$, und 3.4.12 beweist die Behauptung. Sei nun angenommen, daß π_W lang ist. Dann ist π_W vom Typ (T), i.e. $W = W_1 \bigoplus W_2$ und π_{W_1}, π_{W_2} sind Transvektionen. Da $\mathrm{B}^2(\pi) \neq \mathrm{B}(\pi)$ ist, gibt es nach 3.4.3 einen Vektor $a \in \mathrm{B}(\pi) \backslash \mathrm{B}^2(\pi)$, so daß $q_\pi(a) \in F^*$ ist. Die Symmetrie $\sigma := \sigma_a$ erfüllt dann $\dim \mathrm{B}(\pi\sigma) = 2$ und $\dim \mathrm{B}(\pi\sigma)/\mathrm{radB}(\pi\sigma) = 1$, cf. 3.2.2 (a) and 3.3.6 (a). Wegen $\det \pi\sigma = 1$ impliziert dies, daß $\pi\sigma$ zyklisch mit Minimalpolynom $(x-1)^3$ ist. Insbesondere ist $\pi\sigma$ kurz und 3.4.12 ergibt $\mathrm{l}(\pi\sigma) = 2$, also $\mathrm{l}(\pi) = 3$.
Fall 2: $\mathrm{F}_{-1}(\pi)$ ist singulär. Dann ist $(x+1)^k$ ein Teiler von $\mathrm{mip}(\pi)$ für ein $k \geq 2$. Wegen $\dim \mathrm{B}(\pi) = 3$ und $\det \pi = -1$ muß $k = 3$ sein. Somit gilt $V = U \bigoplus X$, π_U ist zyklisch mit Minimalpolynom $(x+1)^3$ und $\pi_X = 1_X$. Dann ist $-\pi_U$ kurz, $\dim \mathrm{B}(-\pi_U) = 2$ und $\det -\pi_U = 1$. Aus 3.4.12 folgt $-\pi_U = \rho\sigma$ für geeignete Symmetrie ρ, σ. Weil $-\rho$ ein Produkt von zwei Symmetrien ist (Beachte, daß $\dim U = 3$ ist!), schließen wir $\mathrm{l}(\pi) = \mathrm{l}(\pi_U) = 3$.

Lemma 3.4.15 *Sei* $\pi \in \mathrm{U}(V, f)$ *kurz mit* $\dim \mathrm{B}(\pi) = 3$. *Falls* $\det \pi = -1$, $\mathrm{F}_{-1}(\pi) = \{0\}$ *und* $\mathrm{B}(\pi)$ *regulär ist, gilt* $\mathrm{l}(\pi) = 3$.

Beweis. Wir können $\dim V = 3$ annehmen. Weil π kurz ist, gibt es eine Symmetrie σ, so daß $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ ist. Angenommen $\pi\sigma$ ist vom Typ (N). Wähle dann ein $a \in V$, so daß $\mathrm{B}(\sigma) = \langle a(\pi^2 - 1)\rangle$ ist. Dann ist $\mathrm{F}_{-1}(\pi\sigma) = \langle a(\pi - 1)\rangle$ isotrop; cf.3.2.2 (angewandt auf $-\pi$). Hieraus erhalten wir

$$q_\pi(a(\pi-1)^2) = f(a(\pi-1), a(\pi-1)(\pi-1)) = f(a(\pi-1), a(\pi-1)(\pi+1)) = -q_{-\pi}(a(\pi^2-1)) \in F^*.$$

Sei σ' die Symmetrie mit $\mathrm{B}(\sigma') = \langle a(\pi-1)^2\rangle$. Dann ist $\mathrm{F}(\pi\sigma') = \langle a(\pi-1)\rangle$ isotrop, also $(x-1)^2$ ein Teiler von $\mathrm{mip}(\pi\sigma')$. Nun folgert man aus $\dim V = 3, \dim \mathrm{B}(\pi\sigma') = 2$ und $\det \pi\sigma' = 1$, daß $\mathrm{mip}(\pi\sigma') = (x-1)^3$ ist. Also ist $\pi\sigma'$ kurz. Nun zeigt 3.4.12, daß $\mathrm{l}(\pi\sigma') = 2$ ist. ∎

Korollar 3.4.16 *Ist* $\pi \in \mathrm{U}(f)$ *kurz,* $\det \pi = -1, \dim \mathrm{B}(\pi) = 3$ *und* $\mathrm{B}(\pi)$ *regulär, so ist* $\mathrm{l}(\pi) = 3$.

Beweis. Für $\mathrm{F}_{-1}(\pi) \neq 0$ liefert 3.4.14 das Ergebnis. Andernfalls folgt die Behauptung aus 3.4.15. ∎

Lemma 3.4.17 *Sei* $\pi \in \mathrm{U}(f)$ *und* $V = U \bigoplus W$ *für* π*-Moduln* U *und* W *mit* $\dim U = 2 = \dim W$. *Es sei* π_U *eine Transvektion,* π_W *keine Homothetie,* $\det \pi_W = -1$ *und* $\mathrm{B}(\pi_W)$ *regulär. Ist* $|F| > 3$, *so ist* $\mathrm{l}(\pi) = 3$. *Falls* $|F| = 3$ *ist, findet man eine Symmetrie* σ, *für die* $\dim \mathrm{B}(\pi\sigma) = 1$ *gilt und* $\pi\sigma$ *zum Typ* (N) *gehört.*

Beweis. Die Abbildung π_W ist zyklisch mit Minimalpolynom $x^2+\lambda x-1$, wobei $\bar{\lambda}=-\lambda$ ist. Nach 3.4.7 gibt es eine Basis $\mathcal{B}$ von V, so daß sich folgende Koordinatendarstellung ergibt:

$$\mathcal{M}_{\mathcal{B}}(\pi)=\begin{bmatrix} 1 & 1 & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & -\lambda \end{bmatrix} \text{ and } \mathcal{M}_{\mathcal{B}}(f)=\begin{bmatrix} 0 & \omega & & \\ \bar{\omega} & 0 & & \\ & & 0 & \nu \\ & & \nu & 0 \end{bmatrix}.$$

Dabei gilt $\bar{\omega}=-\omega\in K^*$ und $\bar{\nu}=\nu\in F^*$. Sei $\gamma\in K$. Wähle $\alpha\in K$, so daß $\alpha\bar{\alpha}=-(\nu\lambda/4\omega)(\gamma\bar{\gamma}+1+\gamma+\bar{\gamma}+2^{-1}\lambda(\gamma-\bar{\gamma}))$ ist, cf.3.3.7. Für $z=(\alpha,0,\gamma,1)\in V$ und $a:=z(\pi-1)(\pi+1)=z(\pi^2-1)$ berechnet man

$$\begin{aligned} q_\pi(a) &= f(z(\pi+1),z(\pi^2-1))=2^{-1}\nu\lambda^2(\gamma+\bar{\gamma})\in F, \\ q_{-\pi}(a) &= -f(z(\pi-1),z(\pi^2-1))=\nu\lambda(\gamma\bar{\gamma}+1-(\gamma+\bar{\gamma})+\gamma\lambda). \end{aligned}$$

Sei zunächst $|F|>3$. Wähle $\gamma\in F^*\backslash\{\pm1\}$, Dann ist $\alpha\bar{\alpha}=-(\nu\lambda/4\omega)(\gamma+1)^2$ und $q_\pi(a)=\nu\lambda^2\gamma\in F^*$, $q_{-\pi}(a)=\nu\lambda(\gamma-1)^2+\nu\gamma\lambda^2\notin F$ und (wegen $\alpha\neq0$) $a\in \mathrm{B}(\pi)\backslash W$. Somit erfüllt $\sigma:=\sigma_a$ nach 3.2.2 $\dim\mathrm{B}(\pi\sigma)=2$. Aus 3.2.2 (b) und $q_{-\pi}(a)\notin F$ folgt $\dim\mathrm{F}_{-1}(\pi\sigma)=0$. Deshalb ist $-\pi\sigma$ keine Transvektion. Weiterhin gilt $a\in\mathrm{B}(\pi)\backslash\mathrm{B}^2(\pi)$, da $B^2(\pi)=W$ ist. Somit ist $\pi\sigma$ nicht vom Typ (T); cf. 3.3.6 (a). Demnach ist $\pi\sigma$ kurz und 3.4.12 ergibt $\mathrm{l}(\pi\sigma)=3$.
Ist $|F|=3$, so wähle $\gamma:=1+\lambda$. Dann gilt $q_{-\pi}(a)=-\nu=q_\pi(a)\in F^*$ und $\alpha\bar{\alpha}=-(\nu\lambda/4\omega)\neq0$. Die Symmetrie $\sigma:=\sigma_a$ erfüllt dann $\dim\mathrm{B}(\pi\sigma)=2$, $\dim\mathrm{F}_{-1}(\pi\sigma)=1$ (cf. 3.2.2 (a)). Wegen $\alpha\neq0$ ist $a\in\mathrm{B}(\pi)\backslash\mathrm{B}^2(\pi)$, so daß $\pi\sigma$ nicht vom Typ (N*) ist; cf. 3.3.6 (a). Folglich gehört $\pi\sigma$ zum Typ (N). ■

Lemma 3.4.18 *Seien $|F|>3$, $\pi\in\mathrm{U}(f)$ und $\dim\mathrm{B}(\pi)=3$. Falls $\det(\pi)=-1$, $\mathrm{F}_{-1}(\pi)=\{0\}$ und $B(\pi)$ singulär ist, gilt $\mathrm{l}(\pi)=3$.*

Beweis. Zunächst halten wir fest, daß $\mathrm{B}(\pi)$ nicht totalisotrop und $\dim\ \mathrm{rad}\ \mathrm{B}(\pi)\neq2$ ist (Dies folgt unmittelbar aus $\det\pi=-1$, $\dim\mathrm{B}(\pi)=3$ und $\mathrm{F}_{-1}(\pi)=\{0\}$). Dies liefert $\dim\ \mathrm{rad}\ \mathrm{B}(\pi)=1$. Demnach gibt es eine Zerlegung $V=U\oplus W\oplus X$, wobei $\dim U=2$, π_U eine Transvektion und $\mathrm{B}(\pi_W)=W$ ein zweidimensionaler Raum mit $\mathrm{F}_{-1}(\pi_W)=\{0\}$ und $\det\pi_W=-1$ ist. Weiterhin ist $\pi_X=1_X$ und wir können $X=\{0\}$ annehmen. Ist π_W keine Homothetie, so liefert 3.4.17 die Behauptung. Nehmen wir nun an, daß π_W eine μ-Homothetie ist, so gibt es nach Lemma 3.4.6 (a) eine Symmetrie σ mit $\dim\mathrm{B}(\pi\sigma)=2$ und $\det\pi\sigma=1$. Ferner ist $\mathrm{F}_\mu(\pi\sigma)\neq0$. Deshalb ist $\pi\sigma$ kurz und $\mathrm{l}(\pi\sigma)=2$ nach 3.4.12, also $\mathrm{l}(\pi)=3$. ■

Proposition 3.4.19 *Seien $|F|>3$, $\pi\in\mathrm{U}^{\pm}(f)$ kurz und $\dim\mathrm{B}(\pi)=3$. Für $\det\pi=-1$ ist $\mathrm{l}(\pi)=3$ und für $\det\pi=1$ ist $\mathrm{l}(\pi)=4$.*

Beweis. Sei zunächst $\det\pi=-1$ angenommen. Ist $\mathrm{F}_{-1}(\pi)\neq\{0\}$, wende cf. 3.4.14 an; andernfalls liefern 3.4.15 (für reguläre Bahn) und 3.4.18 (für singuläre Bahn) das gewünschte Ergebnis. Sei nun $\det\pi=1$ angenommen. Nach 3.4.6 (a) gibt es eine Symmetrie σ, so daß $\dim\mathrm{B}(\pi\sigma)=2$ und $\det\pi\sigma=-1$ ist. Damit ist $\pi\sigma$ nicht vom Typ (T) oder (N). Folglich ist $\pi\sigma$ vom Typ (H) oder kurz, und 3.4.13 und 3.4.12 ergeben $\mathrm{l}(\pi\sigma)=3$. ■

Beweis des Satzes

Seien $\pi \in \mathrm{U}^{\pm}(f)$ und $m := \dim \mathrm{B}(\pi)$. Nach 3.3.2 und 3.4.4 kann $\mathrm{l}(\pi)$ nicht kleiner als behauptet sein. Der Beweis von 3.4.5 erfolgt durch Induktion über $\dim \mathrm{B}(\pi)$.
(i) Wir betrachten zuerst den Fall, daß π kurz ist. Ist $\dim \mathrm{B}(\pi) \leq 3$, so liefern 3.4.12 (für $\dim \mathrm{B}(\pi) = 2$) und 3.4.19 (für $\dim \mathrm{B}(\pi) = 3$) die Behauptung. Wir können daher $\dim \mathrm{B}(\pi) \geq 4$ annehmen. Ist π eine Involution, so ist π das Produkt von m Symmetrien, deren Bahnen paarweise orthogonal in $\mathrm{B}(\pi)$ sind. Wir können daher $\pi^2 \neq 1_V$ annehmen. Nach 3.4.6 b) gibt es dann eine Symmetrie σ, so daß $\dim \mathrm{B}(\pi\sigma) = m - 1$ und $\pi\sigma$ kurz ist. Nach Induktionsannahme gilt dann $\mathrm{l}(\pi\sigma) = m - 1$ (für $\det \pi\sigma = (-1)^{m-1}$) oder $\mathrm{l}(\pi\sigma) = m$ (für $\det \pi\sigma \neq (-1)^{m-1}$), also $\mathrm{l}(\pi) = m$ beziehungsweise $\mathrm{l}(\pi) = m + 1$.
(ii) Sei schließlich π eine lange Abbildung. Dann gilt $V = U \oplus W$ für π-Moduln U und W, wobei $\dim U = 2$ und π_U eine Transvektion oder eine negative Transvektion oder eine μ-Homothetie für ein $\mu \in K \backslash \{\pm 1\}$ ist. Man findet nun eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq U$, so daß $\pi\sigma$ kurz ist. Weiterhin gilt dann $\dim \mathrm{B}(\pi\sigma) = m$, falls π is vom Typ (H) oder (N) ist, und $\dim \mathrm{B}(\pi\sigma) = m + 1$, falls π vom Typ (T) ist. Die Behauptung folgt nun aus (i). ∎

3.4.2 $|F| = 3$

In diesem Abschnitt setzen wir $|F| = 3$ voraus. Wie bereits aus 3.4.11 ersichtlich, treten in diesem Fall weitere lange Abbildungen auf. Es stellt sich heraus, daß 3.4.11 bereits auf alle weiteren Ausnahmeabbildungen führt. Dies präzisieren wir in der

Definition 3.4.20 *Seien $\pi \in \mathrm{U}(f)$ und $\tilde{\pi}$ die von π auf $\mathrm{B}(\pi)/\mathrm{radB}(\pi)$ induzierte Abbildung. Nenne π lang, falls π lang im Sinne von 3.4.1 ist oder wenn $\dim \mathrm{B}(\pi)/\mathrm{radB}(\pi) = 2$ und $\tilde{\pi}$ unzerlegbar ist. Somit gilt:*
(S1) $\mathrm{mip}(\tilde{\pi}) = (x - \alpha)^2$ *für ein* $\bar{\alpha} = -\alpha \neq 0$
oder
(S2) $\mathrm{mip}(\tilde{\pi}) = (x - 1)^2$, *i.e. $\tilde{\pi}$ ist eine Transvektion,*
oder
(S3) $\mathrm{mip}(\tilde{\pi}) = (x + 1)^2$, *i.e. $\tilde{\pi}$ ist eine negative Transvektion.*
Dann hat π eine der folgenden Formen (S1) oder (S2) oder (S3).

(S1) *$V = U \oplus W$, $\dim U = 2$, $\bar{\alpha}\pi_U$ ist eine Transvektion mit $\bar{\alpha} = -\alpha \in K^*$ (insbesondere ist $\det_{\pi_U} = -1$) und π_W ist vom Typ (T) oder 1_W.*
(S2) *$V = U \oplus W$, $\dim U = 4$, π_U ist zyklisch mit $\mathrm{mip}(\pi_U) = (x - 1)^4$ und π_W ist vom Typ (T) oder 1_W.*
(S3) *$V = U \oplus W$, $\dim U = 2$, π_U ist eine negative Transvektion und π_W ist vom Typ (T) oder 1_W.*

Wir sagen, daß π vom Typ (S) *ist, wenn π vom Typ* (S1) *oder* (S2) *oder* (S3) *ist.*

Weiterhin, nennen wir π lang vom Typ (M), *wenn $V = U \oplus W \oplus X$, $\dim U = 2 = \dim W$ und $\mathrm{mip}(\pi_U) = (x - \nu)^2 = \mathrm{mip}(\pi_W)$ für ein $\nu \in K^*$ mit $\bar{\nu} = -\nu$ und $\pi_X = 1_X$. Eine Isometrie, welche nicht lang ist, nennen wir kurz.*

Satz 3.4.21 *Seien* $|F| = 3$, $\pi \in \mathrm{U}(f)$ *und* $m := \dim \mathrm{B}(\pi)$.
(a) *Ist* π *kurz, so gilt*

$$\mathrm{l}(\pi) = \begin{cases} m & , falls\ \det \pi = (-1)^m\ ist, \\ m+1 & , falls\ \det \pi \neq (-1)^m\ ist. \end{cases}$$

(b) *Ist* π *lang, so gilt*

$$\mathrm{l}(\pi) = \begin{cases} m+1 & , falls\ \pi\ vom\ Typ\ (\mathrm{H})\ und\ (-1)^m \neq \det \pi\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{H})\ und\ (-1)^m = \det \pi\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{T}),\ \dim V \geq 3\ und\ (-1)^m = 1\ ist, \\ m+3 & , falls\ \pi\ vom\ Typ\ (\mathrm{T}),\ \dim V \geq 3\ und\ (-1)^m \neq 1\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{N})\ und\ \dim V \geq 3\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{S}),\ \dim V \geq 3\ und\ (-1)^m = \det(\pi)\ ist, \\ m+3 & , falls\ \pi\ vom\ Typ\ (\mathrm{S}),\ \dim V \geq 3\ und\ (-1)^m \neq \det(\pi)\ ist, \\ 6 = m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{M})\ ist. \end{cases}$$

(c) *Falls* $\dim V = 2$ *und* $\det \pi = -1$ *und* π *weder eine Symmetrie noch eine Homothetie ist, so ist* π *kein Produkt von Symmetrien.*

Bemerkung 3.4.22 *Sei* $\dim V = 2$. *Mit* S^k *bezeichnen wir die Menge von Produkten von* k *Symmetrien. Dann ist* $\langle S \rangle$ *eine echte Untergruppe von* $\mathrm{U}^{\pm}(f)$. *Wir haben* $\langle S \rangle = S^2 \dot{\cup} S \dot{\cup} S^3 \backslash S$ *und* S^2 *ist ein Normalteiler in* $\langle S \rangle$ *vom Index 2 und Ordnung 8, der aus* $1_V, -1_V$ *und 6 Transformationen* ϕ *mit* $\mathrm{mip}(\phi) = x^2 + 1$ *besteht.* S^2 *ist die Quaternionengruppe. Ferner besteht* $S^3 \backslash S$ *aus den 2 Homothetien* $i \cdot 1_V$ *und* $-i \cdot 1_V$, *wobei* $\bar{i} = -i$ *ist, und* S *enthält 6 Symmetrien.* ■

$|F| = 3$; untere Schranken

Lemma 3.4.23 (Untere Schranken für (S)) *Seien* $\pi \in \mathrm{U}^{\pm}(f)$ *vom Typ* (S) *und* $m := \dim \mathrm{B}(\pi)$. *Dann ist*

$$\mathrm{l}(\pi) \geq \begin{cases} m+2 & , falls\ (-1)^m = \det(\pi)\ ist, \\ m+3 & , falls\ (-1)^m \neq \det(\pi)\ ist. \end{cases}$$

Beweis. Sei $k := \mathrm{l}(\pi) \leq m+1$ angenommen. Dann gibt es Symmetrien $\sigma_1, \ldots, \sigma_k$, so daß $\pi = \sigma_1 \cdots \sigma_k$. Nach 3.3.3 und 3.3.1 , gilt $\mathrm{B}(\sigma_i) \leq B(\pi)$. Dies bedeutet $\mathrm{F}(\pi) \leq \mathrm{F}(\sigma_i)$, und σ_i induziert eine Symmetrie $\tilde{\sigma_i}$ auf $\mathrm{B}(\pi)/\mathrm{radB}(\pi)$. Nun ist aber $\tilde{\pi} = \tilde{\sigma_1} \cdots \tilde{\sigma_k}$ ein Widerspruch zu 3.4.11.

Lemma 3.4.24 (Untere Schranken für (M)) *Sei* $\pi \in \mathrm{U}^{\pm}(f)$ *vom Typ (M). Dann ist* $\mathrm{l}(\pi) \geq 6$.

Beweis. Nach Definition des Typs (M) gibt es ein $\nu \in K^* \backslash \{\pm 1\}$, so daß $\dim \mathrm{radB}(\bar{\nu}\pi) = 2$ ist. Sei σ eine beliebige Symmetrie. Wenn $\dim \mathrm{B}(\pi\sigma) \geq \dim \mathrm{B}(\pi) = 4$ ist, folgt $\mathrm{l}(\pi\sigma) \geq 5$ aus $\det(\pi\sigma) = -\det(\pi) = -1$. Wir können deshalb $\dim \mathrm{B}(\pi\sigma) = 3$ annehmen. Nun ist $\dim \mathrm{radB}(\bar{\nu}\pi\sigma) \geq \dim \mathrm{radB}(\bar{\nu}\pi) - 1 = 1$, und $\mathrm{F}(\pi\sigma) \neq \{0\}$ impliziert, daß $(x-\nu)^2(x-1)$ ein Teiler von $\mathrm{mip}(\pi\sigma)$ ist. Wegen $\det(\pi\sigma) = -1$ und $\nu^2 = -1$ folgern wir $\mathrm{mip}(\pi\sigma) = (x-\nu)^2(x-1)^2$. Damit ist $\pi\sigma$ vom Typ (S1). Nun ergibt 3.4.23, daß $\mathrm{l}(\pi\sigma) \geq 5$, also $\mathrm{l}(\pi) \geq 6$. ■

$|F| = 3$**; Induktion**

Um den Beweis von 3.4.32 übersichtlich zu gestalten, geben wir nun eine Reihe vorbereitender Lemmata an.

Lemma 3.4.25 *Seien $\pi \in \mathrm{U}(f)$, $v \in V$, $\alpha \in K^*\backslash\{\pm 1\}$ mit $\alpha\bar{\alpha} = 1$ und $a = v(\pi-1)(\alpha\pi-1)$. Es gelte $q_{\alpha\pi}(a), q_\pi(a) \in F^*$, und $v(\pi-1)$ sei isotrop. Der Vektor $a' := v(\pi-1)(\bar{\alpha}\pi-1)$ erfüllt dann $q_{\bar{\alpha}\pi}(a') = q_\pi(a') = -q_{\alpha\pi}(a) \in F^*$.*

Beweis. Beachte: aus $q_{\alpha\pi}(a), q_\pi(a) \in F^*$ folgt $f(v(\pi-1), v(\alpha\pi-1)) = 0$, cf. 3.2.2 angewandt auf π und $\alpha\pi$. Hiermit berechnen wir nun

$$\begin{aligned}
q_\pi(a') &= f(v(\bar{\alpha}\pi-1), a') = f(v((\pi-1)+(\bar{\alpha}-1)\pi)), a') \\
&= q_{\bar{\alpha}\pi}(a') + (\alpha+1)f(v(\pi-1), v(\bar{\alpha}\pi-1)) = q_{\bar{\alpha}\pi}(a') + (\alpha+1)(\alpha-1)f(v(\pi-1), v\pi) \\
&= q_{\bar{\alpha}\pi}(a') - (\alpha-1)f(v(\pi-1), (\alpha-1)v\pi) = q_{\bar{\alpha}\pi}(a') - (\alpha-1)f(v(\pi-1), v(\alpha\pi-1)) \\
&= q_{\bar{\alpha}\pi}(a') = f(v(\pi-1), v(\pi-1)(\bar{\alpha}\pi-1)) \\
&= f(v(\pi-1), v(\pi-1)(\bar{\alpha}\pi+1)) = -f(v(\pi-1), v(\pi-1)(\alpha\pi-1)) \\
&= -q_{\alpha\pi}(a) \in F^*. \qquad \blacksquare
\end{aligned}$$

Bemerkung 3.4.26 *Ist $\dim V = 2$, $\epsilon \in \{\pm 1\}$ und $\pi \in \mathrm{U}(f)$ zyklisch mit $\mathrm{mip}(\pi) = (x-\alpha)^2$, $-\bar{\alpha} = \alpha \in K^*$, so gibt es eine Symmetrie σ derart, daß $\epsilon\pi\sigma$ eine Transvektion ist.*

Beweis. Wegen $\mathrm{mip}(\epsilon\pi) = (x-\epsilon\alpha)^2$ gibt es nach 3.4.3 and 3.2.2 (a) eine Symmetrie σ mit $\dim F_\epsilon(\pi\sigma) = 1$. Nun folgt aus $\det \pi\sigma = 1$, daß $\epsilon\pi\sigma$ eine Transvektion ist. ■

Lemma 3.4.27 *Sei $\pi \in \mathrm{U}(f)$, so daß $V = U_1 \textcircled{\perp} U_2$ für π-Moduln U_k mit $\dim U_k = 2$, $\mathrm{mip}(\pi_1) = (x+i)^2$ und $\mathrm{mip}(\pi_2) = (x-i)^2$ (π_k bezeichne π_{U_k}, und es sei $\bar{i} = -i \in K^*$). Dann gibt es einen anisotropen Vektor $v \in V$, so daß $q_\pi(v(\pi-1)) \in F^*$ ist.*

Beweis. Nach 3.4.7 und 3.3.7 findet man eine Basis $\mathcal{B}$ von V, so daß sich folgende Matrixdarstellungen ergeben

$$\mathcal{M}_\mathcal{B}(\pi) = \begin{bmatrix} 0 & 1 & & \\ 1 & i & & \\ & & 0 & 1 \\ & & 1 & -i \end{bmatrix} \text{ und } \mathcal{M}_\mathcal{B}(f) = \begin{bmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix}.$$

Wähle $v := (1, -1, 1, -1)$. Dann ist $f(v, v) = -1 = q_\pi(v(\pi-1))$. ■

Lemma 3.4.28 *Sei $\pi \in U^\pm(V, f)$ kurz. Es gelte $\dim \mathrm{B}(\pi) = 4$, $\det \pi = 1$, $\dim \mathrm{F}_{-1}(\pi) = 1$ und $\dim \mathrm{F}_\mu(\pi) \cap \mathrm{B}(\pi) \leq 1$ für jedes $\mu \in K$. Dann gibt es eine Symmetrie σ, so daß $\dim \mathrm{B}(\pi\sigma) = 3$ und $\pi\sigma$ kurz ist.*

Beweis. Einfache Überlegungen ergeben, daß V sich auf eine der im folgenden angegebenen Weisen in π-Moduln zerlegen läßt:

(a) $V = U \bigoplus W$, $\dim U = 1$, $\pi_U = -1_U$ und π_W ist kurz;
(b) $V = U \bigoplus W \bigoplus X \bigoplus Y$, $\dim U = 1$, $\pi_U = -1_U$, $\dim W = 2$, π_W ist eine Transvektion, $\mathrm{mip}(\pi_X) = (x-\alpha)^2$ mit $\bar{\alpha} = -\alpha \neq 0$ und $\pi_Y = 1_Y$;
(c) $V = U \bigoplus W \bigoplus X \bigoplus Y$, $\dim U = 2$, π_U ist eine negative Transvektion, $\dim W = 1 = \dim X$, $\pi_W = -i \cdot 1_W$, $\pi_X = i \cdot 1_X$ und $\pi_Y = 1_Y$;
(d) $V = U \bigoplus W \bigoplus X$, $\dim U = 2$, π_U ist eine negative Transvektion, $\dim W = 3$, $\mathrm{mip}(\pi_W) = (x-1)^3$ und $\pi_X = 1_X$;
(e) $V = U \bigoplus W$, $\dim U = 4$, $\mathrm{mip}(\pi_U) = (x+1)^4$, $\pi_W = 1_W$.

(a) Wähle $\sigma := \sigma_U$.
(b) Nach 3.4.3 und 3.2.2 (a) gibt es eine Symmetrie σ mit $B(\sigma) \leq X$, so daß $(\pi\sigma)_X$ eine Transvektion ist. Dann ist $\dim \mathrm{B}(\pi\sigma) = 3$ und $\pi\sigma$ kurz.
(c) Nach 3.4.2 und 3.2.2 (a) angewandt auf $\pi_{U \oplus W}$ gibt es eine Symmetrie σ, so daß $\mathrm{B}(\sigma) \leq U \oplus W$ und $\dim B(\pi\sigma) = 3$ ist. Weil $X \leq F_i(\pi\sigma)$ regulär ist, ist $\pi\sigma$ nicht vom Typ (S1). Wegen $-1 = \det \pi\sigma \neq -i = i^3$ ist $\pi\sigma$ nicht vom Typ (H). Folglich ist $\pi\sigma$ kurz.
(d) Nach 3.4.3 angewandt auf π_W, gibt es ein $w \in \mathrm{B}(\pi_W)$ mit $q_\pi(w) \in F^*$. Wähle ein $u \in F_{-1}(\pi)\backslash\{0\}$ und setze $a := u + w$. Dann ist $q_\pi(a) = q_\pi(w) \in F^*$ und $\sigma := \sigma_a$ erfüllt $\dim \mathrm{B}(\pi\sigma) = 3$. Wegen $B(\sigma) \leq V(\pi+1)$ gilt $F_{-1}(\pi) \leq F_{-1}(\pi\sigma)$. Ist $\dim F_{-1}(\pi\sigma) = 2$, so folgt aus $\mathrm{B}(\sigma) = \langle a \rangle \nsubseteq V(\pi+1)^2$ und 3.3.6 (a) angewandt auf $-\pi$, daß $F_{-1}(\pi\sigma)$ eine hyperbolische Ebene ist, ein Widerspruch zu $\det \pi\sigma = -1$. Folglich ist $\mathrm{F}_{-1}(\pi\sigma) = \mathrm{F}_{-1}(\pi)$ totalisotrop. Nun folgt aus $\det \pi\sigma = -1$, daß $\mathrm{mip}(\pi\sigma) = (x+1)^3(x-1)$ ist. Hieraus schließen wir, daß $\pi\sigma$ kurz ist.
(e) Wir können $W = 0$ annehmen. Wegen $\mathrm{B}(\pi)(\pi+1) \neq \mathrm{B}(\pi)$ liefert 3.4.3 einen Vektor $v(\pi-1) \in \mathrm{B}(\pi)\backslash\mathrm{B}(\pi)(\pi+1)$ mit $q_\pi(v(\pi-1)) \in F^*$. Falls v isotrop ist, setze $\lambda := f(v, v(\pi+1)^3)$ und $v' := v + \epsilon\lambda v(\pi+1)^3 \in \mathrm{B}(\pi)\backslash\mathrm{B}(\pi)(\pi+1)$. Dabei sei $\epsilon \in \{\pm 1\}$. Es ist $\lambda \neq 0$, da $\langle v(\pi+1)^3\rangle^\perp = V(\pi+1)$. Somit gilt $f(v', v') = 2\epsilon\lambda\bar{\lambda} \neq 0$ und

$$\begin{aligned} q_\pi(v'(\pi-1)) &= f(v', v'(\pi-1)) = f(v + \epsilon\lambda v(\pi+1)^3, v(\pi-1) + \epsilon\lambda v(\pi+1)^3) \\ &= f(v, v(\pi-1)) + \epsilon\bar{\lambda}\lambda + \epsilon\lambda f(v(\pi+1)^3, v + v(\pi+1)) = f(v, v(\pi-1)) - \epsilon\bar{\lambda}\lambda \\ &= q_\pi(v(\pi-1)) - \epsilon\bar{\lambda}\lambda \in F. \end{aligned}$$

Demnach ist $q_\pi(v'(\pi-1)) \in F^*$ für ein geeignetes $\epsilon \in \{\pm 1\}$. Wir können daher annehmen, daß v anisotrop ist. Die Symmetrie $\sigma := \sigma_a$ erfüllt dann $\dim \mathrm{B}(\pi\sigma) = 3$, $\mathrm{F}_{-1}(\pi\sigma) = \{0\}$ (da $\mathrm{B}(\sigma) \nsubseteq V(\pi+1)$), $\dim \mathrm{radB}(\pi\sigma) = \langle v\rangle \cap \langle v\rangle^\perp = \{0\}$ und $\dim F_\mu(\pi\sigma) \leq 1$ für jedes $\mu \in K$ (,da $\dim F_\mu(\pi) = 0$ für jedes $\mu \in K\backslash\{-1\}$ gilt). Somit ist $\pi\sigma$ kurz. ∎

Lemma 3.4.29 *Sei* $\pi \in U^\pm(f)$ *kurz, und es gelte* $\dim \mathrm{B}(\pi) = 5$, $\det \pi = -1$, $\dim \mathrm{F}_{-1}(\pi) = 2$, $\dim \mathrm{radB}(\pi) = 1$ *und* $\dim \mathrm{F}_\mu(\pi) \cap \mathrm{B}(\pi) \leq 1$ *für jedes* $\mu \in K\backslash\{-1\}$. *Dann gibt es eine Symmetrie* σ, *so daß* $\dim \mathrm{B}(\pi\sigma) = 4$ *und* $\pi\sigma$ *kurz ist.*

Beweis. Beachte, daß $\mathrm{F}_{-1}(\pi)$ nicht totalisotrop sein kann. Sonst müßte $V = U \bigoplus W \bigoplus X$ für π-Moduln U, W, X mit $\dim U = 2 = \dim W$ gelten und $-\pi_U, -\pi_W, \pi_X$ wären Transvektionen, ein Widerspruch zu $\det \pi = -1$. Wähle einen anisotropen Vektor $a \in \mathrm{F}_{-1}(\pi)$ und setze $U := \langle a\rangle^\perp$. Angenommen π_U ist lang. Dann ist π_U vom Typ (S3), da $\dim F_{-1}(\pi_U) = 1$ und $\mathrm{radB}(\pi_U) =$

$\mathrm{radB}(\pi) \neq \{0\}$ gilt. Wir erhalten nun den Widerspruch $1 = \dim \mathrm{radB}(\pi) = \dim \mathrm{radB}(\pi_U) = \dim \mathrm{B}(\pi_U) - 2 = \dim \mathrm{B}(\pi) - 3 = 2$. Somit sind π_U und $\pi\sigma_a = 1_{\langle a\rangle} \bigoplus \pi_U$ kurz. Weiterhin ist $\dim \mathrm{B}(\pi\sigma_a) = 4$. ■

Lemma 3.4.30 *Ist $\pi \in \mathrm{U}(f)$ kurz und $\dim \mathrm{B}(\pi)/\mathrm{radB}(\pi) = 2$, so ist $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma$ kurz für eine Symmetrie σ.*

Beweis. Sei $\tilde{\pi}$ die von π auf $\mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi)$ induzierte Abbildung. Es sei zunächst $\det \pi = -1$ angenommen. Weil π nicht vom Typ (S1) ist , ist $\tilde{\pi}$ eine Symmetrie oder eine μ-Homothetie für ein $\mu \in K\backslash\{\pm 1\}$ mit $\mu^2 = -1 = -\mu\bar{\mu}$, cf. 3.4.20. Wenn $\tilde{\pi}$ eine Symmetrie ist, gibt es eine Zerlegung $V = U \bigoplus W \bigoplus X$ in π-Moduln U, W und X, so daß $\dim U = 1, \pi_U = -1_U$, $\dim W = 3$ und $\mathrm{mip}(\pi_W) = (x-1)^3$ und π_X von Typ (T) oder 1_X ist. Nun läßt sich $\pi_W = \rho_1\rho_2$ als ein Produkt von zwei Symmetrien ρ_i schreiben, cf. 3.4.12. Wähle $\sigma := 1_U \bigoplus \rho_2 \bigoplus 1_X$. Dann ist $\pi\sigma = -1_U \bigoplus \rho_1 \bigoplus \pi_X$ kurz und $\dim \mathrm{B}(\pi\sigma) < \dim \mathrm{B}(\pi)$. Falls $\tilde{\pi}$ eine μ-Homothetie ist, so hat man, da π nicht vom Typ (H) ist, eine Zerlegung $V = U \bigoplus W$ in π-Moduln U und W, wobei $\dim U = 2, \pi_U = \mu \cdot 1_U$ und π_W vom Typ (T) ist. In diesem Fall liefert 3.4.6 a) eine Symmetrie σ mit $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) - 1$ und $\det \pi\sigma = 1$. Ferner gilt $\dim \mathrm{F}_\mu(\pi\sigma) = 1$ wegen $\mathrm{F}_\mu(\pi) \nsubseteq \mathrm{F}(\sigma)$, somit ist $\pi\sigma$ kurz.

Sei nun $\det \pi = 1$ angenommen. Weil π weder zum Typ (S2) noch (S3) gehört, schließen wir, daß $\tilde{\pi} = 1$ oder $\mathrm{mip}(\tilde{\pi}) = x^2 + 1$ gilt. Im ersten Fall folgt $V = U_1 \bigoplus U_2 \bigoplus W$ für π-Moduln U_i und W, wobei $\dim U_i = 3, \mathrm{mip}(\pi_{U_i}) = (x-1)^3$ und π_W vom Typ (T) oder 1_W ist. Weil π_{U_i} kurz ist, liefert 3.4.12 Symmetrien ρ_1, ρ_2, so daß $\pi_{U_1} = \rho_1\rho_2$ ist. Wähle $\sigma := \rho_2 \bigoplus 1_{U_1^\perp}$. Dann ist $\pi\sigma = \rho_1 \bigoplus \pi_{U_1^\perp}$ kurz und $\dim \mathrm{B}(\pi\sigma) < \dim \mathrm{B}(\pi)$. Ist $\mathrm{mip}(\tilde{\pi}) = x^2 + 1$, so haben wir $V = U \bigoplus W$ für π-Moduln U und W, $\dim U = 2, \mathrm{mip}(\pi_U) = x^2 + 1$, und π_W ist vom Typ (T) oder 1_W. Wiederum findet man nach 3.4.12 Symmetrien ρ_1, ρ_2, für die $\pi_U = \rho_1\rho_2$ gilt. Sei $\sigma := \rho_2 \bigoplus 1_W$. Dann ist $\pi\sigma = \rho_1 \bigoplus \pi_W$ kurz und $\dim \mathrm{B}(\pi\sigma) < \dim \mathrm{B}(\pi)$. ■

Lemma 3.4.31 *Sei $\pi \in \mathrm{U}^{\pm}(V, f)$ kurz mit $\mathrm{F}_{-1}(\pi) = \{0\}$und $\dim \mathrm{B}(\pi) = 4 = \dim V$. Für alle $v \in V$ gelte:*
$(*)$ Ist $q_\pi(v(\pi - 1)) \in F^*$, so ist v isotrop.
Dann ist $\dim \ker(\pi - \alpha)^2 \geq 2$ für ein $\alpha \in K^*$ mit $\bar{\alpha} = -\alpha$.

Beweis. Weil π kurz ist, findet man nach 3.4.3 einen Vektor $u \in V$, der $q_\pi(u) = s(u,u) + i^{-1}d(u,u) \in F^*$ erfüllt, cf.3.2.3. Dies bedeutet $s(u,u) \neq 0 = d(u,u)$. Sei $W := u^{\perp_d}$. Wegen d-rad$V = \mathrm{F}_{-1}(\pi) = \{0\}$ ist $\dim W = 3$. Aus $\mathrm{F}(\pi) = \{0\}$ folgt $\phi := (\pi - 1)^{-1} \in \mathrm{GL}(V)$.

Fall 1: Ein $w \in W$ erfüllt $d(w,w) = 0 \neq f(w\phi, w\phi)$. Dann ist $U := \langle u, w\rangle$ d-totalisotrop, nicht s-totalisotrop, da $s(u,u) \neq 0$, und $U\phi$ ist nicht f-totalisotrop, da $f(w\phi, w\phi) \neq 0$ ist. Wegen $|F| = 3$ gibt es mindestens 6 s-reguläre 1-dimensionale Unterräume von U und höchstens 4 f-singuläre 1-dimensionale Unterräume von $U\phi$. Wir finden daher einen Vektor $v \in U\phi$ mit $f(v,v) \neq 0 \neq s(v(\pi-1), v(\pi-1))$. Nun ergibt $q_\pi(v(\pi-1)) = s(v(\pi-1), v(\pi-1)) \in F^*$ einen Widerspruch zu $(*)$.

Fall 2: Für alle $w \in W$ folgt aus $d(w,w) = 0$ auch $f(w\phi, w\phi) = 0$.

Weil V d-regulär ist, folgt $\dim W/d\text{-rad}W \geq 2$. Wegen $\mathcal{N}(K) = F$ enthält W eine d-hyperbolische

Ebene. Nach 3.1.2 gibt es dann ein $\lambda \in F$, so daß $f \circ (\phi \times \phi)_{W\times W} = \lambda d_{W\times W}$, i.e. $f(a\phi, b\phi) = \lambda i \cdot f(a\phi, b(1+\pi^{-1}))$ für alle $a, b \in W$ gilt. Da $W\phi$ nicht f-totalisotrop ist, folgt $\lambda \in F^*$. Hieraus leitet man $Z\phi(\lambda^{-1}i - (\pi - \pi^{-1})) \subseteq Z^\perp$ ab, wobei $Z := W\phi$ sei. Aus $\dim Z = 3$ und $\dim Z^\perp = 1$ ergibt sich nun $\dim\ker(\lambda^{-1}i - (\pi - \pi^{-1})) \geq 2$. Dies bedeutet $\dim\ker(\pi^2 - \lambda^{-1}i\pi - 1) \geq 2$. Sei $\alpha := -\lambda^{-1}i$. Dann ist $\dim\ker(\pi - \alpha)^2 \geq 2$. ∎

Lemma 3.4.32 (Induktions-Lemma.) *Sei* $\pi \in \mathrm{U}^\pm(f)$, $\pi^2 \neq 1$.
(a) *Ist* π *kurz, so gilt* $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ *für eine Symmetrie* σ.
(b) *Ist* π *kurz und* $m := \dim \mathrm{B}(\pi) \geq 4$, *so ist* $\pi\sigma$ *kurz, und es gilt* $\dim \mathrm{F}(\pi\sigma) > \dim \mathrm{F}(\pi)$, *falls* $\det \pi = (-1)^m$, *beziehungsweise* $\dim \mathrm{F}(\pi\sigma) \geq \dim \mathrm{F}(\pi)$, *falls* $\det\pi \neq (-1)^m$ *ist, für eine Symmetrie* σ.

Beweis. (a) Sei π kurz. Wenn π nicht vom Typ (N*) ist, gibt es nach 3.4.3 (mit $W = \{0\}$) und 3.2.2 eine Symmetrie σ', so daß $\mathrm{F}(\pi\sigma') > \mathrm{F}(\pi)$ ist. Ist π vom Typ (N*), so gibt es eine Zerlegung $V = U \bigoplus W \bigoplus X$ in π-Moduln U, W, X derart, daß $\dim U = 2, \pi_U$ eine Transvektion, $\pi_W = -1_W$, $\dim W \geq 1$ und $\pi_X = 1_X$ ist. Wir können daher eine Symmetrie σ' mit $\mathrm{B}(\sigma') \leq W$ wählen und erhalten $\mathrm{F}(\pi\sigma') > \mathrm{F}(\pi)$. Im Fall $\dim W \geq 2$ ist $\pi\sigma'$ wiederum vom Typ (N*) (, also insbesondere kurz). Dies beweist (a).
Für den Beweis von (b) sei nun $\dim \mathrm{B}(\pi) \geq 4$ vorausgesetzt. Falls $\pi\sigma'$ bereits kurz ist, ist auch (b) gezeigt. Wir können deshalb annehmen, daß π nicht vom Typ (N*) und $\pi\sigma'$ lang ist, i.e. zu einem der Typen (H), (T), (N), (S), (M) gehört.
Entsprechend dieser Möglichkeiten gehen wir im Beweis von (b) vor. Hierbei machen wir die folgenden Fallunterscheidungen.

I $\pi\sigma'$ ist vom Typ (H) oder (T) oder (N).
Behauptung C I : $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma$ ist kurz, für eine geeignete Symmetrie σ

II $\pi\sigma'$ ist vom Typ (S).
Behauptung C II : $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma$ gehört weder zum Typ (S) noch (M) für eine Symmetrie σ, womit I anwendbar ist.
Wir unterscheiden folgende Unterfälle:
- II.1 $\mathrm{radB}(\pi) \neq \{0\}$.
- II.2 $\mathrm{radB}(\pi) = \{0\}$.
  - II.2.(a) $\mathrm{radB}(\pi) = \{0\}$ and $\mathrm{F}_{-1}(\pi) \neq 0$.
  - II.2.(b) $\mathrm{radB}(\pi) = \{0\}$ and $\mathrm{F}_{-1}(\pi) = 0$.

III $\pi\sigma'$ ist vom Typ (M).
Behauptung CIII : $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma$ gehört nicht zum Typ (M) für eine Symmetrie σ, weshalb I oder II zutrifft.

Wir beginnen mit dem Fall I.
In (i), (ii), (iii) sei σ eine Symmetrie mit $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$.

(i) Gehört $\pi\sigma'$ zum Typ (H), so ist $\pi\sigma$ kurz oder vom Typ (H) oder (M) und es gilt $\dim \mathrm{B}(\pi) = 5$, $\det \pi = -1$, $\dim F_{-1}(\pi) = 1$, $\dim \mathrm{F}_\mu(\pi) = 3$ und $\dim \mathrm{rad}B(\bar{\mu}\pi) = 1$ für ein $\mu \in K^*$ mit $\bar{\mu} = -\mu$.

Beweis. Nach Voraussetzung haben wir $\mathrm{F}_\mu(\pi\sigma') = \mathrm{B}(\pi\sigma')$ für ein $\mu \in K\backslash\{\pm 1\}$. Es ist $\dim \mathrm{F}_\mu(\pi) \geq \dim \mathrm{B}(\pi\sigma') - 1 = \dim \mathrm{B}(\pi) - 2 \geq 2$, also $\dim \mathrm{F}_\mu(\pi\sigma) \geq 1$. Somit ist $\pi\sigma$ kurz oder vom Typ (H) oder (S1) oder (M). Wäre $\pi\sigma$ vom Typ (S1), würde $\dim \mathrm{F}_\mu(\pi\sigma) = 1$, $\dim \mathrm{B}(\pi) = 4$ und $\bar{\mu} = \mu^3 = \det \pi\sigma' = \det \pi\sigma = -1$ gelten, ein Widerspruch. Gehört $\pi\sigma$ zum Typ (M), so folgt $\dim \mathrm{B}(\pi) = 5$, $\det \pi = -\det \pi\sigma = -1$, $2 = \dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{radB}(\bar{\mu}\pi\sigma)$, $\dim \mathrm{F}_\mu(\pi) = 3$, $\dim \mathrm{F}_\mu(\pi\sigma') = 4$ und $1 = \dim \mathrm{radB}(\bar{\mu}\pi\sigma') + 1 \geq \dim \mathrm{radB}(\bar{\mu}\pi) \geq \dim \mathrm{radB}(\bar{\mu}\pi\sigma) - 1 = 1$. Dies impliziert $\dim \mathrm{F}_{-1}(\pi) = 1$. ■

Ist $\pi\sigma'$ vom Typ (H), erhält man $\dim \mathrm{F}_\mu(\pi) \geq 2$ für ein $\mu \in K\backslash\{1, -1\}$. Somit $\mathrm{B}(\pi)(\pi - \mu) \neq \mathrm{B}(\pi)$. Nach 3.4.3 gibt es einen Vektor $a \in \mathrm{B}(\pi)\backslash\mathrm{B}(\pi)(\pi - \mu)$, so daß $q_\pi(a) \in F^*$ ist. Gemäß 3.3.6 (b) erfüllt $\sigma := \sigma_a$ $\dim \mathrm{F}(\pi\sigma) > \dim \mathrm{F}(\pi)$ und $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) \neq 0$, da π nicht vom Typ (H) ist. Demnach ist $\pi\sigma$ nicht vom Typ (H). Gemäß (i) können wir nun annehmen, daß $\pi\sigma$ zum Typ (M) gehört und $V = U \bigoplus W \bigoplus X \bigoplus Y$ für π-Modulen U, W, X, Y gilt, wobei $\dim U = 2 = \dim W$, $\mathrm{mip}(\pi_U) = (x - \mu)^2$, $\pi_W = \mu \cdot 1_W$, $\dim X = 1$, $\pi_X = -1_X$ und $\pi_Y = 1_Y$ ist. Dann erfüllt $\sigma'' := \sigma_X$ $\mathrm{F}(\pi\sigma'') > \mathrm{F}(\pi)$, und $\pi\sigma''$ ist kurz.

(ii) Falls $\pi\sigma'$ vom Typ (T) ist, ist $\pi\sigma$ entweder kurz oder vom Typ (T) oder (S2) oder (S3).

Beweis. Nach 3.3.5 (b) ist $\dim \mathrm{rad}\ \mathrm{B}(\pi) \geq \dim \mathrm{B}(\pi\sigma') - 1 \geq 2$, also $\mathrm{rad}\ \mathrm{B}(\pi\sigma) \neq 0$ und damit $\pi\sigma$ kurz oder vom Typ (T) oder (S). Wegen $\det \pi\sigma = \det \pi\sigma' = 1$ kann $\pi\sigma$ nicht vom Typ (S1) sein. ■

Wir betrachten nun den Fall, daß $\pi\sigma'$ vom Typ (T) ist. Dann ist $\mathrm{B}(\pi\sigma')$ totalisotrop und $\mathrm{radB}(\pi) \neq \{0\}$. Folglich ist $\mathrm{B}^2(\pi) \neq \mathrm{B}(\pi)$. Nach 3.4.3 findet man ein $a \in \mathrm{B}(\pi)\backslash\mathrm{B}^2(\pi)$ mit $q_\pi(a) \in F^*$. Nach 3.3.6 (a) ist $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \neq 0$ (, da π nicht vom Typ (T) ist). Also ist $\pi\sigma$ nicht vom Typ (T). Aus (ii) folgt nun, daß $\pi\sigma$ kurz oder vom Typ (S1) oder (S2) ist. Gehört $\pi\sigma$ zum Typ (S1) oder (S2), so gilt $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = \dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) = 2$. Nun beweist 3.4.30 die Behauptung.

(iii) Wenn $\pi\sigma'$ zum Typ (N) gehört, ist $\pi\sigma$ entweder kurz oder vom Typ (N) oder [vom Typ (S1) und $\dim \mathrm{B}(\pi) = 4$, $\det \pi = 1$, $\dim \mathrm{F}_{-1}(\pi) = 1$ und $\dim \mathrm{F}_\mu(\pi) \leq 1$ für jedes $\mu \in K$] oder [vom Typ (S3) und $\dim \mathrm{B}(\pi) = 5$, $\det \pi = -1$, $\dim \mathrm{F}_{-1}(\pi) = 2$, $\dim \mathrm{rad}\ \mathrm{B}(\pi) = 1$ und $\dim \mathrm{F}_\mu(\pi) \leq 1$ für jedes $\mu \in K\backslash\{-1\}$].

Beweis. Sei $\pi\sigma'$ vom Typ (N) angenommen. Aus (i) und (ii) folgt, daß $\pi\sigma$ nicht vom Typ (H) oder (T) ist. Nimmt man nun an, daß $\pi\sigma$ lang aber nicht vom Typ (N) ist, so folgt im Fall $\dim \mathrm{B}(\pi) \geq 5$:

$$1 \geq \dim \mathrm{F}_{-1}(\pi\sigma) \geq \dim \mathrm{F}_{-1}(\pi) - 1 \geq \dim \mathrm{F}_{-1}(\pi\sigma') - 2 = \dim \mathrm{B}(\pi\sigma') - 3 = \dim \mathrm{B}(\pi) - 4 \geq 1.$$

Deshalb ist $\pi\sigma$ vom Typ (S3), $\dim \mathrm{B}(\pi) = 5$ und $\det \pi = -\det \pi\sigma = -1$. Ferner folgt aus

$$2 = \dim \mathrm{B}(\pi\sigma) - 2 = \dim \mathrm{radB}(\pi\sigma) \leq \dim \mathrm{radB}(\pi) + 1 \leq \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma') + 2 = 2,$$

daß $\dim \mathrm{radB}(\pi) = 1$ ist. Im Fall $\dim \mathrm{B}(\pi) = 4$ gilt $\det \pi\sigma = \det \pi\sigma' = (-1)^3 = -1$. Folglich ist $\pi\sigma$ vom Typ (S1), was wiederum $1 = \dim F_{-1}(\pi\sigma) + 1 \geq \dim \mathrm{F}_{-1}(\pi) \geq \dim \mathrm{F}_{-1}(\pi\sigma') - 1 = 1$ nach sich zieht. ■

Ist nun $\pi\sigma'$ vom Typ (N), so ist $\dim \mathrm{F}_{-1}(\pi) \geq 1$. Insbesondere gilt $\mathrm{B}(\pi)(\pi + 1) \neq \mathrm{B}(\pi)$. Demnach liefert 3.4.3 ein $a \in \mathrm{B}(\pi)\backslash\mathrm{B}(\pi)(\pi + 1)$, so daß $q_\pi(a) \in F^*$. Nach 3.3.6 (b), gilt dann $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_{-1}(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{F}_{-1}(\pi) \neq 1$ (, da π nicht vom Typ (N) oder (N^*)) ist. Also ist $\pi\sigma$ nicht vom Typ (N). Gemäß (iii) können wir deshalb annehmen, daß $\pi\sigma$ vom [Typ (S1) ist und $\dim \mathrm{B}(\pi) = 4$, $\det \pi = 1$, $\dim \mathrm{F}_{-1}(\pi) = 1$ und $\dim \mathrm{F}_\mu(\pi) \leq 1$ für jedes $\mu \in K$ gilt] oder [zum Typ (S3) gehört und $\dim \mathrm{B}(\pi) = 5$, $\det \pi = -1$, $\dim \mathrm{F}_{-1}(\pi) = 2$, $\dim \mathrm{rad}\ \mathrm{B}(\pi) = 1$ und $\dim \mathrm{F}_\mu(\pi) \leq 1$ für jedes $\mu \in K\backslash\{-1\}$ erfüllt ist]. Im ersten Fall liefert 3.4.28 und im zweiten 3.4.29 die Behauptung.

Wir haben nun den Fall I abgehandelt.

II. Angenommen $\pi\sigma'$ ist vom Typ (S). Wir wollen nun CII beweisen. Zuerst betrachten wir den Fall

II.1 $\mathrm{radB}(\pi) \neq 0$.

Wähle $a \in \mathrm{B}(\pi)\backslash\mathrm{B}^2(\pi)$ mit $q_\pi(a) \in F^*$, cf. 3.4.3. Sei $\sigma := \sigma_a$. Lemma 3.3.6 (a) ergibt $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) - 1$ und $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = \dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma)$. Ist $\pi\sigma$ vom Typ (S), folgt $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = \dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) = 2$ und 3.4.30 liefert das gewünschte Ergebnis.

Wir können deshalb annehmen, daß $\pi\sigma$ vom Typ (M) ist.

Wir berechnen: $\det \pi = -\det \pi\sigma = -1$, $\dim \mathrm{B}(\pi) = \dim \mathrm{B}(\pi\sigma) + 1 = 5$ und $1 \leq \dim \mathrm{rad}\ \mathrm{B}(\pi) \leq \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) + 1 = 1$. Also ist $\det \pi\sigma' = 1$ und damit $\pi\sigma'$ vom Typ (S2) oder (S3). Es gibt ein $\nu \in K^*$ mit $\bar{\nu} = -\nu$, so daß $\mathrm{F}_\nu(\pi\sigma)$ ein zweidimensionaler, totalisotroper Teilraum ist. Insbesondere ist $\mathrm{radF}_\nu(\pi) \neq \{0\}$. Wegen $1 = \dim \mathrm{F}_\nu(\pi\sigma) - 1 \leq \dim F_\nu(\pi) \leq \dim \mathrm{F}_\nu(\pi\sigma') + 1 = 1$, schließen wir, daß $a \in \mathrm{B}(\bar{\nu}\pi) \cap \mathrm{B}(\pi) = V(\pi - 1)(\bar{\nu}\pi - 1)$ und $q_{\bar{\nu}\pi}(a) \in F^*$ gilt, cf. 3.2.2. Sei $v \in V$ mit $a = v(\pi - 1)(\bar{\nu}\pi - 1)$. Dann ist $v(\pi - 1) \in \mathrm{F}_\nu(\pi\sigma)$ isotrop und (nach 3.2.2 (a)) $v(\bar{\nu}\pi - 1) \in \mathrm{F}(\pi\sigma)$. Es ist $b := v(\pi - 1)(\nu\pi - 1) \in \mathrm{B}(\pi)\backslash\mathrm{B}^2(\pi)$ und $q_{\nu\pi}(b), q_\pi(b) \in F^*$ nach 3.4.25. Nach 3.3.6 (a) hat $\rho := \sigma_b$ die Eigenschaften : $\mathrm{F}(\pi\rho) > \mathrm{F}(\pi)$, $\mathrm{F}_{\bar{\nu}}(\pi\rho) > \mathrm{F}_{\bar{\nu}}(\pi)$ und $\dim \mathrm{B}(\pi\rho)/\mathrm{radB}(\pi\rho) = \dim \mathrm{B}(\pi)/\mathrm{radB}(\pi) = 4$. Deshalb kann $\pi\rho$ nicht vom Typ (S) sein. Angenommen $\pi\rho$ ist vom Typ (M). Dann gibt es ein $\mu \in K^*$ derart, daß $\bar{\mu} = -\mu$ und μ der einzige Eigenwert $\neq 1$ von $\pi\rho$ ist. Aus $\mathrm{F}_{\bar{\nu}}(\pi\rho) \neq \{0\}$ folgt daher $\mu = \bar{\nu}$. Wegen $\dim \mathrm{F}_{\bar{\nu}}(\pi\rho) = 2$ und weil $\mathrm{F}_{\bar{\nu}}(\pi\rho)$ totalisotrop ist, erhalten wir $\mathrm{radF}_{\bar{\nu}}(\pi) \neq \{0\}$. Wir haben bereits gesehen, daß $\mathrm{radF}_\nu(\pi) \neq \{0\}$ ist, und folgern hieraus $\mathrm{mip}(\pi) = (x-\nu)^2(x-\bar{\nu})^2(x-1)^2$. Dies ist ein Widerspruch zu $\dim \mathrm{B}(\pi) = 5$ und $\det \pi = -1$.

Betrachte nun den Fall

II.2 $\mathrm{radB}(\pi) = \{0\}$.

Dann ist $1 = \dim\mathrm{rad}\ \mathrm{B}(\pi) + 1 \geq \dim\mathrm{rad}\ \mathrm{B}(\pi\sigma') = \dim\mathrm{B}(\pi\sigma') - 2 = \dim\mathrm{B}(\pi) - 3 \geq 1$ und die beteiligten Größen sind gleich. Wir können daher

(1) $\dim V = 4$ and $\mathrm{F}(\pi) = \{0\}$

annehmen. Falls es einen anisotropen Vektor $v \in V$ mit $q_\pi(v(\pi-1)) = 0$ gibt, erfüllt die Symmetrie $\sigma := \sigma_{v(\pi-1)}$ die Bedingungen $\dim\mathrm{B}(\pi\sigma) = 3$ und $\mathrm{rad}\ \mathrm{B}(\pi\sigma) = \langle v\rangle \cap \langle v\rangle^\perp = \{0\}$. Folglich ist $\pi\sigma$ weder vom Typ (S) noch (M) und wir sind fertig. Wir können deshalb annehmen:

(2) $q_\pi(v(\pi-1)) \in F^*$ impliziert $f(v,v) = 0$ für alle $v \in V$.

Insbesondere muß dann $F_{-1}(\pi)$ totalisotrop sein.

II.2.(a) Sei $\mathrm{F}_{-1}(\pi) \neq 0$.

Dann ist $(x+1)^k$ ein Teiler von $\mathrm{mip}(\pi)$ für ein $k \in \{2,3,4\}$. Aus (1) und (2) erhalten wir $k \neq 3$. Somit ist $\mathrm{mip}(\pi) \in \{(x+1)^2, (x+1)^4, (x^2+1)(x+1)^2, (x-\nu)(x+1)^2, (x-\nu)^2(x+1)^2\}$, wobei $\bar{\nu} = -\nu \neq 0$ gilt.
Ist $\mathrm{mip}(\pi) = (x+1)^2$, so ist $\mathrm{B}(\sigma')$ nicht in dem totalisotropen Unterraum $V(\pi+1) = F_{-1}(\pi)$ enthalten. Mit 3.3.6 (b) folgern wir hieraus $\dim\mathrm{F}_{-1}(\pi\sigma') = 1 = \dim\mathrm{radF}_{-1}(\pi\sigma')$. Nun folgt aus $\det\pi\sigma' = -\det\pi = -1$ aber $\mathrm{mip}(\pi\sigma') = (x+1)^3(x-1)$, ein Widerspruch, da $\pi\sigma'$ vom Typ (S) ist.
Ist $\mathrm{mip}(\pi) \in \{(x+1)^4, (x^2+1)(x+1)^2\}$, so liefert 3.4.28 die Behauptung.
Falls $\mathrm{mip}(\pi) = (x-\nu)(x+1)^2$ ist, gilt $1 = \dim\mathrm{F}_\nu(\pi) - 1 \leq \dim F_\nu(\pi\sigma')$ und $\det\pi\sigma' = -\det\pi = 1$, ein Widerspruch zu der Annahme, daß $\pi\sigma'$ vom Typ (S) ist.
Ist $\mathrm{mip}(\pi) = (x-\nu)^2(x+1)^2$, so erhalten wir eine Zerlegung $V = U \bigoplus W$ in π-Moduln U, W mit $\dim U = 2 = \dim W$, so daß $-\pi_U$ und $\bar{\nu}\pi_W$ Transvektionen sind. Nach 3.4.26 gibt es nun eine Symmetrie σ'', so daß $\mathrm{B}(\sigma'') \leq W$ und $-(\pi\sigma'')_W$ eine Transvektion ist. Dann gilt $\dim\mathrm{B}(\pi\sigma'') = \dim\mathrm{B}(\pi) = 4$ and $1 = \det\pi\sigma'' = (-1)^4$ und $\pi\sigma''$ ist kurz.

II.2.(b) Sei $\mathrm{F}_{-1}(\pi) = \{0\}$.

II.2.(b_1) Zuerst betrachten wir den Fall, daß $\mathrm{mip}(\pi)$ einen Teiler $(x-\nu)^2$ für ein $\nu \in K^*$ mit $\bar{\nu} = -\nu$ hat.
Ist $\mathrm{mip}(\pi) = (x-\nu)^4$, so folgt $\mathrm{mip}(\phi) = (x-1)^4$, wobei $\phi := \bar{\nu}\pi$ sei. Dann ist $q_\phi(a) \in F^*$ für ein $a \in \mathrm{B}(\phi)$ (c.f. 3.4.3) und $a \notin \mathrm{B}^2(\phi)$, da $B^2(\phi)$ totalisotrop ist. Setze $\sigma := \sigma_a$. Nach 3.3.6 (a) ist $\mathrm{F}(\phi\sigma)$ zweidimensional und regulär. Ferner haben wir $\det\phi\sigma = -1$. Dies impliziert $\mathrm{mip}(\phi\sigma) = (x-\mu)^2(x-1)$ für ein $\mu \in K^*$ mit $\bar{\mu} = -\mu$. Ist $\nu = \mu$, so läßt sich $a = v(\phi-1)(\bar{\nu}\phi-1)$ für ein $v \in V$ schreiben (cf. 3.2.2 (b)) und $\langle v(\phi-1)\rangle = \mathrm{F}_\nu(\phi\sigma)$ ist isotrop. Dann erfüllt $a' := v(\phi-1)(\nu\phi-1) = v(\bar{\nu}\pi-1)(\pi-1)$ $q_\pi(a'), q_\phi(a') \in F^*$, cf. 3.4.25. Für $\rho := \sigma_{a'}$ ist deshalb $\dim\mathrm{F}(\phi\rho) = 2$ und $\mathrm{mip}(\phi\rho) = (x-\bar{\nu})^2(x-1)$. Ist $\mu \neq \nu$, folgt $\mu = \bar{\nu}$. Also ist $\eta = \rho$ beziehungsweise

$\eta = \sigma$ eine Symmetrie mit der Eigenschaft $\mathrm{mip}(\phi\eta) = (x-\bar{\nu})^2(x-1)$, i.e. $\mathrm{mip}(\pi\eta) = (x-1)^2(x-\nu)$. Damit ist $\pi\eta$ kurz und $\dim \mathrm{B}(\pi\eta) = 3$.
Falls $\mathrm{mip}(\pi) \neq (x-\nu)^4$ ist, gibt es eine Zerlegung $V = U \bigoplus W$ in π-Moduln U, W mit $\mathrm{mip}(\pi_U) \in \{(x-\nu)^3, (x-\nu)^2\}$. Da π nicht vom Typ (M) ist, folgt $\mathrm{mip}(\pi_W) \neq (x-\nu)^2$. Aus (2) und 3.4.27 erhalten wir $\mathrm{mip}(\pi_W) \neq (x-\bar{\nu})^2$. Wir wenden nun 3.4.2 und 3.2.2 (a) auf π_U an und erhalten eine Symmetrie σ derart, daß $\mathrm{B}(\sigma) \subseteq U$, $\dim \mathrm{B}(\pi\sigma) = 3$ und $\pi\sigma = \pi_U\sigma_U \bigoplus \pi_W$ weder zum Typ (S) noch (M) gehört.

II.2.b$_2$) Als nächstes nehmen wir an, daß $(x-\nu)^2$ kein Teiler von $\mathrm{mip}(\pi)$ für alle $\nu \in K^*$ mit $\bar{\nu} = -\nu$ ist. Wegen $F_{-1}(\pi) = \{0\}$, finden wir ein $\alpha \in K^*$, so daß $\bar{\alpha} = -\alpha$ und $\dim \ker(\pi - \alpha)^2 \geq 2$ ist; cf. 3.4.31. Nach Annahme ist weder $(x-\alpha)^2$ noch $(x-\bar{\alpha})^2$ ein Teiler von $\mathrm{mip}(\pi)$. Dies impliziert $2 \leq \dim \mathrm{F}_\alpha(\pi) \leq \dim \mathrm{F}_\alpha(\pi\sigma') + 1 \leq 2$. Also ist $\dim \mathrm{F}_\alpha(\pi) = 2$ und $\pi\sigma'$ vom Typ (S1). Insbesondere gilt $\det \pi = -\det \pi\sigma' = 1$, so daß wir $V = U \bigoplus W$ schreiben können, wobei $\dim U = 2 = \dim W$, $\pi_U = \alpha \cdot 1_U$ und $\det \pi_W = -1$ ist. Aus $\mathrm{F}(\pi) = \{0\} = \mathrm{F}_{-1}(\pi)$, $\dim \mathrm{F}_{\bar{\alpha}}(\pi) \leq \dim \mathrm{F}_{\bar{\alpha}}(\pi\sigma') + 1 = 1$ und $\mathrm{F}_\alpha(\pi_W) = \{0\}$ erhalten wir nun $\mathrm{mip}(\pi_W) = (x-\bar{\alpha})^2$ entgegen unserer Annahme.

III. Betrachte schließlich den Fall, daß $\pi\sigma'$ vom Typ (M) ist.

Wir beweisen nun CIII. Beachte, daß $\det \pi = -\det \pi\sigma' = -1$, $\dim \mathrm{B}(\pi) = \dim \mathrm{B}(\pi\sigma') + 1 = 5$ und $\mathrm{F}_\nu(\pi\sigma')$ ein zweidimensionaler totalisotroper Unterraum von $\mathrm{B}(\pi)$ für ein $\nu \in K^*$ mit $\bar{\nu} = -\nu$ ist. Aus 3.3.5 (b) erhalten wir $2 \geq \dim \mathrm{radB}(\bar{\nu}\pi) \geq \dim \mathrm{radB}(\bar{\nu}\pi\sigma') - 1 \geq 1$. Demnach ist $(x-\nu)^2$ ein Teiler von $\mathrm{mip}(\pi)$. Wegen $\mathrm{B}(\pi)(\pi-\nu) \neq \mathrm{B}(\pi)$ gibt es einen Vektor $a \in \mathrm{B}(\pi)\backslash\mathrm{B}(\pi)(\pi-\nu)$ mit $q_\pi(a) \in F^*$, cf. 3.4.3. Aus 3.3.6 (b) folgt $\dim \mathrm{B}(\pi\sigma_a) = 4$ und $\dim \mathrm{radB}(\bar{\nu}\pi\sigma_a) \leq 1$. Wir können annehmen, daß $\pi\sigma_a$ vom Typ (M) ist. Wie oben folgern wir hieraus, daß auch $(x-\bar{\nu})^2$ ein Teiler von $\mathrm{mip}(\pi)$ sein muß. Wegen $\dim \mathrm{B}(\pi) = 5$ und $\det \pi = -1$ muß es dann eine Zerlegung $V = U \bigoplus W \bigoplus X \bigoplus Y$ in π-Moduln U, W, X und Y geben, so daß $\dim U = 2 = \dim W$, $\mathrm{mip}(\pi_U) = (x-\nu)^2$, $\mathrm{mip}(\pi_U) = (x-\bar{\nu})^2$, $\dim X = 1$, $\pi_X = -1_X$ und $\pi_Y = 1_Y$ ist. Wähle $\sigma'' := \sigma_X$. Dann ist $\dim \mathrm{B}(\pi\sigma'') = 4$ und $\pi\sigma'' = \pi_U \bigoplus \pi_W \bigoplus 1_{X\oplus Y}$ kurz. ■

$|F| = 3$; Bahn-Dimension ≤ 3 außer lange Abbildungen

Proposition 3.4.33 *Sei $\pi \in \mathrm{U}^\pm(f)$ kurz mit $\dim \mathrm{B}(\pi) = 2$. Ist $\det(\pi) = 1$, so ist $\mathrm{l}(\pi) = 2$. Ist $\det(\pi) = -1$, so ist $\mathrm{l}(\pi) = 3$.*

Beweis. Die Länge kann nicht kleiner als vermutet sein, cf. 3.3.2. Sei $\det \pi = 1$. Lemma 3.4.6 (a) liefert eine Symmetrie σ, so daß $\dim \mathrm{B}(\pi\sigma) = 1$ ist. Wegen $\det \pi\sigma = -1$ ist $\pi\sigma$ eine Symmetrie. Sei nun $\det(\pi) = -1$ angenommen. Weil π kurz ist, muß π vom Typ (N*) sein und 3.4.8 zeigt die Behauptung. ■

Lemma 3.4.34 *Wenn $\pi \in \mathrm{U}^\pm(f)$ kurz ist, $\dim \mathrm{B}(\pi) = 3$ und $\det \pi = 1$ gilt, gibt es eine Symmetrie σ, so daß $\dim \mathrm{B}(\pi\sigma) \leq 3$ und $\pi\sigma$ kurz ist.*

Beweis. Für $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 2$ liefert 3.4.30 die Behauptung. Ist $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 1$, so haben wir $V = U \bigoplus W$ für π-Moduln U und W, wobei $\dim U = 3$, $\mathrm{mip}(\pi_U) = (x-1)^3$

und π_W vom Typ (T) ist. Aus 3.4.33 angewandt auf π_U, erhalten wir Symmetrien σ, ρ, so daß $\pi\sigma = \rho_U \bigoplus \pi_W$ ist. Damit ist $\pi\sigma$ kurz und $\dim \mathrm{B}(\pi\sigma) = 2$. Wir können deshalb annehmen, daß $\mathrm{B}(\pi)$ regulär und $\dim V = 3$ ist. Ist $\mathrm{F}_{-1}(\pi) \neq 0$ zeigen Standardargumente, daß $\mathrm{F}_{-1}(\pi)$ ein regulärer eindimensionaler Unterraum von V sein muß. Also haben wir $V = U \bigoplus W$ für π-Moduln U, W, wobei $\dim U = 1$, $\pi_U = -1_U$, $\dim W = 2$ und $\mathrm{mip}\pi_W \in \{(x-\nu)^2, x-\nu\}$ für ein $\nu \in K^*$ mit $\bar{\nu} = -\nu$ gilt. Ist $\mathrm{mip}(\pi_W) = (x-\nu)^2$, so findet man nach 3.4.3 angewandt auf π_W eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq W$, so daß $(\pi\sigma)_W$ eine Transvektion ist. Dann ist $\pi\sigma$ kurz und $\dim \mathrm{B}(\pi\sigma) = 2$. Falls $\pi_W = \nu \cdot 1_W$ ist, erfüllt jede Symmetrie σ mit $\mathrm{B}(\sigma) \leq W$ bereits $\mathrm{mip}(\pi\sigma) = (x^2+1)(x+1)$. Insbesondere ist $\pi\sigma$ kurz und $\dim B(\pi\sigma) = 3$. Sei nun $\mathrm{F}_{-1}(\pi) = \{0\}$ angenommen. Dann ist $\dim \mathrm{B}(-\pi) = 3$ und $-\pi$ kurz. Nach 3.4.6 (a) gibt es eine Symmetrie σ mit $\dim \mathrm{F}_{-1}(\pi\sigma) = 1$. Wegen $\det \pi\sigma = -1$, ist $\pi\sigma$ nicht vom Typ (N) oder (S3); also ist $\pi\sigma$ kurz und $\dim \mathrm{B}(\pi\sigma) \leq 3$. ■

Proposition 3.4.35 *Sei* $\pi \in \mathrm{U}^{\pm}(f)$ *kurz mit* $\dim \mathrm{B}(\pi) = 3$. *Ist* $\det(\pi) = -1$, *so ist* $\mathrm{l}(\pi) = 3$. *Ist* $\det(\pi) = 1$, *so ist* $\mathrm{l}(\pi) = 4$.

Beweis. Sei zunächst $\det(\pi) = -1$ angenommen. Wenn $\mathrm{F}_{-1}(\pi) \neq \{0\}$ ist, folgt die Behauptung wie in 3.4.14. Wir können daher $\mathrm{F}_{-1}(\pi) = \{0\}$ annehmen. Falls $\mathrm{B}(\pi)$ regulär ist, kann man den in 3.4.15 angegebenen Beweis übernehmen. Wir können also weiterhin annehmen, daß $\mathrm{B}(\pi)$ singulär ist. Wir erhalten dann eine Zerlegung $V = U \bigoplus W \bigoplus X$ in π-Moduln U, W, X, so daß $\dim U = 2$, π_U eine Transvektion, $\mathrm{B}(\pi_W) = W$ ein zweidimensionaler Raum mit $\mathrm{F}_{-1}(\pi) = \{0\}$, $\det \pi_W = -1$ und $\pi_X = 1_X$ ist (vergleiche mit 3.4.18). Wir können $X = \{0\}$ annehmen. Weil π nicht vom Typ (S1) ist, ist π_W eine ν-Homothetie. Nach 3.4.6 (a) gibt es eine Symmetrie σ mit $\dim \mathrm{B}(\pi\sigma) = 2$ und $\det(\pi\sigma) = 1$. Weiterhin ist $\mathrm{F}_\nu(\pi\sigma) \neq 0$. Deshalb ist $\pi\sigma$ kurz und $\mathrm{l}(\pi\sigma) = 2$ nach 3.4.33, i.e. $\mathrm{l}(\pi) = 3$. Sei nun $\det \pi = 1$. Aus 3.4.34 erhalten wir eine Symmetrie σ, für die $\dim \mathrm{B}(\pi\sigma) \leq 3$ und $\pi\sigma$ kurz ist. Aus 3.4.33 und dem vorigen Ergebnis folgt nun $\mathrm{l}(\pi\sigma) = 3$ und $\mathrm{l}(\pi) = 4$. ■

$|F| = 3$; Beweis des Satzes

Sei $\pi \in \mathrm{U}^{\pm}(f)$ mit $m := \dim \mathrm{B}(\pi)$. Aus 3.3.2, 3.4.4, 3.4.23, 3.4.24 und 3.4.11 folgt, daß $\mathrm{l}(\pi)$ nicht kleiner als behauptet sein kann. Der Beweis von 3.4.21 erfolgt durch Induktion über $\dim \mathrm{B}(\pi)$.

(a) Als erstes behandeln wir den Fall, daß π kurz ist. Für $\dim \mathrm{B}(\pi) \leq 3$ haben wir den Beweis in 3.4.33 (,falls $\dim \mathrm{B}(\pi) = 2$ ist,) und 3.4.35 (,falls $\dim \mathrm{B}(\pi) = 3$ ist,) geführt. Wir können daher $\dim \mathrm{B}(\pi) \geq 4$ annehmen. Ist π eine Involution, so ist π bekanntlich ein Produkt von m paarweise kommutierenden Symmetrien. Wir können deshalb $\pi^2 \neq 1_V$ annehemen. Falls $\det \pi = (-1)^m$ ist, gibt es nach 3.4.32 (b) eine Symmetrie σ, so daß $\dim \mathrm{B}(\pi\sigma) = m-1$ und $\pi\sigma$ kurz ist. Dann ist $\mathrm{l}(\pi\sigma) = m-1$ gemäß Induktionsannahme und damit $\mathrm{l}(\pi) = m$. Falls $\det \pi \neq (-1)^m$ ist, gibt es nach 3.4.32 (b) eine Symmetrie σ, so daß $\dim \mathrm{B}(\pi\sigma) \leq m$ und $\pi\sigma$ kurz ist. In diesem Fall folgt $\mathrm{l}(\pi\sigma) = m$ entweder aus dem vorangehenden Ergebnis oder aus der Induktionsannahme. Somit ist $\mathrm{l}(\pi) = m+1$.

(b) Sei π vom Typ (H). Weil $\mathrm{B}(\pi)$ regulär ist, gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq \mathrm{B}(\pi)$. Dann ist $\dim \mathrm{B}(\pi\sigma) = m$ und $\pi\sigma$ kurz. Die Behauptung folgt nun aus (a).

(c) Sei π vom Typ (T) und $\dim V \geq 3$. Falls $\mathrm{F}(\pi)$ nicht totalisotrop ist, wähle eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq F(\pi)$; dann ist $\mathrm{mip}(\pi\sigma) = (x-1)^2(x+1)$, $\pi\sigma$ kurz, $\dim \mathrm{B}(\pi\sigma) = m+1$ und (a) liefert das gewünschte Ergebnis. Falls $\mathrm{F}(\pi)$ totalisotrop ist, gilt $V = U \bigoplus W \bigoplus X$ für π-Moduln U, W und X, wobei $\dim U = 2 = \dim W$ ist, π_U und π_W Transvektionen sind, und π_X vom Typ (T) oder $X = \{0\}$ ist. Weil $-\pi_{U \oplus W}$ kurz ist, findet man eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq U \oplus W$, so daß $\dim \mathrm{F}_{-1}(\pi\sigma) = 1$ ist. Wegen $\det \pi\sigma = -1$ und $\dim \mathrm{radB}((\pi\sigma)_{U \oplus W}) \geq \dim \mathrm{radB}(\pi_{U \oplus W}) - 1 = 1$, erhalten wir $\mathrm{mip}((\pi\sigma)_{U \oplus W}) = (x-1)^3(x+1)$. Deshalb ist $\pi\sigma$ kurz und $\dim B(\pi\sigma) = m+1$. Wiederum beweist nun (a) die Vermutung.

(d) Sei π vom Typ (N) und $\dim V \geq 3$. Es gibt dann eine Zerlegung $V = U \bigoplus W \bigoplus X$, wobei $\dim U = 2$, $-\pi_U$ eine Transvektion, $\pi_W = -1_W$ und $\pi_X = 1_X$ ist. Im Fall $W \neq \{0\}$ wähle eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq U$. Dann ist $\pi\sigma$ kurz, $\dim \mathrm{B}(\pi\sigma) = m$ und die Behauptung folgt aus (a). Ist $W = \{0\}$, so muß $X \neq \{0\}$ sein, da $\dim V \geq 3$ ist. Sei $u \in U$ ein isotroper Vektor mit $U = \langle u, u(\pi+1) \rangle$ und $w \in X \backslash \{0\}$ mit $f(w,w) = 1$. Setze $a := (u-w)(\pi+1) = u(\pi+1)+w \in B(-\pi)$. Dann ist $f(a,a) = 1$ und daher $\sigma := \sigma_a$ eine wohl definierte Symmetrie. Wegen $\mathrm{B}(\sigma) \not\subseteq \mathrm{B}(\pi)$ zeigt 3.3.3, daß $\dim \mathrm{B}(\pi\sigma) = m+1 = 3$ ist. Ferner ist $q_{-\pi}(a) = 1 - f(u, u(\pi+1)) \notin F^*$, so daß $\mathrm{F}_{-1}(\pi\sigma) = \mathrm{F}_{-1}(\pi)$ ein eindimensionaler totalisotroper Unterraum ist, cf. 3.2.2 (b). Nun folgt aus $\det \pi\sigma = -1$, daß $\mathrm{mip}(\pi\sigma) = (x+1)^3$ und $\pi\sigma$ damit kurz ist. Nach (a) ist $\mathrm{l}(\pi\sigma) = 3$ und wir schließen $\mathrm{l}(\pi) = 4$.

(e) Sei π vom Typ (S3) und $\dim V \geq 3$. Ist $\dim \mathrm{B}(\pi) = 2$, so folgt die Behauptung aus (d). Ist $\dim \mathrm{B}(\pi) \geq 3$, so zerlegen wir $V = U \bigoplus W \bigoplus X$ in π-Moduln U, W und X mit $\dim U = 2 = \dim W$ derart, daß $-\pi_U$ und π_W Transvektionen sind und $\pi_X = 1_X$ ist. Wähle eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq W$. Dann ist $\pi\sigma$ kurz, $\dim \mathrm{B}(\pi\sigma) = m+1$ und (a) ergibt wiederum das Gewünschte.

(f) Sei π vom Typ (S1) und $\dim V \geq 3$. Falls $m = 2$ ist, gibt es nach Lemma 3.4.26 eine Symmetrie σ, so daß $\pi\sigma$ vom Typ (N) und $\dim\, \mathrm{B}(\pi\sigma) = 2$ ist. Aus (d) folgt $\mathrm{l}(\pi\sigma) = 4$, also $\mathrm{l}(\pi) = 5$. Falls $m \geq 3$ ist, gibt es nach Lemma 3.4.17 eine Symmetrie σ, so daß $\pi\sigma$ vom Typ (S3) und $\dim \mathrm{B}(\pi\sigma) = m-1$ ist. In diesem Fall folgt das Ergebnis aus (e).

(g) Sei π vom Typ (S2). Dann gilt $V = U \bigoplus W$ für π-Moduln U und W, wobei π_U zyklisch mit $\mathrm{mip}(\pi_U) = (x-1)^4$ und π_W vom Typ (T) oder $= 1_W$ ist. Aus 3.4.32 (a) angewandt auf π_U findet man eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq U$ und $\dim \mathrm{B}(\pi\sigma) = m-1$. Weil $U(\pi-1)^2$ totalisotrop ist, folgt $\mathrm{B}(\sigma) \not\subseteq U(\pi-1)^2$. Nach 3.3.6 (a) ist dann $(\pi\sigma)_U$ vom Typ (S1). Demnach ist auch $\pi\sigma$ vom Typ (S1) und die Behauptung folgt aus (f).

(h) Sei π vom Typ (M). Dann gilt $V = U \bigoplus W \bigoplus X$ für π-Moduln U, W und X, wobei $\dim U = 2 = \dim W$, $\mathrm{mip}(\pi_U) = (x-\nu)^2 = \mathrm{mip}(\pi_W)$ für ein $\nu \in K^*$ mit $\bar{\nu} = -\nu$ und $\pi_X = 1_X$ ist. Nach 3.4.26 findet man eine Symmetrie σ, so daß $\mathrm{B}(\sigma) \leq U$ und $-\pi\sigma_U$ eine Transvektion ist. Dann ist $\pi\sigma$ kurz, $\dim \mathrm{B}(\pi\sigma) = 4$ und $\det \pi = -1$. Aus (a) erhalten wir $\mathrm{l}(\pi\sigma) = 5$, i.e. $\mathrm{l}(\pi) = 6$.

Die Behauptung (c) von Theorem 3.4.21 wurde in 3.4.11 bewiesen. ■

3.5 $\mathrm{char}(K) = 2$

Für das folgende setzen wir $\mathrm{char}(K) = 2$ und wiederum die Surjektivität der Normabbildung voraus.

Das Symmetrienlängenproblem läßt sich in dieser Situation für Körper, die mehr als vier Ele-

mente enthalten, relativ mühelos lösen. Nach den üblichen Vorbereitungen umfaßt die wesentliche Induktion 3.5.6 kaum mehr als eine Textseite.
Anders sieht es hingegen für den kleinstmöglichen Skalarenkörper unitärer Gruppen $K = F_4$ aus, wo mit unseren Methoden viele Einzelfälle separat betrachtet werden müssen.

Definition 3.5.1 *Sei $\pi \in \mathrm{SU}(f)$. Nenne π lang, falls π eine der folgenden Eigenschaften* (H) *oder* (N) *besitzt. Andernfalls heiße π kurz.*

(H) $\pi \neq 1$ *und* $\pi|_{\mathrm{B}(\pi)}$ *ist eine μ-Homothetie für ein $\mu \in K\backslash\{1\}$;*

(N) $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 1$.

Dann hat π eine der folgenden Formen.

(H) $V = U \bigoplus X$, *wobei* $\pi_U = \mu \cdot 1_U$ *für ein* $\mu \in K\backslash\{1\}$ *mit* $\mu\bar{\mu} = 1$ *und* $\pi_X = 1_X$ *gilt (,i.e. π induziert auf U eine Homothetie $\neq 1$).*

(N) $V = U \bigoplus W$, *wobei* $\dim U = 3$, $\mathrm{mip}(\pi_U) = (x+1)^3$ *und* π_W *eine Involution ist.*

Lemma 3.5.2 *Seien $\pi \in \mathrm{U}(f)$ und W ein Unterraum von $\mathrm{B}(\pi)$, $W \neq \mathrm{B}(\pi)$. Ist $|F| = 2$, so gelte $\dim W \leq \dim \mathrm{B}(\pi) - 2$ oder $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \geq 4$. Ferner enthalte $\mathrm{B}(\pi)$ eine hyperbolische Ebene. Es gibt dann ein $a \in \mathrm{B}(\pi)\backslash W$, so daß $q_\pi(a) \in F^*$ ist, außer wenn π auf $\mathrm{B}(\pi)$ eine μ-Homothetie für ein $\mu \in K^*\backslash\{1\}$ mit $\mu\bar{\mu}$ induziert.*

Beweis. Für jedes $a \in \mathrm{B}(\pi)$ sind die folgenden Aussagen äquivalent (cf. 3.2.3):

(i) $q_\pi(a) \in F^*$;

(ii) $f(a,a) = s(a,a) = 0$ und $d(a,a) \neq 0$.

Angenommen es gibt kein $a \in \mathrm{B}(\pi)\backslash W$ mit obigen Eigenschaften. Nach 3.2.3 folgt dann aus $s(a,a) = 0$ auch $d(a,a) = 0$ für alle $a \in \mathrm{B}(\pi)\backslash W$. Nach 3.1.3 (falls $|F| > 2$ oder $\dim W \leq \dim \mathrm{B}(\pi) - 2$) und 3.1.4 (falls $|F| = 2$ und $\dim W = \dim \mathrm{B}(\pi) - 1$) gilt $d = \lambda s$ für ein $\lambda \in F$. Ist $\lambda = 0$, so induziert π auf $\mathrm{B}(\pi)$ eine $i\bar{i}^{-1}$-Homothetie (cf. 3.2.3). Andernfalls folgt $s = \lambda^{-1} d$. Weil π wegen $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \geq 2$ keine Involution sein kann erhält man in diesem Fall die Behauptung aus 3.2.4. ■

Lemma 3.5.3 *Seien $\pi \in \mathrm{U}(f)$, $\pi^2 \neq 1$ und W ein Unterraum von $\mathrm{B}(\pi)$, $W \neq \mathrm{B}(\pi)$. Dann gibt es ein $a \in \mathrm{B}(\pi)\backslash W$ mit $q_\pi(a) \in F^*$, außer wenn eine der folgenden Situationen vorliegt:*

- $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 1$,
- $|F| = 2$ *und* $\dim W = \dim \mathrm{B}(\pi) - 1$ *und* $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \leq 3$,
- *π induziert eine μ-Homothetie auf* $\mathrm{B}(\pi)$ *für ein $\mu \in K^*\backslash\{1\}$ mit $\mu\bar{\mu}$.*

Ist $\pi \in \mathrm{SU}(f)$ und [$|F| > 2$ oder $\dim W \leq \dim \mathrm{B}(\pi) - 2$ oder $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \geq 4$], so ist dies genau dann der Fall, wenn π vom Typ (N) *oder* (H) *ist.*

Beweis. Enthält $\mathrm{B}(\pi)$ eine d-hyperbolische Ebene, so folgt die Behauptung aus 3.5.2. Andernfalls ist $\dim \mathrm{B}(\pi)/d\text{-rad } \mathrm{B}(\pi) \leq 1$, da $\mathcal{N}(K) = F$ ist, cf. 3.3.7. Demnach gilt $\dim \mathrm{B}(\pi)/\text{rad } \mathrm{B}(\pi) = 1$, da $\pi^2 \neq 1$ ist. Ist $\det \pi = 1$, so hat auch die von π auf $\mathrm{B}(\pi)/\text{rad } \mathrm{B}(\pi)$ induzierte Abbildung die Determinante 1. Demnach ist π vom Typ (N).

Lemma 3.5.4 (Untere Schranken für lange Abbildungen.) *Seien $\pi \in \mathrm{SU}(f)$ lang und $m := \dim \mathrm{B}(\pi)$. Dann gilt*

$$\mathrm{l}(\pi) \geq \begin{cases} m+1 & , \textit{falls } \pi \textit{ vom Typ } (\mathrm{H}) \textit{ ist,} \\ m+2 & , \textit{falls } \pi \textit{ vom Typ } (\mathrm{N}) \textit{ ist.} \end{cases}$$

Beweis. Ist π vom Typ (H) und σ eine beliebige Symmetrie, so ist $\dim \mathrm{B}(\pi\sigma) = m$, falls $\mathrm{B}(\sigma) \leq \mathrm{B}(\pi)$ ist. Andernfalls folgt aus 3.3.3, daß $\dim \mathrm{B}(\pi\sigma) = m+1$ ist. Also ist $\mathrm{l}(\pi\sigma) \geq m$ nach 3.3.1 (angewandt auf $\pi\sigma$). Sei nun π vom Typ (N). Die Annahme $\mathrm{l}(\pi) \leq m+1$, i.e. $\pi = \sigma_1 \cdots \sigma_k$ für Symmetrien σ_i und ein $k \in \{m, m+1\}$ hat $\mathrm{B}(\sigma_i) \leq \mathrm{B}(\pi)$ für jedes $i \in \mathbb{N}_{\leq k}$ zur Folge. Da $\dim \mathrm{B}(\pi)/\text{rad } \mathrm{B}(\pi) = 1$ ist, liegt jeder isotrope Vektor von $\mathrm{B}(\pi)$ in rad $\mathrm{B}(\pi)$. Hieraus folgt $\mathrm{B}(\pi) \leq \mathrm{B}(\sigma_1) + \cdots + \mathrm{B}(\sigma_k) \leq \text{rad } \mathrm{B}(\pi)$, ein Widerspruch. ■

3.5.1 $|F| > 2$

Satz 3.5.5 *Seien $|F| > 2$ und $\pi \in \mathrm{SU}(f)$, $m := \dim \mathrm{B}(\pi)$. Dann ist π ein Produkt von Symmetrien.*
(a) *Ist π kurz, so gilt $\mathrm{l}(\pi) = m$*
(b) *Ist π lang, so gilt*

$$\mathrm{l}(\pi) = \begin{cases} m+1 & , \textit{falls } \pi \textit{ vom Typ } (\mathrm{H}) \textit{ ist,} \\ m+2 & , \textit{falls } \pi \textit{ vom Typ } (\mathrm{N}) \textit{ ist.} \end{cases}$$

$|F| > 2$; Induktion

Lemma 3.5.6 (Induktions-Lemma.) *Sei $\pi \in \mathrm{SU}(f)\backslash\{1_V\}$ kurz. Es gibt dann eine Symmetrie σ mit den folgenden Eigenschaften:*

(a) $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$,

(b) *$\pi\sigma$ ist kurz.*

Beweis. (a) Nach 3.5.3 (mit $W = \{0\}$) und 3.2.2 (a) gibt es eine Symmetrie σ', so daß $\mathrm{F}(\pi\sigma') > \mathrm{F}(\pi)$ ist. Dies beweist (a).

(b) Ist $\pi\sigma'$ kurz, so ist (b) erfüllt. Wir können daher annehmen, daß $\pi\sigma'$ lang ist, i.e. zu einem der Typen (H),(N) gehört. Dann gilt insbesondere $\dim \mathrm{B}(\pi) \geq 3$. (Ist $\dim \mathrm{B}(\pi) \leq 2$, so ist $\pi\sigma'$ eine Symmetrie oder die Identität und damit insbesondere kurz.) Ist π eine Involution, so ist π bekanntlich ein Produkt von $m := \dim \mathrm{B}(\pi)$ Symmetrien $\sigma_1, \ldots, \sigma_m$. Die Symmetrie σ_m hat dann die gewünschten Eigenschaften. Wir können daher weiterhin annehmen, daß π keine Involution ist. In (i), (ii) sei σ eine beliebige Symmetrie mit $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$.

(i) Ist $\pi\sigma'$ vom Typ (H), so ist $\pi\sigma$ kurz oder ebenfalls vom Typ (H).

Beweis. Nach Vorraussetzung gilt $\mathrm{F}_\mu(\pi\sigma') = \mathrm{B}(\pi\sigma')$ für ein $\mu \in K\backslash\{1\}$. Aus $\mu^2 \neq 1 = \det \pi\sigma'$ folgt $\dim \mathrm{B}(\pi) \geq 4$. Dies liefert $\dim \mathrm{F}_\mu(\pi) \geq \dim \mathrm{B}(\pi\sigma') - 1 = \dim \mathrm{B}(\pi) - 2 \geq 2$, also $\dim \mathrm{F}_\mu(\pi\sigma) \geq 1$. Folglich ist $\pi\sigma$ kurz oder vom Typ (H).

Ist $\pi\sigma'$ vom Typ (H), so gilt $\dim \mathrm{B}(\pi) \geq 4$, wie wir im Beweis von (i) gesehen haben. Dies bedeutet $\dim \mathrm{F}_\mu(\pi) \geq 2$ für ein $\mu \in K\backslash\{1\}$, also $\dim \mathrm{B}(\pi)(\pi + \mu) \leq \dim \mathrm{B}(\pi) - 2$. Demnach liefert 3.5.3 ein $a \in \mathrm{B}(\pi)\backslash\mathrm{B}(\pi)(\pi + \mu)$, so daß $\alpha := q_\pi(a) \in F^*$ ist. Nach 3.3.6 (b) erfüllt $\sigma := \sigma_{\alpha^{-1},a}$ die Bedingungen $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) \neq 0$ (,da π nicht vom Typ (H) ist). Somit ist $\pi\sigma$ nicht vom Typ (H) und (i) ergibt, daß $\pi\sigma$ kurz ist.

(ii) Ist $\pi\sigma'$ vom Typ (N), so ist $\pi\sigma$ kurz oder ebenfalls vom Typ (N).
Dies folgt aus (i), indem man σ und σ' vertauscht.

Abschließend betrachten wir den Fall, daß $\pi\sigma'$ vom Typ (N) ist. Zunächst sei $B^2(\pi) < B(\pi)$ angenommen. Analog zum ersten Fall finden wir eine Symmetrie σ mit $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) > 1$ (,da π keine Involution und nicht vom Typ (N) ist). Demnach ist $\pi\sigma$ nicht vom Typ (N) und (ii) zeigt nun, daß $\pi\sigma$ kurz ist. Ist $\mathrm{B}^2(\pi) = \mathrm{B}(\pi)$, so gilt $\mathrm{rad}\ \mathrm{B}(\pi) = \{0\}$. Wir können dann $V = B(\pi)$ und $\mathrm{F}(\pi) = \{0\}$ annehmen. Man berechnet

$$\begin{aligned} \dim \mathrm{B}(\pi) &= \dim \mathrm{B}(\pi) - \mathrm{F}(\pi) \\ &\leq \dim \mathrm{B}(\pi) - (\dim \mathrm{F}(\pi\sigma') - 1) \\ &= \dim \mathrm{B}(\pi) - (\dim \mathrm{B}(\pi\sigma') - 2) = 3. \end{aligned}$$

Dies ergibt $\dim \mathrm{B}(\pi) = 3$. Weiterhin ist $\phi := (\pi - 1)^{-1} \in \mathrm{GL}(V)$, so daß $g := f \circ \phi \times \phi$ eine wohldefinierte $^-$-hermitesche Form auf V ist. Falls es ein $a \in B(\pi)$ mit $s(a,a) = 0$ und $d(a,a) \neq 0 \neq g(a,a)$ gibt, gilt $\alpha := q_\pi(a) \in F^*$ und die Symmetrie $\rho := \sigma_{\alpha^{-1},a}$ erfüllt $\mathrm{F}(\pi\rho) = \langle a\phi\rangle \not\leq \mathrm{B}(\pi\rho) = \langle a\phi\rangle^\perp$, da $a\phi$ anisotrop ist. Demnach ist $\pi\rho$ kurz. Wir können daher annehmen:
$s(a,a) = 0$ impliziert $d(a,a) = 0$ oder $g(a,a) = 0$ für alle $a \in V$.
Wegen $|F| \geq 4$ und da π kurz ist folgt aus 3.1.6, daß $g = \lambda s$ für ein $\lambda \in F$ gilt. Eine einfache Rechnung zeigt nun, daß $\mathrm{mip}(\pi)$ ein Teiler von $x^2 + \lambda^{-1}x + 1$ ist. Da π keine Homothetie ist, erhalten wir $\mathrm{mip}(\pi) = x^2 + \lambda^{-1}x + 1$. Nun erzwingen $\dim V = 3$ und $\deg(\mathrm{mip}(\pi)) = 2$ jedoch $\mathrm{mip}(\pi) = (x - \mu)(x - \nu)$ und $\dim F_\mu(\pi) = 2$ für geeignete $\mu, \nu \in K^*\backslash\{1\}$. Dies impliziert wiederum $\dim F_\mu(\pi\sigma') \geq 1$, ein Widerspruch. ■

$|F| > 2$; Beweis des Satzes

Seien $\pi \in \mathrm{SU}(f)\backslash\{1_V\}$ und sei $m := \dim \mathrm{B}(\pi)$. Nach 3.3.1 und 3.5.4 kann $\mathrm{l}(\pi)$ nicht kleiner als behauptet sein. Der Beweis von 3.5.5 erfolgt durch Induktion über $\dim \mathrm{B}(\pi)$.
(i) Als erstes betrachten wir den Fall, daß π kurz ist. Ist $m = 1$, so ist π eine Symmetrie. Ist $m > 1$ so gibt es nach 3.5.6 eine Symmetrie σ, so daß $\dim \mathrm{B}(\pi\sigma) = m - 1$ und $\pi\sigma$ kurz ist. Nach Induktionsannahme gilt dann $\mathrm{l}(\pi\sigma) = m - 1$, also $\mathrm{l}(\pi) = m$.
(ii) Sei nun π eine lange Abbildung. Ist π vom Typ (H), so gilt $\pi_{\mathrm{B}(\pi)} = \mu 1_{\mathrm{B}(\pi)}$ für ein $\mu \in K^*\backslash\{1\}$ mit $\mu\bar{\mu} = 1$. Wähle eine beliebige Symmetrie σ mit $\mathrm{B}(\sigma) \leq B(\pi)$. Dann gilt $\dim \mathrm{B}(\pi\sigma) =$

$\dim \mathrm{B}(\pi) = m$ und $\mathrm{mip}((\pi\sigma)_{\mathrm{B}(\pi\sigma)}) = (x+\mu)^2$. Folglich ist $\pi\sigma$ kurz und $\mathrm{l}(\pi\sigma) = m$ nach (i). Dies ergibt $\mathrm{l}(\pi) = m+1$. Ist schließlich π vom Typ (N), so gilt $V = U \bigoplus W$ für π-Moduln U und W mit $\dim U = 3$ und $\mathrm{mip}(\pi_U) = (x+1)^3$. Wähle ein $\mu \in K^* \backslash \{1\}$ mit $\mu\bar{\mu} = 1$. Dann gilt $\mathrm{mip}(\mu\pi_U) = (x+\mu)^3$ und 3.5.3 und 3.2.2 liefern eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq U$ und $\dim \mathrm{F}((\mu\pi\sigma)_U) = 1$, i.e. $\dim \mathrm{F}_{\bar{\mu}}(\pi\sigma) = \dim \mathrm{F}_{\bar{\mu}}((\pi\sigma)_U) = 1$. Somit ist $\pi\sigma$ kurz. Aus (i) folgt nun $\mathrm{l}(\pi\sigma) = \dim \mathrm{B}(\pi\sigma) \leq m+1$ und somit $\mathrm{l}(\pi) \leq m+2$. ■

3.5.2 $|F| = 2$

Wir wollen nun die eigentlich interessante Situation $K = \mathrm{F}_4$ studieren. Zusätzlich zu den Typen (H) und (N) (cf. 3.5.1) treten hier vier weitere Ausnahmetypen auf, welche eine größere Symmetrienlänge haben, als es ihre Bahndimension zunächst erwarten läßt. Der Grund hierfür liegt darin, daß $SU(3,2)$ nicht von Symmetrien erzeugt wird. Dieser 'Defekt' spiegelt sich auch, wie wir es schon für $SU(2,3)$ im Fall $K = \mathrm{F}_9$ beobachten konnten, in höheren Dimensionen wieder.

Definition 3.5.7 *Ein* $\pi \in \mathrm{SU}(f)$ *heiße*
vom Typ (A), *wenn* $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 3$ *ist und* π *auf* $\mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi)$ *eine unzerlegbare Abbildung* $\tilde{\pi}$ *induziert. Weil* $(x+\alpha)^3$, $\alpha \in K^*$, *die einzigen Polynome in* $F_2[x]$ *vom Grad* 3 *mit konstantem Glied* 1 *sind, welche Potenzen irreduzibler Polynome sind, folgt:*
(A1) $\mathrm{mip}(\tilde{\pi}) = (x+\mu)^3$ *für ein* $\mu \in K\backslash F$ *und* $V = A \bigoplus B$ *für* π*-Moduln* A, B *mit* $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+\mu)^3$ *und* $\pi_B^2 = 1_B$*;*
oder
(A2) $\mathrm{mip}(\tilde{\pi}) = (x+1)^5$ *und* $V = A \bigoplus B$ *für* π*-Moduln* A, B *mit* $\dim A = 5$, $\mathrm{mip}(\pi_A) = (x+1)^5$ *und* $\pi_B^2 = 1_B$.

vom Typ (B), *wenn* $\dim \mathrm{B}(\pi)/F_\mu(\pi) = 2$ *für ein* $\mu \in K\backslash F$ *gilt,* π *auf* $\mathrm{B}(\pi)/\mathrm{F}_\mu(\pi)$ *eine unzerlegbare Abbildung* $\hat{\pi}$ *induziert und* π *nicht vom Typ* (N),(A) *ist. Weil* $(x+\alpha)^2$, $\alpha \in K\backslash F$, *die einzigen Polynome in* $F_2[x]$ *vom Grad* 2 *mit konstantem Glied* $\neq 0$ *sind, die Potenzen irreduzibler Polynome sind, folgt:*
(B1) $\mathrm{mip}(\hat{\pi}) = (x+\bar{\mu})^2$, $V = A \bigoplus F_\mu(\pi) \bigoplus \mathrm{F}(\pi)$ *für einen* π*-Modul* A *mit* $\dim A = 2$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^2$ *und* $\dim F_\mu(\pi) \equiv 2 \pmod 3$*;*
oder
(B2) $\mathrm{mip}(\hat{\pi}) = (x+1)^2$, $V = A \bigoplus F_\mu(\pi) \bigoplus B$ *für* π*-Moduln* A, B *mit* $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+1)^3$, $B \leq \mathrm{F}(\pi)$ *und* $0 \neq \dim F_\mu(\pi) \equiv 0 \pmod 3$*;*
oder
(B3) $\mathrm{mip}(\hat{\pi}) = (x+\mu)^2$, $V = A \bigoplus C \bigoplus \mathrm{F}(\pi)$ *für* π*-Moduln* A, C *mit* $C \leq \mathrm{F}_\mu(\pi)$, $0 \neq \dim C \equiv 0 \pmod 3$, $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+\mu)^3$.

vom Typ (C), *wenn* $\dim \mathrm{B}(\pi) = 5$ *ist und es ein* $\mu \in K\backslash F$ *gibt, so daß* $\mathrm{F}_\mu(\pi)$ *eindimensional und regulär und* $\mathrm{F}_{\bar{\mu}}(\pi)$ *zweidimensional und totalisotrop ist. Es gilt dann* $V = \mathrm{F}_\mu(\pi) \bigoplus A \bigoplus B \bigoplus \mathrm{F}(\pi)$ *für* π*-Moduln* A, B *mit* $\dim A = 2 = \dim B$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^2 = \mathrm{mip}(\pi_B)$.

vom Typ (D), *wenn* $\dim \mathrm{B}(\pi) = 6$ *ist und es ein* $\mu \in K \backslash F$ *gibt, so daß* $\mathrm{F}_\mu(\pi)$ *dreidimensional und totalisotrop ist. Es gibt dann eine Zerlegung* $V = A_1 \oplus A_2 \oplus A_3 \oplus \mathrm{F}(\pi)$ *in* π*-Moduln* A_i *mit* $\dim A_i = 2$, $\mathrm{mip}(\pi_{A_i}) = (x+\mu)^2$.

Ziel aller weiteren Untersuchungen wird es sein, den folgenden Satz zu beweisen.

Satz 3.5.8 *Seien* $|F| = 2$, $\pi \in \mathrm{SU}(f)$ *und* $m := \dim \mathrm{B}(\pi)$.
(a) *Ist* π *kurz, so gilt* $\mathrm{l}(\pi) = m$
(b) *Ist* π *lang, so gilt*

$$\mathrm{l}(\pi) = \begin{cases} m+1 & , falls\ \pi\ vom\ Typ\ (\mathrm{H})\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{N})\ und\ \dim V \neq 3\ ist, \\ \infty & , falls\ \pi\ vom\ Typ\ (\mathrm{N})\ und\ \dim V = 3\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{A1})\ und\ \dim V \neq 3\ ist, \\ \infty & , falls\ \pi\ vom\ Typ\ (\mathrm{A1})\ und\ \dim V = 3\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{A2})\ ist, \\ m+1 & , falls\ \pi\ vom\ Typ\ (\mathrm{B})\ ist, \\ 6 & , falls\ \pi\ vom\ Typ\ (\mathrm{C})\ ist, \\ 7 & , falls\ \pi\ vom\ Typ\ (\mathrm{D})\ ist. \end{cases}$$

Lemma 3.5.9 *Sei* $\dim V = 3$. *Dann ist* $|\mathrm{SU}(f)| = 2^3 \cdot 3^3$, $\mathrm{SU}(f)$ *besitzt genau eine* 3*-Sylowgruppe* S *und es gilt* $\mathrm{SU}(f) \cong SQ_8$, *wobei* Q_8 *die Quaternionengruppe der Ordnung* 8 *bezeichne. Die von den Symmetrien erzeugte Untergruppe ist die Kommutatorgruppe* $\mathrm{SU}(f)' = S\mathbb{Z}_2$ *der Ordnung* $2 \cdot 3^3$, *wobei* $\mathbb{Z}_2$ *die zyklische Gruppe der Ordnung* 2 *sei. Insbesondere wird* $\mathrm{SU}(f)$ *nicht von Symmetrien erzeugt.*

Beweis. Siehe [69] Kapitel 10, S. 123 f. oder auch [42] Kapitel II, §10, Beweis von Satz 10.14. ■

Korollar 3.5.10 *Ist* $\dim V = 3$ *und* $\pi \in \mathrm{SU}(f)$ *unzerlegbar, so ist* π *kein Produkt von Symmetrien.*

Beweis. Wegen $\mathrm{mip}(\pi) \in \{(x+\alpha)^3, \alpha \in K^*\}$ hat π die Ordnung 4, falls $\alpha = 1$ ist, oder 12, falls $\alpha \neq 1$ ist. In jedem Fall teilt 4 die Ordnung von π. Wegen $|\mathrm{SU}(f)'| = |S\mathbb{Z}_2| = 2 \cdot 3^3$ (cf. 3.5.9) teilt 4 nicht die Ordnung von $\mathrm{SU}(f)'$. Folglich gilt $\pi \notin \mathrm{SU}(f)'$. Nach 3.5.9 ist π deshalb kein Produkt von Symmetrien. ■

Wir wollen am Rande die Situation für $\dim V = 3$ näher erläutern. Hierfür werden die Längenangaben des später zu beweisenden Satzes 3.5.8 bereits im voraus benutzt. Um Unsicherheiten auszuschließen, werden wir deshalb im weiteren Text an keiner Stelle auf die Ergebnisse der nun folgenden Bemerkung zurückgegriffen.

Bemerkung 3.5.11 *Seien* $\dim V = 3$, $\mathcal{S}$ *die Menge der Symmetrien in* $\mathrm{SU}(f)$ *und* $\mu \in K \backslash F$. *Es gilt:*

(1) $|\mathcal{S}| = 9$;

(2) $\mathcal{S}^2 = \{\pi \in \mathrm{SU}(f); \mathrm{mip}(\pi) = x^3 + 1 = (x+\mu)(x+\bar{\mu})(x+1)\} \cup \{1_V\}$ *und* $|\mathcal{S}^2| = 25$;

(3) *$\mathcal{S}^2 \cap \mathcal{S}^3 = \emptyset$, $\mathcal{S}^3 = K^*\mathcal{S}$, $\mathcal{S}^3 \backslash \mathcal{S} = (K\backslash F)\mathcal{S}$ und $|\mathcal{S}^3\backslash\mathcal{S}| = |K\backslash F||\mathcal{S}| = 18$;*

(4) *$\mathcal{S}^4 \cap \mathcal{S}^3 = \emptyset$, $\mathcal{S}^4\backslash\mathcal{S}^2 = (K\backslash F)\{1_V\} == \{\mu 1_V, \bar{\mu}1_V\}$, $|\mathcal{S}^4\backslash\mathcal{S}^2| = 2$ und $\langle\mathcal{S} = \mathcal{S} \dot{\cup} \mathcal{S}^2 \dot{\cup} \mathcal{S}^3\backslash\mathcal{S} \dot{\cup} \mathcal{S}^4\backslash\mathcal{S}^2$;*

(5) *$S := \mathcal{S}^2 \cup \mathcal{S}^4$ ist die nicht-abelsche Gruppe vom Exponenten 3 der Ordnung 3^3, die aus 1_V und allen Elementen der Ordnung 3 aus $\mathrm{SU}(f)$ besteht. Insbesondere ist sie eine und auch die einzige 3-Sylowgruppe von $\mathrm{SU}(f)$ (vgl. 3.5.9). Es ist $\mathrm{Z}(S) = \mathrm{Z}(\mathrm{SU}(f)) = K^*\{1_V\}$ und $S/\mathrm{Z}(S)$ eine elementarabelsche Gruppe der Ordnung 9, also isomorph zu $F_3 \oplus F_3$ (cf.[42] Kapitel I., §14, Satz 14.10 b)).*

Beweis. (1). Nach 3.1.1 (b) enthält V genau 9 eindimensionale singuläre Teilräume, und jeder dieser ist die Bahn von genau einer Symmetrie.

(2) Sei $\pi \in \mathrm{SU}(f)$ mit $\mathrm{mip}(\pi) = (x+\mu)(x+\bar{\mu})(x+1)$. Dann ist π kurz und $\dim \mathrm{B}(\pi) = 2$. Nach 3.5.8 gilt $\mathrm{l}(\pi) = 2$, also insbesondere $\pi \in \mathcal{S}^2$. Sind $\rho, \sigma \in \mathcal{S}$ zwei verschiedene Symmetrien, so gilt $\mathrm{B}(\rho) \not\perp \mathrm{B}(\sigma)$, da V den Wittindex 1 hat. Es gibt deshalb ein $a \in \mathrm{B}(\rho)$ und ein $b \in \mathrm{B}(\sigma)$ mit $f(a,b) = 1$. Man berechnet nun

$$(a+\mu b)\rho\sigma = (\bar{\mu}a + \mu b)\sigma = \bar{\mu}(a+\mu b)$$

und analog $(a+\bar{\mu}b)\rho\sigma = \mu(a+\bar{\mu})b$. Es folgt $\rho\sigma = \bar{\mu}1_{\langle a+\mu b\rangle} \bigcirc\!\!\!\!\perp\, \mu 1_{\langle a+\bar{\mu}b\rangle} \bigcirc\!\!\!\!\perp\, 1_{\langle a,b\rangle^\perp}$. Damit ist $\mathrm{mip}(\rho\sigma) = (x+\mu)(x+\bar{\mu})(x+1)$.
Ein $\pi \in \mathcal{S}^2\backslash\{1_V\}$ ist eindeutig durch das Tripel $(\mathrm{F}_\mu(\pi), \mathrm{F}_{\bar{\mu}}(\pi), \mathrm{F}(\pi))$ festgelegt, das aus drei paarweise zueinander senkrechten eindimensionalen regulären Teilräumen besteht. Weil es in einem m-dimensionalen regulären unitären Vektorraum über F_{q^2}, q eine Primzahlpotenz, genau

$$(q^{2n} - 1 - (q^{n-1} - (-1)^{n-1})(q^n - (-1)^n)/(q^2-1)$$

reguläre eindimensionale Teilräume gibt (cf.3.1.1), gibt es in V genau

$$((4^3-1) - (2^2-1)(2^3+1))((4^2-1) - (2+1)(2^2-1))((4^3-1) - (2^0-1)(2+1))/27 = 24$$

solche Tripel. Demnach gilt $|\mathcal{S}^2| = 24 + 1 = 25$.

(3). Wir zeigen zunächst: Sind $\rho, \sigma, \eta \in \mathcal{S}$ derart, daß $\dim(\mathrm{B}(\rho) + \mathrm{B}(\sigma) + \mathrm{B}(\eta)) \leq 2$ ist, so gilt $\rho\sigma\eta \in \mathcal{S}$.

Die Behauptung ist trivial, wenn $|\{\rho,\sigma,\eta\}| \leq 2$ ist. Man kann daher annehmen, daß ρ, σ, η paarweise verschieden sind. Nach Voraussetzung gilt dann $\mathrm{B}(\eta) \leq \mathrm{B}(\rho) \oplus \mathrm{B}(\sigma)$. Im Beweis von (2) haben wir gesehen, daß $H := \mathrm{B}(\rho) \oplus \mathrm{B}(\sigma)$ eine hyperbolische Ebene ist und man deshalb ein $a \in \mathrm{B}(\rho)$ und ein $b \in \mathrm{B}(\sigma)$ mit $f(a,b) = 1$ findet. Weil H genau 3 singuläre eindimensionale Teilräume besitzt, nämlich $\langle a\rangle, \langle b\rangle, \langle a+b\rangle$, folgt $\mathrm{B}(\eta) = \langle a+b\rangle$. Man berechnet nun

$$b\rho\sigma\eta = (a+b)\sigma\eta = a\eta = b,$$

i.e. $b \in \mathrm{F}((\rho\sigma\eta)_H)$. Weil $(\rho\sigma\eta)_H \neq 1_H$ ist, ist $(\rho\sigma\eta)_H$ eine Symmetrie, also trifft dies auch auf $\rho\sigma\eta = (\rho\sigma\eta)_H \textcircled{\perp}\ 1_{H^\perp}$ zu.

Es sei angenommen, daß es $\sigma_1, \sigma_2, \eta_1, \eta_2, \eta_3 \in \mathcal{S}$ gibt, so daß $\sigma_1\sigma_2 = \eta_1\eta_2\eta_3$ ist. Dann muß $\dim(\mathrm{B}(\eta_1) + \mathrm{B}(\eta_2) + \mathrm{B}(\eta_3)) \leq \dim \mathrm{B}(\sigma_1) + \dim \mathrm{B}(\sigma_2) \leq 2$ sein. Aus der Vorbemerkung folgt nun der Widerspruch $\sigma_1\sigma_2 = \eta_1\eta_2\eta_3 \in \mathcal{S} \cap \mathcal{S}^2 = \emptyset$.

Ist $\pi \in \mathcal{S}^3 \backslash \mathcal{S}$, so folgt aus der Vorbemerkung, daß $\dim \mathrm{B}(\pi) = 3 = \mathrm{l}(\pi)$ ist. Weil $(x+1)(x+\mu)(x+\bar{\mu}), (x+\nu)^3$, $\nu \in K^*$ die $^-$-symmetrischen Polynome vom Grad 3 mit konstantem Glied 1 in $F_4[x]$ sind. Folgt $\mathrm{char}(\pi) = (x+\nu)^3$ für ein $\nu \in K \backslash F$. Nach 3.5.8 ist π kurz. Dies erzwingt $\mathrm{mip}(\pi) = (x+\nu)^2$, i.e. $\bar{\nu}\pi \in \mathcal{S}$. Ist umgekehrt $\pi \in (K\backslash F)\mathcal{S}$, so ist π kurz mit $\dim \mathrm{B}(\pi) = 3$. Nach 3.5.8 ist $\mathrm{l}(\pi) = 3$. Insbesondere ist $\pi \in \mathcal{S}^3$.

(4). Als nächstes nehmen wir an, daß es $\sigma_1, \sigma_2, \sigma_3, \eta_1, \eta_2, \eta_3, \eta_4 \in \mathcal{S}$ gibt, so daß $\sigma_1\sigma_2\sigma_3 = \eta_1\eta_2\eta_3\eta_4$ ist. Gemäß (3) finden wir ein $\nu \in K^*$ und eine Symmetrie $\sigma \in \mathcal{S}$, so daß $\eta_1\eta_2\eta_3\eta_4 = \sigma_1\sigma_2\sigma_3 = \nu\sigma$ ist. Wegen $K^*\mathcal{S}^3 = K^*(K^*\mathcal{S}) = K^*\mathcal{S} = \mathcal{S}^3$ folgt nun

$$\bar{\nu}\eta_1\eta_2\eta_3 = \sigma\eta_4 \in K^*\mathcal{S}^3 \cap \mathcal{S}^2 = \mathcal{S}^3 \cap \mathcal{S}^2 = \emptyset,$$

ein Widerspruch.

Nach 3.5.8 (b) ist $\mathrm{l}(\nu 1_V) = 4$ für $\nu \in K\backslash F$. Damit gilt $(K\backslash F)\{1_V\} \subseteq \mathcal{S}^4 \backslash \mathcal{S}^2$. Andererseits gilt für ein $\pi \in \mathcal{S}^4 \backslash \mathcal{S}^2$ nach obigem $\mathrm{l}(\pi) > 3 \geq \dim \mathrm{B}(\pi)$. Nach 3.5.8 ist π lang und vom Typ (H).

Nach 3.5.8 ist jedes $\pi \in \langle \mathcal{S} \rangle$ ein Produkt von höchstens vier Symmetrien, so daß die letzte Gleichung in (4) unmittelbar aus den vorherigen Überlegungen folgt.

(5). Es ist $1_V \in \mathcal{S}^2 \subseteq S$. Offenbar ist S gegen Inversenbildung abgeschlossen. Seien $\pi, \psi \in S$. Sind $\pi, \psi \in \mathcal{S}^2$, so ist $\pi\psi \in \mathcal{S}^4 \subseteq S$. Sind $\pi, \psi \in \mathcal{S}^4 \backslash \mathcal{S}^2$, so sind π, ψ Homothetien (cf. (4)). Demnach ist auch $\pi\psi$ eine Homothetie und damit in S enthalten. Ist $\pi \in \mathcal{S}^2$ und $\psi \in \mathcal{S}^4 \backslash \mathcal{S}^2$ enthalten, so ist $\mathrm{mip}(\pi) = x^3 + 1$ (cf. (2)) und $\psi = \nu 1_V$ für ein $\nu \in K\backslash F$ (cf. (4)). Folglich ist $\mathrm{mip}(\pi\psi) = x^3 + 1$ und $\pi\psi$ nach (2) in $\mathcal{S}^2 \subseteq S$ enthalten. Folglich gilt $S \cdot S \subseteq S$, i.e. S ist eine Gruppe. Nach (2) und (4) besteht $S\backslash\{1_V\}$ gerade aus den Elementen der Ordnung 3 in $\mathrm{SU}(f)$ und es gilt $|S| = |\mathcal{S}^2| + |\mathcal{S}^4 \backslash \mathcal{S}^2| = 25 + 2 = 27$. Wegen $\mathrm{Z}(\mathrm{SU}(f)) = K^*\{1_V\} \subseteq S$ gilt $\mathrm{Z}(\mathrm{SU}(f)) \leq \mathrm{Z}(S)$. Ist $\pi \in S\backslash K^*\{1_V\} = \mathcal{S}^2 \backslash \{1_V\}$, so gibt es zwei verschiedene Symmetrien $\rho, \sigma \in \mathcal{S}$ mit $\pi = \rho\sigma$. Seien $a \in \mathrm{B}(\rho)$ und $b \in \mathrm{B}(\sigma)$, so daß $f(a,b) = 1$ ist. Weil V von isotropen Vektoren erzeugt wird und den Wittindex 1 hat, findet man einen isotropen Vektor $c \in V\backslash\langle a, b\rangle$ mit $f(a,c) = 1$. Sei η die Symmetrie mit $\mathrm{B}(\eta) = \langle c \rangle$. Dann gilt $\rho\sigma\rho\eta = \sigma^\rho\eta$ und $\rho\eta\rho\sigma = \eta^\rho\sigma$ und daher

$$\mathrm{B}(\rho\sigma\rho\eta) = \mathrm{B}(\sigma)\rho \oplus \mathrm{B}(\eta) = \langle a+b, c\rangle \neq \langle a+c, b\rangle = \mathrm{B}(\eta)\rho \oplus \mathrm{B}(\sigma) = \mathrm{B}(\rho\eta\rho\sigma).$$

Insbesondere ist $\pi(\rho\eta) \neq (\rho\eta)\pi$ und damit $\pi \notin \mathrm{Z}(S)$. Es folgt $\mathrm{Z}(S) = \mathrm{Z}(\mathrm{SU}(f))$. Weil $|S/\mathrm{Z}(S)| = 9$ ein Primzahlquadrat ist, ist $S/\mathrm{Z}(S)$ abelsch. Weil jedes Element $\neq 1_V$ von S die Ordnung 3 hat, gilt dies auch in $S/\mathrm{Z}(S)$. ∎

$|F| = 2$; untere Schranken

Weil im fortlaufenden Text häufig die genaue Kenntnis bestimmter $^-$-symmetrischer Polynome mit kleinem Grad in $K[x]$ nötig ist, listen wir diejenigen vom Grad $2, 3, 4$ mit nichtverschwindendem konstanten Glied und die vom Grad 5 mit konstantem Glied 1 auf.

Bemerkung 3.5.12 *Sei* $p \in K[x]$ $^-$*-symmetrisch mit* $\deg(p) \in \{2, 3, 4, 5\}$ *und* $p(0) \neq 0$. *Sei ferner* $\nu \in K \backslash F$. *Dann gilt :*

(a) $p \in \{(x+1)^2, (x+\nu)(x+\bar{\nu})\}$, *falls* $\deg(p) = 2$ *und* $p(0) = 1$;

(b) $p \in \{(x+1)(x+\nu), (x+\bar{\nu})^2\}$, *falls* $\deg(p) = 2$ *und* $p(0) = \nu$;

(c) $p \in \{(x+1)^3\} \cup \{(x+1)(x+\xi)(x+\bar{\xi}), (x+\xi)^3; \xi \in K \backslash F\}$, *falls* $\deg(p) = 3$ *und* $p(0) = 1$;

(d) $p \in \{(x^3+\nu), (x+\bar{\nu})^2(x+1), (x+\nu)(x+1)^2, (x+\nu)^2(x+\bar{\nu})\}$, *falls* $\deg(p) = 3$ *und* $p(0) = \nu$;

(e) $p \in \{(x+1)^4\} \cup \{(x+\xi)^2(x+\bar{\xi})^2, (x+1)^2(x+\xi)(x+\bar{\xi}), (x+\xi)(x^3+\bar{\xi}), (x+1)(x+\xi)^3, (x^2+\xi x+1)(x^2+\bar{\xi}x+1); \xi \in K \backslash F\}$, *falls* $\deg(p) = 4$ *und* $p(0) = 1$;

(f) $p \in \{(x+\nu)^4, (x+1)(x^3+\nu), (x+\bar{\nu})(x^3+\bar{\mu}), (x+1)(x+\bar{\nu})(x+\nu)^2, (x+\nu)(x+\bar{\nu})^3, (x+1)^3(x+\nu), (x+1)^2(x+\bar{\nu})^2, (x^2+\bar{\nu}x+\bar{\nu})(x^2+x+\bar{\nu})\}$, *falls* $\deg(p) = 4$ *und* $p(0) = \nu$;

(g) $p \in \{(x+1)^5\} \cup \{(x^2+\xi x+1)(x^2+\bar{\xi}x+1)(x+1), (x+1)^3(x+\xi)(x+\bar{\xi}), (x+\xi)^2(x^3+\xi), (x+1)(x+\xi)^2(x+\bar{\xi})^2, (x+\xi)(x^2+\xi x+\xi)(x^2+x+\xi), (x+\xi)(x+\bar{\xi})^4, x^5+\xi x^4+x^3+x^2+\bar{\xi}x+1, (x+1)^2(x+\xi)^3, (x+1)(x+\bar{\xi})(x^3+\xi); \xi \in K \backslash F\}$, *falls* $\deg(p) = 5$ *und* $p(0) = 1$ *ist.*

Beweis. (a). Sei $p = x^2 + ax + 1$, $a \in K$. Es gilt $p = p^* = x^2 + \bar{a}x + 1$ genau dann, wenn $a \in F$ ist. Für $a = 0$ folgt $p = x^2 + 1 = (x+1)^2$ und für $a = 1$ folgt $p = x^2 + x + 1 = (x+\nu)(x+\bar{\nu})$.

(b). Sei $p = x^2 + ax + \nu$, $a \in K$. Es gilt $p = p^* = x^2 + \nu\bar{a}x + \nu$ genau dann, wenn $a = 0$ oder $\bar{a} = a^2 = \nu$ ist. Für $a = 0$ folgt $p = x^2 + \nu = (x+\bar{\nu})^2$ und für $a = \bar{\nu}$ folgt $p = x^2 + \bar{\nu}x + \nu = (x+1)(x+\nu)$.

(c). Sei $p = x^3 + ax^2 + bx + 1$, $a, b \in K$. Es gilt $p = p^* = x^3 + \bar{b}x^2 + \bar{a}x + 1$ genau dann, wenn $b = \bar{a}$ ist.
(1) $a = 0$. Dann gilt $p = x^3 + 1 = (x+1)(x+\nu)(x+\bar{\nu})$.
(2) $a = 1$. Dann gilt $p = x^3 + x^2 + x + 1 = (x+1)^3$.
(3) $a \in K \backslash F$. Dann gilt $p = x^3 + ax^2 + \bar{a}x + 1 = (x+a)^3$.

(d). Sei $p = x^3 + ax^2 + bx + \nu$, $a, b \in K$. Es gilt $p = p^* = x^3 + \nu\bar{b}x^2 + \nu\bar{a}x + \nu$ genau dann, wenn $b = \nu\bar{a}$.
(1) $a = 0$. Dann gilt $p = x^3 + \nu$.
(2) $a = 1$. Dann gilt $p = x^3 + x^2 + \nu x + \nu = (x+\bar{\nu})^2(x+1)$.
(3) $a = \nu$. Dann gilt $p = x^3 + \nu x^2 + x + \nu = (x+\nu)(x+1)^2$.
(4) $a = \bar{\nu}$. Dann gilt $p = x^3 + \bar{\nu}x^2 + \bar{\nu}x + \nu = (x+\nu)^2(x+1)$.

(e). Sei $p = x^4 + ax^3 + bx^2 + cx + 1$, $a, b, c \in K$. Es gilt $p = p^* = x^4 + \bar{c}x^3 + \bar{b}x^2 + \bar{a}x + 1$ genau dann, wenn $c = \bar{a}$ und $b \in F$.
(1) $a = 0 = b$. Dann gilt $p = x^4 + 1 = (x+1)^4$.
(2) $a = 0, b = 1$. Dann gilt $p = x^4 + x^2 + 1 = (x+\nu)^2(x+\bar{\nu})^2$.
(3) $a = 1, b = 0$. Dann gilt $p = x^4 + x^3 + x + 1 = (x+a)^3 = (x+1)^2(x+\nu)(x+\bar{\nu})$.
(4) $a = 1 = b$. Dann gilt $p = x^4 + x^3 + x^2 + x + 1 = (x^2 + \nu x + 1)(x^2 + \bar{\nu}x + 1)$.
(5) $a \in K\backslash F, b = 0$. Dann gilt $p = x^4 + ax^3 + \bar{a}x + 1 = (x+a)(x^3+\bar{a})$.
(6) $a \in K\backslash F, b = 1$. Dann gilt $p = x^4 + ax^3 + x^2 + \bar{a}x + 1 = (x+1)(x+\bar{a})^3$.

(f). Sei $p = x^4 + ax^3 + bx^2 + cx + \nu$, $a, b, c \in K$. Es gilt $p = p^* = x^4 + \nu\bar{c}x^3 + \nu\bar{b}x^2 + \nu\bar{a}x + \nu$ genau dann, wenn $c = \nu\bar{a}$ und [$b = 0$ oder $b = \bar{\nu}$].
(1) $a = 0 = b$. Dann gilt $p = x^4 + \nu = (x+\nu)^4$.
(2) $a = 0, b = \bar{\nu}$. Dann gilt $p = x^4 + \bar{\nu}x^2 + \nu = (x+\bar{\nu})^2(x+1)^2$.
(3) $a = 1, b = 0$. Dann gilt $p = x^4 + x^3 + \nu x + \nu = (x+a)^3 = (x^3+\nu)(x+1)$.
(4) $a = 1, b = \bar{\nu}$. Dann gilt $p = x^4 + x^3 + \bar{\nu}x^2 + \nu x + \nu = (x+\nu)(x+\bar{\nu})^3$.
(5) $a = \nu, b = 0$. Dann gilt $p = x^4 + \nu x^3 + x + \nu = (x+1)(x+\bar{\nu})(x+\nu)^2$.
(6) $a = \nu, b = \bar{\nu}$. Dann gilt $p = x^4 + \nu x^3 + \bar{\nu}x^2 + x + \nu = (x^2 + \bar{\nu}x + \bar{\nu})(x^2 + x + \bar{\nu})$.
(7) $a = \bar{\nu}, b = 0$. Dann gilt $p = x^4 + \bar{\nu}x^3 + \bar{\nu}x + \nu = (x+\bar{\nu})(x^3+\bar{\nu})$.
(8) $a = \bar{\nu} = b$. Dann gilt $p = x^4 + \bar{\nu}x^3 + \bar{\nu}x^2 + \bar{\nu}x + \nu = (x+1)^3(x+\nu)$.

(g). Sei $p = x^5 + ax^4 + bx^3 + cx^2 + dx + 1$, $a, b, c, d \in K$. Es gilt $p = p^* = x^4 + \bar{d}x^4 + \bar{c}x^3 + \bar{b}x^2 + \bar{a}x + 1$ genau dann, wenn $d = \bar{a}$ und $c = \bar{b}$.
(1) $a = 0 = b$. Dann gilt $p = x^5 + 1 = (x+1)(x^2 + \xi x + 1)(x^2 + \bar{\xi}x + 1)$, $\xi \in K\backslash F$.
(2) $a = 0, b = 1$. Dann gilt $p = x^5 + x^3 + x^2 + 1 = (x+1)^3(x+\xi)(x+\bar{\xi})$, $\xi \in K\backslash F$.
(3) $a = 0, b \in K\backslash F$. Dann gilt $p = x^5 + bx^3 + \bar{b}x^2 + 1 = (x+\bar{b})^2(x^3+\bar{b})$.
(4) $a = 1, b = 0$. Dann gilt $p = x^5 + x^4 + x + 1 = (x+1)^5$.
(5) $a = 1 = b$. Dann gilt $p = x^5 + x^4 + x^3 + x^2 + x + 1 = (x+1)(x+\xi)^2(x+\bar{\xi})^2$, $\xi \in K\backslash F$.
(6) $a = 1, b \in K\backslash F$. Dann gilt $p = x^5 + x^4 + bx^3 + \bar{b}x^2 + x + 1 = (x+\bar{b})(x^2 + \bar{b}x + \bar{b})(x^2 + x + \bar{b})$.
(7) $a \in K\backslash F, b = 0$. Dann gilt $p = x^5 + ax^4 + \bar{a}x + 1 = (x+a)(x+\bar{a})^4$.
(8) $a \in K\backslash F, b = 1$. Dann ist $p = x^5 + ax^4 + x^3 + x^2 + \bar{a}x + 1$ irreduzibel.
(9) $a \in K\backslash F, b = a$. Dann gilt $p = x^5 + ax^4 + ax^3 + \bar{a}x^2 + \bar{a}x + 1 = (x+1)^2(x+a)^3$.
(10) $a \in K\backslash F, b = \bar{a}$. Dann gilt $p = x^5 + ax^4 + barax^3 + ax^2 + \bar{a}x + 1 = (x+1)(x+\bar{a})(x^3+a)$. ■

Das folgende Lemma dient dazu, untere Schranken von $l(\pi)$ für unitäre Transformationen π vom Typ (B) zu etablieren.

Lemma 3.5.13 *Ist $\pi \in \mathrm{SU}(f)$ vom Typ* (B) *und σ eine Symmetrie mit* $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$, *so ist $\pi\sigma$*

(a) *vom Typ* (A1) *oder* (H), *falls π vom Typ* (B1) *und* $\dim \mathrm{B}(\pi) = 4$ *ist,*
(b) *vom Typ* (B3) *oder* (H), *falls π vom Typ* (B1) *und* $\dim \mathrm{B}(\pi) > 4$ *ist,*
(c) *vom Typ* (B1), *falls π vom Typ* (B2) *ist,*

(d) *vom Typ* (B2), *falls* π *vom Typ* (B3) *ist.*

Beweis. Wegen $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ ist $B(\sigma)$ in $\mathrm{B}(\pi)$ enthalten. Sei $z \in \mathrm{B}(\sigma)\backslash\{0\}$. Nach 3.5.7 gilt $V = A \bigoplus C \bigoplus D$ für π-Moduln A, B und

- $\dim A = 2$, $\mathrm{mip}(\pi_A) = (x+\bar\mu)^2$, $C = \mathrm{F}_\mu(\pi)$, $D = \mathrm{F}(\pi)$, $\dim F_\mu(\pi) \equiv 2 \pmod 3$, falls π vom Typ (B1) ist,
- $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+1)^3$, $C = \mathrm{F}_\mu(\pi)$, $0 \neq \dim F_\mu(\pi) \equiv 0 \pmod 3$, $D \leq \mathrm{F}(\pi)$, falls π vom Typ (B2) ist,
- $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+\mu)^3$, $C \leq \mathrm{F}_\mu(\pi)$, $0 \neq \dim C \equiv 0 \pmod 3$, $D = \mathrm{F}(\pi)$, falls π vom Typ (B3) ist.

Wegen $z \in \mathrm{B}(\pi) = A(\pi+1) \bigoplus C$ gibt es ein $a \in A(\pi+1)$ und ein $c \in C$, so daß $z = a + b$ ist. Man berechnet

(1) $0 = f(z,z) = f(a,a) + f(c,c)$

und

(2) $1 = f_\pi(z,z) = f_\pi(a,a) + f_\pi(b,b) = f_\pi(a,a) + \mu f(c,c)$.

Im folgenden sei ϕ die von $\pi\sigma$ auf $\mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma)$ induzierte Abbildung. Dann gilt

(3) $1 = \det \pi\sigma = \det\phi \det \pi_{\mathrm{F}_\mu(\pi\sigma)} = \mu^{\dim \mathrm{F}_\mu(\pi\sigma)} \det\phi$.

(a) und (b). Sei π vom Typ (B1).
Fall A: $c = 0$. Dann gilt $\dim \mathrm{F}((\pi\sigma)_A) = 1 = \dim \mathrm{B}((\pi\sigma)_A)$. Wegen $\det(\pi\sigma)_A = \mu$ folgt $\mathrm{mip}((\pi\sigma)_A) = (x+1)(x+\mu) = \mathrm{mip}(\pi\sigma)$. Somit ist $\pi\sigma$ vom Typ (H).

Fall B. $c \neq 0$. Angenommen c ist anisotrop. Wegen (1) ist dann auch a anisotrop. Insbesondere liegt a nicht in $A(\pi+\bar\mu)$, da $A(\pi+\bar\mu)$ totalisotrop ist. Aus (2) folgert man $f_\pi(a) = \mu + 1$. Sei $y := a(\pi_A+1)^{-1} \in A\backslash A(\pi+\bar\mu)$. Es ist $y(\pi+\bar\mu) \in \ker(\pi+\bar\mu)$ und damit

(4) $0 = f(y(\pi+\bar\mu), y(\pi+\bar\mu)) = \mu f(y(\pi+\bar\mu), y) + \bar\mu f(y, y(\pi+\bar\mu))$.

Es ist $f(y, y(\pi+\bar\mu)) \neq 0$, da sonst $y(\pi+\bar\mu) \in \mathrm{rad}\ A$ folgen würde, was im Widerspruch zu $0 \neq y(\pi+\bar\mu)$ und $\mathrm{rad}\ A = \{0\}$ stünde. Aus (4) folgt damit

(5) $\bar\mu = f(y(\pi+\bar\mu), y) = f(y\pi, y) + \bar\mu f(y,y)$.

Wegen $1 = f(a,a) = f(y, y\pi) + f(y\pi, y)$ folgt $f(y, y\pi) \notin F$. Aus (5) folgt $\mu f(y\pi, y) = f(y,y) + 1 \in F^* = \{1\}$. Somit gilt $f(y\pi, y) = \bar\mu$ und $f(y,y) = 0$. Es folgt der Widerspruch $\bar\mu = f_\pi(a,a) = f(y, y(\pi+1)) = f(y, y\pi) = \mu$.
Folglich ist c isotrop. Wegen $c \notin V(\pi+\mu)$ gilt $\dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi) - 1$, somit $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 2$, $\dim \mathrm{F}_\mu(\pi\sigma) \equiv 1 \pmod 3$ und $c \in \mathrm{F}_\mu(\pi) \cap c^\perp = \mathrm{F}_\mu(\pi\sigma)$. Folglich gilt $1 \leq \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) \leq \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) + 1 = 1$, i.e.

(6) $\dim \mathrm{rad}\ F_\mu(\pi\sigma) = 1$.

Insbesondere ist damit $x+\mu$ ein Teiler von $\mathrm{char}(\phi)$. Aus (3) folgt $1 = \mu \det\phi$, i.e. $\det\phi = \bar{\mu} = \mu^2$. Wegen $\deg(\mathrm{char}(\phi)) = 2$ erhält man $\mathrm{char}(\phi) = (x+\mu)^2$. Wegen (6) gilt $\mathrm{mip}(\phi) = (x+\mu)^2$. Damit ist $\pi\sigma$ vom Typ (B3), falls $\dim \mathrm{B}(\pi) > 4$ ist, und vom Typ (A) falls $\dim \mathrm{B}(\pi) = 4$ ist.

(c). Sei π vom Typ (B2). Wäre $c = 0$, so würde $\mathrm{B}(\sigma) = \langle a\rangle \leq A$ und damit $\mathrm{F}((\pi\sigma)_A) > \mathrm{F}(\pi_A)$ gelten. Folglich wäre $(\pi\sigma)_A$ eine Symmetrie und damit π_A ein Produkt von Symmetrien. Dies ist jedoch nach 3.5.10 nicht möglich, da π_A unzerlegbar ist. Somit ist $c \neq 0$. Dies bedeutet $\mathrm{B}(\sigma) \nsubseteq \mathrm{B}(\bar{\mu}\pi)$, also $\dim \mathrm{B}(\pi\sigma)/F_\mu(\pi\sigma) = \dim \mathrm{B}(\pi)/F_\mu(\pi) = 2$, $\dim F_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi) - 1 \equiv 2 \pmod 3$ und $\mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi) \cap c^\perp$.

Als nächstes nehmen wir an, daß c isotrop ist. Nach (1) ist dann auch a isotrop und nach (2) ist $f_\pi(a,a) = 1$. Die Symmetrie $\rho := \sigma_a$ würde dann $\mathrm{F}((\pi\rho)_A) > \mathrm{F}(\pi_A)$ liefern. Dies führt wie im Vorigen zu einem Widerspruch.

Folglich ist c anisotrop und damit $\mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi) \cap c^\perp$ regulär. Dies bedeutet, daß $x+\mu$ kein Teiler von $\mathrm{char}(\phi)$ ist. Aus (3) folgt $1 = \mu^2 \det\phi$, i.e. $\mathrm{char}(\phi)(0) = \det\phi = \mu$. Weil $(x+1)(x+\mu), (x+\bar{\mu})^2$ die einzigen $^-$-symmetrischen Polynome in $F_4[x]$ vom Grad 2 mit konstantem Glied μ sind, folgt $\mathrm{char}(\phi) = (x+\bar{\mu})^2$. Wegen $\dim \mathrm{F}_{\bar{\mu}}(\pi\sigma) \leq \dim \mathrm{F}_{\bar{\mu}}(\pi) + 1 = 1$, folgt $\mathrm{mip}(\phi) = (x+\bar{\mu})^2$. Damit ist $\pi\sigma$ vom Typ (B1).

(d) Sei $\pi\sigma$ vom Typ (B3).

Fall A: c ist isotrop. Nach (1) ist a isotrop und nach (2) gilt $f_\pi(a,a) = 1$. Weil $A(\pi+\mu)^2$ ein totalisotroper π-Modul und jeder Vektor aus $A(\pi+\mu)\backslash A(\pi+\mu)^2$ anisotrop ist, folgt demnach $a \notin A(\pi+\mu) = \mathrm{B}(\bar{\mu}\pi_A)$. Insbesondere gilt $\mathrm{B}(\sigma) = \langle z\rangle \nsubseteq \mathrm{B}(\bar{\mu}\pi)$. Dies impliziert $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 2$, $0 \neq \dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi) - 1 \equiv 0 \pmod 3$ und $\mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi) \cap z^\perp$.
Es soll nun gezeigt werden, daß $\mathrm{F}_\mu(\pi\sigma)$ regulär ist. Ist $c = 0$, so gilt $\mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi) \cap a^\perp = C$. Man kann daher $c \neq 0$ annehmen. Weil C regulär ist, gibt es ein $v \in C$ mit $f(v,c) = 1$. Wegen $(A(\pi+\mu)^2)^\perp \cap A = A(\pi+\mu)$ und $a \notin A(\pi+\mu)$ folgt $\lambda := f(a(\pi+\mu)^2, a) \neq 0$. Setzt man $b := v + \lambda^{-1}a(\pi+\mu)^2 \in \mathrm{F}_\mu(\pi)$, so gilt $f(b,z) = f(v,c) + \lambda^{-1} f(a(\pi+\mu)^2, a) = 0$ und $b \notin a^\perp \cap c^\perp$. Dies bedeutet $\mathrm{F}_\mu(\pi\sigma) = (\mathrm{F}_\mu(\pi) \cap c^\perp \cap a^\perp) \oplus \langle b\rangle$. Sei $y \in \mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma)$. Dann gibt es ein $w \in \mathrm{F}_\mu(\pi) \cap c^\perp \cap a^\perp$ und ein $\nu \in K$ mit $y = w + \nu b$. Wegen $c \in \mathrm{rad}\ (\mathrm{F}_\mu(\pi) \cap c^\perp \cap a^\perp)$ folgt $0 = f(c,y) = \bar{\nu} f(c,b) = \bar{\nu} f(c,v) = \bar{\nu}$, i.e. $y = w \in \mathrm{rad}\ (\mathrm{F}_\mu(\pi) \cap c^\perp \cap a^\perp) = \mathrm{rad}\ (C \cap c^\perp) = \langle c\rangle$. Dies ergibt den Widerspruch $0 = f(y,b) = f(c,b) = f(c,v) = 1$.

Weil $F_\mu(\pi\sigma)$ demnach regulär ist, ist $x+\mu$ kein Teiler von $\mathrm{char}(\phi)$. Aus (3) folgt $\mathrm{char}(\phi)(0) = \det\phi = 1$. Weil $(x+1)^2, (x+\mu)(x+\bar{\mu})$ die einzigen $^-$-symmetrischen Polynome in $F_4[x]$ vom Grad 2 mit konstantem Glied 1 sind, folgt $\mathrm{char}(\phi) = (x+1)^2$. Wegen $\dim \mathrm{F}(\phi) = \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) \leq \dim \mathrm{rad}\ \mathrm{B}(\pi) + 1 = 1$, gilt $\mathrm{mip}(\phi) = (x+1)^2$. Folglich ist $\pi\sigma$ vom Typ (B2).

Fall B: c ist anisotrop. Nach (1) ist a anisotrop und nach (2) gilt $f_\pi(a,a) = \bar{\mu}$. Seien $r := c(\pi_C + 1)^{-1} = \mu c$ und $b := a(\pi_A + 1)^{-1} \in A$. Angenommen b ist isotrop. Dann gilt $\bar{\mu} = q_\pi(a) = f(b, b(\pi+1)) = \bar{\mu} f(b, b(\bar{\mu}\pi + 1)) = \bar{\mu} q_{\bar{\mu}\pi}(b(\bar{\mu}\pi+1))$, i.e. $q_{\bar{\mu}\pi}(b(\bar{\mu}\pi+1)) = 1$. Es seien $\psi := \bar{\mu}\pi_A$ und $y := b(\bar{\mu}\pi + 1)$. Nach 3.2.2 (a) ist $\rho := \sigma_b$ eine wohldefinierte Symmetrie aus $\mathrm{U}(f_A)$ mit $\dim \mathrm{B}(\psi\rho) = \dim \mathrm{B}(\psi) - 1 = 1$. Wegen $\det \psi\sigma = 1$ ist $\psi\sigma$ eine Symmetrie und ψ damit insbesondere ein Produkt von Symmetrien, ein Widerspruch zu 3.5.10, da ψ unzerlegbar ist. Folglich ist b anisotrop und damit $z(\pi_{A+C} + 1)^{-1} = r + b$ isotrop. Wegen $\mathrm{F}(\pi\sigma) = \mathrm{F}(\pi) \bigoplus \langle r + b \rangle$ ist $0 \neq r + b \in \mathrm{rad}\ \mathrm{F}(\pi\sigma) = \mathrm{radB}(\pi\sigma)$ und damit $x + 1$ ein Teiler von $\mathrm{char}(\phi)$. Wie im Fall A folgert man hieraus, daß $\pi\sigma$ vom Typ (B2) ist. ■

Lemma 3.5.14 *Seien $\pi \in \mathrm{SU}(f)$ vom Typ* (C) *und σ eine Symmetrie, so daß* $\dim \mathrm{B}(\pi\sigma) = 4$ *ist. Dann ist $\pi\sigma$ vom Typ* (A1) *oder* (B1).

Beweis. Sei $\mu \in K\backslash F$, so daß $\mathrm{F}_\mu(\pi)$ eindimensional und regulär und $\mathrm{F}_{\bar\mu}(\pi)$ zweidimensional und totalisotrop ist. Dann gilt $\dim \mathrm{rad}\ \mathrm{F}_{\bar\mu}(\pi\sigma) \geq \dim \mathrm{rad}\ \mathrm{F}_{\bar\mu}(\pi) - 1 = 1$. Die von $\pi\sigma$ auf $\mathrm{B}(\pi\sigma)$ induzierte Abbildung ϕ hat dann ein charakteristisches Polynom vom Grad 4 mit konstantem Glied 1, das von $(x + \bar\mu)^2$ geteilt wird. Also gilt $\mathrm{char}(\pi) \in \{(x+1)(x+\bar\mu)^3, (x+\bar\mu)^2(x+\mu)^2\}$ (cf. 3.5.12 (f)). Wäre $\dim \mathrm{F}_{\bar\mu}(\pi\sigma) = 2 = \dim \mathrm{F}_{\bar\mu}(\pi)$, so wäre $\mathrm{F}_{\bar\mu}(\pi\sigma) = \mathrm{F}_{\bar\mu}(\pi\sigma)$ totalisotrop und damit $(x+\bar\mu)^4 = \mathrm{char}(\phi)$, ein Widerspruch. Folglich ist $\mathrm{F}_{\bar\mu}(\pi\sigma)$ eindimensional und isotrop. Wäre $\mathrm{F}_\mu(\pi\sigma)$ nicht regulär, so wäre $\mathrm{F}_\mu(\pi\sigma) \neq \mathrm{F}(\pi)$. Hieraus würde bereits $\dim \mathrm{F}_\mu(\pi\sigma) = 2$ folgen. Damit wäre $(x + \mu)^3$ ein Teiler von $\mathrm{char}(\phi)$, ein Widerspruch. Folglich ist $\mathrm{F}_\mu(\pi\sigma)$ regulär. Insgesamt erhält man $\mathrm{mip}(\phi) = (x+1)(x+\bar\mu)^3$ oder $\mathrm{mip}(\phi) = (x+\mu)(x+\bar\mu)^2$. Im ersten Fall ist $\pi\sigma$ vom Typ (A1) und im zweiten vom Typ (B1). ■

Daß beide in der Konklusion des vorigen Lemmas angegebenen Fälle tatsächlich vorkommen, zeigt die

Bemerkung 3.5.15 *Sei $\pi \in \mathrm{SU}(f)$ vom Typ* (C). *Dann gibt es Symmetrien ρ und σ, so daß $\pi\rho$ vom Typ* (B1) *und $\pi\sigma$ vom Typ* (B2) *ist.*

Beweis. Sei $V = \mathrm{F}_\mu(\pi) \bigoplus A \bigoplus B \bigoplus \mathrm{F}(\pi)$ eine Zerlegung von V wie in 3.5.7 angegeben. Nach 3.5.18 gibt es dann eine Symmetrie ρ mit $\mathrm{B}(\rho) \leq A$, so daß $\mathrm{mip}(\pi\rho)_A = (x + \mu)(x + 1)$ ist. Hieraus folgt $\dim \mathrm{F}(\pi\rho) > \dim \mathrm{F}(\pi)$ und $\dim \mathrm{F}_\mu(\pi\rho) = \dim \mathrm{F}_\mu(\pi) + 1 = 2$. Nach 3.5.14 ist $\pi\rho$ vom Typ (B1). Wegen $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = \dim \mathrm{B}(\pi) = 5$, und weil π nicht vom Typ (H) ist, gibt es nach 3.5.3 (mit $W := \mathrm{B}(\pi)(\pi + \mu) = A \bigoplus B$) und 3.2.2 eine Symmetrie σ mit $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\mathrm{B}(\sigma) \nsubseteq \mathrm{B}(\pi)(\pi + \mu)$. Nach 3.3.6 (b) ist $\dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi) - 1 = 0$. Nach 3.5.14 ist $\pi\sigma$ vom Typ (A1). ■

Lemma 3.5.16 *Seien $\pi \in \mathrm{SU}(f)$ vom Typ* (D) *und σ eine Symmetrie, so daß* $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) - 1 = 5$ *ist. Dann ist $\pi\sigma$ vom Typ* (C).

Beweis. Sei $\mu \in K\backslash F$, so daß $\mathrm{F}_\mu(\pi)$ dreidimensional und totalisotrop ist. Weil dann $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) \geq \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) - 1 = 2$ ist, ist $(x + \bar\mu)^4$ ein Teiler des charakteristischen Polynoms der von $\pi\sigma$ auf $\mathrm{B}(\pi\sigma)$ induzierten Abbildung ϕ. Wegen $\deg(\mathrm{char}(\phi)) = \dim \mathrm{B}(\pi\sigma) = 5$ und $\mathrm{char}(\phi)(0) = \det(\phi) = 1$, folgt $\mathrm{char}(\phi) = (x+\mu)^4(x+\bar\mu)$. Demnach ist $\mathrm{F}_{\bar\mu}(\pi\sigma)$ eindimensional und regulär. Folglich ist $\pi\sigma$ vom Typ (C). ■

Wir können nun nachweisen, daß die in 3.5.8 angegebenen Symmetrienlängen langer Abbildungen jedenfalls untere Schranken darstellen.

Lemma 3.5.17 (Untere Schranken für lange Abbildungen) *Sei* $\pi \in \mathrm{SU}(f)$ *eine lange Abbildung,* $m := \dim \mathrm{B}(\pi)$. *Dann gilt*

$$\mathrm{l}(\pi) \geq \begin{cases} m+1 & , falls\ \pi\ vom\ Typ\ (\mathrm{H})\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{N})\ und\ \dim V > 3\ ist, \\ m+2 & , falls\ \pi\ vom\ Typ\ (\mathrm{A})\ und\ \dim V > 3\ ist, \\ m+1 & , falls\ \pi\ vom\ Typ\ (\mathrm{B})\ ist, \\ 6 & , falls\ \pi\ vom\ Typ\ (\mathrm{C})\ ist, \\ 7 & , falls\ \pi\ vom\ Typ\ (\mathrm{D})\ ist. \end{cases}$$

Beweis. Falls π vom Typ (H) oder (N) ist, folgt die Behauptung aus 3.5.4. (Der dort angegebene Beweis ist unabhängig von der Mächtigkeit des Körpers K.)
Sei π vom Typ (A). Seien $\tilde{\pi}$ und $\tilde{f}$ die von π bzw. f auf $W := \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi)$ induzierten Abbildungen. Dann ist $\dim W = 3$, $\tilde{f}$ eine reguläre $^{-}$-hermitesche Form und $\tilde{\pi} \in \mathrm{U}(\tilde{f})$.
Annahme: $\mathrm{l}(\pi) \leq m+1$. Es gibt dann Symmetrien $\sigma_m, \ldots, \sigma_m$ und eine unitäre Abbildung σ_{m+1}, die eine Symmetrie oder die Identität ist, so daß $\pi = \sigma_1 \cdots \sigma_{m+1}$ gilt. Aus 3.3.1 und 3.3.3 folgt $\mathrm{B}(\sigma_i) \leq \mathrm{B}(\pi)$, i.e. $\mathrm{rad}\ \mathrm{B}(\pi) \leq \mathrm{F}(\pi) \leq \mathrm{F}(\sigma_i)$ für alle $i \in \mathbb{N}_{\leq m+1}$. Folglich induzieren die σ_i auf W unitäre Transformationen $\tilde{\sigma_i} \in \mathrm{U}(\tilde{f})$, die Symmetrien oder $= 1_W$ sind. Insbesondere ist $\tilde{\pi}$ damit ein Produkt von Symmetrien. Weil $\tilde{\pi}$ unzerlegbar ist, ist dies ein Widerspruch zu 3.5.10.
Ist π vom Typ (B), so folgt die Behauptung aus 3.5.13 und den bereits betrachteten Fällen.
Ist π vom Typ (C) und σ eine Symmetrie mit $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) - 1 = 4$, so ist $\pi\sigma$ nach 3.5.14 vom Typ (A1) oder (B1). Aus den bereits betrachteten Fällen folgt $\mathrm{l}(\pi\sigma) \geq 5$. Dies impliziert $\mathrm{l}(\pi) \geq 6$.
Ist π vom Typ (D) und σ eine Symmetrie mit $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) - 1 = 5$, so ist $\pi\sigma$ nach 3.5.16 vom Typ (C) und somit $\mathrm{l}(\pi\sigma) \geq 6$. Dies impliziert $\mathrm{l}(\pi) \geq 7$. ■

$|F| = 2$; Induktion

Um den Induktionsbeweis ohne Abschweifungen führen zu können, geben wir eine Reihe von Hilfssätzen an. Sie stehen in der Reihenfolge, wie sie im Beweis des Induktionssatzes 3.5.35 auftreten.
Dem Leser wird empfohlen, direkt zu diesem überzugehen, und von dort aus je nach Bedarf auf jene zuzugreifen.

Hilfssatz 3.5.18 *Seien* $\dim V = 2$ *und* $\pi \in \mathrm{U}(f)$ *keine Homothetie oder Symmetrie. Dann gibt es eine Symmetrie* σ*, so daß* $\mathrm{mip}(\pi\sigma) = (x+1)(x+\det\pi)$ *ist.*

Beweis. Weil π nicht die Identität auf V und keine Symmetrie ist, ist $\mathrm{B}(\pi)$ regulär, i.e. $\dim B(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = \dim V = 2$. Weil π keine Homothetie ist, gibt es nach 3.5.3 und 3.2.2 (a) eine Symmetrie σ mit $\dim \mathrm{F}(\pi\sigma) = \dim \mathrm{F}(\pi) + 1 = 1$. Hieraus folgt $\mathrm{mip}(\pi\sigma) = (x+1)(x+\det\pi)$. ■

Hilfssatz 3.5.19 *Seien* $\dim V = 3$, $\mu \in K \backslash F$ *und* $\pi \in \mathrm{SU}(f)$ *mit* $\mathrm{mip}(\pi) = (x+\mu)^3$. *Dann gibt es eine Symmetrie* σ*, so daß* $\mathrm{mip}(\pi\sigma) = (x+1)^3$ *ist.*

Beweis. Wegen $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = \dim V = 3$ und weil π keine Homothetie ist, gibt es nach 3.5.3 und 3.2.2 (a) eine Symmetrie σ mit $\dim \mathrm{F}(\pi\sigma) = \dim \mathrm{F}(\pi) + 1 = 1$. Insbesondere ist $x+1$ ein Teiler von $\mathrm{mip}(\pi\sigma)$. Nach 3.5.10 gilt dann bereits $\mathrm{mip}(\pi\sigma) = (x+1)^3$. ■

Hilfssatz 3.5.20 *Seien* $\dim V = 4$ *und* $\pi \in \mathrm{SU}(f)$ *mit* $\mathrm{mip}(\pi) = (x+1)^4$. *Dann gibt es Symmetrien* σ, η, *so daß* $\mathrm{mip}(\pi\sigma) = (x+1)(x+\mu)(x+\bar{\mu})$ *für* $\mu \in K\backslash F$ *und* $\pi\eta$ *eine Involution ist. Insbesondere gilt* $\dim \mathrm{F}(\pi\sigma) = 2 = \dim \mathrm{F}(\pi\eta)$.

Beweis. Wegen $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 2$, wird $\mathrm{B}(\pi)$ von isotropen Vektoren erzeugt. Es gibt daher ein isotropes $v(\pi+1) \in \mathrm{B}(\pi)\backslash \mathrm{B}^2(\pi)$, $v \in V$.
(a). Es gilt

$$0 = f(v(\pi+1), v(\pi+1)) = f(v, v(\pi+1)) + f(v(\pi+1), v) = q_\pi(v(\pi+1)) + \overline{q_\pi(v(\pi+1))},$$

i.e. $q_\pi(v(\pi+1)) \in F$. Ist $q_\pi(v(\pi+1)) = 0$, so wähle $\nu \in K\backslash F$ und setze $v' := v + \nu v(\pi+1)^2$. Dann ist $v'(\pi+1) = v(\pi+1) + \nu v(\pi+1)^3 \in \mathrm{B}(\pi)\backslash \mathrm{B}^2(\pi)$. Wegen $v \notin \mathrm{B}(\pi) = \mathrm{F}(\pi)^\perp = \langle v(\pi+1)^3\rangle^\perp$ gilt $0 \neq f(v, v(\pi+1)^3) = f(v, v(\pi+1)^3\pi^{-3}) = f(v(\pi+1)^3, v)$, i.e. $1 = f(v, v(\pi+1)^3) = f(v, v(\pi+1)^3\pi^{-1}) = f(v(\pi+1), v(\pi+1)^2)$. Man berechnet nun

$$\begin{aligned} q_\pi(v'(\pi+1)) &= f(v + \nu v(\pi+1)^2, v(\pi+1) + \nu v(\pi+1)^3) \\ &= f(v, v(\pi+1)) + \bar{\nu} f(v, v(\pi+1)^3) + \nu f(v(\pi+1)^2, v(\pi+1)) + f(v(\pi+1)^2, v(\pi+1)^3) \\ &= 0 + \bar{\nu} + \nu + 0 = 1. \end{aligned}$$

Man kann daher o.B.d.A. annehemen, daß $q_\pi(v(\pi+1)) = 1$ ist. Nach 3.2.2 (a) ist $\sigma := \sigma_{v(\pi+1)}$ eine wohldefinierte Symmetrie, die $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) - 1 = 2$ erfüllt. Wegen $\mathrm{B}(\sigma) \nsubseteq \mathrm{B}^2(\pi)$, gilt $\dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) = \dim \mathrm{rad}\ \mathrm{B}(\pi) - 1 = 0$, cf. 3.3.6 (a). Nach 3.5.12 (a) muß dann die von $\pi\sigma$ auf $\mathrm{B}(\pi\sigma)$ induzierte Abbildung das charakteristische Polynom $(x+\mu)(x+\bar{\mu})$, $\mu \in K\backslash F$, haben. Hieraus folgt $\mathrm{mip}(\pi\sigma) = (x+\mu)(x+\bar{\mu})(x+1)$.

(b). Weil $\mathrm{B}^2(\pi)$ totalisotrop ist, ist

(∗) $b := v(\pi+1)^2$ isotrop.

Ferner gilt

$$q_\pi(b) = f(v(\pi+1), v(\pi+1)^2) = f(v, v(\pi+1)^3\pi^{-1}) = f(v, v(\pi+1)^3) \neq 0,$$

da $v \notin \mathrm{B}(\pi) = \langle v(\pi+1)^\perp\rangle$. Mit (∗) folgt $q_\pi(b) \in F^*$. Nach 3.2.2 (a) ist $\eta := \sigma_b$ eine wohldefinierte Symmetrie mit

$$\mathrm{F}(\pi\eta) = \mathrm{F}(\pi) \oplus \langle v(\pi+1)\rangle = \mathrm{rad}\ \mathrm{B}(\pi) \oplus \langle v(\pi+1)\rangle \subseteq \mathrm{B}(\pi) \cap v(\pi+1)^\perp = \mathrm{B}(\pi\eta).$$

Folglich ist $\pi\eta$ eine Involution. ■

Hilfssatz 3.5.21 *Seien* $\pi \in \mathrm{SU}(f)$ *kurz und* $\mu \in K\backslash F$ *derart, daß folgende Bedingungen erfüllt sind:*

(1) $\dim \mathrm{B}(\pi) = 6$;

(2) $\dim \mathrm{rad}\ \mathrm{B}(\pi) = 1$;

(3) $\dim \mathrm{F}_\mu(\pi) \leq 2$ *und* $\mathrm{F}\mu(\pi)$ *ist nicht totalisotrop;*

(4) $2 \geq \dim \mathrm{F}_{\bar{\mu}}(\pi) \geq \dim \mathrm{rad}\ \mathrm{F}_{\bar{\mu}}(\pi) \geq 1$;

(5) *Ist* $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 2$, *so ist* $\mathrm{F}_{\bar{\mu}}(\pi)$ *totalisotrop.*

Dann gibt es eine Symmetrie σ *so, daß* $\dim \mathrm{B}(\pi\sigma) = 5$ *und* $\pi\sigma$ *kurz ist.*

Beweis. Sei ϕ die von π auf $\mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi)$ induzierte Abbildung. Nach (1) und (2) gilt $\deg(\mathrm{char}(\phi)) = \dim \mathrm{B}(\pi) - \dim \mathrm{rad}\ \mathrm{B}(\pi) = 5$. Nach (4) ist $(x+\bar{\mu})^2$ ein Teiler von $\mathrm{char}(\phi)$, i.e. es gibt ein $^-$-symmetrisches $p \in \mathrm{F}_4[x]$, so daß $\mathrm{char}(\phi) = p(x+\bar{\mu})^2$. Aus $p(0) \cdot \bar{\mu}^2 = \mathrm{char}(\phi)(0) = \det \phi = \det \pi = 1$ folgt $p(0) = \bar{\mu}$. Aus 3.5.12 (d) erhält man $p \in \{x^3 + \bar{\mu}, (x+\bar{\mu})(x+1)^2, (x+\bar{\mu})^2(x+\mu), (x+\mu)^2(x+1)\}$.

Fall 1. $p = x^3 + \bar{\mu}$. Es ist $A := \ker(\pi+1)^2$ ein regulärer π-Modul. Nach (2) ist $\sigma := \pi_A \bigoplus 1_{A^\perp}$ eine wohldefinierte Symmetrie. Weil nun $\pi\sigma = \pi_{A^\perp}$ ist, ist $\dim \mathrm{B}(\pi\sigma) = \dim A^\perp = 5$, $\mathrm{mip}(\pi_{A^\perp}) = (x^3+\bar{\mu})(x+\bar{\mu})^2$ und $\pi\sigma$ kurz.

Fall 2. $p = (x+\bar{\mu})(x+1)^2$. Weil $(x+\bar{\mu})^2$ kein Teiler von p ist folgt aus (2), (4) und (5), daß $\dim \mathrm{rad}\ \mathrm{F}_{\bar{\mu}}(\pi) = \dim \mathrm{F}_{\bar{\mu}}(\pi) = 1$ und $\mathrm{mip}(\pi) = (x+\bar{\mu})^3(x+1)^4$ ist. Seien $U := \ker(\pi+\bar{\mu})^3$ und $W := \ker(\pi+1)^4 = U^\perp$. Nach 3.5.19 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq U$, so daß $\mathrm{mip}((\pi\sigma)_U) = (x+1)^3$ ist. Damit ist $\pi\sigma = (\pi\sigma)_U \bigoplus \pi_W$ kurz und erfüllt $\dim \mathrm{B}(\pi\sigma) = 5$.

Fall 3. $p = (x+\bar{\mu})^2(x+\mu)$.
3.1. $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 1 = \dim \mathrm{rad}\ \mathrm{F}_{\bar{\mu}}(\pi)$. Dann gilt $\mathrm{mip}(\pi) = (x+\bar{\mu})^4(x+\mu)(x+1)^2$. Wie im Fall 1. ist $A := \ker(\pi+1)^2$ ein regulärer π-Modul und $\sigma := \pi_A \bigoplus 1_{A^\perp}$ eine wohldefinierte Symmetrie. Wegen $\pi\sigma = \pi_{A^\perp}$ und $\mathrm{mip}(\pi_{A^\perp}) = (x+\bar{\mu})^4(x+\mu)$ ist $\pi\sigma$ kurz mit $\dim \mathrm{B}(\pi\sigma) = \dim A^\perp = 5$.
3.2. $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 2$. Nach (5) ist $\mathrm{F}_{\bar{\mu}}(\pi)$ dann totalisotrop. Es gibt daher eine Zerlegung $V = A \bigoplus C \bigoplus \mathrm{F}_\mu(\pi) \bigoplus D \bigoplus E$, wobei A, C, D, E π-Moduln sind und $\dim A = \dim C = \dim D = 2$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^2 = \mathrm{mip}(\pi_C)$, $\mathrm{mip}(\pi_D) = (x+1)^2$ und $\dim \mathrm{F}_\mu(\pi) = 1$ gilt. Nach 3.5.18 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq C$ und $\mathrm{mip}((\pi\sigma)_C) = (x+\mu)(x+1)$. Insbesondere gilt $\dim \mathrm{B}(\pi\sigma) = 5$. Wegen $\mathrm{mip}(\pi\sigma) = (x+\bar{\mu})^2(x+\mu)(x+1)^2$ ist $\pi\sigma$ kurz.

Fall 4. $p = (x+\mu)^2(x+1)$. Aus $\dim F_\mu(\pi) = 1$ würde nach (3) folgen, daß $\mathrm{F}_\mu(\pi)$ regulär ist. Damit wäre $(x+\mu)^2$ kein Teiler von p, ein Widerspruch. Aus (3) folgt daher $\dim \mathrm{F}_\mu(\pi) = 2$. Wäre $\mathrm{F}_\mu(\pi)$ nicht regulär, so wäre $(x+\mu)^3$ ein Teiler von $\mathrm{char}(\phi)$, ein Widerspruch. Folglich ist $\mathrm{F}_\mu(\pi)$ regulär und es gibt eine Zerlegung $V = A \bigoplus F_\mu(\pi) \bigoplus C \bigoplus D$, wobei A, C, D π-Moduln sind und $\dim A = 2$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^2$, $\dim C = 3$, $\mathrm{mip}(\pi_C) = (x+1)^3$ und $D \leq \mathrm{F}(\pi)$ gilt. Weil A als hyperbolische Ebene von isotropen Vektoren erzeugt wird, gibt es ein isotropes $a \in A \backslash A(\pi+\bar{\mu})$. Weil $F_{\bar{\mu}}(\pi) = \langle a(\pi+\bar{\mu}) \rangle$ isotrop und $A = \langle a, a(\pi+\bar{\mu}) \rangle$ regulär ist, ist $\alpha := f(a, a(\pi+\bar{\mu})) \neq 0$. Man berechnet $0 = f(a(\pi+\bar{\mu}), a(\pi+\bar{\mu})) = \mu\bar{\alpha} + \bar{\mu}\alpha$. Dies impliziert $\alpha = \mu$ und somit

$$q_\pi(a(\pi+1)) = f(a, a(\pi+1)) = f(a, a(\pi+\bar{\mu})) = \mu.$$

Sei $w \in C \backslash C(\pi+1)$. Wegen $\langle w(\pi+1)^2\rangle^{\perp} \cap C = C(\pi+1)$ ist

$$f(w(\pi+1), w(\pi+1)) = f(w, w(\pi+1)^2\pi^{-1}) = f(w, w(\pi+1)^2) \neq 0.$$

Für $\beta := f(w, w(\pi+1))$ bedeutet dies: $1 = f(w(\pi+1), w(\pi+1)) = \beta + \bar{\beta}$, i.e. $\beta \in \{\mu, \bar{\mu}\}$. Ist $\beta = \mu$, so setze $w' := w(\pi+\bar{\mu}) \in C \backslash C(\pi+1)$. Dann gilt

$$\begin{aligned} f(w', w'(\pi+1)) &= f(w(\pi+1) + \mu w, w(\pi+1)^2 + \mu w(\pi+1)) \\ &= f(w(\pi+1), w(\pi+1)^2) + \mu f(w, w(\pi+1)^2) \\ &\quad + \bar{\mu} f(w(\pi+1), w(\pi+1)) + f(w, w(\pi+1)) \\ &= 0 + \mu + \bar{\mu} + \mu = \bar{\mu}. \end{aligned}$$

Man kann daher o.B.d.A.

$$q_\pi(w(\pi+1)) = \beta = \bar{\mu}$$

annehmen. Für $z := (a+w)(\pi+1)$ gilt dann $q_\pi(z) = q_\pi(a(\pi+1)) + q_\pi(w(\pi+1)) = \mu + \bar{\mu} = 1$. Nach 3.2.2 ist $\sigma := \sigma_z$ eine wohldefinierte Symmetrie, so daß $\dim \mathrm{B}(\pi\sigma) = 5$ ist. Wegen $\mathrm{B}(\sigma) = \langle a(\pi+1) + w(\pi+1)\rangle \not\subseteq \mathrm{B}^2(\pi) = A + F_\mu(\pi) + \langle w(\pi+1)^2\rangle$,$\mathrm{B}(\pi)(\pi+\bar{\mu}) = \langle a(\pi+\bar{\mu})\rangle + \mathrm{F}_\mu(\pi) + C(\pi+1)$, gilt

$$\dim \mathrm{F}_{\bar{\mu}}(\pi\sigma) = \dim \mathrm{F}_{\bar{\mu}}(\pi) - 1 = 0 = \dim \mathrm{rad}\ \mathrm{B}(\pi) - 1 = \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma).$$

Wegen $\mathrm{F}_\mu(\pi) \leq \mathrm{F}(\sigma)$, ist $\mathrm{F}_\mu(\pi) \leq \mathrm{F}_\mu(\pi\sigma)$. Insgesamt erhält man, daß $\mathrm{char}(\pi\sigma_{\mathrm{B}(\pi\sigma)}) = q(x+\mu)^2$ für ein $^-$symmetrisches $q \in \mathrm{F}_4[x]$ vom Grad 3 mit konstantem Glied μ gilt, das nicht von $x+1, x+\bar{\mu}$ geteilt wird. Aus 3.5.12 (d) folgt $q = x^3 + \mu$. Damit ist $\pi\sigma$ kurz. ∎

Hilfssatz 3.5.22 *Seien $\pi \in \mathrm{SU}(f)$ kurz und $\mu \in K \backslash F$ derart, daß folgende Bedingungen erfüllt sind:*

(1) $\dim \mathrm{B}(\pi) = 6$;
(2) $\mathrm{rad}\ \mathrm{B}(\pi) = \{0\}$;
(3) $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) < \dim \mathrm{F}_\mu(\pi) = 2$;
(4) $\dim \mathrm{F}_{\bar{\mu}}(\pi) = \dim \mathrm{rad}\ \mathrm{F}_{\bar{\mu}}(\pi) = 1$.

Dann gibt es eine Symmetrie σ so, daß $\dim \mathrm{B}(\pi\sigma) = 5$ und $\pi\sigma$ kurz ist.

Beweis. Sei ϕ die von π auf $\mathrm{B}(\pi)$ induzierte Abbildung. Wegen (1) ist $\deg(\mathrm{char}(\phi)) = \dim \mathrm{B}(\pi) = 6$. Aus (3) und (4) folgt $\mathrm{char}(\phi) = p(x+\mu)^2(x+\bar{\mu})^2$ für ein $^-$-symmetrisches $p \in \mathrm{F}_4[x]$ vom Grad 2 mit konstantem Glied $p(0) = 1$. Weil $x+1$ wegen (2) kein Teiler von p ist, folgt $p = (x+\mu)(x+\bar{\mu})$ (cf. 3.5.12 (a)). Wegen (3) impliziert dies $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) = 1$. Man erhält demnach eine Zerlegung $V = A \bigoplus C \bigoplus D \bigoplus \mathrm{F}(\pi)$ in π-Moduln A, C, D mit $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^3$, $\dim C = 2$, $\mathrm{mip}(\pi_C) = (x+\mu)^2$, $\dim D = 1$, $D \leq \mathrm{F}_\mu(\pi)$. Nach 3.5.18 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq C$ und $\mathrm{mip}(\pi\sigma) = (x+1)(x+\bar{\mu})$, somit gilt $\dim \mathrm{B}(\pi\sigma) = 5$ und $\mathrm{mip}(\pi\sigma) = (x+\bar{\mu})^3(x+\mu)(x+1)$. Folglich ist $\pi\sigma$ kurz. ∎

Hilfssatz 3.5.23 *Seien $\pi \in \mathrm{SU}(f)$ kurz und $\mu \in K \backslash F$ derart, daß folgende Bedingungen erfüllt sind:*

(1) $\dim \mathrm{B}(\pi) = 6$*;*

(2) $\dim \mathrm{rad}\ \mathrm{B}(\pi) \leq 1$*;*

(3) $\dim \mathrm{F}_{\mu}(\pi) \leq 2$ *und* $\mathrm{F}_{\mu}(\pi)$ *ist nicht totalisotrop;*

(4) $3 = \dim \mathrm{F}_{\bar{\mu}}(\pi) \geq \dim \mathrm{rad}\ \mathrm{F}_{\bar{\mu}}(\pi) \geq 1$.

Dann gibt es eine Symmetrie σ *so, daß* $\dim \mathrm{B}(\pi\sigma) = 5$ *und* $\pi\sigma$ *kurz ist.*

Beweis. Sei ϕ die von π auf $\mathrm{B}(\pi)$ induzierte Abbildung. Nach (1) ist $\deg(\mathrm{char}(\phi)) = \dim \mathrm{B}(\pi) = 6$. Nach (3) und (4) gilt $\mathrm{char}(\phi) = p(x + \bar{\mu})^4$ für ein $^-$-symmetrisches $p \in \mathrm{F}_4[x]$ vom Grad 2 mit konstantem Glied $p(0) = \mu$. Nach 3.5.12 (b) ist $p \in \{(x+1)(x+\mu), (x+\bar{\mu})^2\}$.
Fall 1. $p = (x+1)(x+\mu)$. Dann induziert π auf dem regulären π-Modul $U := \ker(\pi+1)^2$ eine Symmetrie. Demnach ist $\sigma := \pi_U \mathbin{\bigcirc\!\!\!\!\!\perp}\ 1_{U\perp}$ eine wohldefinierte Symmetrie mit $\dim \mathrm{B}(\pi\sigma) = 5$. Ferner ist $\pi_{U^\perp} \mathbin{\bigcirc\!\!\!\!\!\perp}\ 1_U = \pi\sigma$ kurz.
Fall 2. $p = (x+\bar{\mu})^2$. Weil π nicht vom Typ (D) ist, ist $\mathrm{F}_{\bar{\mu}}(\pi)$ nicht totalisotrop.
2.1. $\dim \mathrm{radF}_{\bar{\mu}}(\pi) = 2$. Dann gibt es eine Zerlegung $V = A \mathbin{\bigcirc\!\!\!\!\!\perp}\ C \mathbin{\bigcirc\!\!\!\!\!\perp}\ D \mathbin{\bigcirc\!\!\!\!\!\perp}\ F(\pi)$, wobei A, C, D π-Moduln sind und $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^3$, $\dim C = 2$, $\mathrm{mip}(\pi_C) = (x+\bar{\mu})^2$, $\dim D = 1$, $D \leq \mathrm{F}_{\bar{\mu}}(\pi)$ gilt. Nach 3.5.18 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq C$ und $\mathrm{mip}((\pi\sigma)_C) = (x+1)(x+\mu)$. Dann ist $\dim \mathrm{B}(\pi\sigma) = 5$ und $\pi\sigma = \pi_A \mathbin{\bigcirc\!\!\!\!\!\perp}\ (\pi\sigma)_C \mathbin{\bigcirc\!\!\!\!\!\perp}\ \bar{\mu}1_D \mathbin{\bigcirc\!\!\!\!\!\perp}\ 1_{\mathrm{F}(\pi)}$ kurz.
2.2. $\dim \mathrm{radF}_{\bar{\mu}}(\pi) = 1$. Dann gibt es eine Zerlegung $V = A \mathbin{\bigcirc\!\!\!\!\!\perp}\ C \mathbin{\bigcirc\!\!\!\!\!\perp}\ F(\pi)$, wobei A, C π-Moduln sind mit $\dim A = 4$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^4$, $\dim C = 2$, $C \leq \mathrm{F}_{\bar{\mu}}(\pi)$. Weil $\mu\pi_A$ das Minimalpolynom $(x+1)^4$ hat gibt es nach 3.5.20 eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$, so daß $\mathrm{mip}((\mu\pi\sigma)_A) = (x+1)(x+\mu)(x+\bar{\mu})$ ist. Dann gilt auch $\mathrm{mip}((\pi\sigma)_A) = (x+1)(x+\mu)(x+\bar{\mu})$. Weil daraus $\dim \mathrm{F}(\pi\sigma)_A = 1$ folgt, ist $\dim \mathrm{B}(\pi) = 5$. Wegen $\pi\sigma = (\pi\sigma)_A \mathbin{\bigcirc\!\!\!\!\!\perp}\ \bar{\mu}1_C \mathbin{\bigcirc\!\!\!\!\!\perp}\ 1_{\mathrm{F}(\pi)}$ ist $\mathrm{mip}(\pi\sigma) = (x+1)(x+\mu)(x+\bar{\mu})$. Demnach ist $\pi\sigma$ kurz. ■

Hilfssatz 3.5.24 *Sei* $\pi \in \mathrm{SU}(f)$ *kurz. Es sei* $\dim \mathrm{B}(\pi)/\mathrm{radB}(\pi) = 2$*. Dann gibt es eine Symmetrie* σ *so, daß* $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ *und* $\pi\sigma$ *kurz ist.*

Beweis. Sei ϕ die von π auf $\mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi)$ induzierte Abbildung. Dann ist $\mathrm{char}(\phi)(0) = \det\phi = \det\pi = 1$. Weil $(x+1)^2, (x+\mu)(x+\bar{\mu})$, $\mu \in K \backslash F$, die einzigen $^-$-symmetrischen Polynome in $F_4[x]$ vom Grad 2 mit konstantem Glied 1 sind (cf. 3.5.12 (a)), stimmt $\mathrm{char}(\phi)$ mit einem dieser überein.

Fall 1. $\mathrm{char}(\phi) = (x+1)^2$.
1.1. $\mathrm{mip}(\phi) = (x+1)^2$. Dann gilt $V = A \mathbin{\bigcirc\!\!\!\!\!\perp}\ B$ für π-Moduln A, B, so daß $\dim A = 4$, $\mathrm{mip}(\pi_A) = (x+1)^4$ und π_B eine Involution ist. Nach 3.5.20 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$, $\dim \mathrm{F}(\pi\sigma) > \dim \mathrm{F}(\pi)$ und $\mathrm{mip}((\pi\sigma)_A) = (x+1)(x+\mu)(x+\bar{\mu})$, $\mu \in K\backslash F$. Demnach ist $\pi\sigma = (\pi\sigma)_A \mathbin{\bigcirc\!\!\!\!\!\perp}\ \pi_B$ kurz.

1.2. $\mathrm{mip}(\phi) = x+1$. Dann gilt $V = A \mathbin{\bigcirc\!\!\!\!\!\perp}\ B \mathbin{\bigcirc\!\!\!\!\!\perp}\ C$ für π-Moduln A, B, C mit $\dim A = 3 = \dim B$, $\mathrm{mip}(\pi_A) = (x+1)^3 = \mathrm{mip}(\pi_B)$, $\pi_C^2 = 1_C$. Seien $D := A \mathbin{\bigcirc\!\!\!\!\!\perp}\ B$ und $\psi := \pi_D$. Wegen $\dim \mathrm{B}^2(\psi) \leq \dim \mathrm{B}(\psi) - 2$, gibt es nach 3.5.3 (mit $W = \mathrm{B}^2(\psi)$) und 3.2.2 (a) eine Symmetrie ρ mit $\mathrm{B}(\rho) \not\leq \mathrm{B}^2(\psi)$ und $\dim \mathrm{B}(\psi\rho) = \dim \mathrm{B}(\psi) - 1 = 3$. Nach 3.3.6 (a) gilt

(1) $\dim \mathrm{B}(\psi\rho)/\mathrm{rad}\ \mathrm{B}(\psi\rho) = \dim \mathrm{B}(\psi)/\mathrm{rad}\ \mathrm{B}(\psi) = 2,$

und

(2) $\dim \mathrm{rad}\ \mathrm{B}(\psi\rho) = \dim \mathrm{rad}\ \mathrm{B}(\psi) - 1 = 1.$

Sei η die von ψ auf $\mathrm{B}(\psi)/\mathrm{rad}\ \mathrm{B}(\psi)$ induzierte Abbildung. Aus (1) folgt $\deg(\mathrm{char}(\eta)) = 2$. Wegen $\mathrm{char}(\eta)(0) = \det \eta = \det \psi = 1$ und weil nach 3.5.12 (a) $(x+1)^2, (x+\mu)(x+\bar{\mu})$, $\mu \in K\backslash F$ die einzigen $^-$-symmetrischen Polynome in $F_4[x]$ vom Grad 2 mit konstantem Glied 1 sind, folgt nun mit (2), daß $\mathrm{mip}(\psi\rho) \in \{(x+1)^4, (x+1)^2(x+\mu)(x+\bar{\mu})\}$. Demnach ist $\psi\rho$ kurz. Setzt man nun $\sigma := \rho \mathbin{\bigcirc\!\!\!\!\perp} 1_C$, so trifft dies auch auf $\pi\sigma = (\psi\rho) \mathbin{\bigcirc\!\!\!\!\perp} \pi_C$ zu und es gilt $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$.

Fall 2. $\mathrm{char}(\phi) = (x+\mu)(x+\bar{\mu})$. Dann gilt $V = \mathrm{F}_\mu(\pi) \mathbin{\bigcirc\!\!\!\!\perp} \mathrm{F}_{\bar{\mu}}(\pi) \mathbin{\bigcirc\!\!\!\!\perp} C$, $\dim \mathrm{F}_\mu(\pi) = 1 = \dim \mathrm{F}_{\bar{\mu}}(\pi)$ und $C = \ker(\pi+1)^2$. Sei $D := \mathrm{F}_\mu(\pi) \mathbin{\bigcirc\!\!\!\!\perp} \mathrm{F}_{\bar{\mu}}(\pi)$. Nach 3.5.18 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq D$ so, daß $(\pi\sigma)_D$ eine Symmetrie ist. Insbesondere ist $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma = (\pi\sigma)_D \mathbin{\bigcirc\!\!\!\!\perp} \pi_C$ eine Involution, also kurz. ■

Hilfssatz 3.5.25 *Sei $\pi \in \mathrm{SU}(f)$ kurz. Es gelte $\dim \mathrm{B}(\pi)/\mathrm{radB}(\pi) = 3$ und $\dim \mathrm{F}_\mu(\pi) \leq 1$ für alle $\mu \in K\backslash F$. Dann gibt es eine Symmetrie σ so, daß $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma$ kurz ist.*

Beweis. Sei ϕ die von π auf $\mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi)$ induzierte Abbildung. Es ist dann $\mathrm{char}(\phi)(0) = \det \phi = \det \pi = 1$. Weil $(x+1)^3, (x+1)(x+\mu)(x+\bar{\mu}), (x+\mu)^3$, $\mu \in K\backslash F$, nach 3.5.12 (c) die einzigen $^-$-symmetrischen Polynome in $F_4[x]$ vom Grad 3 mit konstantem Glied 1 sind, stimmt $\mathrm{char}(\phi)$ mit einem dieser überein. Nimmt man an, daß $\mathrm{char}(\phi) = (x+\mu)^3$ für ein $\mu \in K\backslash F$ ist, so ist $\mathrm{mip}(\phi) \neq (x+\mu)^3$, da π nicht vom Typ (A1) ist. Dies bedeutet $\mathrm{mip}(\phi) \in \{(x+\mu), (x+\mu)^2\}$, was wiederum $\dim \mathrm{F}_\mu(\pi) \geq 2$ nach sich zieht, ein Widerspruch.

Fall 1. $\mathrm{char}(\phi) = (x+1)^3$. Weil π nicht vom Typ (A2) ist, gilt $\mathrm{mip}(\phi) \neq (x+1)^3$.
1.1. $\mathrm{mip}(\phi) = (x+1)^2$. Dann gilt $V = A \mathbin{\bigcirc\!\!\!\!\perp} B \mathbin{\bigcirc\!\!\!\!\perp} C$ für π-Moduln A, B, C mit $\dim A = 4$, $\mathrm{mip}(\pi_A) = (x+1)^4$, $\dim B = 3$, $\mathrm{mip}(\pi_B) = (x+1)^3$, $\pi_C^2 = 1_C$. Sei $\psi := \pi_A$. Weil $\mathrm{B}(\psi)$ nicht totalisotrop ist, gibt es ein anisotropes $a \in \mathrm{B}(\psi)$. Weil $\mathrm{B}^2(\psi)$ totalisotrop ist, ist a nicht in $\mathrm{B}^2(\psi)$ enthalten. Seien $v \in A\backslash\mathrm{B}(\psi)$ mit $a = v(\psi+1)$ und $b := a(\psi+1) = v(\psi+1)^2 \in \mathrm{B}^2(\psi)$. Man berechnet nun

$$q_\psi(b) = f(v(\psi+1), v(\psi+1)^2) = f(v, v(\psi+1)^3\psi^{-1}) = f(v, v(\psi+1)^3) \neq 0,$$

da $v \notin A(\psi+1) = v(\psi+1)^\perp$. Weil b isotrop ist, gilt $q_\psi(b) \in F^*$. Nach 3.2.2 (a) ist $\rho := \sigma_b$ eine wohldefinierte Symmetrie mit

$$\mathrm{F}(\psi\rho) = \mathrm{F}(\psi) \oplus \langle a \rangle = \mathrm{rad}\ \mathrm{B}(\psi) \mathbin{\bigcirc\!\!\!\!\perp} \langle a \rangle.$$

Weil a anisotrop ist, folgert man

$$\mathrm{rad}\ \mathrm{B}(\psi\rho) = \mathrm{rad}\ \mathrm{F}(\psi\rho) = \mathrm{rad}\ \mathrm{B}(\psi) = \langle v(\psi+1)^3 \rangle,$$

also $\dim \mathrm{radB}(\psi\rho) = 1$. Dies bedeutet $\dim \mathrm{B}(\psi\rho)/\mathrm{radB}(\psi\rho) = 1$. Demnach ist $\psi\rho$ vom Typ (N). Setzt man $\sigma := \rho \mathbin{\bigcirc\!\!\!\!\perp} 1_{A^\perp}$, so gilt $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma = (\psi\rho) \mathbin{\bigcirc\!\!\!\!\perp} \pi_B \mathbin{\bigcirc\!\!\!\!\perp} \pi_C$ ist kurz.

Fall 1.2. $\mathrm{mip}(\phi) = x+1$. Dann gilt $V = A \bigoplus B \bigoplus C \bigoplus D$ für π-Moduln A, B, C, D mit $\dim A = \dim B = \dim C$, $\mathrm{mip}(\pi_A) = \mathrm{mip}(\pi_B) = \mathrm{mip}(\pi_C) = (x+1)^3$, $\pi_D^2 = 1_D$. Seien $E := A \bigoplus B$ und $\psi := \pi_E$. Nach 3.5.24 Fall 1.2 gibt es eine Symmetrie $\rho \in \mathrm{U}(f_D)$ derart, daß $\mathrm{F}(\psi\rho) > \mathrm{F}(\pi)$ und $\mathrm{mip}(\psi\rho) \in \{(x+1)^4, (x+1)^2(x+\mu)(x+\bar{\mu})\}$, $\mu \in K \backslash F$, gilt. Setzt man $\sigma := \rho \bigoplus 1_{E^\perp}$, so gilt $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma = (\psi\rho) \bigoplus \pi_C \bigoplus \pi_D$ ist kurz.

Fall 2. $\mathrm{char}(\pi) = \mathrm{mip}(\pi) = (x+1)(x+\mu)(x+\bar{\mu})$, $\mu \in K\backslash F$. Dann gilt $V = \mathrm{F}_\mu(\pi) \bigoplus \mathrm{F}_{\bar{\mu}}(\pi) \bigoplus A \bigoplus B$ für π-Moduln A, B, wobei $\dim \mathrm{F}_\mu(\pi) = 1 = \dim \mathrm{F}_{\bar{\mu}}(\pi)$, $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+1)^3$ und $\pi_B^2 = 1_B$ ist. Seien $C := \mathrm{F}_{\bar{\mu}}(\pi) \bigoplus A$ und $\psi := \pi_C$. Wegen $\dim \mathrm{B}(\psi)/\mathrm{rad}\ \mathrm{B}(\psi) = 2$ und weil ψ wegen $\mathrm{char}(\psi_{\mathrm{B}(\psi)}) = (x+\bar{\mu})(x+1)^2$ keine Homothetie auf $\mathrm{B}(\psi)$ induziert, gibt es nach 3.5.3 und 3.2.2 (a) eine Symmetrie $\rho \in \mathrm{U}(f_C)$ mit $\dim \mathrm{B}(\psi\rho) = \dim \mathrm{B}(\psi) - 1 = 2$. Weil $\psi_A \in \mathrm{SU}(f_A)$ unzerlegbar und somit nach 3.5.10 kein Produkt von Symmetrien ist, gilt $\mathrm{B}(\rho) \nsubseteq A = \mathrm{B}(\mu\psi)$. Nach 3.3.6 (b) bedeutet dies $\dim \mathrm{F}_{\bar{\mu}}(\psi\rho) = \dim \mathrm{F}_{\bar{\mu}}(\psi) - 1 = 0$. Wegen $\det \psi\rho = \det \psi = \bar{\mu}$ und weil nach 3.5.12 (b) $(x+\mu)^2, (x+1)(x+\bar{\mu})$ die einzigen $^-$-symmetrischen Polynome in $F_4[x]$ vom Grad 2 mit konstantem Glied $\bar{\mu}$ sind, hat die von $\psi\rho$ auf $\mathrm{B}(\psi\rho)$ induzierte Abbildung das Minimalpolynom $(x+\mu)^2$. Dies impliziert $\mathrm{mip}(\psi\rho) = (x+\mu)^2(x+1)$. Setzt man nun $\sigma := \rho \bigoplus 1_{C^\perp}$, so gilt $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma = \mu 1_{\mathrm{F}_\mu(\pi)} \bigoplus (\psi\rho) \bigoplus \pi_B$ ist kurz. ■

Hilfssatz 3.5.26 *Sei* $\pi \in \mathrm{SU}(f)$ *kurz und* $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \geq 4$. *Ferner gelte eine der folgenden Bedingungen:*

- $\dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 1$;
- $\dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) \in \{3, 4\}$ *und* $\dim \mathrm{F}_\mu(\pi) \geq 3$;
- $\dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 4$ *und* $\dim \mathrm{F}_\mu(\pi) = 2$ *und* $\dim \mathrm{rad}\ \mathrm{B}(\pi) = 0$.

für ein $\mu \in K\backslash F$. *Dann gibt es eine Symmetrie* σ *so, daß* $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ *und* $\pi\sigma$ *nicht vom Typ* (A), (B) *ist.*

Beweis. Nach 3.5.3 (mit $W = \mathrm{F}_\mu(\pi)$) und 3.2.2 (a) gibt es eine Symmetrie σ mit $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\mathrm{B}(\sigma) \nsubseteq \mathrm{F}_\mu(\pi)$. Nach 3.3.6 (b) impliziert dies $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) \in \{1, 3, 4\}$. Ist $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = 1$, so ist $\pi\sigma$ kurz, weil keine lange Abbildung diese Eigenschaft hat. Andernfalls gilt nach Voraussetzung $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) \in \{3, 4\}$. Angenommen $\pi\sigma$ ist vom Typ (B). Dann gibt es ein $\nu \in K\backslash F$ mit $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\nu(\pi\sigma) = 2$. Folglich ist $\mu \neq \nu$ und damit $\nu = \bar{\mu}$. Ist $\pi\sigma$ von Typ (B2) oder (B3), so gilt $\mathrm{F}_\mu(\pi\sigma) = \{0\}$ und damit $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{B}(\pi\sigma) \geq 5$, ein Widerspruch. Demnach wäre $\pi\sigma$ vom Typ (B1) und $\dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = \dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = 3$. Nach Voraussetzung gilt dann $1 = \dim \mathrm{F}_\mu(\pi\sigma) \geq \dim \mathrm{F}_\mu(\pi) - 1 \geq 2$, ein Widerspruch. Demnach ist $\pi\sigma$ nicht vom Typ (B). Ist $\dim \mathrm{F}_\mu(\pi\sigma) \geq 2$, so ist $\pi\sigma$ nicht vom Typ (A).
Man kann daher $1 = \dim \mathrm{F}_\mu(\pi\sigma) \geq \dim \mathrm{F}_\mu(\pi) - 1$ annehmen. Dann ist $\dim \mathrm{F}_\mu(\pi) = 2$ und die Voraussetzung liefert, daß $\mathrm{B}(\pi)$ regulär und $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) - 1 = 5$ ist. Wäre $\pi\sigma$ vom Typ (A), so wäre $\dim\ \mathrm{rad}\mathrm{B}(\pi\sigma) \geq \dim\ \mathrm{rad}\mathrm{B}(\pi) - 1 = \dim \mathrm{B}(\pi\sigma) - 4 = 1$, ein Widerspruch. ■

Hilfssatz 3.5.27 *Sei* $\pi \in \mathrm{SU}(f)$ *kurz. Es gelte* $\dim \mathrm{B}(\pi) \geq 5$ *und* $\dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 2$ *für ein* $\mu \in K\backslash F$. *Dann gibt es eine Symmetrie* σ *so, daß* $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ *und* $\pi\sigma$ *kurz ist.*

Beweis. Sei ϕ die von π auf $\mathrm{B}(\pi)/\mathrm{F}_\mu(\pi)$ induzierte Abbildung. Weil π nicht vom Typ (B) ist, ist ϕ zerlegbar, i.e. $\mathrm{mip}(\phi)$ ist ein Polynom in $F_4[x]$ vom Grad ≤ 2 mit konstantem Glied $\neq 0$, das keine Potenz eines irreduziblen Polynoms ist. Weil $x+1, x+\mu, x+\bar{\mu}, (x+1)(x+\mu), (x+1)(x+\bar{\mu}), (x+\mu)(x+\bar{\mu})$ alle Polynome in $F_4[x]$ mit diesen Eigenschaften sind, stimmt $\mathrm{mip}(\phi)$ mit einem dieser überein. Es werden nun alle Fälle nacheinander abgehandelt.

Fall 1. $\mathrm{mip}(\phi) = x+1$. Es gilt dann $V = A \bigoplus B \bigoplus \mathrm{F}_\mu(\pi) \bigoplus C$ für π-Moduln A, B, C, $\dim A = 2 = \dim B$, π_A und π_B sind Symmetrien, $3 \leq \dim \mathrm{F}_\mu(\pi) \equiv 0 \pmod 3$ und $C \leq \mathrm{F}(\pi)$. Wähle $\sigma := \pi_A \bigoplus 1_{A^\perp}$. Dann gilt $\pi\sigma = 1_A \bigoplus \pi_{A^\perp}$, also $F(\pi\sigma) > \mathrm{F}(\pi)$. Weil $\pi_{A^\perp}$ kurz ist, trifft dies auch auf $\pi\sigma$ zu.

Fall 2. $\mathrm{mip}(\phi) = x+\mu$. Es gilt dann $V = A \bigoplus B \bigoplus C \bigoplus \mathrm{F}(\pi)$ für π-Moduln A, B, C, D, $\dim A = 2 = \dim B$, $\mathrm{mip}(\pi_A) = (x+\mu)^2 = \mathrm{mip}(\pi_B)$, $C \leq \mathrm{F}_\mu(\pi)$ und $\dim \mathrm{F}_\mu(\pi) \equiv 1 \pmod 3$. Nach 3.5.18 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$, so daß $\mathrm{mip}((\pi\sigma)_A) = (x+1)(x+\bar{\mu})$ ist. Man liest nun ab, daß $\pi\sigma = (\pi\sigma)_A \bigoplus \pi_{A^\perp}$ kurz ist.

Fall 3. $\mathrm{mip}(\phi) = x+\bar{\mu}$. Es gilt dann $V = \mathrm{F}_{\bar{\mu}}(\pi) \bigoplus \mathrm{F}_\mu(\pi) \bigoplus \mathrm{F}(\pi)$, $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 2$, $\dim \mathrm{F}_\mu(\pi) \equiv 2 \pmod 3$. Seien $a, b \in \mathrm{F}_{\bar{\mu}}(\pi)$ und $c \in \mathrm{F}_\mu(\pi)$ anisotrop und es gelte $f(a,b) = 0$. Setzt man $C := \langle a \rangle \bigoplus \langle c \rangle$, so gibt es nach 3.5.18 eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq C$, so daß $(\pi\sigma)_C$ eine Symmetrie ist. Ferner ist $\pi\sigma = (\pi\sigma)_C \bigoplus \bar{\mu}1_{\langle b \rangle} \bigoplus \mu 1_{c^\perp} \bigoplus 1_{\mathrm{F}(\pi)}$ kurz.

Fall 4. $\mathrm{mip}(\phi) = (x+1)(x+\mu)$. Es gilt dann $V = A \bigoplus B \bigoplus C \bigoplus D$ für π-Moduln A, B, C, D mit $\dim A = 2 = \dim B$, $\mathrm{mip}(\pi_A) = (x+1)^2$ $\mathrm{mip}(\pi_B) = (x+\mu)^2$, $C \leq \mathrm{F}_\mu(\pi)$, $\dim \mathrm{F}_\mu(\pi) \equiv 2 \pmod 3$ und $D \leq \mathrm{F}(\pi)$. Es ist dann $\sigma := \pi_A \bigoplus 1_{A^\perp}$ eine wohldefinierte Symmetrie, welche $A \leq \mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ erfüllt. Weil $\pi_{A^\perp}$ kurz ist, trifft dies auch auf $\pi\sigma = 1_A \bigoplus \pi_{A^\perp}$ zu.

Fall 5. $\mathrm{mip}(\phi) = (x+1)(x+\bar{\mu})$. Es gilt dann $V = A \bigoplus \mathrm{F}_{\bar{\mu}}(\pi) \bigoplus \mathrm{F}_\mu(\pi) \bigoplus B$, für π-Moduln A, B, $\dim A = 2$, $\pi_A^2 = 1_A$, $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 1$, $\dim \mathrm{F}_\mu(\pi) \equiv 1 \pmod 3$ und $B \leq \mathrm{F}(\pi)$. Wie im Fall 4. sieht man, daß $\sigma := \pi_A \bigoplus 1_{A^\perp}$ die gewünschten Eigenschaften hat.

Fall 6. $\mathrm{mip}(\phi) = (x+\mu)(x+\bar{\mu})$. Es gilt dann $V = \mathrm{F}_{\bar{\mu}}(\pi) \bigoplus A \bigoplus B \bigoplus \mathrm{F}(\pi)$, für π-Moduln A, B, $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 1$, $\dim A = 2$, $\mathrm{mip}(\pi_A) = (x+\mu)^2$, $B \leq \mathrm{F}_\mu(\pi)$ und $\dim B \equiv 2 \pmod 3$. Nach 3.5.18 findet man eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$, so daß $\mathrm{mip}((\pi\sigma)_A) = (x+1)(x+\bar{\mu})$ ist. Weil dann $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$, $V = \mathrm{F}_{\bar{\mu}}(\pi\sigma) \bigoplus \mathrm{F}_\mu(\pi\sigma) \bigoplus \mathrm{F}(\pi\sigma)$, $\dim \mathrm{F}_{\bar{\mu}}(\pi\sigma) = 2$ und $\dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi) - 1 \geq 1$ ist, ist $\pi\sigma$ kurz. ∎

Hilfssatz 3.5.28 *Sei $\pi \in \mathrm{SU}(f)$ kurz. Es gelte*

(1) $\dim \mathrm{B}(\pi) = 5$,

(2) $\dim \mathrm{rad}\ \mathrm{B}(\pi) \leq 1$,

(3) $\dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 3$,

(4) $\dim \mathrm{F}_\mu(\pi) = 2$,

(5) $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) \leq 1$,

für ein $\mu \in K \backslash F$. Dann gibt es eine Symmetrie σ so, daß $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma$ kurz ist.

Beweis. Sei ϕ die von π auf $\mathrm{B}(\pi)/\mathrm{F}_\mu(\pi)$ induzierte Abbildung. Es gilt dann $\deg(\mathrm{char}(\phi)) = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 3$ und $\mathrm{char}(\phi)(0) = \det \pi \det \pi^{-1}_{\mathrm{F}_\mu(\pi)} = \mu^{-2} = \mu$. Aus 3.5.12 (d) erhält man

$$\mathrm{char}(\phi) \in \{(x+\mu)^2(x+\bar{\mu}), (x+\mu)(x+1)^2, (x+\bar{\mu})^2(x+1), (x^3+\mu)\}.$$

Die Voraussetzungen (2) und (5) implizieren nun

$$\mathrm{mip}(\phi) \in \{(x+\mu)^2(x+\bar{\mu}), (x+\mu)(x+1)^2, (x+\bar{\mu})^2(x+1), (x+\bar{\mu})(x+1), (x^3+\mu)\}.$$

Fall 1. $\mathrm{mip}(\phi) = (x+\mu)^2(x+\bar{\mu})$. Dann gilt $V = A \oplus B \oplus \mathrm{F}_{\bar{\mu}}(\pi) \oplus \mathrm{F}(\pi)$ für π-Moduln A, B mit $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+\mu)^3$, $\dim B = 1$ und $B \leq \mathrm{F}_\mu(\pi)$. Weil π_A nicht vom Typ (H),(N) ist gibt es nach 3.5.3 (mit $W = \{0\}$) und 3.2.2 (a) eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$ und $\dim \mathrm{F}((\pi\sigma)_A) = 1$. Weil π_A unzerlegbar ist, muß $(\pi\sigma)_A$ nach 3.5.10 ebenfalls unzerlegbar sein. Folglich ist $\mathrm{mip}(\pi\sigma)_A = (x+1)^3$ und $\pi\sigma$ damit kurz.

Fall 2. $\mathrm{mip}(\phi) = (x+\mu)(x+1)^2$. Dann gilt $V = A \oplus B \oplus C \oplus D$ für π-Moduln A, B, C, D mit $\dim A = 2$, $\mathrm{mip}(\pi_A) = (x+\mu)^2$, $\dim B = 1$, $B \leq \mathrm{F}_\mu(\pi)$, $\dim C = 3$, $\mathrm{mip}(\pi_C) = (x+1)^3$, $D \leq F(\pi)$. Wie in 3.5.27 Fall 2. findet man eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$ und $\mathrm{mip}((\pi\sigma)_A) = (x+1)(x+\bar{\mu})$, so daß $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma$ kurz ist.

Fall 3. $\mathrm{mip}(\phi) = (x+\bar{\mu})^2(x+1)$. Dann gilt $V = \mathrm{F}_\mu(\pi) \oplus A \oplus B \oplus C$ für π-Moduln A, B, C mit $\dim A = 2 = \dim B$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^2$, $\mathrm{mip}(\pi_B) = (x+1)^2$ und $C \leq \mathrm{F}(\pi)$. Wie in 3.5.27 Fall 2. findet man eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$ und $\mathrm{mip}((\pi\sigma)_A) = (x+1)(x+\mu)$, so daß $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ ist. Ferner ist $\pi\sigma = \mu 1_{\mathrm{F}_\mu(\pi\sigma)} \oplus \pi_B \oplus 1_{\mathrm{F}(\pi\sigma)}$ kurz.

Fall 4. $\mathrm{mip}(\phi) = (x+\bar{\mu})(x+1)$. Dann gilt $V = \mathrm{F}_\mu(\pi) \oplus \mathrm{F}_{\bar{\mu}}(\pi) \oplus A \oplus B$ für π-Moduln A, B, $\dim F_\mu(\pi) = \dim \mathrm{F}_{\bar{\mu}}(\pi) = \dim A = 2$, $\mathrm{mip}(\pi_A) = (x+1)^2$, $B \leq \mathrm{F}(\pi)$. Setzt man $\sigma := \pi_A \oplus 1_{A^\perp}$, so ist σ eine wohldefinierte Symmetrie mit $A \leq \mathrm{F}(\pi\sigma)$. Weiterhin ist $\pi\sigma = \mu 1_{\mathrm{F}_\mu(\pi)} \oplus \bar{\mu} 1_{\mathrm{F}_{\bar{\mu}}(\pi)} \oplus 1_{A \oplus \mathrm{F}(\pi)}$ kurz.

Fall 5. $\mathrm{mip}(\phi) = (x^3+\mu)$. Dann gilt $V = \mathrm{F}_\mu(\pi) \oplus A \oplus \mathrm{F}(\pi)$ für einen π-Modul A, $\dim A = 3$, $\mathrm{mip}(\pi_A) = x^3+\mu$ und $\dim F_\mu(\pi) = 2$. Seien $\mathrm{F}_\mu(\pi) = \langle a \rangle \oplus \langle b \rangle$ und $C := \langle b \rangle \oplus A$. Es ist $\dim \mathrm{B}(\pi_C) = \dim C = 4$ und damit insbesondere $\dim \mathrm{rad}\ \mathrm{B}(\pi_C) = \{0\}$. Weil π_C auf $\mathrm{B}(\pi_C)$ keine Homothetie induziert, gibt es nach 3.4.3 (mit $W = A = C(\pi+\mu)$) und 3.2.2 (a) eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq C$, $\mathrm{B}(\sigma) \nsubseteq A$ und $\dim \mathrm{F}((\pi\sigma)_C) = 1$. Aus 3.3.6 (b) ergibt sich $\dim \mathrm{F}_\mu(\pi\sigma) = \mathrm{F}_\mu(\pi) - 1 = 1$, i.e. $\mathrm{F}_\mu(\pi\sigma) = a^\perp$ ist regulär und eindimensional. Weil keine lange Abbildung diese Eigenschaft besitzt, ist $\pi\sigma$ kurz. ■

Hilfssatz 3.5.29 *Sei $\pi \in \mathrm{SU}(f)$ kurz. Es gelte*

(1) $\dim \mathrm{B}(\pi) = 5$,
(2) $\dim \mathrm{rad}\ \mathrm{B}(\pi) \leq 1$,
(3) $\dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 4$,
(4) $\dim \mathrm{F}_\mu(\pi) = 1$,
(5) $\dim \mathrm{F}_{\bar{\mu}}(\pi) \leq 2$

für ein $\mu \in K \backslash F$. Dann gibt es eine Symmetrie σ so, daß $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ *und $\pi\sigma$ nicht vom Typ* (A),(B) *ist.*

Beweis. Sei ϕ die von π auf $\mathrm{B}(\pi)/\mathrm{F}_\mu(\pi)$ induzierte Abbildung. Wegen (3) gilt $\deg(\mathrm{char}(\phi)) = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 4$. Aus (4) und $\det \pi = 1$ folgt $\mathrm{char}(\phi)(0) = \det(\phi) = \bar{\mu}$. Dies bedeutet gemäß 3.5.12 (f), daß

$$\begin{aligned}\mathrm{char}(\phi) \quad \in \quad & \{(x+\bar{\mu})^4, (x^3+\bar{\mu})(x+1), (x+1)^3(x+\bar{\mu}), (x^2+\mu x+\mu)(x^2+x+\mu), (x+\mu)(x^3+\mu), \\ & (x+1)(x+\mu)(x+\bar{\mu})^2, (x+\mu)^3(x+\bar{\mu}), (x+1)^2(x+\mu)^2\}.\end{aligned}$$

Fall 1. $\mathrm{char}(\phi) = (x+\bar{\mu})^4$. Aus $\dim \mathrm{radF}_{\bar{\mu}}(\pi) = 2$ würde gemäß (5) folgen, daß $\mathrm{F}_{\bar{\mu}}(\pi)$ totalisotrop ist. Die Eigenschaften (1) und (4) würden dann erzwingen, daß π vom Typ (C) ist, ein Widerspruch. Folglich ist $\dim \mathrm{radF}_{\bar{\mu}}(\pi) \leq 1$. Wäre $\mathrm{F}_{\bar{\mu}}(\pi)$ regulär, so müßte $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 4$ sein, ein Widerspruch zu (5). Man erhält demnach $\dim \mathrm{radF}_{\bar{\mu}}(\pi) = 1$.
1.1. $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 1$. Dann gibt es eine Zerlegung $V = A \textcircled{\perp}\ \mathrm{F}_\mu(\pi) \textcircled{\perp}\ \mathrm{F}(\pi)$, wobei A ein π-Modul mit $\dim A = 4$ und $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^4$ ist. Weil dann $\mathrm{mip}(\mu\pi_A) = (x+1)^4$ ist, gibt es nach 3.5.20 eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$ und $\mathrm{mip}((\mu\pi\sigma)_A) = (x+1)(x+\mu)(x+\bar{\mu})$. Dies impliziert $\mathrm{mip}((\pi\sigma)_A) = (x+1)(x+\mu)(x+\bar{\mu}) = \mathrm{mip}(\pi\sigma)$. Damit ist $\dim \mathrm{F}((\pi\sigma)_A) = 1 > \dim \mathrm{F}(\pi_A)$ und $\pi\sigma$ kurz.
1.2. $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 2$. Dann gibt es eine Zerlegung $V = A \textcircled{\perp}\ C \textcircled{\perp}\ \mathrm{F}_\mu(\pi) \textcircled{\perp}\ \mathrm{F}(\pi)$, wobei A, C π-Moduln mit $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^3$, $\dim C = 1$ und $C \leq \mathrm{F}_{\bar{\mu}}(\pi)$ sind. Nach 3.5.19 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$ und $\mathrm{mip}((\pi\sigma)_A) = (x+1)^3$. Dann ist $\dim F((\pi\sigma)_A) = 1 > \dim \mathrm{F}(\pi_A)$ und $\pi\sigma = (\pi\sigma)_A \textcircled{\perp}\ \bar{\mu}1_C \textcircled{\perp}\ \mu 1_{\mathrm{F}_\mu(\pi)} \textcircled{\perp}\ 1_{\mathrm{F}(\pi)}$ kurz.

Fall 2. $\mathrm{char}(\phi) = (x^3+\bar{\mu})(x+1)$. Dann gilt $V = \mathrm{F}_\mu(\pi) \textcircled{\perp}\ A \textcircled{\perp}\ C$ für π-Moduln A, C, so daß $\dim A = 3$, $\mathrm{mip}(\pi_A) = (x^3+\bar{\mu})$ und π_C eine Symmetrie ist (cf.(2)). Wähle $\sigma := 1_{C^\perp} \textcircled{\perp}\ \pi_C$. Dann ist $\pi\sigma = \pi_{C^\perp} \textcircled{\perp}\ 1_C$ kurz.

Fall 3. $\mathrm{char}(\phi) = (x+1)^3(x+\bar{\mu})$. Nach (2) und (4) ist $\dim \mathrm{rad}\ \mathrm{B}(\pi) = 1 = \dim \mathrm{F}_{\bar{\mu}}(\pi)$. Es folgt $V = \mathrm{F}_\mu(\pi) \textcircled{\perp}\ \mathrm{F}_{\bar{\mu}}(\pi) \textcircled{\perp}\ A \textcircled{\perp}\ C$ für π-Moduln A, C mit $\dim A = 4$, $\mathrm{mip}(\pi_A) = (x+1)^4$ und $C \leq \mathrm{F}(\pi)$. Nach 3.5.18 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq D := \mathrm{F}_\mu(\pi) \textcircled{\perp}\ \mathrm{F}_{\bar{\mu}}(\pi)$, so daß $(\pi\sigma)_D$ eine Symmetrie ist. Damit ist $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma = (\pi\sigma)_D \textcircled{\perp}\ \pi_A \textcircled{\perp}\ 1_C$ kurz.

Fall 4. $\mathrm{char}(\phi) = (x^2+\mu x+\mu)(x^2+x+\mu)$. Es ist $(x^2+\mu x+\mu)^* = (x^2+x+\mu)$ irreduzibel und nicht $^-$-symmetrisch. Daher gibt es eine Zerlegung $V = \mathrm{F}_\mu(\pi) \textcircled{\perp}\ (A \oplus B) \textcircled{\perp}\ \mathrm{F}(\pi)$, wobei $A := \ker(\pi^2+\mu\pi+\mu)$ und $B := \ker(\pi^2+\pi+\mu)$ zweidimensionale, totalisotrope π-Moduln sind. Seien $C := A \oplus B$ und $\psi := \pi_C$. Es gibt dann geordnete Basen (a_1, a_2), (b_1, b_2) von A bzw. B, so daß man bezüglich der Basis $\mathcal{C} := (a_1, a_2, b_1, b_2)$ von C folgende Matrizendarstellungen erhält:

$$\mathcal{M}_{\mathcal{C}}(\psi) = \left[\begin{array}{cc|cc} & 1 & & \\ \mu & \mu & & \\ \hline & & 1 & 1 \\ & & \mu & \end{array}\right], \ \mathcal{M}_{\mathcal{C}}(f_C) = \left[\begin{array}{cc|cc} & & 1 & \\ & & & 1 \\ \hline 1 & & & \\ & 1 & & \end{array}\right].$$

Hieraus berechnet man

$$\mathcal{M}_{\mathcal{C}}(f_\psi) = \left[\begin{array}{cc|cc} & & \bar{\mu} & 1 \\ & & \mu & 1 \\ \hline \bar{\mu} & \bar{\mu} & & \\ 1 & & & \end{array}\right], \ \mathcal{M}_{\mathcal{C}}(f_{\mu\psi}) = \left[\begin{array}{cc|cc} & & \mu & 1 \\ & & \bar{\mu} & 1 \\ \hline & \mu & & \\ \bar{\mu} & \bar{\mu} & & \end{array}\right].$$

Sei $a := a_2 + b_2$. Dann gilt $q_\psi(a) = f_\psi(a, a) = 1$ und $q_{\mu\psi}(a) = f_{\mu\psi}(a, a) = \mu \neq 1$. Nach 3.2.2 ist $\sigma := \sigma_a$ eine wohldefinierte Symmetrie mit $\mathrm{B}(\sigma) = \langle a \rangle \leq C$, $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\dim \mathrm{F}_{\bar{\mu}}(\pi\sigma) = \dim \mathrm{F}(\mu\pi\sigma) \leq \dim \mathrm{F}_{\bar{\mu}}(\pi) = 0$. Damit ist $\pi\sigma$ nicht vom Typ (B1) und damit nicht vom Typ (B) (cf. (1)). Weil $\mathrm{F}_\mu(\pi)$ regulär und in $\mathrm{F}_\mu(\pi\sigma)$ enthalten ist, ist $\pi\sigma$ auch nicht vom Typ (A).

In jedem der restlichen Fälle ist $(x + \mu)$ ein Teiler von $\mathrm{char}(\phi)$. Wegen (4) ist $\mathrm{F}_\mu(\pi)$ stets totalisotrop.
Die folgenden beiden Fälle werden gemeinsam behandelt.
Fall 5. $\mathrm{char}(\phi) = (x + \mu)(x^3 + \mu)$. Es gilt dann $V = A \obot C \obot \mathrm{F}(\pi)$ für π-Moduln A, C mit $\dim A = 2$, $\mathrm{mip}(\pi_A) = (x + \mu)^2$, $\dim C = 3$ und $\mathrm{mip}(\pi_C) = (x^3 + \mu)$.
Fall 6. $\mathrm{char}(\phi) = (x+1)(x+\bar{\mu})^2(x+\mu)$. Es gilt dann $V = A \obot C \obot D$ für π-Moduln A, C, D mit $\dim A = 2$, $\mathrm{mip}(\pi_A) = (x + \mu)^2\}$, $\dim C = 2$ und $\mathrm{mip}(\pi_C) \in \{(x + \bar{\mu}), (x + \bar{\mu})^2$ und π_D ist eine Symmetrie.
In jedem der beiden Fälle findet man nach 3.5.18 eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$ und $\mathrm{mip}((\pi\sigma)_A) = (x + 1)(x + \bar{\mu})$. Es ist $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\pi\sigma = (\pi\sigma)_A \obot \pi_C \obot \pi_D$ kurz.

Fall 7. $\mathrm{char}(\phi) = (x + \mu)^3(x + \bar{\mu})$. Es gilt dann $V = A \obot \mathrm{F}_{\bar{\mu}}(\pi) \obot \mathrm{F}(\pi)$ für einen π-Modul A mit $\dim A = 4$ und $\mathrm{mip}(\pi_A) = (x+\mu)^4$. Die Behauptung folgt nun aus dem bereits betrachteten Fall 1.1 mit μ und $\bar{\mu}$ in vertauschten Rollen.

Fall 8. $\mathrm{char}(\phi) = (x + 1)^2(x + \mu)^2$. Aus (2) folgt $\dim \mathrm{rad}\ \mathrm{B}(\pi) = 1$. Man erhält somit eine Zerlegung $V = A \obot C \obot D$ in π-Moduln A, C, D mit $\dim A = 3 = \dim C$, $\mathrm{mip}(\pi_A) = (x + \mu)^3$, $\mathrm{mip}(\pi_C) = (x + 1)^3$ und $D \leq F(\pi)$. Nach 3.5.19 findet man eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq A$ und $\mathrm{mip}((\pi\sigma)_A) = (x + 1)^3 = \mathrm{mip}(\pi_C) = \mathrm{mip}((\pi\sigma)_C)$. Dann hat σ die gewünschten Eigenschaften. ■

Hilfssatz 3.5.30 *Sei $\pi \in \mathrm{SU}(f)$ kurz. Es gelte*

(1) $\dim \mathrm{B}(\pi) = 6$,

(2) $1 \leq \dim \mathrm{rad}\ \mathrm{B}(\pi) \leq 2$,

(3) $\dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = 4$,

(4) $\dim \mathrm{F}_\mu(\pi) = 2$,

(5) $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) \leq 1$,

(6) $\dim \mathrm{F}_{\bar{\mu}}(\pi) \leq 1$

für ein $\mu \in K \backslash F$. *Dann gibt es eine Symmetrie* σ *so, daß* $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ *und* $\pi\sigma$ *nicht vom Typ* (A), (B) *ist.*

Beweis. Aus (1) und (2) folgt $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \geq 4$. Wegen (2) ist $\mathrm{B}^2(\pi) < \mathrm{B}(\pi)$. Nach 3.5.3 und 3.2.2 (a) gibt es eine Symmetrie σ, so daß $\mathrm{B}(\sigma) \not\subseteq \mathrm{B}^2(\pi)$ und $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) - 1 = 5$ ist. Insbesondere ist $\pi\sigma$ nicht vom Typ (B1),(B3). Nach 3.3.6 (a) gilt $s := \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) = \dim \mathrm{rad}\ \mathrm{B}(\pi) - 1 \in \{0, 1\}$. Demnach ist $\pi\sigma$ nicht vom Typ (A). Ist $s = 0$, so ist $\pi\sigma$ auch nicht vom Typ (B2). Ist $s = 1$, so ist $\dim \mathrm{rad}\ \mathrm{B}(\pi) = s + 1 = 2$, also $\dim \mathrm{B}(\pi)/(\mathrm{rad}\ \mathrm{B}(\pi) + \mathrm{F}_\mu(\pi)) = 2$. Die von π auf $\mathrm{B}(\pi)/(\mathrm{rad}\ \mathrm{B}(\pi) + \mathrm{F}_\mu(\pi))$ induzierte Abbildung ϕ hat daher ein $^-$-symmetrisches charakteristisches Polynom vom Grad 2 mit konstantem Glied μ (cf. (4)). Nach 3.5.12 (b) folgt $\mathrm{char}(\phi) \in \{(x+1)(x+\mu), (x+\bar{\mu})^2\}$.

Fall 1. $\mathrm{char}(\phi) = (x+1)(x+\mu)$. Dann gibt es eine Zerlegung $V = A \bigoplus B \bigoplus C \bigoplus D \bigoplus E$ in π-Moduln A, B, C, D, E mit $\dim A = 2$, $\mathrm{mip}(\pi_A) = (x+\mu)^2$, $\dim B = 1$, $B \leq \mathrm{F}_\mu(\pi)$, $\dim C = 3$, $\mathrm{mip}(\pi_C) = (x+1)^3$, $\dim D = 2$, $\mathrm{mip}(\pi_D) = (x+1)^2$ und $E \leq \mathrm{F}(\pi)$. Dann ist $\sigma := 1_{D^\perp} \bigoplus \pi_D$ eine wohldefinierte Symmetrie mit den gewünschten Eigenschaften.

Fall 2. $\mathrm{char}(\phi) = (x + \bar{\mu}^2)$. Aus (6) folgt, daß $\mathrm{F}_{\bar{\mu}}(\pi)$ totalisotrop ist. Man erhält eine Zerlegung $V = \mathrm{F}_\mu(\pi) \bigoplus A \bigoplus B \bigoplus C \bigoplus D$ in π-Moduln A, B, C, D, so daß $\dim A = \dim B = \dim C = 2$, $\mathrm{mip}(\pi_A) = (x+\bar{\mu})^2$, $\mathrm{mip}(\pi_B) = (x+1)^2 = \mathrm{mip}(\pi_C)$ und $D \leq \mathrm{F}(\pi)$ gilt. Dann ist $\sigma := \pi_C \bigoplus 1_{C^\perp}$ eine wohldefinierte Symmetrie, welche die geforderten Bedingungen erfüllt. ■

Hilfssatz 3.5.31 *Sei* $\pi \in \mathrm{SU}(f)$ *kurz mit* $\dim \mathrm{B}(\pi) \geq 4$. *Es gelte* $\mathrm{rad}\ \mathrm{B}(\pi) \neq \{0\}$ *und* $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \neq 3$. *Dann gibt es eine Symmetrie* σ *derart, daß* $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ *und* $\pi\sigma$ *nicht vom Typ* (A) *ist.*

Beweis. Wir können annehmen, daß π keine Involution ist, i.e. $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \neq 0$. Für $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 2$ haben wir das Behauptete bereits in 3.5.24 eingesehen. Andernfalls folgt $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \geq 4$ aus der Voraussetzung und weil π nicht vom Typ (N) ist.
Nach 3.5.3 und 3.3.6 (a) finden wir eine Symmetrie σ mit $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$ und $\mathrm{B}(\sigma) \not\subseteq \mathrm{B}^2(\pi)$, i.e. $\dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \neq 3$, so daß $\pi\sigma$ nicht vom Typ (A) ist. ■

Hilfssatz 3.5.32 *Sei* $\pi \in \mathrm{SU}(f)$ *kurz mit*

(1) $\dim \mathrm{B}(\pi) \geq 4$,

(2) $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 3$ *und*

(3) $\dim \mathrm{F}_\mu(\pi) \leq 2$ *für alle* $\mu \in K \backslash F$.

Dann gibt es eine Symmetrie σ *so, daß* $\dim \mathrm{F}(\pi\sigma) > \dim \mathrm{F}(\pi)$ *und* $\pi\sigma$ *nicht vom Typ* (A) *ist.*

Beweis. Seien ϕ die von π und g die von f auf $U := \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi)$ induzierten Abbildungen. Dann ist g eine reguläre $^-$-hermitesche Form und $\phi \in \mathrm{SU}(g)$.

Fall 1. π ist unipotent. Dann hat π insbesondere keinen Eigenwert $\mu \in K\backslash F$, so daß 3.5.25 anwendbar ist.
Fall 2. π ist nicht unipotent. Dann ist auch ϕ nicht unipotent, also insbesondere nicht vom Typ (N). Wegen (3) ist ϕ nicht vom Typ (H). Nach 3.5.3 gibt es ein $u \in U$, mit $g(u, u(\phi+1)) = 1$. Sei $v \in B(\pi)$ mit $v + \mathrm{rad}\ \mathrm{B}(\pi) = u$. Für $a := v(\pi+1) \in \mathrm{B}^2(\pi)$ erhält man $q_\pi(a) = f(v, v(\pi+1)) = g(u, u(\phi+1)) = 1$. Aus 3.2.2 (a) folgt $\mathrm{F}(\pi\sigma) = \mathrm{F}(\pi) \oplus \langle v \rangle$ für die Symmetrie $\sigma := \sigma_a$. Wegen $v \in \mathrm{B}(\pi) = \mathrm{F}(\pi)^\perp$ berechnet man nun:

$$\begin{aligned}
\mathrm{radB}(\pi\sigma) &= \mathrm{B}(\pi\sigma) \cap \mathrm{F}(\pi\sigma) = \mathrm{B}(\pi) \cap v^\perp \cap (\mathrm{F}(\pi) \oplus \langle v \rangle) \\
&\supseteq \mathrm{B}(\pi) \cap v^\perp \cap \mathrm{F}(\pi) = \mathrm{B}(\pi) \cap \mathrm{F}(\pi) \\
&= \mathrm{rad}\ \mathrm{B}(\pi).
\end{aligned}$$

Hieraus folgt

$$\begin{aligned}
\dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) &= \dim \mathrm{B}(\pi) - 1 - \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) \\
&\leq \dim \mathrm{B}(\pi) - 1 - \dim \mathrm{rad}\ \mathrm{B}(\pi) \\
&= \dim \mathrm{rad}\ \mathrm{B}(\pi) - 1 \leq 2.
\end{aligned}$$

Demnach ist $\pi\sigma$ nicht vom Typ (A). ■

Hilfssatz 3.5.33 *Seien* $\dim V = 4$ *und* $\pi \in \mathrm{SU}(f)$ *kurz mit* $\mathrm{F}(\pi) = \{0\}$. *Dann gibt es eine Symmetrie* σ *so, daß* $\dim \mathrm{F}(\pi\sigma) = 1$ *und* $\pi\sigma$ *nicht vom Typ* (A) *ist.*

Beweis. Wegen $\mathrm{F}(\pi) = \{0\}$ ist $x+1$ kein Teiler von $\mathrm{mip}(\pi)$. Nach 3.5.12 (e) gibt es daher ein $\mu \in K\backslash F$, so daß $\mathrm{char}(\pi) \in \{(x+\mu)^2(x+\bar\mu)^2, (x^2+\mu x+1)(x^2+\bar\mu x+1), (x+\mu)(x^3+\bar\mu)\}$ ist. Weil π nicht vom Typ (B1) ist, gilt $\mathrm{mip}(\pi) \in \{(x+\mu)^2(x+\bar\mu)^2, (x+\mu)(x+\bar\mu), (x^2+\mu x+1)(x^2+\bar\mu x+1), (x+\mu)(x^3+\bar\mu)\}$. Ist $\mathrm{mip}(\pi) \in \{(x+\mu)^2(x+\bar\mu)^2, (x+\mu)(x+\bar\mu), (x^2+\mu x+1)(x^2+\bar\mu x+1)\}$, so muß π bereits ähnlich zu π^{-1} sein. Nach 2.3.6 ist π dann ein Produkt von zwei unitären Involutionen ρ, η. Wegen $\mathrm{B}(\rho) \cap \mathrm{B}(\eta) \leq \mathrm{F}(\pi) = \{0\}$, ist $V = \mathrm{B}(\pi) = \mathrm{B}(\rho) \oplus \mathrm{B}(\eta)$. Somit ist $\pi = \rho\eta = \sigma_1 \cdots \sigma_4$ ein Produkt von vier Symmetrien σ_i. Die Symmetrie σ_4 hat dann die geforderten Eigenschaften (cf. 3.5.17). Ist $\mathrm{mip}(\pi) = (x+\mu)(x^3+\bar\mu)$, so ist $\mathrm{F}_\mu(\pi)$ eindimensional und regulär. Weil $U := \ker(\pi^3+\bar\mu)$ dreidimensional und regulär ist, und weil π keine Homothetie auf U induziert, gibt es nach 3.5.3 und 3.2.2 (a) eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq U$ und $\mathrm{F}((\pi\sigma)_U) > \mathrm{F}(\pi_U)$. Wegen $\mathrm{F}_\mu(\pi) \leq \mathrm{F}_\mu(\pi\sigma)$ ist $\pi\sigma$ nicht vom Typ (A). ■

Hilfssatz 3.5.34 *Seien* $\dim V = 5$ *und* $\pi \in \mathrm{SU}(f)$ *kurz mit*

(1) $\mathrm{F}(\pi) = \{0\}$ *und*

(2) $\dim \mathrm{F}_\nu(\pi) \leq 2$ *für alle* $\nu \in K\backslash F$.

Dann gibt es eine Symmetrie σ *so, daß* $\dim \mathrm{F}(\pi\sigma) = 1$ *und* $\pi\sigma$ *nicht vom Typ* (A) *ist.*

Beweis. Weil $x+1$ kein Teiler von $\mathrm{char}(\pi)$ ist (cf. (1)), liefert 3.5.12 (g), daß es ein $\mu \in K\backslash F$ mit $\mathrm{char}(\pi) \in \{(x+\mu)^2(x^3+\mu), (x+\mu)(x^2+\mu x+\mu)(x^2+x+\mu), (x+\mu)(x+\bar\mu)^4, x^5+\mu x^4+x^3+x^2+\bar\mu x+1\}$ gibt.

Die ersten drei Fälle werden gemeinsam behandelt. Setze

$$U := \begin{cases} \ker(\pi+\mu)^2 & \text{, falls } \mathrm{mip}(\pi) = (x+\mu)^2(x^3+\mu) \text{ ist,} \\ \mathrm{F}_\mu(\pi) & \text{, falls } \mathrm{mip}(\pi) \in \{(x+\mu)(x^2+\mu x+\mu)(x^2+x+\mu), (x+\mu)(x+\bar\mu)^4\} \text{ ist,} \end{cases}$$

und

$$W := \begin{cases} \ker(\pi^3+\mu) & \text{, falls } \mathrm{mip}(\pi) = (x+\mu)^2(x^3+\mu) \text{ ist,} \\ \ker(\pi^2+\mu\pi+\mu)(\pi^2+\pi+\mu) & \text{, falls } \mathrm{mip}(\pi) = (x+\mu)(x^2+\mu x+\mu)(x^2+x+\mu) \text{ist,} \\ \ker(x+\bar\mu)^4 & \text{, falls } \mathrm{mip}(\pi) = (x+\mu)(x+\bar\mu)^4 \text{ist.} \end{cases}$$

Dann ist $V = U \bigoplus W$, $\dim W \geq 3$ und π_W keine Homothetie, cf. (2). Nach 3.5.3 und 3.2.2 (a) gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \leq W$ und $\mathrm{F}(\pi\sigma) > \mathrm{F}(\pi)$. Wegen $\pi\sigma = \pi_U \bigoplus (\pi\sigma)_W$, ist $\pi\sigma$ nicht vom Typ (A).
Sei schließlich $\mathrm{mip}(\pi) = x^5 + \mu x^4 + x^3 + x^2 + \bar\mu x + 1$. Setze

$$P := \begin{bmatrix} & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \\ 1 & \bar\mu & 1 & 1 & \mu \end{bmatrix} \text{ und } G := \begin{bmatrix} 0 & 0 & 1 & \mu & 0 \\ 0 & 0 & 0 & 1 & \mu \\ 1 & 0 & 0 & 0 & 1 \\ \bar\mu & 1 & 0 & 0 & 0 \\ 0 & \bar\mu & 1 & 0 & 0 \end{bmatrix}$$

Es ist $\det G = 1$, $\bar{G}^t = G$ folglich gibt es eine Basis $\mathcal{B}$ von V, so daß $\mathcal{M}_\mathcal{B}(f) = G$ ist. Wegen $PG\bar{P}^t = G$, gehört die Abbildung $\phi \in \mathrm{GL}(V)$ mit $\mathcal{M}_\mathcal{B}(\phi) = P$ zu $\mathrm{U}(f)$. Weil die Abbildungen π und ϕ zyklisch sind und dasselbe Minimalpolynom $x^5 + \mu x^4 + x^3 + x^2 + \bar\mu x + 1$ besitzen, sind sie ähnlich und damit bereits zueinander konjugiert (cf. 1.3.24). Wir können daher o.B.d.A. $\pi = \phi$ annehmen. Für $v := (1,1,0,0,1)$ berechnet man $a := v(\pi+1) = (0,\bar\mu,0,1,\bar\mu)$, $f(v,v) = 1 = q_\pi(a)$. Für die Symmetrie $\sigma := \sigma_a$ ist dann $\mathrm{F}(\pi\sigma) = \langle v\rangle$ anisotrop (cf. 3.2.2 (a)) und damit insbesondere $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 4$. Also ist $\pi\sigma$ nicht vom Typ (A). ∎

Wir kommen nun zum Hauptsatz dieses Abschnittes.

Satz 3.5.35 *Sei $\pi \in \mathrm{SU}(f)$ kurz und keine Involution. Es sei $m := \dim \mathrm{B}(\pi) \geq 2$. Dann gibt es eine Symmetrie σ so, daß gilt:*

(I) $\dim \mathrm{B}(\pi\sigma) < \dim \mathrm{B}(\pi)$,
(II) *$\pi\sigma$ ist kurz.*

Beweis. Wenn π eine Involution ist, gilt bekanntlich $\pi = \sigma_1 \cdots \sigma_m$ für m paarweise kommutierende Symmetrien σ_i. Jede dieser erfüllt dann (I) und (II). Wir können daher im weiteren Beweis annehmen, daß π keine Involution ist.
Weil π kurz und damit insbesondere nicht vom Typ (H) oder (N) ist, gibt es nach 3.5.3 (mit $W = \{0\}$) und 3.2.2 (a) eine Symmetrie σ, so daß (I) erfüllt ist. Man kann daher annehmen, daß $\pi\sigma$ lang ist, also zu einem der Typen (H),(N),(A),(B),(C),(D) gehört. Im folgenden werden diese sechs Fälle unterschieden. Dabei gehen wir aus beweistechnischen Gründen in der Reihenfolge (C),(D),(H),(N),(B),(A) vor. Nummeriert man die Ausnahmetypen in dieser Reihenfolge von 1 bis 6 durch, so kann man folgenden Standardschluß anwenden:

Hat man für Fälle 1 bis i, $i \leq 5$, bereits gezeigt, daß es eine Symmetrie ρ gibt, so daß $\mathrm{F}(\pi\rho) > \mathrm{F}(\pi)$ und $\pi\rho$ kurz ist, so braucht man im Fall $i+1$ nur zu zeigen, daß es eine Symmetrie η mit $\mathrm{F}(\pi\eta) > \mathrm{F}(\pi)$ gibt, so daß $\pi\eta$ nicht vom Typ $j \geq i$ ist. Denn dann ist $\pi\eta$ entweder kurz und die Behauptung somit bewiesen, oder $\pi\eta$ hat einen Typ $l < i$ und die Behauptung folgt aus den bereits betrachteten Fällen, wobei η an die Stelle von σ tritt.

Fall 1. $\pi\sigma$ ist vom Typ (C) Dann gilt

(1) $\dim \mathrm{B}(\pi) = \dim \mathrm{B}(\pi\sigma) + 1 = 6$;

(2) $\dim \mathrm{radB}(\pi) \leq \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) + 1 = 1$.

Ferner gibt es ein $\mu \in K \backslash F$, so daß $\mathrm{F}_\mu(\pi\sigma)$ eindimensional und regulär und $\mathrm{F}_{\bar{\mu}}(\pi)$ zweidimensional und totalisotrop ist. Hieraus folgt bekanntlich

(3) $\dim \mathrm{F}_\mu(\pi) \leq \dim \mathrm{F}_\mu(\pi\sigma) + 1 \leq 2$;

(3') Ist $\mathrm{F}_\mu(\pi) \neq \{0\}$, so ist $(\mathrm{F}_\mu(\pi\sigma) \subseteq)\mathrm{F}_\mu(\pi)$ nicht totalisotrop;

(4) $3 \geq \dim \mathrm{F}_{\bar{\mu}}(\pi) \geq \dim \mathrm{rad}\ \mathrm{F}_{\bar{\mu}}(\pi) \geq 1$;

(5) Ist $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 2$, so ist $\mathrm{F}_{\bar{\mu}}(\pi) = \mathrm{F}_{\bar{\mu}}(\pi\sigma)$ totalisotrop.

Zeige nun: Ist ρ eine Symmetrie derart, daß $\dim \mathrm{B}(\pi\rho) = 5$ und $\pi\rho$ lang ist, so gilt einer der folgenden Fälle:

(a) $\pi\rho$ ist vom Typ (A), $\dim \mathrm{rad}\ \mathrm{B}(\pi) = 1$ und $\dim \mathrm{F}_{\bar{\mu}}(\pi) \leq 2$;

(b) $\pi\rho$ ist vom Typ (B), $\dim F_\mu(\pi) = 2$ und $\dim \mathrm{F}_{\bar{\mu}}(\pi) = 1$;

(c) $\pi\rho$ ist vom Typ (C), $\dim F_{\bar{\mu}}(\pi\rho) = 2$.

Beweis: Wäre $\pi\rho$ vom Typ (H), so würde $\dim F_\nu(\pi) \geq \dim \mathrm{F}_\nu(\pi\rho) - 1 = 4$ für ein $\nu \in K \backslash F$ gelten, ein Widerspruch zu (3), (4). Wäre $\pi\rho$ vom Typ (N), so würde $\dim \mathrm{rad}\ \mathrm{B}(\pi) \geq \dim \mathrm{radB}(\pi\rho) - 1 = \dim \mathrm{B}(\pi\rho) - 2 = 3$ gelten, ein Widerspruch zu (2).
Ist $\pi\rho$ vom Typ (A), so folgt mit (2), daß $1 \geq \dim \mathrm{rad}\ \mathrm{B}(\pi) \geq \dim \mathrm{radB}(\pi\rho) - 1 = \dim \mathrm{B}(\pi\rho) - 4 = 1$ gilt. Ferner gilt $\dim \mathrm{F}_{\bar{\mu}}(\pi) \leq \dim \mathrm{F}_{\bar{\mu}}(\pi\rho) + 1 \leq 2$.
Ist $\pi\rho$ vom Typ (B) so muß $\pi\rho$ nach (1) vom Typ (B2) sein. Es gibt dann ein $\nu \in K \backslash F$, so daß $\mathrm{F}_\nu(\pi)$ regulär und dreidimensional ist. Nimmt man an, daß $\nu = \bar{\mu}$ ist, so gilt $2 = \dim \mathrm{F}_{\bar{\mu}}(\pi\rho) - 1 \leq \dim \mathrm{F}_{\bar{\mu}}(\pi) < 3 = \dim \mathrm{F}_{\bar{\mu}}(\pi\rho)$ (,sonst wäre $\mathrm{F}_{\bar{\mu}}(\pi) = \mathrm{F}_{\bar{\mu}}(\pi\rho)$ regulär im Widerspruch zu (4)). Aus (5) erhält man nun den Widerspruch, $1 = \dim \mathrm{rad}\ \mathrm{F}_{\bar{\mu}}(\pi) - 1 \leq \dim \mathrm{rad}\ \mathrm{F}_{\bar{\mu}}(\pi\rho) = 0$. Es folgt $\nu = \mu$ und somit $\dim \mathrm{F}_\mu(\pi) \geq \dim \mathrm{F}_\mu(\pi\rho) - 1 = 2$ und $\dim \mathrm{F}_{\bar{\mu}}(\pi) \leq \dim \mathrm{F}_\mu(\pi\rho) + 1 = 1$. Die letzten beiden Aussagen aus (b) folgen nun mit (3) und (4).
Ist $\pi\rho$ vom Typ (C), so gibt es ein $\nu \in K \backslash F$ mit $\dim \mathrm{rad}\ \mathrm{F}_\nu(\pi\rho) = 2$, also $\dim \mathrm{rad}\ \mathrm{F}_\nu(\pi) \geq 1$. Aus $\nu = \mu$, würde wegen (3') bereits $\dim \mathrm{F}_\mu(\pi) \geq 2 = \dim \mathrm{radF}_\mu(\pi\rho)$ folgen. Weil $\mathrm{F}_\mu(\pi\rho)$ totalisotrop ist, gilt $\mathrm{F}_\mu(\pi\rho) \neq \mathrm{F}_\mu(\pi)$. Dies impliziert $\dim \mathrm{F}_\mu(\pi) \geq 3$, ein Widerspruch zu (3). Demnach ist $\nu = \bar{\mu}$, i.e. $\dim F_{\bar{\mu}}(\pi\rho) = 2$.

Aus (1) und (2) ergibt sich $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \geq 5$ und aus (4) erhält man $W := \mathrm{B}(\pi)(\pi + \bar{\mu}) < \mathrm{B}(\pi)$. Nach 3.5.3 und 3.2.2 (a) gibt es eine Symmetrie ρ mit $\dim \mathrm{B}(\pi\rho) = 5$ und $\mathrm{B}(\rho) \nsubseteq W$. Dies impliziert $\dim \mathrm{F}_{\bar{\mu}}(\pi) = \dim \mathrm{F}_{\bar{\mu}}(\pi) - 1$.

Ist $\pi\rho$ lang, so ist nach (a),(b) und (c) genau eine der drei folgenden Aussagen wahr:

A: $\dim \mathrm{F}_{\bar\mu}(\pi) \le 2$ und $\dim \mathrm{rad}\ \mathrm{B}(\pi) = 1$;
B: $\dim \mathrm{F}_{\bar\mu}(\pi) = \dim \mathrm{rad}\ \mathrm{F}_{\bar\mu}(\pi) = 1$, $\dim \mathrm{F}_{\mu}(\pi) = 2$ und $\mathrm{rad}\ \mathrm{B}(\pi) = 0$;
C: $\dim \mathrm{F}_{\bar\mu}(\pi) = \dim \mathrm{F}_{\bar\mu}(\pi\rho) + 1 = 3$.

Die Behauptung folgt nun aus 3.5.21 (Fall A), 3.5.22 (Fall B) und 3.5.23 (Fall C).

Fall 2. $\pi\sigma$ ist vom Typ (D). Dann gilt

(1) $\dim \mathrm{B}(\pi) = 7$,

und es gibt ein $\mu \in K\backslash F$, so daß $\mathrm{F}_\mu(\pi\sigma)$ ein dreidimensionaler totalisotroper Unterraum ist. Dies impliziert

(2) $4 = \dim \mathrm{F}_\mu(\pi\sigma) + 1 \ge \dim F_\mu(\pi) \ge \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) \ge \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) - 1 = 2$;
(3) Ist $\dim \mathrm{F}_\mu(\pi) = 3 = \dim \mathrm{F}_\mu(\pi\sigma)$ so ist $\mathrm{F}_\mu(\pi) = \mathrm{F}_\mu(\pi\sigma)$ totalisotrop;
(4) $\dim \mathrm{F}_{\bar\mu}(\pi) \le \dim \mathrm{F}_{\bar\mu}(\pi\sigma) + 1 = 1$;
(5) $\dim \mathrm{rad}\ \mathrm{B}(\pi) \le \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) + 1 = 1$.

Sei $W := \mathrm{B}(\pi)(\pi+\mu) + \mathrm{F}_\mu(\pi)$. Dann gilt $\dim W = \dim \mathrm{B}(\pi) - \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) \le \dim \mathrm{B}(\pi) - 2$. Weil π nicht vom Typ (H) ist, gibt es nach 3.5.3 und 3.2.2 (a) eine Symmetrie ρ mit $\mathrm{B}(\rho) \not\subseteq W$ und

(6) $\dim \mathrm{B}(\pi\rho) = 6$.

Nach 3.3.6 (b) gilt

(7) $3 \ge \dim \mathrm{F}_\mu(\pi) - 1 = \dim \mathrm{F}_\mu(\pi\rho) \ge \dim \mathrm{rad}\mathrm{F}_\mu(\pi\rho) = \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) - 1 \ge 1$.

Wegen (6) ist $\pi\rho$ nicht vom Typ (B1),(B2),(C). Wegen (7) ist $\pi\rho$ nicht vom Typ (H),(N),(A2),(B3). Wäre $\pi\rho$ vom Typ (A1), so müßte $\dim \mathrm{rad}\ \mathrm{B}(\pi) \ge \dim \mathrm{rad}\ \mathrm{B}(\pi\rho) - 1 = \dim \mathrm{B}(\pi\rho) - 4 = 2$ gelten, ein Widerspruch zu (5).
Wäre $\pi\rho$ vom Typ (D), so würde $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) = \dim \mathrm{rad}\mathrm{F}_\mu(\pi\rho) + 1 = 4$ gelten. (Beachte: Wegen (7) kann $\mathrm{F}_{\bar\mu}(\pi\rho)$ nicht dreidimensional und totalisotrop sein.) Dies impliziert jedoch $\dim \mathrm{B}(\pi) \ge 2 \cdot \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) = 8$, ein Widerspruch zu (1).

Fall 3. $\pi\sigma$ ist vom Typ (H). Es gibt dann ein $\mu \in K\backslash F$, so daß $\pi\sigma$ auf $\mathrm{B}(\pi\sigma)$ eine μ-Homothetie induziert. Insbesondere gilt $1 = \det \pi\sigma = \mu^{m-1}$. Weil μ die Ordnung 3 hat, folgt $\dim \mathrm{F}_\mu(\pi) \ge \dim \mathrm{F}_\mu(\pi\sigma) - 1 = m - 2 \ge 2$, i.e. $\dim \mathrm{B}(\pi)(\pi+\mu) \le m-2$. Nach 3.5.3 (mit $W = \mathrm{B}(\pi)(\pi+\mu)$) und 3.2.2 (a) gibt es eine Symmetrie σ' mit $\mathrm{F}(\pi\sigma') > \mathrm{F}(\pi)$ und $\mathrm{B}(\sigma') \not\subseteq \mathrm{B}(\pi)(\pi+\mu)$. Nach 3.3.6 (b) gilt dann $\dim \mathrm{B}(\pi\sigma')/\dim \mathrm{F}_\mu(\pi\sigma') = \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) \ne 0$, da π nicht vom Typ (H) ist. Wegen $\dim \mathrm{F}_\mu(\pi\sigma') \ge \dim \mathrm{F}_\mu(\pi) - 1 \ge 1$, ist $\pi\sigma'$ nicht vom Typ (N),(A2).

3.1. $\pi\sigma'$ ist vom Typ (A1). Man berechnet $\dim \mathrm{F}_\mu(\pi) = \dim \mathrm{F}_\mu(\pi\sigma') + 1 = 2$, $m = \dim \mathrm{B}(\pi\sigma) + 1 = \dim \mathrm{F}_\mu(\pi\sigma) + 1 \le \dim \mathrm{F}_\mu(\pi) + 2 = 4$, $m = \dim \mathrm{B}(\pi\sigma') + 1 \ge 4$, i.e. $m = 4$. Seien $U := \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi)$ und ϕ die von π auf U induzierte Abbildung. Es ist $\dim U = 2$. Weil π

nicht vom Typ (B) ist, ist ϕ zerlegbar. Wegen $\mathrm{char}(\phi)(0) = \mu$, $\dim \mathrm{F}_{\bar{\mu}}(\pi) \leq \dim \mathrm{F}_{\bar{\mu}}(\pi\sigma') + 1 = 1$ und weil $(x+\bar{\mu})^2, (x+1)(x+\mu)$ die einzigen $^-$-symmetrischen Polynome in $\mathrm{F}_4[x]$ vom Grad 2 mit konstantem Glied μ sind (cf. 3.5.12 (b)), gilt $\mathrm{char}(\phi) = \mathrm{mip}(\phi) = (x+1)(x+\mu)$. Es folgt $V = A \bigoplus B \bigoplus C \bigoplus D$ für π-Moduln A, B, C, D mit $\dim A = 2$, $\mathrm{mip}(\pi_A) = x + \mu^2$, $\dim B = 1$, $B \leq \mathrm{F}_\mu(\pi)$, $\dim C = 2$, $\mathrm{mip}(\pi_C) = (x+1)^2$ und $D \leq \mathrm{F}(\pi)$. Demnach ist $\rho := \pi_C \bigoplus 1_{C^\perp}$ eine Symmetrie mit den gewünschten Eigenschaften.

3.2. $\pi\sigma'$ ist vom Typ (B). Dann gilt $\dim \mathrm{B}(\pi\sigma')/\mathrm{F}_\nu(\pi\sigma') = 2$ für ein $\nu \in K\backslash F$ und $\dim \mathrm{B}(\pi\sigma') \geq 4$. Weil dann $\dim F_\mu(\pi) \geq m - 2 \geq 3$ ist, folgt $\dim \mathrm{F}_\mu(\pi\sigma') \geq \dim \mathrm{F}_\mu(\pi) - 1 \geq 2$. Dies liefert $\nu = \mu$, also $\dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) = \dim \mathrm{B}(\pi\sigma')/\mathrm{F}_\mu(\pi\sigma') = 2$. Wegen $1 = \det \pi\sigma = \mu^{\dim \mathrm{B}(\pi\sigma)} = \mu^{\dim \mathrm{B}(\pi\sigma')}$, muß $\dim \mathrm{B}(\pi\sigma') \equiv 0 \pmod 3$ sein. Dies bedeutet, daß $\pi\sigma'$ vom Typ (B3) ist. Sei ϕ die von π auf $\mathrm{B}(\pi)/\mathrm{F}_\mu(\pi)$ induzierte Abbildung. Weil π nicht vom Typ (B) ist, ist ϕ zerlegbar. Wegen $\mathrm{char}(\phi)(0) = \det \phi = \bar{\mu}^{\dim \mathrm{F}_\mu(\pi)} = \bar{\mu}^{\dim \mathrm{F}_\mu(\pi\sigma')+1} = \bar{\mu}^2 = \mu$. Wie im Fall 3.1 (findet man nun) eine Symmetrie mit den gewünschten Eigenschaften.

Fall 4. $\pi\sigma$ ist vom Typ (N). Dann gilt $\dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) = 1$. Weil π nicht vom Typ (N) ist, folgert man $1 < \dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \leq \dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) + 2 = 3$, i.e. $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \in \{2, 3\}$. Für alle $\mu \in K\backslash F$ gilt weiterhin $\dim \mathrm{F}_\mu(\pi) \leq \dim \mathrm{F}_\mu(\pi\sigma) + 1 = 1$. Nun liefern 3.5.24 für den Fall $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 2$ und 3.5.25 für den Fall $\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 3$ das gewünschte Ergebnis.

Fall 5. $\pi\sigma$ ist vom Typ (B). Dann gilt $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = 2$ für ein $\mu \in K\backslash F$, $\dim \mathrm{F}_\mu(\pi) \geq \dim \mathrm{F}_\mu(\pi\sigma) - 1 \geq 1$, $\dim \mathrm{B}(\pi) = \dim \mathrm{B}(\pi\sigma) + 1 \geq 5$, $r := \dim \mathrm{B}(\pi)/\mathrm{F}_\mu(\pi) \leq \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) + 2 = 4$. Ferner gilt $\dim \mathrm{B}(\pi)/\mathrm{rad}\mathrm{B}(\pi) = \dim \mathrm{B}(\pi) - \dim \mathrm{rad}\mathrm{B}(\pi) \geq \dim \mathrm{B}(\pi\sigma) + 1 - (\dim \mathrm{rad}\mathrm{B}(\pi\sigma) + 1) = \dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\mathrm{B}(\pi\sigma) \geq 4$. Die Behauptung folgt nun aus 3.5.26 , falls $r = 1$ oder [$r \in \{3, 4\}$ und $\dim \mathrm{F}_\mu(\pi) \geq 3$] oder [$r = 4$ und $\dim \mathrm{F}_\mu(\pi) = 2$ und $\mathrm{rad}\mathrm{B}(\pi) = 0$] gilt, und aus 3.5.27 für $r = 2$. Ist $r = 3$ und $\dim \mathrm{F}_\mu(\pi) \leq 2$, so folgt $\dim \mathrm{B}(\pi) = 5$ und $\dim \mathrm{F}_\mu(\pi) = 2$. Deshalb muß $\pi\sigma$ vom Typ (B1) sein. Dies wiederum impliziert $\dim \mathrm{rad}\ \mathrm{B}(\pi) \leq \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) + 1 = 1$ und $\dim \mathrm{rad}\mathrm{F}_\mu(\pi) \leq \dim \mathrm{rad} F_\mu(\pi\sigma) + 1 = 1$, so daß die Behauptung aus 3.5.28 folgt. Ist $r = 4$ und $\dim \mathrm{F}_\mu(\pi) = 1$, so folgt $\dim \mathrm{B}(\pi) = 5$ und $\pi\sigma$ ist vom Typ (B1), so daß $\dim \mathrm{rad}\ \mathrm{B}(\pi) \leq 1$ und $\dim \mathrm{F}_{\bar{\mu}}(\pi) \leq \dim \mathrm{F}_{\bar{\mu}}(\pi\sigma) + 1 = 2$ gilt. Somit sind die Voraussetzungen von 3.5.29 erfüllt. Ist $r = 4$ und $\dim \mathrm{F}_\mu(\pi) = 2$ und $\dim \mathrm{rad}\ \mathrm{B}(\pi) \neq 0$, so folgt $\dim \mathrm{B}(\pi) = 6$ und $\pi\sigma$ ist vom Typ (B2). Dies liefert $1 \leq \dim \mathrm{rad}\ \mathrm{B}(\pi) \leq \dim \mathrm{rad}\ \mathrm{B}(\pi\sigma) + 1 = 2$ und $\dim \mathrm{rad}\ \mathrm{F}_\mu(\pi) \leq \dim \mathrm{rad}\ \mathrm{F}_\mu(\pi\sigma) + 1 = 1$. Demnach läßt sich 3.5.30 anwenden. In jedem der beiden Fälle findet man eine Symmetrie η, so daß $F(\pi\eta) > \mathrm{F}(\pi)$ und $\pi\eta$ nicht vom Typ (B),(A) ist. Mit dem Standardschluß folgt hieraus die Behauptung.

Fall 6. $\pi\sigma$ ist vom Typ (A). Insbesondere ist dann $\dim \mathrm{B}(\pi) = \dim \mathrm{B}(\pi\sigma) + 1 \geq 4$ und $\dim \mathrm{F}_\mu(\pi) \leq \mathrm{F}_\mu(\pi\sigma) + 1 \leq 2$ für alle $\mu \in K\backslash F$. Weil π keine Involution und nicht vom Typ (N) ist, erhält man

$$2 \leq \dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \leq \dim \mathrm{B}(\pi\sigma)/\mathrm{rad}\ \mathrm{B}(\pi\sigma) + 2 = 5.$$

Ist $\mathrm{B}(\pi)$ nicht regulär, so folgt die Behauptung aus 3.5.31 ($\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) \neq 3$) und 3.5.32

$(\dim \mathrm{B}(\pi)/\mathrm{rad}\ \mathrm{B}(\pi) = 3)$. Ist $\mathrm{B}(\pi)$ regulär, so kann man o.B.d.A. $V = \mathrm{B}(\pi)$ und $\mathrm{F}(\pi) = \{0\}$ annehmen. Die Behauptung folgt nun aus 3.5.33 ($\dim \mathrm{B}(\pi) = 4$) und 3.5.34 ($\dim \mathrm{B}(\pi) = 5$). ■

$|F| = 2$**; Beweis des Satzes**

Seien $\pi \in \mathrm{SU}(f)\backslash\{1_V\}$ und $m := \dim \mathrm{B}(\pi)$. Nach 3.3.1 und 3.5.17 kann $\mathrm{l}(\pi)$ nicht kleiner als behauptet sein. Der Beweis von 3.5.8 erfolgt durch Induktion über $\dim \mathrm{B}(\pi)$.

(i) Als erstes betrachten wir den Fall, daß π kurz ist. Ist $m = 1$, so ist π eine Symmetrie und damit $\mathrm{l}(\pi) = 1 = m$. Ist $m > 1$, so gibt es nach 3.4.32 eine Symmetrie σ derart, daß $\dim \mathrm{B}(\pi\sigma) = m - 1$ und $\pi\sigma$ kurz ist. Nach Induktionsannahme gilt $\mathrm{l}(\pi\sigma) = m - 1$, also ist $\mathrm{l}(\pi) = m$.

(ii) Sei nun π eine lange Abbildung.

1. Ist π vom Typ (H), so gilt $\pi_{\mathrm{B}(\pi)} = \mu 1_{\mathrm{B}(\pi)}$ für ein $\mu \in K^*\backslash\{1\}$ mit $\mu\bar{\mu} = 1$. Wähle eine beliebige Symmetrie σ mit $\mathrm{B}(\sigma) \le B(\pi)$. Dann gilt $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) = m$ und $\dim \mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{F}_\mu(\pi) - 1$, also $\dim \mathrm{B}(\pi\sigma)/\mathrm{F}_\mu(\pi\sigma) = \dim \mathrm{B}(\pi\sigma) - 1$. Weil keine lange Abbildung diese Eigenschaft hat, ist $\pi\sigma$ kurz und somit $\mathrm{l}(\pi\sigma) = m$ nach (i). Dies ergibt $\mathrm{l}(\pi) = m + 1$.

2. Sei π vom Typ (N). Die Behauptung ist für $\dim V = 3$ bereits, mit 3.5.17 gezeigt, so daß man $\dim V > 3$ annehmen kann. Dann gibt es eine Zerlegung $V = U \oplus W$ in π-Moduln U, W mit $\dim U = 3$, $\mathrm{mip}(\pi_U) = (x+1)^3$, $W \neq \{0\}$ und π_W ist eine Involution. Nach (i) ist π_W ein Produkt von $\dim \mathrm{B}(\pi_W)$ Symmetrien. Man kann daher o.B.d.A. $\pi_W = 1_W$ und $\dim W = 1$ annehmen. Weil $\mathrm{B}(\pi_U)$ nicht totalisotrop ist, gibt es ein anisotropes $u \in \mathrm{B}(\pi_U)$. Sei $w \in W\backslash\{0\}$. Dann ist $a := u + w \notin \mathrm{B}(\pi)$ isotrop. Sei $\sigma := \sigma_a$ die Symmetrie mit Bahn $\langle a\rangle$. Dann gilt

$$(*)\quad \dim \mathrm{F}(\pi\sigma) = \dim \mathrm{F}(\pi) - 1 = 1.$$

Damit ist

$$\mathrm{F}(\pi\sigma) = \mathrm{F}(\pi) \cap a^\perp = \langle u(\pi+1), w\rangle \cap (u+w)^\perp = \langle u(\pi+1)\rangle = \mathrm{F}(\pi_U)$$

totalisotrop. Folglich ist $(x+1)^2$ ein Teiler von $\mathrm{mip}(\pi\sigma)$. Mit 3.5.12 (e) folgt $\mathrm{char}(\pi\sigma) \in \{(x+1)^4, (x+1)^2(x+\mu)(x+\bar{\mu})\}$, $\mu \in K\backslash F$. Wegen $(*)$ folgt hieraus $\mathrm{mip}(\pi\sigma) = \mathrm{char}(\pi\sigma)$. Damit ist $\pi\sigma$ kurz. Aus (i) folgt nun $\mathrm{l}(\pi\sigma) = \dim \mathrm{B}(\pi\sigma) = 3$, also $\mathrm{l}(\pi) = 4 = \dim \mathrm{B}(\pi) + 2$.

3. Sei π vom Typ (B). Indem man 3.5.13 wiederholt anwendet kann man o.B.d.A. annehmen, daß π vom Typ (B1) und $\dim V = \dim \mathrm{B}(\pi) = 4$ ist. Sei $\mu \in K\backslash F$ derart, daß $V = \mathrm{F}_\mu(\pi) \oplus \ker(\pi+\bar{\mu})^2$ gilt. Nach 3.5.18 gibt es eine Symmetrie σ mit $\mathrm{B}(\sigma) \le W := \ker(\pi+\bar{\mu})^2$, so daß $\mathrm{mip}((\pi\sigma)_W) = (x+1)(x+\mu)$ ist. Hieraus folgt $\dim \mathrm{F}_\mu(\pi\sigma) = 3$ und $\pi\sigma$ ist vom Typ (H). Nach 1. ist $\mathrm{l}(\pi\sigma) = 4$ und damit $\mathrm{l}(\pi) = 5 = \dim \mathrm{B}(\pi) + 1$.

4. Sei π vom Typ (A1). Der Fall $\dim V = 3$ ist bereits in 3.5.17 abgehandelt, so daß man $\dim V > 3$ annehmen kann. Es gibt dann eine Zerlegung $V = U \oplus W$ in π-Moduln U, $W \neq \{0\}$, so daß $\dim U = 3$, $\mathrm{mip}(\pi_U) = (x+\mu)^3$ für ein $\mu \in K\backslash F$ gilt und π_W eine Involution ist. Nach (i) ist π_W ein Produkt von $\dim \mathrm{B}(\pi_W)$ Symmetrien. Man kann daher $\pi_W = 1_W$ und $\dim W = 1$ annehmen. Weil U von anisotropen Vektoren erzeugt wird,

findet man ein anisotropes $a \in U \backslash U(\pi + \mu)$. Für $b \in W \backslash \{0\}$ ist dann $c := a + b$ isotrop. Sei $\sigma := \sigma_c$ die Symmetrie mit $\mathrm{B}(\sigma) = \langle c \rangle \nsubseteq U \cup U(\pi + \mu) + W = \mathrm{B}(\pi) \cup \mathrm{B}(\bar{\mu}\pi)$. Demnach ist $\dim \mathrm{F}(\pi\sigma) = \dim \mathrm{F}(\pi) - 1 = 0 = \dim \mathrm{F}_\mu(\pi) - 1 = \dim \mathrm{F}_\mu(\pi\sigma)$. Ferner ist $\dim \mathrm{F}_{\bar{\mu}}(\pi\sigma) \leq \dim \mathrm{F}_{\bar{\mu}}(\pi) + 1 = 1$. Wegen $\dim \mathrm{B}(\pi\sigma) = 4$ ist $\pi\sigma$ kurz. Nach (i) ist $\pi\sigma$ ein Produkt von 4 Symmetrien, so daß $\mathrm{l}(\pi) = 5 = \dim \mathrm{B}(\pi) + 2$ folgt.

5. Sei π vom Typ (A2). Weil dann $V = U \bigoplus W$ für π-Moduln U, W mit $\dim U = 5$, $\mathrm{mip}(\pi_U) = (x+1)^5$, $\pi_W^2 = 1_W$ gilt, kann man o.B.d.A. annehmen, daß $W = \{0\}$ ist. Weil V von isotropen Vektoren erzeugt wird, findet man einen isotropen Vektor $a \in V \backslash \mathrm{B}(\pi)$. Sei $\sigma := \sigma_a$ die Symmetrie mit $\mathrm{B}(\sigma) = \langle a \rangle \nsubseteq \mathrm{B}(\pi)$. Dann gilt $\dim \mathrm{B}(\pi\sigma) = \dim \mathrm{B}(\pi) + 1 = 5 = \dim V$, $\dim \mathrm{F}(\pi\sigma) = 0$ und $\dim \mathrm{F}_\mu(\pi\sigma) \leq \dim \mathrm{F}_\mu(\pi) + 1$ für alle $\mu \in K \backslash F$. Damit ist $\pi\sigma$ kurz. Aus (i) folgt $\mathrm{l}(\pi\sigma) = 5$, also $\mathrm{l}(\pi) = 6 = \dim \mathrm{B}(\pi) + 2$.

6. Sei π vom Typ (C). Nach 3.5.15 gibt es eine Symmetrie σ, so daß $\dim \mathrm{B}(\pi\sigma) = 4$ und $\pi\sigma$ vom Typ (B1) ist. Nach 3. ist dann $\mathrm{l}(\pi\sigma) = 5$, also $\mathrm{l}(\pi) = 6$.

7. Sei π schließlich vom Typ (D). Nach 3.5.3 und 3.2.2 (a) gibt es eine Symmetrie σ mit $\dim \mathrm{B}(\pi\sigma) = m - 1 = 5$. Nach 3.5.16 ist $\pi\sigma$ vom Typ (C) und damit nach 6. ein Produkt von 6 Symmetrien. Dies impliziert $\mathrm{l}(\pi) = 7$. ■

3.6 Offene Fragen

(1) Sei f anisotrop und $\mathrm{char}(K) \neq 2$. Man beweise oder widerlege durch ein Gegenbeispiel, daß $\mathrm{U}^\pm(f)$ von Symmetrien erzeugt wird. Gleichwertig zu diesem Problem ist die Frage, ob es zu je zwei Vektoren a, b mit $f(a, a) = f(b, b)$ ein Produkt π von Symmetrien gibt, so daß $a\pi = b$ ist.

(2) Mit (1) steht das folgende Verkürzungsproblem in engem Zusammenhang:

Sei V eine Ebene. Gibt es eine natürliche Zahl k, so daß sich ein Produkt von mehr als k beliebigen Symmetrien stets als ein Produkt von $\leq k$ Symmetrien schreiben läßt? Wie sieht das kleinste solche $k = k_{min}$ aus?

(3) Für beliebige Körper K klassifiziere man diejenigen Isometrien in $\mathrm{U}(f)$, für die $\mathrm{B}(\pi)$ keine d-hyperbolische Ebene enthält (cf.3.2.3). Mit anderen Worten: Für welche $\pi \in \mathrm{U}(f)$ folgt aus $v \in V \backslash \mathrm{F}(\pi^2)$ stets $f(v, v\pi) \notin F$. Hierauf aufbauend versuche man einen allgemeinen Induktionssatz zu beweisen, der in etwa folgende Form hat:

Sei $\pi \in \mathrm{U}^\pm(f)$ derart, daß π auf $\mathrm{B}(\pi)$ keine Homothetie induziert und $\mathrm{B}(\pi)$ eine d_π-hyperbolische Ebene enthält. Dann gibt es eine Symmetrie σ mit $\dim \mathrm{F}(\pi\sigma) = \dim \mathrm{F}(\pi) + 1$, so daß $\pi\sigma$ eine Involution ist oder [$\pi\sigma$ auf $\mathrm{B}(\pi\sigma)$ keine Homothetie induziert und $\mathrm{B}(\pi\sigma)$ wiederum eine $d_{\pi\sigma}$-hyperbolische Ebene enthält].

(4) Man überlege sich ein Beispiel eines nichtendlichen Körpers F mit Charakteristik $\neq 2$, für den $F[x]$ ein normiertes, irreduzibles Polynom $p = x^2 + \alpha x + \beta$ vom Grad 2 enthält, $\alpha, \beta \in F$, so daß in dem Zerfällungskörper $K = F(\xi, \zeta)$, $p = (x + \xi)(x + \zeta)$, der involutorische Körperautomorphismus $^-$, der ξ und ζ vertauscht und F festläßt, eine surjektive Normabbildung $\mathcal{N} : K \to F, k \mapsto k\bar{k}$ induziert.

ad (2). Wir haben gesehen, daß bei surjektiver Norm $k_{min} = 4$ für $\mathrm{char}(K) \neq 2$ und $k_{min} = 2$ für $\mathrm{char}(K) = 2$ auftrat. Im Abschnitt 4.4 des nächsten Kapitels werden wir sehen, daß auch $k_{min} = 5$ möglich ist (cf.4.4.14). (Für allgemeinere Fragestellungen zu Relationen zwischen einfachen unitären Isometrien sei auf die Arbeiten von M.Götzky [34], [35] §5, [36] hingewiesen.)

ad (3). Ist π eine Abbildung mit den in (3) angegebenen Eigenschaften, so sieht man leicht, daß es keinen π-invarianten Unterraum W mit $W(\pi - 1) \nsubseteq \mathrm{F}_{-1}(\pi)$ und $W(\pi - 1) \perp W(\pi + 1)$ geben kann.[Sonst wähle $w \in W$, so daß $a := w(\pi - 1) \in W(\pi - 1)$ nicht in $\mathrm{F}_{-1}(\pi)$ liegt. Dann gilt $a \notin d\text{-rad } \mathrm{B}(\pi) = \mathrm{F}_{-1}(\pi)$ und $d(a, a) = if(w(\pi + 1), w(\pi - 1)) = 0$. Folglich muß a in einer d-hyperbolischen Ebene von $\mathrm{B}(\pi)$ enthalten sein.]
Hieraus folgern wir sofort, daß $\mathrm{mip}(\pi)$ nur Teiler der Form $(x \pm 1)^i$, $i \leq 2$ und $p \neq x \pm 1$, p irreduzibel und $^-$-symmetrisch, haben kann.

Kapitel 4

Produkte von Involutionen in unitären Gruppen

Wir betrachten die Menge I der Involutionen aus $\mathrm{U}(f)$ als Erzeugendensystem und interessieren uns für folgende Probleme:

- (Involutionen-Längenproblem) Bestimme zu vorgegebenem

  $$\pi \in \langle I \rangle = \{\iota_1 \cdots \iota_m | \iota_i \in I, m \in \mathbb{N}\}$$

  die kleinste Zahl $\mathrm{l}_I(\pi) := \inf\{m \in \mathbb{N} | \pi = \iota_1 \cdots \iota_m, \iota_i \in I, m \in \mathbb{N}\}$ von Faktoren aus I in einem Produkt, daß π darstellt!

- (obere Schranken) Finde eine (kleinste) obere Schranke t so, daß jedes $\pi \in \langle I \rangle$ ein Produkt von t Elementen aus I ist!

Die von den unitären Involutionen erzeugte Gruppe $\langle I \rangle$ ist in $\mathrm{U}^{\pm}(f)$, der Untergruppe der unitären Transformationen mit Determinante ± 1, enthalten. Ist der Witt-Index von $f \ \geq 1$, i.e. gibt es isotrope Vektoren, so stimmen beide Gruppen außer im Fall $(\dim V, |F|) \in \{(2,3),(3,2)\}$ überein. Für anisotropes f ist dies merkwürdigerweise ungeklärt. [J. Dieudonné nahm die Gleichheit in [17] S.66 an. Er berichtigte sich in einer Fußnote in [18].]
Es stellt sich heraus, daß obige Fragestellungen stark Körper-abhängig sind, so daß eine einheitliche Betrachtung nicht möglich ist.
In den Abschnitten 4.3 und 4.4 gehen wir näher auf Körper mit surjektiver Normabbildung $\mathcal{N} : K \to F, \alpha \mapsto \alpha\bar{\alpha}$ und $|F| > 3$ bzw. algebraisch abgeschlossene Körper ein. In beiden Fällen wird $\mathrm{U}^{\pm}(f)$ von Involutionen erzeugt, und wir beweisen jeweils die 5-Spiegeligkeit von $\mathrm{U}^{\pm}(f)$ (cf. 4.3.1, 4.4.16).
Eine Vorgehensweise in den Beweisen besteht darin, das Problem durch geschicktes 'Heranmultiplizieren' von Involutionen auf die Situation zu reduzieren, daß V ein hyperbolischer Raum ist.
Involutionen-Längen in hyperbolischen Räumen werden im Abschnitt 4.1 in größerer Allgemeinheit behandelt. Dort wird gezeigt, daß es für $|F| > 3$ stets eine $\mathrm{SU}(f)$-Konjugiertenklasse Ω in $\mathrm{SU}(f)$

gibt mit

$$(\mathrm{SU}(f)\backslash \mathrm{Z}(\mathrm{SU}(f))) \cup \{1_V\} \subseteq \Omega^2.$$

Dabei läßt sich Ω als Konjugiertenklasse eines Produktes von zwei unitären Involutionen wählen (cf. 4.1.19, 4.1.23). Dies beweist auch die Vermutungen von O. Ore und J.G. Thompson für die endlichen einfachen projektiven speziellen unitären Gruppen $\mathrm{PSU}_{2m}(\mathrm{F}_{q^2})$, $m \in \mathbb{N}$, q eine Primzahlpotenz > 3. Die Vermutung von Ore besagt, daß jedes Element einer endlichen einfachen nichtabelschen Gruppe ein Kommutator ist. Die schärfere Vermutung von Thompson besagt, daß es unter gleichen Voraussetzungen bereits eine Konjugiertenklasse Ω von G gibt, so daß $G = \Omega^2$ gilt.
Wir geben eine möglicherweise lückenhafte Übersicht über die endlichen einfachen nichtabelschen Gruppen, für die diese Vermutungen verifiziert wurden.

Gruppe G	Ore-Vermutung	Thompson-Vermutung
A_n, $n \geq 5$	O. Ore [58], Ito [44]	Cheng-Hao Xu [80]
$\mathrm{PSL}_n(\mathrm{F}_q)$, $(n,q) \neq (2,2),(2,3)$	R.C. Thompson [70],[71],[72]	J.L. Brenner $n \in \{2,3\}$; $q > n+1$ und q ungerade; $q > n$ und q gerade; A. Lev [51], $q \geq 4$
$\mathrm{PSp}(n,q)$		R. Gow [39] q ungerade und 4 teilt $q-1$
${}^2B_2(q^2)$		Z. Arad, M. Herzog [1] et al.
Einfache Gruppen vom Typ ${}^3D_4(q^3)$, $F_4(q)$, ${}^2F_4(q^2)$ (inklusive der Tits-Gruppe), $G_2(q)$, ${}^2G_2(q^2)$	O. Bonten [6]	
$\|G\| < 10^6$, M11, M12, M22, M23, M24, J1, J2, J3, HS, Suz, McL, Ru, HE, On, C3		S. Karni [46]
sporadische Gruppen		Cleuvers, Neubüser, Pahlings [16]
Klassen von Chevalley Gruppen		E.W. Ellers, N. Gordeev [32], [33]

[Für Abkürzungen verweisen wir auf [37] part 1, ch. 1, p. 8,9, (Tafeln 1 und 2).]

Wie in der Einleitung zu Kapitel 2 angegeben sind orthogonale Gruppen und symplektische Gruppen über Körpern mit Charakteristik 2 zwei-spiegelig. Der Beweis vereinfacht sich entscheidend dadurch, daß man sich auf orthogonal unzerlegbare Isometrien zurückziehen kann. Diese Reduktion ist in unitären Gruppen natürlich nicht möglich, da kurz formuliert $\pi = \phi \bigoplus \psi \in \mathrm{U}^{\pm}(f)$ aber $\det \phi \neq \pm 1 \neq \det \psi$ möglich ist. Trotzdem hielten wir es für interessant, einige Involutionen-Längen orthogonal unzerlegbarer unitärer Isometrien festzuhalten. Dies geschieht in Abschnitt 4.2.

Abschließend gehen wir im Abschnitt 4.5 auf das Erzeugendensystem sogenannter Quasi-Involutionen ein. Eine unitäre Transformation π heißt Quasi-Involution, falls es eine orthogonale Zerlegung $V = V_1 \bigoplus \ldots \bigoplus V_n$ von V in $1-$dimensionale π-Moduln V_i gibt. Dies bedeutet, daß π ein Produkt von kommutierenden Quasi-Symmetrien ist. Dabei ist eine Quasi-Symmetrie eine unitäre Transformation mit eindimensionaler regulärer Bahn. Jede Quasi-Symmetrie ist von der Gestalt

$$V \to V, v \mapsto v + (\alpha - 1)\frac{f(v,a)}{f(a,a)}a,$$

$\alpha \in K^*\backslash\{1\}$, $\alpha\bar{\alpha} = 1$, $a \in V$ anisotrop.

Quasi-Involution wurden erstmals von E.W. Ellers in [28] als unitäres Analogon von Involutionen in orthogonalen Gruppen betrachtet, welche Produkte von paarweise kommutierenden Symmetrien sind.

Er beweist in [28] für anisotrope hermitesche Formen, daß jede unitäre Transformation ein Produkt von zwei Quasi-Involutionen ist.

Ein Ergebnis von Dieudonné besagt, daß jedes $\pi \in \mathrm{U}(f)$ ein Produkt von Quasi-Symmetrien also insbesondere ein Produkt von Quasi-Involutionen ist mit der einzigen Ausnahme $K = \mathrm{F}_4$ und $\dim V = 2$ (cf. [20]).

Im Kontext dieser Arbeit scheint es sinnvoll nur solche Situationen zu betrachten, in denen nicht-triviale Involutionen existieren und diese spezielle Quasi-Involutionen sind. Weil dies genau dann der Fall ist, wenn $\mathrm{char}(K) \neq 2$ ist, setzen wir dies im Abschnitt 4.5 voraus. Insbesondere ist dann jede unitäre Transformation ein Produkt von Quasi-Involutionen.

Unser Hauptergebnis besagt, daß jede unitäre Transformation ein Produkt von vier Quasi-Involutionen ist. Genauer ist jede unitäre Transformation ein Produkt von zwei unitären Involutionen und zwei Quasi-Involutionen. Falls K algebraisch abgeschlossen ist, reichen eine unitäre Involution und zwei Quasi-Involutionen aus (cf. 4.5.11, 4.5.13).

4.1 Blockzerlegung unitärer Matrizen

Notation 4.1.1 *Für eine Matrix $A \in K^{l \times m}$, $l, m \in \mathbb{N}$, und $(j,k) \in \mathbb{N}_{\leq l} \times \mathbb{N}_{\leq m}$ bezeichne $A_{(j)}$ die j-te Zeile, $A^{(k)}$ die k-te Spalte von A und $A_{j,k}$ den (j,k)-Eintrag von A. Weiterhin sei* $\mathrm{rank} A := \dim\langle A_{(j)}; j \in \mathbb{N}_{\leq l}\rangle = \dim\langle A^{(k)}; k \in \mathbb{N}_{\leq m}\rangle$ *der Rang von A.*

Wir notieren nun zwei sehr technisch wirkende Lemmata, welche mit elementaren Methoden der Linearen Algebra bewiesen werden und deren Bedeutung erst das anschließende Korollar 4.1.5 klärt.

Lemma 4.1.2 *Seien $m \in \mathbb{N}$, $A, B \in K^{m\times m}$ derart, daß $C := (A|B) \in K^{m\times 2m}$ den Rang m hat. Dann gibt es ein $X \in K^{m\times m}$ mit $\bar{X}^t = -X$, so daß $A + BX \in K^{m\times m}$ regulär ist.*

Beweis. Der Beweis erfolgt mittels Induktion über $r := \mathrm{rank}A$.
Induktionsanfang: $r = m$. Wähle $X := 0$.

Induktionsschritt: Sei $r < m$. Wähle eine Indexmenge $I \subseteq \mathbb{N}_{\leq m}$ mit $|I| = r$ derart, daß die Spaltenvektoren $A^{(i)}$, $i \in I$, linear unabhängig sind. Wegen rank $C = m > r$ gibt es nach dem Basis-
ergänzungssatz für Vektorräume (cf. [52] Part One, Chapter III, §5, Theorem 5.1) eine Indexmenge $J \subseteq \mathbb{N}_{\leq m}$ mit $|J| = m - |I| = m - r > 0$ derart, daß die Spaltenvektoren $A^{(i)}, B^{(j)}, i \in I, j \in J$, linear unabhängig sind. Falls $\{B^{(l)}; l \in \mathbb{N}_{\leq m}\backslash I\} \not\subseteq \langle A^{(i)}; i \in I\rangle$ gilt, kann J so gewählt werden , daß

$$J \not\subseteq I \tag{4.1.1}$$

gilt.

Fall A: $J \not\subseteq I$. Wähle $j \in J\backslash I$ und $\iota \in K^*$ mit $\bar{\iota} = -\iota$.(Im Fall char$(K) = 2$ gilt dann $\iota \in F^*$.) Sei $Y \in K^{m\times m}$ definiert durch

$$Y_{k,l} = \begin{cases} \iota & \text{, falls } (k, l) = (j, j) \text{ ist,} \\ 0 & \text{sonst.} \end{cases}$$

Dann gilt $\bar{Y}^t = -Y$. Wegen $j \notin I$ gilt $A^{(j)} \in \langle A^{(i)}; i \in I\rangle$ und somit

$$\langle A^{(i)}; i \in I\rangle \cap \langle A^{(j)} + \iota B^{(j)}\rangle = \{0\}.$$

Es folgt

$$\mathrm{rank}A + BY \geq \dim(\langle A^{(i)}; i \in I\rangle \oplus \langle A^{(j)} + \iota B^{(j)}\rangle) = r + 1.$$

Wegen

$$D := \begin{bmatrix} I_m & 0 \\ Y & I_m \end{bmatrix} \in \mathrm{GL}_{2m}(K)$$

gilt $m = \mathrm{rank}(A|B)D = \mathrm{rank}(A + BY|B)$, so daß nach Induktionsannahme ein $Z \in K^{m\times m}$ existiert mit $\bar{Z}^t = -Z$ und $A + B(Y + Z) \in \mathrm{GL}_m(K)$. Setze nun $X := Y + Z$. Dann gilt $\bar{X}^t = \bar{Y}^t + \bar{Z}^t = -Y - Z = -X$.

Fall B: $J \subseteq I$. Wähle $s \in \mathbb{N}_{\leq m}\backslash I$ und $j \in J \subseteq I$. Wegen $|K| > 2$ gibt es zwei verschiedene Elemente $\nu, \mu \in K^*$. Es gilt dann

$$A^{(j)} - \bar{\mu}B^{(s)} \notin \langle A^{(i)}; i \in I\backslash\{j\}\rangle \tag{4.1.2}$$

oder

$$A^{(j)} - \bar{\nu}B^{(s)} \notin \langle A^{(i)}; i \in I\backslash\{j\}\rangle,$$

da sonst $A^{(j)} = (\bar\nu - \bar\mu)^{-1}(\bar\nu(A^{(j)} - \bar\mu B^{(s)}) - \bar\mu(A^{(j)} - \bar\nu B^{(s)})) \in \langle A^{(i)}; i \in I\backslash\{j\}\rangle$ folgen würde, ein Widerspruch. O.B.d.A. gelte daher (4.1.2). Sei $Y \in K^{m\times m}$ definiert durch

$$Y_{k,l} = \begin{cases} \mu & \text{, falls } (k,l) = (j,s) \text{ ist,} \\ -\bar\mu & \text{, falls } (k,l) = (s,j) \text{ ist,} \\ 0 & \text{sonst.} \end{cases}$$

Dann gilt $\bar{Y}^t = -Y$. Weil nach Wahl von J (c.f. (4.1.1)) $B^{(s)} \in \langle A^{(i)}; i \in I\backslash\rangle$ gilt, erhält man

$$\operatorname{rank} A + BY \geq \dim(\langle A^{(i)}; i \in I\backslash\{j\}\rangle \oplus \langle A^{(j)} - \bar\mu B^{(s)}\rangle \oplus \langle A^{(s)} + \mu B^{(j)}\rangle) = r + 1.$$

Wie im Fall A findet man nun eine Matrix $X \in K^{m\times m}$ mit den gewünschten Eigenschaften. ∎

Lemma 4.1.3 *Seien $K = \mathrm{F}_4$, $\lambda \in K^*$, $m \in \mathbb{N}_{\geq 2}$ und $B \in K^{m\times m}$ derart, daß $B_{i,i} = \lambda$ für ein $i \in \mathbb{N}_{\leq m}$ gilt. Dann gibt es ein $T \in \mathrm{GL}_m(K)$ und ein $X \in K^{m\times m}$ mit $\bar{X}^t = X$, so daß $\lambda I_m + TB\bar{T}^t X$ regulär und keine Homothetie ist.*

Beweis. Wegen $m \geq 2$ gibt es ein $j \in \mathbb{N}_{\leq m}\backslash\{i\}$. Setze $\alpha := B_{i,j}$, $\beta := B_{j,i}$ und $\gamma := B_{j,j}$. Es sei g die $^-$-Sesquilinearform auf dem Vektorraum K^2 mit Gramscher Matrix

$$G := \begin{bmatrix} \lambda & \alpha \\ \beta & \gamma \end{bmatrix}$$

bezüglich der Standardbasis des K^2.

Fall A: g ist regulär. Dann besitzt g mindestens zwei verschiedene Formwerte, i.e. $|\{g(v,v); v \in K^2\}| \geq 2$. Folglich gibt es eine Basis (v,w) des K^2 mit $g(v,v) \neq \lambda$. Es gilt dann $H := \mathcal{M}_{(v,w)}(g) = SG\bar{S}^t$ für ein $S \in \mathrm{GL}_2(K)$. Sei nun $T \in K^{m\times m}$ definiert durch

$$T_{k,l} := \begin{cases} S_{1,1} & \text{, falls } (k,l) = (i,i) \text{ ist,} \\ S_{1,2} & \text{falls } (k,l) = (i,j) \text{ ist,} \\ S_{2,1} & \text{falls } (k,l) = (j,i) \text{ ist,} \\ S_{2,2} & \text{falls } (k,l) = (j,j) \text{ ist,} \\ 1 & \text{falls } k = l \neq i,j \text{ ist,} \\ 0 & \text{sonst.} \end{cases} \tag{4.1.3}$$

Dann gilt $\det T = \det S \neq 0$, also $T \in \mathrm{GL}_m(K)$ und

$$(TB\bar{T}^t)_{i,i} = H_{1,1} = g(v,v) \neq \lambda,\ (TB\bar{T}^t)_{j,i} = H_{2,1} = g(w,v).$$

Wegen $\det H \neq 0$ gilt $(TB\bar{T}^t)_{i,i} = H_{1,1} \neq 0$ oder $(TB\bar{T}^t)_{j,i} = H_{2,1} \neq 0$. Sei $X \in K^{m\times m}$ mit $X_{i,i} = 1$ und $X_{l,k} = 0$ für alle $(l,k) \in \mathbb{N}_{\leq m} \times \mathbb{N}_{\leq m}\backslash\{(i,i)\}$. Dann gilt $\bar{X}^t = X$, und $\lambda I_m + TB\bar{T}^t X$ ist regulär und keine Homothetie.

Fall B: g ist singulär. Sei $e := (1,0) \in K^2$. Wegen $|K^*| > 1$ gibt es ein
$b \in l\text{-rad } g\backslash\{0\}$ mit $g(e,b) \neq \lambda$. Setze und $c := e + b$. Dann gilt $\omega := g(e,c) = \lambda + g(e,b) \neq 0$ und

$$H := \mathcal{M}_{(e,c)}(g) = \begin{bmatrix} \lambda & \omega \\ \lambda & \omega \end{bmatrix}.$$

Sei $S \in GL_2(K)$ mit $SG\bar{S}^t = H$. Definiere $T \in \mathrm{GL}_m(K)$ wie in (4.1.3). Sei $X \in K^{m\times m}$ mit $X_{i,i} = 1 = X_{j,j}$ und $X_{l,k} = 0$ für alle $(l,k) \in \mathbb{N}_{\le m} \times \mathbb{N}_{\le m} \backslash \{(i,i),(j,j)\}$. Dann gilt $\bar{X}^t = X$ und $\lambda I_m + TB\bar{T}^t X$ ist regulär und keine Homothetie. ∎

Für den Rest dieses Abschnittes setzen wir voraus, daß V ein hyperbolischer Raum ist. Insbesondere hat V dann eine gerade Dimension $n = 2m$, $m \in \mathbb{N}$.

Bemerkung 4.1.4 *Seien $\pi \in \mathrm{GL}(V)$, $A, B, C, D \in K^{m\times m}$ und $\mathcal{B}$ eine Basis von V so, daß*

$$\mathcal{M}_{\mathcal{B}}(\pi) = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \text{ und } \mathcal{M}_{\mathcal{B}}(f) = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix} \tag{4.1.4}$$

gilt. Es ist π genau dann eine unitäre Transformation, wenn folgende Bedingungen erfüllt sind:

(i) $B\overline{A}^t = -A\overline{B}^t$;

(ii) $D\overline{C}^t = -C\overline{D}^t$;

(iii) $B\overline{C}^t + A\overline{D}^t = E$;

(iv) $D\overline{A}^t + C\overline{B}^t = E$.

Insbesondere definieren folgende 'elementaren' Matrizen unitäre Transformationen:

(EL1) $\begin{bmatrix} T & 0 \\ 0 & \overline{T^{-1}}^t \end{bmatrix}$, $T \in \mathrm{GL}_m(K)$;

(EL2) $\begin{bmatrix} I_m & 0 \\ X & I_m \end{bmatrix}$, $\begin{bmatrix} I_m & X \\ 0 & I_m \end{bmatrix}$, $X \in K^{m\times m}$, $\bar{X}^t = -X$;

(EL3) $\begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$.

Es sei angemerkt, daß $\mathrm{U}(f)$ von den Elementarmatrizen vom Typ (EL1), (EL2), (EL3) erzeugt wird (cf. [64] ch.7, §7, Th. 7.5).

Lemma 4.1.5 *Sei $\pi \in \mathrm{U}(f)$. Dann gibt es eine Basis $\mathcal{B}$ von V so, daß (4.1.4) aus 4.1.4 für ein A in $\mathrm{GL}_m(K)$ erfüllt ist. Falls π keine Homothetie und $m \ge 2$ ist, kann $\mathcal{B}$ so gewählt werden, daß A keine Homothetie ist.*

Beweis. Seien $\mathcal{A}$ eine Basis von V und $E, G, H, J \in K^{m\times m}$ so, daß

$$\mathcal{M}_{\mathcal{A}}(f) = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix} \text{ und } \mathcal{M}_{\mathcal{A}}(\pi) = \begin{bmatrix} E & G \\ H & J \end{bmatrix}$$

gilt. Wegen $\pi \in \mathrm{GL}(V)$ ist dann $\mathrm{rank}(E|G) = m$. Nach 4.1.2 gibt es ein $X \in K^{m\times m}$ mit $\bar{X}^t = -X$, so daß $A := E + GX$ regulär ist. Sei $\phi \in \mathrm{U}(f)$ definiert durch

$$\mathcal{M}_{\mathcal{A}}(\phi) = \begin{bmatrix} I_m & 0 \\ X & I_m \end{bmatrix}.$$

(cf.4.1.4 (EL2)). Für die unitäre Transformation $\pi^\phi = \phi^{-1}\pi\phi$ erhält man

$$\mathcal{M}_{\mathcal{A}}(\pi^\phi) = \begin{bmatrix} I_m & 0 \\ -X & I_m \end{bmatrix} \begin{bmatrix} E & G \\ H & J \end{bmatrix} \begin{bmatrix} I_m & 0 \\ X & I_m \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

für geeignete $B, C, D \in K^{m\times m}$. Also erfüllt $\mathcal{B} := \mathcal{A}\phi^{-1}$ das Gewünschte. Dies beweist den ersten Teil der Behauptung. Seien nun π keine Homothetie und $m > 1$. Falls A keine Homothetie ist, folgt die Behauptung. Sei daher angenommen, daß A eine λ-Homothetie für ein $\lambda \in K^*$ ist. Falls $B = C = 0$ gilt, ist $D \neq A$, weil π keine Homothetie ist. Wähle ein $\iota \in K^*$ mit $\bar{\iota} = -\iota$. Sei $\psi \in \mathrm{U}(f)$ definiert durch

$$\mathcal{M}_{\mathcal{A}}(\psi) = \begin{bmatrix} I_m & 0 \\ \iota I_m & I_m \end{bmatrix}.$$

(cf. 4.1.4 (EL2)). Für die unitäre Transformation π^ψ erhält man

$$\mathcal{M}_{\mathcal{A}}(\pi^\psi) = \begin{bmatrix} I_m & 0 \\ -\iota I_m & I_m \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} I_m & 0 \\ \iota I_m & I_m \end{bmatrix} = \begin{bmatrix} A & 0 \\ \iota(D-A) & D \end{bmatrix}.$$

Wegen $D - A \neq 0$ kann man daher o.B.d.A. $B \neq 0$ oder $C \neq 0$ annehmen. Falls $B = 0$ ist, ist D eine $\bar{\lambda}^{-1}$-Homothetie. Sei $\rho \in \mathrm{U}(f)(V)$ definiert durch

$$\mathcal{M}_{\mathcal{A}}(\rho) = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$$

(cf.4.1.4 (EL3)). Es gilt dann

$$\mathcal{M}_{\mathcal{A}}(\pi^\rho) = \begin{bmatrix} D & C \\ B & A \end{bmatrix}.$$

Man kann daher weiterhin o.B.d.A. $B \neq 0$ annehmen. Falls $\lambda + \mu\iota B_{i,i} = 0$ für alle $\mu \in F^*$ und alle $i \in \mathbb{N}_{\leq m}$ mit $B^{(i)} \neq 0$ gilt, folgt $F = F_2$ $(K = F_4)$ und $[B_{i,i} = \lambda$ oder $B^{(i)} = 0]$ für alle $i \in \mathbb{N}_{\leq m}$. In diesem Fall gibt es nach 4.1.3 ein $T \in \mathrm{GL}_m(K)$ und ein $X \in K^{m\times m}$ mit $\bar{X}^t = X$, so daß $A + TB\bar{T}^tX$ regulär und keine Homothetie ist. Sei $\eta \in \mathrm{GL}(V)$ definiert durch

$$\mathcal{M}_{\mathcal{A}}(\eta) = \begin{bmatrix} T^{-1} & 0 \\ \overline{T}^t X & \overline{T}^t \end{bmatrix}.$$

Dann gilt $\eta \in \mathrm{U}(f)$ (cf.4.1.4 (EL1), (EL2)) und

$$\mathcal{M}_{\mathcal{A}}(\pi^\eta) = \begin{bmatrix} A + TB\bar{T}^tX & * \\ * & * \end{bmatrix}.$$

Man kann daher annehmen, daß es ein $\mu \in F^*$ und ein $i \in \mathbb{N}_{\leq m}$ mit $B^{(i)} \neq 0$ ist, so daß $\lambda + \mu\iota B_{i,i} \neq 0$ gilt. Sei $X \in K^{m\times m}$ mit $X_{i,i} = \mu\iota$ und $X_{l,k} = 0$ für alle $(l,k) \in \mathbb{N}_{\leq m} \times \mathbb{N}_{\leq m} \backslash \{(i,i)\}$. Dann gilt $\bar{X}^t = -X$. Sei $\kappa \in \mathrm{U}(f)$ definiert durch

$$\mathcal{M}_{\mathcal{A}}(\kappa) = \begin{bmatrix} I_m & 0 \\ X & I_m \end{bmatrix}.$$

Weiterhin ist

$$\mathcal{M}_{\mathcal{A}}(\pi^\kappa) = \begin{bmatrix} A + BX & * \\ * & * \end{bmatrix},$$

wobei $A + BX$ regulär und keine Homothetie ist. ■

Satz 4.1.6 (Blockzerlegungssatz) *Seien* $\pi \in \mathrm{U}(f)$ *und* $\mathcal{B}$ *eine Basis von* V *so, daß (4.1.4) für ein* $A \in \mathrm{GL}_m(K)$ *und* $B, C, D \in K^{m\times m}$ *erfüllt ist. Seien* $G, H \in \mathrm{GL}_m(K)$ *mit* $GH = A$. *Dann sind die durch*

$$\mathcal{M}_{\mathcal{B}}(\phi) = \begin{bmatrix} G & 0 \\ CH^{-1} & \overline{G^{-1}}^t \end{bmatrix} \text{ und } \mathcal{M}_{\mathcal{B}}(\psi) = \begin{bmatrix} H & G^{-1}B \\ 0 & \overline{H^{-1}}^t \end{bmatrix} \tag{4.1.5}$$

definierten Abbildungen $\phi, \psi \in \mathrm{GL}(V)$ *unitäre Transformationen, deren Produkt* π *ist.*

Beweis. Aus Bedingung (i) von 4.1.4 folgt $A^{-1}B = -\overline{B}^t\overline{A^{-1}}^t$. Aus Bedingung (iv) von 4.1.4 folgt $D = \overline{A^{-1}}^t - C\overline{B}^t\overline{A^{-1}}^t$. Hieraus ergibt sich $D = \overline{A^{-1}}^t + CA^{-1}B$. Dies liefert $\pi = \phi\psi$. Mit (ii) und (iii) aus 4.1.4 folgt weiterhin

$$\overline{CA^{-1}}^t + CA^{-1} = (D - CA^{-1}B)\bar{C}^t + CA^{-1} = D\bar{C}^t - CA^{-1}(E - A\overline{D}^t) + CA^{-1} = 0.$$

Dies impliziert $\phi \in \mathrm{U}(f)$ und somit auch $\psi = \phi^{-1}\pi \in \mathrm{U}(f)$. ∎

Korollar 4.1.7 *Seien* π *und* A *wie in 4.1.6. Dann gilt* $\det A = \det\pi\overline{\det A}$. *Insbesondere gilt* $\det A \in F^*$, *falls* $\pi \in \mathrm{SU}(f)$.

Beweis. Wähle in 4.1.6 $G = A$ und $H = I_m$. Es folgt $\det\pi = \det\phi\det\psi = \det A\det\overline{A^{-1}}^t = \det A\overline{\det A}^{-1}$. ∎

Das Lemma 4.1.5 führt auf natürliche Weise zu der Frage, für welche Matrizen $A \in K^{m\times m}$ es eine Basis $\mathcal{B}$ von V gibt, so daß (4.1.4) für geeignete $B, C, D \in K^{m\times m}$ gilt. Bezeichnet man die Menge dieser Matrizen mit $\mathrm{M}(\pi)$, so ist offensichtlich $\mathrm{M}(\pi) = \mathrm{M}(\phi)$, falls π und ϕ zu derselben unitären Konjugiertenklasse Ω gehören, so daß $\mathrm{M}(\Omega) := \mathrm{M}(\pi)$ wohldefiniert ist. Man sieht leicht, daß mit A auch jede zu A ähnliche Matrix $B^{-1}AB$, $B \in \mathrm{GL}_m(K)$, in $\mathrm{M}(\Omega)$ enthalten ist. Die Bestimmung von $\mathrm{M}(\Omega)$ ist ein ungelöstes Problem (vgl. [57]). Lemma 4.1.5 besagt, daß $\mathrm{M}(\Omega)$ stets Konjugiertenklassen von $\mathrm{GL}_m(K)$ enthält und sogar eine nichtzentrale, falls Ω nichtzentral ist. Korollar 4.1.7 liefert die notwendige Bedingung $\det A = \det\Omega\overline{\det A}$ an $A \in \mathrm{GL}_m(K)$, um ein Element von $\mathrm{M}(\Omega)$ zu sein. Das folgende Lemma zeigt, daß diese Bedingung für den Trivialfall $m = 1$ auch hinreichend ist. Anschließend beweisen wir, daß im Fall $m \geq 2$ für jedes $\pi \in \mathrm{U}(f)$, das keine Homothetie ist, und jedes $a \in K^*$ mit $a = \overline{a}\det\pi$ ein $A \in GL_m(K)$ existiert, das ebenfalls keine Homothetie ist und $\det A = a$ erfüllt.

Lemma 4.1.8 (Wahl des linken oberen Blockes I) *Seien* $\dim V = 2$, $\pi \in \mathrm{U}(f)$ *keine Homothetie und* $\nu \in K$ *mit* $\nu = \bar{\nu}\det\pi$. *Dann gibt es eine Basis* $\mathcal{B}$ *von* V *mit*

$$\mathcal{M}_{\mathcal{B}}(\pi) = \begin{bmatrix} \nu & * \\ * & * \end{bmatrix} \text{ und } \mathcal{M}_{\mathcal{B}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Beweis. Wähle gemäß 4.1.5 eine Basis $\mathcal{B}$ von V, so daß

$$\mathcal{M}_{\mathcal{B}}(\pi) = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \text{ und } \mathcal{M}_{\mathcal{B}}(f) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

für ein $\alpha \in K^*$ und $\beta, \gamma, \delta \in K$ gilt. Nach 4.1.7 ist dann $\alpha = \bar{\alpha} \det \pi$. Aus Bedingung (i) von 4.1.4 folgt $\bar{\beta} = -\beta \det \pi^{-1}$. Falls $\beta \neq 0$ ist, setze $\mu := \frac{\nu - \alpha}{\beta}$. Dann gilt $\bar{\mu} = -\mu$, so daß die durch

$$\mathcal{M}_{\mathcal{B}}(\phi) = \begin{bmatrix} 1 & 0 \\ \mu & 1 \end{bmatrix}$$

definierte lineare Abbildung ϕ zu $\mathrm{U}(f)$ gehört (cf.4.1.4 (EL2)). Wie man leicht nachrechnet gilt

$$\mathcal{M}_{\mathcal{B}}(\pi^{\phi}) = \begin{bmatrix} \nu & * \\ * & * \end{bmatrix}.$$

Der Fall $\beta = 0$ und $\gamma \neq 0$ wird analog behandelt. Falls $\beta = 0 = \gamma$ ist, ist $\alpha \neq \delta$, weil π keine Homothetie ist. Wähle $\iota \in K^*$ mit $\bar{\iota} = -\iota$. Dann gehört die durch

$$\mathcal{M}_{\mathcal{B}}(\psi) = \begin{bmatrix} 1 & \iota \\ 0 & 1 \end{bmatrix}$$

definierte lineare Abbildung ψ zu $\mathrm{U}(f)$ und es gilt

$$\mathcal{M}_{\mathcal{B}}(\pi^{\psi}) = \begin{bmatrix} \alpha & \iota(\alpha - \gamma) \\ 0 & \gamma \end{bmatrix}.$$

Dabei ist $\iota(\alpha - \gamma) \neq 0$, so daß die Behauptung auch in diesem Fall aus dem zuerst betrachteten folgt. ∎

Hilfssatz 4.1.9 *Seien $m \geq 2$, $A \in \mathrm{GL}_m(K)$ und $B \in K^{m \times m} \backslash \{0\}$. Dann gibt es ein $T \in \mathrm{GL}_m(K)$, so daß*

$$(T^{-1} B \overline{T^{-1}}^t)^{(1)} \notin \langle (T^{-1} A T)^{(j)}; j \in \mathbb{N}_{\leq m} \backslash \{1\} \rangle \tag{4.1.6}$$

gilt.

Beweis. Wegen $\bar{A}^t \in \mathrm{GL}_m(K)$ und $B \neq 0$ ist $G := B\bar{A}^t \neq 0$. Wegen $^- \neq 1_K$ gibt es bekanntlich ein $v \in K^m \backslash \{0\}$ mit $vG\bar{v}^t \neq 0$. Sei $S \in \mathrm{GL}_m(K)$ mit $e_1 S^{-1} = v$. Es folgt :

$$\begin{aligned} & (S^{-1} B \overline{A}^t \overline{S^{-1}}^t)_{1,1} = vG\bar{v}^t \neq 0 \\ \Leftrightarrow \quad & B \overline{(A^{-1}S)^{-1}}^t e_1^t \notin \langle S e_j^t; j \in \mathbb{N}_{\leq m} \backslash \{1\} \rangle \\ \Leftrightarrow \quad & (A^{-1}S)^{-1} B \overline{(A^{-1}S)^{-1}}^t e_1^t \notin \langle (A^{-1}S)^{-1} A (A^{-1}S) e_j^t; j \in \mathbb{N}_{\leq m} \backslash \{1\} \rangle. \end{aligned}$$

Also ist (4.1.6) für $T := A^{-1}S$ erfüllt. ∎

Hilfssatz 4.1.10 *Seien $|F| \geq 3$, $m \geq 2$, $a, \lambda \in K^*$ mit $\lambda^m = a$ und $B \in K^{m \times m} \backslash \{0\}$ mit $\bar{B}^t = -\bar{\lambda}\lambda^{-1} B$. Dann gibt es ein $T \in \mathrm{GL}_m(K)$ und ein $X \in K^{m \times m}$ mit $\bar{X}^t = -X$, so daß $A' := \lambda I_m + T^{-1} B \overline{T^{-1}}^t X$ keine Homothetie ist und $\det A' = a$ gilt.*

Beweis. Seien $\gamma := -\bar{\lambda}\lambda^{-1}$ und $A := \lambda I_m$. Die $^-$-Sesquilinearform

$$g : K^m \times K^m \to K, v \mapsto vB\bar{v}^t$$

erfüllt nach Voraussetzung $\overline{g(v, w)} = \gamma g(w, v)$ für alle $v, w \in K^m$.

Fall A: g ist regulär. Wegen $m \geq 2$ enthält K^m eine g-reguläre Ebene U. Weil U von g-anisotropen Vektoren erzeugt wird, findet man zwei linear unabhängige, g-anisotrope Vektoren $u, v \in U$. Wegen $|F| > 2$ gilt $|\{g(\nu v, \nu v); \nu \in K^*\}| > 1$. Folglich kann man v so wählen, daß $g(u,u) \neq -g(v,v)$ ist. Falls $g(u,v) = 0$ ist, setze $v' := u + v$. Dann gilt $g(u, v') = g(u,u) + g(v,v) \neq 0$. Für ein $\nu \in K^*$ gilt wiederum $g(u,u) \neq -g(\nu v', \nu v')$, so daß man $c := g(u,v) \neq 0$ annehmen kann. Setze $b := g(u,u)$, $d := g(v,v)$,

$$G := \mathcal{M}_{(u,v)}(g_U) = \begin{bmatrix} b & c \\ \overline{\gamma c} & d \end{bmatrix}.$$

Wegen $K^m = U \bigoplus{}_g U^{\perp_g}$ gibt es ein $T \in \mathrm{GL}_m(K)$, so daß $T^{-1} B \overline{T^{-1}}^t = \mathrm{diag}(G, H)$ für ein geeignetes $H \in K^{m-2 \times m-2}$ gilt. Setze $g := \det G$ und $\nu := -(b+d)\lambda g^{-1}$. Es gilt $\bar{g} = \det \bar{G}^t = \gamma^2 \det G = \gamma^2 g$, $\nu \neq 0$ wegen $b \neq -d$ und $\bar{\nu} = -\gamma(b+d)\bar{\lambda}\gamma^{-2} g^{-1} = -\nu$. Folglich erfüllt $X := \mathrm{diag}(\nu I_2, 0, \ldots, 0) \in K^{m \times m}$ die Gleichung $\bar{X}^t = -X$. Weiterhin gilt

$$\det(A + T^{-1} B \overline{T^{-1}}^t X) = a + \nu(b+d)\lambda^{n-1} + \nu^2 g \lambda^{n-2} = a + \nu((b+d)\lambda + \nu g)\lambda^{n-2} = a.$$

Wegen $(A + T^{-1} B \overline{T^{-1}}^t X)_{1,2} = \nu c \neq 0$ ist $(A + T^{-1} B \overline{T^{-1}}^t X)$ keine Homothetie.

Fall B: g ist nicht regulär. Sei $u \in g\text{-rad } K^m$. Wegen $g \neq 0$ gibt es einen anisotropen Vektor $v \in K^m$. Setze $w := u + v$, $Y := \langle v, w \rangle$, $b := g(v,v)$ und

$$G := \mathcal{M}_{(v,w)}(g_Y) = \begin{bmatrix} b & b \\ b & b \end{bmatrix}.$$

Sei Z ein Komplement von $\langle u \rangle$ in $\langle v \rangle^{\perp_g}$. Dann gilt $K^m = Y \bigoplus{}_g Z$. Folglich gibt es ein $T \in \mathrm{GL}_m(K)$, so daß $T^{-1} B \overline{T^{-1}}^t = \mathrm{diag}(G, H)$ für ein geeignetes $H \in K^{m-2 \times m-2}$ gilt. Sei $\nu \in K^*$ mit $\bar{\nu} = -\nu$ und $X := \mathrm{diag}(\nu, -\nu, 0, \ldots, 0) \in K^{m \times m}$. Dann gilt $\bar{X}^t = -X$ und

$$\det(A + T^{-1} B \overline{T^{-1}}^t X) = a + \nu b \lambda^{n-1} - \nu b \lambda^{n-1} - \nu^2 \det G \lambda^{n-2} = a.$$

Wegen $(A + T^{-1} B \overline{T^{-1}}^t X)_{1,2} = -\nu b \neq 0$ ist $(A + T^{-1} B \overline{T^{-1}}^t X)$ keine Homothetie. ∎

Hilfssatz 4.1.11 *Seien $m \geq 2$ und $A \in \mathrm{GL}_m(K)$ keine Homothetie. Es gibt dann ein $X \in K^{m \times m}$ mit $\bar{X}^t = -X$ und $AX - X\overline{A^{-1}}^t \neq 0$.*

Beweis. Sei $\iota \in K^*$ mit $\bar{\iota} = -\iota$. Falls $A \neq \overline{A^{-1}}^t$ gilt, hat $X := \iota I_m$ die gewünschten Eigenschaften. Man kann daher $A = \overline{A^{-1}}^t$ annehmen. Falls es $i, j \in N_{\leq m}$ mit $i \neq j$ und $A_{i,j} \neq 0$ gibt, sei $X \in K^{m \times m}$ definiert durch $X_{j,j} := \iota$ und $X_{r,s} := 0$ für alle $(r,s) \in \mathbb{N}_{\leq m} \times \mathbb{N}_{\leq m} \backslash \{(j,j)\}$. Dann gilt $\bar{X}^t = -X$, $(AX - X\overline{A^{-1}}^t)_{i,j} = \iota A_{i,j} \neq 0$. Folglich kann man weiterhin annehmen, daß A eine Diagonalmatrix ist. Weil A keine Homothetie ist, gibt es verschiedene $i, j \in \mathbb{N}_{\leq m}$, für die $A_{i,i} \neq A_{j,j}$ gilt. Sei $X \in K^{m \times m}$ definiert durch $X_{i,j} := 1$, $X_{j,i} := -1$ und $X_{r,s} := 0$ für alle $(r,s) \in \mathbb{N}_{\leq m} \times \mathbb{N}_{\leq m} \backslash \{(i,j), (j,i)\}$. Dann gilt $\bar{X}^t = -X$ und $(AX - X\overline{A^{-1}}^t)_{i,j} = (AX - XA)_{i,j} = A_{i,i} - A_{j,j} \neq 0$. ∎

Satz 4.1.12 (Wahl des linken oberen Blockes II) *Seien $m \geq 2$, $\pi \in \mathrm{U}(f)$ keine Homothetie und $e \in K^*$ mit $e = \bar{e} \det \pi$. Es gibt dann ein $E \in \mathrm{M}(\pi)$, das keine Homothetie ist und $\det E = e$ erfüllt.*

Beweis. Nach 4.1.5 gibt es ein $A \in \mathrm{GL}_m(K)$, welches keine Homothetie ist, so daß (4.1.4) für eine Basis $\mathcal{B}$ und geeignete $B, C, D \in K^m$ gilt. Ist $a := \det A = e$, so folgt die Behauptung. Man kann daher $a \neq e$ annehmen. Weil nach 4.1.7 auch $a = \bar{a} \det \pi$ gilt, folgt dann insbesondere $|F| > 2$. Falls $B = C = 0$ ist, wähle gemäß 4.1.11 ein $X \in K^{m \times m}$, so daß $\bar{X}^t = -X$ und $AX - X\overline{A^{-1}}^t$ gilt. Die durch

$$\mathcal{M}_{\mathcal{B}}(\psi) = \begin{bmatrix} I_m & X \\ 0 & I_m \end{bmatrix}$$

definierte lineare Abbildung ψ ist dann eine unitäre Transformation (cf. 4.1.4 (EL2)). Konjugation mit ψ liefert

$$\mathcal{M}_{\mathcal{B}}(\pi^{\psi}) = \begin{bmatrix} I_m & -X \\ 0 & I_m \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & \overline{A^{-1}}^t \end{bmatrix} \begin{bmatrix} I_m & X \\ 0 & I_m \end{bmatrix} = \begin{bmatrix} A & AX - X\overline{A^{-1}}^t \\ 0 & \overline{A^{-1}}^t \end{bmatrix}.$$

Man kann daher o.B.d.A. $B \neq 0$ oder $C \neq 0$ annehmen. Falls $B = 0$ ist, ist $D = \overline{A^{-1}}^t \in \mathrm{GL}_m(K)$ keine Homothetie. Nach 4.1.4 (EL3) wird durch

$$\mathcal{M}_{\mathcal{B}}(\rho) = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}.$$

ein $\rho \in \mathrm{U}(f)$ definiert. Man berechnet

$$\mathcal{M}_{\mathcal{B}}(\pi^{\rho}) = \begin{bmatrix} D & C \\ B & A \end{bmatrix}.$$

Man kann daher weiterhin o.B.d.A. $B \neq 0$ annehmen. Wähle gemäß 4.1.9 ein $T \in \mathrm{GL}_m(K)$, so daß (4.1.6) erfüllt ist. Konjugiert man π mit der durch $\mathcal{M}_{\mathcal{B}}(\phi) := \mathrm{diag}(T, \overline{T^{-1}}^t)$ definierten unitären Transformation ϕ, so erhält man

$$\mathcal{M}_{\mathcal{B}}(\pi^{\phi}) = \begin{bmatrix} T^{-1}AT & T^{-1}B\overline{T^{-1}}^t \\ * & * \end{bmatrix},$$

so daß man o.B.d.A.

$$B^{(1)} \notin \langle A^{(j)}; j \in \mathbb{N}_{\leq m} \backslash \{1\} \rangle$$

annehmen kann. Folglich gilt $b := \det(B^{(1)}, A^{(2)}, \ldots, A^{(m)}) \neq 0$. Wegen $|F| > 2$ gibt es ein $\iota \in K^* \backslash \{-ab^{-1}\}$, das $\bar{\iota} = -\iota$ erfüllt. Sei $X \in K^{m \times m}$ definiert durch $X_{1,1} := \iota$ und $X_{r,s} := 0$ für alle $(r, s) \in \mathbb{N}_{\leq m} \times \mathbb{N}_{\leq m} \backslash \{(1, 1)\}$. Wegen $\bar{X}^t = -X$ wird durch

$$\mathcal{M}_{\mathcal{B}}(\eta) = \begin{bmatrix} I_m & 0 \\ X & I_m \end{bmatrix}$$

eine unitäre Transformation η definiert. Es folgt :

$$\mathcal{M}_{\mathcal{B}}(\pi^{\eta}) = \begin{bmatrix} A + BX & B \\ * & * \end{bmatrix}$$

und $\det(A + BX) = a + \iota b \neq 0$. Nach 4.1.7 gilt $a + \iota b = \overline{(a + \iota b)} \det \pi$ und somit $b = -\bar{b} \det \pi$. Wegen $e \neq a$ ist $\iota' := (e - a)b^{-1} \neq 0$ und es gilt $\overline{\iota'} = -\iota'$. Definiert man X' und η' wie X und η

mit ι' anstelle von ι, so ist η' eine unitäre Transformation, für die

$$\mathcal{M}_{\mathcal{B}}(\pi^{\eta'}) = \begin{bmatrix} A + BX' & B \\ * & * \end{bmatrix}$$

und $\det(A + BX') = a + \iota' b = e$ gilt. Dies liefert die Behauptung, falls $A + BX'$ keine Homothetie ist. Man kann daher o.B.d.A. annehmen, daß bereits A eine λ-Homothetie für ein $\lambda \in K^*$ mit $\lambda^m = e$ ist, und $B \neq 0$ gilt. Nach 4.1.10 gibt es dann ein $T \in \mathrm{GL}_m(K)$ und ein $X \in K^{m\times m}$ mit $\bar{X}^t = -X$ so, daß $A' := A + T^{-1}B\overline{T^{-1}}^t X$ keine Homothetie ist, und $\det A' = e$ gilt. Konjugiert man π mit der durch

$$\mathcal{M}_{\mathcal{B}}(\zeta) = \begin{bmatrix} T & \\ \overline{T^{-1}}^t X & \overline{T^{-1}}^t \end{bmatrix}$$

definierten unitären Transformation ζ (cf. 4.1.4 (EL1), (EL2)), so erhält man

$$\mathcal{M}_{\mathcal{B}}(\pi^{\zeta}) = \begin{bmatrix} A' & * \\ * & * \end{bmatrix}. \qquad \blacksquare$$

Korollar 4.1.13 (Wahl des linken oberen Blockes III) *Seien $\pi \in \mathrm{U}(f)$ keine Homothetie, $e \in K^*$ mit $e = \bar{e}\det\pi$, $\mathcal{B}$ eine Basis von V und $A, B, C, D \in K^{m\times m}$, so daß (4.1.4) aus 4.1.4 gilt. Es gibt dann ein $E \in \mathrm{GL}_m(K)$, das im Fall $m \geq 2$ keine Homothtetie ist und* $\det E = e$ *erfüllt, und ein $\psi \in \mathrm{SU}(f)$ so, daß*

$$\mathcal{M}_{\mathcal{B}}(\pi^{\psi}) = \begin{bmatrix} E & * \\ * & * \end{bmatrix} \tag{4.1.7}$$

gilt.

Beweis. Nach 4.1.8 und 4.1.12 gibt es ein $E \in \mathrm{GL}_m(K)$, das im Fall $m \geq 2$ keine Homothetie ist und $\det E = e$ erfüllt, und ein $\psi \in \mathrm{U}(f)$ so, daß (4.1.7) gilt. Wegen $\det\psi\overline{\det\psi} = 1$ gibt es ein $\mu \in K^*$ so, daß $\det\psi^{-1} = \mu\bar{\mu}^{-1}$ ist. Setze $T := \mathrm{diag}(\mu, I_{m-1}) \in \mathrm{GL}_m(K)$. Die durch $\mathcal{M}_{\mathcal{B}}(\phi) := \mathrm{diag}(T, \overline{T^{-1}}^t)$ definierte unitäre Abbildung ϕ (cf. 4.1.4 (EL1)) hat die Determinante $\det\psi^{-1}$, so daß $\eta := \psi\phi \in \mathrm{SU}(f)$ gilt. Weiterhin gilt

$$\mathcal{M}_{\mathcal{B}}(\pi^{\eta}) = \begin{bmatrix} T^{-1}ET & * \\ * & * \end{bmatrix},$$

$\det T^{-1}ET = \det E = e$ und $T^{-1}ET$ ist keine Homothetie, da E keine Homothetie ist. $\blacksquare$

Die Sätze 4.1.6 und 4.1.13 zeigen, daß jeder Matrix-Zerlegungssatz in $\mathrm{GL}_m(K)$ eine entsprechende unitäre Version nach sich zieht. Dies soll anhand eines Satzes von von A. Lev [51] konkret ausgeführt werden.

Satz 4.1.14 (Lev) *Seien K ein Körper, $m \in \mathbb{N}_{\geq 2}$ und $A, B, M \in \mathrm{GL}_m(K)$. Es sei M keine Homothetie und die Matrizen A, B seien zyklisch,* $\mathrm{mip}(A)$ *zerfalle in $K[x]$ in Linearfaktoren und es gelte* $\det M = \det A \det B$. *Weiterhin seien $\Omega_1 := A^{\mathrm{GL}_m(K)}$ und $\Omega_2 := B^{\mathrm{GL}_m(K)}$ die zu A bzw. B gehörigen Konjugiertenklassen in $\mathrm{GL}_m(K)$. Falls $m \geq 3$ und $|K| \geq 4$ ist, gilt $M \in \Omega_1\Omega_2$. Im Fall $m = 2$ gilt*

$$\{N \in \mathrm{GL}_2(K) | \det N = \det AB \textit{ und } N \textit{ ist keine Homothetie}\} \subseteq \Omega_1\Omega_2$$

genau dann, wenn A zwei verschiedene Eigenwerte hat oder $\mathrm{mip}(B)$ *in* $K[x]$ *in Linearfaktoren zerfällt.*

Eine Diskussion dieses Satzes wird im Anhang geführt. Dort wird eine für die späteren Anwendungen ausreichende einfacherere Version dieses Satzes bewiesen:

Satz 4.1.15 *Seien K ein Körper, $|K| \geq 3$, $m \in \mathbb{N}_{\geq 2}$, $A, B \in \mathrm{GL}_m(K)$ zyklisch und $M \in \mathrm{GL}_m(K)$ keine Homothetie mit* $\det M = \det A \det B$. *Weiterhin seien $\Omega_1 := A^{\mathrm{GL}_m(K)}$ und $\Omega_2 := B^{\mathrm{GL}_n(K)}$ die zu A bzw. B gehörigen Konjugiertenklassen in* $\mathrm{GL}_m(K)$.

(i) *Sei $m = 2$ und A besitze die Eigenwerte $\mu, \nu \in K^*$. Es gilt $M \in \Omega_1\Omega_2$ genau dann, wenn $\mu \neq \nu$ oder* $\mathrm{trace}(M) \neq \mu\mathrm{trace}(B)$ *oder wenn* $\mathrm{mip}(B)$ *in $K[x]$ in Linearfaktoren zerfällt.*

(ii) *Sei $m \geq 3$. Das charakteristische Polynom von A zerfalle in Linearfaktoren, und A besitze einen Eigenwert mit einfacher Vielfachheit. Dann gilt $M \in \Omega_1\Omega_2$.*

Satz 4.1.16 (unitäre Version des Satzes von Lev) *Seien $\pi \in \mathrm{U}(f)$ keine Homothetie und p_1, p_2 normierte Polynome so, daß $p_i(0) \neq 0$ und* $\det(\pi) = p_1(0)p_2(0)\overline{(p_1(0)p_2(0))}^{-1}$ *gilt. Das Polynom p_1 zerfalle in Linearfaktoren. Im Fall $m = 2$ besitze p_1 zwei verschiedene Nullstellen, oder p_2 zerfalle in Linearfaktoren. Es gibt dann unitäre Konjugiertenklassen Ω_i so, daß* $\mathrm{char}(\Omega_i) = p_i p_i^*$ *und* $\mathrm{lcm}(p_i, p_i^*)$ *ein Teiler von* $\mathrm{mip}(\Omega_i)$ *ist, $i = 1, 2$, und $\pi \in \Omega_1\Omega_2$ gilt. Ist p_i teilerfremd zu p_i^*, so ist Ω_i zyklisch und nach 1.3.8 eindeutig bestimmt.*

Beweis. Sei Γ_i die zyklische $\mathrm{GL}_m(K)$-Konjugiertenklasse mit $\mathrm{mip}(\Gamma_i) = p_i$, $i = 1, 2$. Für $\alpha := \det \Gamma_1 \det \Gamma_2 = p_1(0)p_2(0)$ gilt nach Voraussetzung $\alpha = \bar{\alpha} \det \pi$. Nach 4.1.13 gibt es eine Basis $\mathcal{B}$ von V, so daß 4.1.4 für ein $A \in \mathrm{GL}_m(K)$ mit $\det A = \alpha$ gilt, das im Fall $m \geq 2$ keine Homothetie ist. Nach dem Satz von A. Lev 4.1.14 (bzw. aus trivialen Gründen im Fall $m = 1$), Gibt es $G \in \Gamma_1$ und $H \in \Gamma_2$ derart, daß $A = GH$ ist. definiert man $\phi, \psi \in \mathrm{U}(f)$ gemäß Zeile (4.1.5) aus 4.1.6, so haben die zu ϕ und ψ gehörigen unitären Konjugiertenklassen Ω_1 und Ω_2 die gewünschten Eigenschaften. ∎

Analog beweist man mit 4.1.15 anstelle von 4.1.14 den

Satz 4.1.17 (unitäre Version des modifizierten Satzes von Lev) *Seien $\pi \in \mathrm{U}(f)$ keine Homothetie und p_1, p_2 normierte Polynome so, daß $p_i(0) \neq 0$ und* $\det(\pi) = p_1(0)p_2(0)\overline{(p_1(0)p_2(0))}^{-1}$ *gilt. Das Polynom p_1 zerfalle in Linearfaktoren. Im Fall $m = 2$ besitze p_1 zwei verschiedene Nullstellen, oder p_2 zerfalle in Linearfaktoren. Im Fall $m \geq 3$ besitze p_1 eine einfache Nullstelle. Es gibt dann unitäre Konjugiertenklassen Ω_i so, daß* $\mathrm{char}(\Omega_i) = p_i p_i^*$ *und* $\mathrm{lcm}(p_i, p_i^*)$ *ein Teiler von* $\mathrm{mip}(\Omega_i)$ *ist, $i = 1, 2$, und $\pi \in \Omega_1\Omega_2$ gilt. Ist p_i teilerfremd zu p_i^*, so ist Ω_i zyklisch und nach 1.3.8 eindeutig bestimmt.* ∎

Bemerkung 4.1.18 *Besitzt $\pi \in \mathrm{U}(f)$ einen Eigenwert $a \in K^*$ mit $a\bar{a} \neq 1$ und mit einfacher Vielfachheit, so gilt $\pi^{\mathrm{U}(f)} = \pi^{\mathrm{SU}(f)}$.*

Beweis. Sei $\psi \in \mathrm{U}(f)$. Setze $b := \det \psi$. Wegen $b\bar{b} = 1$ gibt es ein $c \in K^*$, so daß $b = c\bar{c}^{-1}$ ist. Weil $H := \ker(\pi - a) \oplus (\pi - \bar{a}^{-1})$ nach Voraussetzung eine f-hyperbolische Ebene mit eindimensionalen isotropen Unterräumen $\ker(\pi-a)$ und $\ker(\pi-\bar{a}^{-1})$ ist, ist $\zeta := (c^{-1}1_{\ker(\pi-a)} \oplus \bar{c}1_{\ker(\pi-\bar{a}^{-1})}) \bigoplus 1_{H^\perp}$ eine wohldefinierte unitäre Transformation, die mit π kommutiert. Wegen $\det \zeta\psi = 1$ folgt $\pi^\psi = \pi^{\zeta\psi} \in \pi^{\mathrm{SU}(f)}$. ∎

Satz 4.1.19 (Ore/Thompson - Vermutung) *Ist $|F| > 3$, so gibt es eine $\mathrm{SU}(f)$-Konjugiertenklasse Ω, deren Minimalpolynom keinen $^-$-symmetrischen Primteiler besitzt und die $(\mathrm{SU}(f) \backslash Z(\mathrm{SU}(f)) \cup \{1_V\} \subseteq \Omega^2$ erfüllt. Insbesondere besitzt dann $\mathrm{PSU}(f)$ in diesem Fall eine Konjugiertenklasse Δ so, daß $\mathrm{PSU}(f) = \Delta^2$ ist.*

Beweis. Wegen $|F| \geq 3$ gibt es ein $a \in K^* \backslash F$ mit $a\bar{a} \neq 1$. Wegen $|F| > 3$ gibt es ein $b \in F^* \backslash \{\pm 1\}$. Setze

$$p := \begin{cases} (x-b) & \text{, falls } m = 1 \text{ ist,} \\ (x-a)(x-\bar{a})(x-b)^{n-2} & \text{, falls } m \geq 2 \text{ ist.} \end{cases}$$

Es gilt $p(0) \in F$, also trivialerweise $p(0)^2\overline{(p)(0)}^{-2} = 1$ und $\gcd(p, p^*) = 1$. Nach 4.1.17 ist jedes $\pi \in \mathrm{SU}(f)$, welches keine Homothetie ist, in dem Quadrat der zyklischen $\mathrm{U}(f)$-Konjugiertenklasse Ω mit $\mathrm{mip}(\Omega) = pp^*$ und $\det \Omega = 1$ enthalten. Weil pp^* symmetrisch ist und keinen $^-$-symmetrischen Primteiler enthält, stimmt Ω nach 1.3.8 mit Ω^{-1} überein. Für $m = 1$ hat der Eigenwert b von Ω die Vielfachheit 1, andernfalls hat a diese Eigenschaft. Wegen $a\bar{a} \neq 1 \neq b^2 = b\bar{b}$, ist Ω nach 4.1.18 eine $\mathrm{SU}(f)$-Konjugiertenklasse. ∎

Bemerkung 4.1.20 *Setzt man den Satz von A. Lev als bewiesen voraus, so kann man mit Hilfe von 4.1.16 zeigen, daß es im Fall $|F| = 3$ und $\dim V \equiv 0 \pmod 4$ eine $\mathrm{U}(f)$-Konjugiertenklasse Ω gibt, deren Minimalpolynom keinen $^-$-symmetrischen Primteiler besitzt und die $(\mathrm{SU}(f) \backslash Z(\mathrm{SU}(f)) \cup \{1_V\} \subseteq \Omega^2$ erfüllt.*

Beweis: Wähle a wie im Beweis von 4.1.19 und setze $q := ((x-a)(x-\bar{a}))^{\frac{m}{2}}$. Der Beweis von 4.1.19 überträgt sich bis auf die letzten beiden Sätze. ∎

Wir gehen abschließend auf das Involutionenlängenproblem ein. Hierfür benötigen wir ein Lemma von Radjavi [59] (Theorem 3).

Lemma 4.1.21 (Radjavi) *Sei W ein n-dimensionaler K Vektorraum und g eine reguläre $^-$-hermitesche Form auf W. Sei $\pi \in \mathrm{U}^\pm(g)$. Es gebe eine Orthogonalbasis $(e_1, \ldots, e_n)$ bestehend aus Eigenvektoren e_i von π mit $\epsilon := g(e_1, e_1) = \cdots = g(e_n, e_n)$. Dann ist π ein Produkt von vier Involutionen aus $\mathrm{U}(g)$.*

Beweis. Sei $\alpha_i \in K$ ein Eigenwerte von π zu dem Eigenvektor e_i, $i \in \mathbb{N}_{\leq n}$. Für $i \in \mathbb{N}_{\leq n}$ seien

$$\beta_i := \begin{cases} \prod_{k=1}^{i-1} \bar{\alpha_k} & \text{, falls } i \text{ ungerade ist,} \\ \prod_{k=1}^{i} \alpha_k & \text{, falls } i \text{ gerade ist,} \end{cases} \quad , \ \gamma_i := \begin{cases} \prod_{k=1}^{i} \alpha_k & \text{, falls } i \text{ ungerade ist,} \\ \prod_{k=1}^{i-1} \bar{\alpha_k} & \text{, falls } i \text{ gerade ist.} \end{cases}$$

Dann ist $\alpha_i = \beta_i\gamma_i$ für alle $i \in \mathbb{N}_{\leq n}$, $\beta_{i+1} = \bar{\beta_i}$ für alle geraden $i \in \mathbb{N}_{<n}$ und $\gamma_{i+1} = \bar{\gamma_i}$ für alle ungeraden $i \in \mathbb{N}_{<n}$. Folglich ist π das Produkt der unitären Transformationen $\beta := \bigoplus_{i=1}^{n} \beta_i 1_{\langle e_i \rangle}$ and $\gamma := \bigoplus_{i=1}^{n} \gamma_i 1_{\langle e_i \rangle}$. Seien $I := \{i \in \mathbb{N}_{<n}; i \text{ ist gerade und } \beta_i \notin \{\pm 1\}\}$ und $J := \{i \in \mathbb{N}_{<n}; i$ ist

ungerade und $\gamma_i \notin \{\pm 1\}\}$. Wir haben

$$\begin{aligned} V &= \bigoplus{}_{i\in I}(\langle e_i\rangle \bigoplus \langle e_{i+1}\rangle) \bigoplus \mathrm{F}(\beta) \bigoplus \mathrm{F}_{-1}(\beta) \\ &= \bigoplus{}_{j\in J}(\langle e_j\rangle \bigoplus \langle e_{j+1}\rangle) \bigoplus \mathrm{F}(\gamma) \bigoplus \mathrm{F}_{-1}(\gamma), \\ \beta &= \bigoplus{}_{i\in I}(\beta_i 1_{\langle e_i\rangle} \bigoplus \bar{\beta}_i 1_{\langle e_{i+1}\rangle}) \bigoplus 1_{\mathrm{F}(\beta)} \bigoplus -1_{\mathrm{F}_{-1}(\beta)} \\ \gamma &= \bigoplus{}_{j\in J}(\gamma_j 1_{\langle e_j\rangle} \bigoplus \bar{\gamma}_j 1_{\langle e_{j+1}\rangle}) \bigoplus 1_{\mathrm{F}(\gamma)} \bigoplus -1_{\mathrm{F}_{-1}(\gamma)}. \end{aligned}$$

Für $\delta \in K^*$ mit $\delta\bar{\delta} = 1$ erhalten wir:

$$\begin{bmatrix} \delta & 0 \\ 0 & \bar{\delta} \end{bmatrix} = \begin{bmatrix} 0 & \delta \\ \bar{\delta} & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \delta \\ \bar{\delta} & 0 \end{bmatrix}^2 = I_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 \tag{4.1.8}$$

und

$$\begin{bmatrix} 0 & \delta \\ \bar{\delta} & 0 \end{bmatrix}\begin{bmatrix} \epsilon & 0 \\ 0 & \epsilon \end{bmatrix}\begin{bmatrix} 0 & \delta \\ \bar{\delta} & 0 \end{bmatrix} = \begin{bmatrix} \epsilon & 0 \\ 0 & \epsilon \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} \epsilon & 0 \\ 0 & \epsilon \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Hieraus folgt unmittelbar, daß es unitäre Involutionen $\iota_1, \iota_2, \iota_3, \iota_4$ gibt mit $\beta = \iota_1\iota_2$, $\mathrm{B}(\iota_1), \mathrm{B}(\iota_2) \leq \mathrm{B}(\beta)$, $\gamma = \iota_3\iota_4$ und $\mathrm{B}(\iota_3), \mathrm{B}(\iota_4) \leq \mathrm{B}(\gamma)$ (vgl. 2.3.7). ■

Korollar 4.1.22 *Sei $\pi \in \mathrm{SU}(f)$ eine Homothetie. Dann ist π ein Produkt von vier unitären Involutionen.*

Beweis. Sei $\lambda \in K^*$ mit $\pi = \lambda 1_V$. Dann gilt $\lambda\bar{\lambda} = 1$ und $1 = \det \pi = (\lambda^m)^2$, i.e. $\epsilon := \lambda^m \in \{\pm 1\}$. Wähle eine Basis $\mathcal{B} = (e_1, \ldots, e_m)$ von V, so daß

$$\mathcal{M}_{\mathcal{B}}(f) = \mathrm{diag}(I_m, -I_m)$$

gilt. Setzt man $W := \langle e_1, \ldots, e_m\rangle$ und $W' := \langle e_{m+1}, \ldots, e_n\rangle$, so gehört π_W zu $\mathrm{U}^{\pm}(f_W)$ und $\pi_{W'}$ zu $\mathrm{U}^{\pm}(f_{W'})$. Nach 4.1.21 gibt es Involutionen $\iota_i \in \mathrm{U}(f_W)$ und $\kappa_i \in \mathrm{U}(f_{W'})$, $i \in \mathbb{N}_{\leq 4}$, derart, daß $\pi_W = \iota_1 \cdots \iota_4$ und $\pi_{W'} = \kappa_1 \cdots \kappa_4$ ist. Also ist $\pi = (\iota_1 \bigoplus \kappa_1) \cdots (\iota_4 \bigoplus \kappa_4)$ das Produkt der vier Involutionen $(\iota_1 \bigoplus \kappa_1), \ldots, (\iota_4 \bigoplus \kappa_4)$ aus $\mathrm{U}(f)$. ■

Daß die Voraussetzung $\det \pi = 1$ in 4.1.22 notwendig ist, werden wir später an einem Beispiel sehen (cf. 4.4.17).

Satz 4.1.23 *Ist $|F| > 3$, so ist jedes $\pi \in \mathrm{SU}(f)$ ein Produkt von vier unitären Involutionen.*

Beweis. Sei $\pi \in \mathrm{SU}(f)$. Falls π eine Homothetie ist, liefert 4.1.22 das Gewünschte. Andernfalls gilt nach 4.1.19 $\pi = \psi\phi$ für unitäre Transformationen ϕ und ψ, die unitär zu ihren Inversen konjugiert sind und deren Minimalpolynome keinen $^{-}$-symmetrischen Primteiler haben. Nach 2.3.2 ist sowohl ϕ als auch ψ ein Produkt von zwei unitären Involutionen. ■

Bemerkung 4.1.24 *Unter den Annahmen von 4.1.20 zeigt man für $|F| = 3$ und $\dim V \equiv 0 \pmod 4$ wörtlich wie im Beweis von 4.1.23, daß jedes $\pi \in \mathrm{SU}(f)$ ein Produkt von vier unitären Involutionen ist.*

4.2 Orthogonal unzerlegbare Isometrien

Wie in der Einleitung erwähnt wird in diesem Abschnitt das Involutionen-Längenproblem für orthogonal unzerlegbare Isometrien aus $\mathrm{U}^{\pm}(f)$ studiert.
Mit den hier entwickelten Methoden können wir dieses jedenfalls für die Isometrien vom Typ III mit Minimalpolynom $(x \pm 1)^t$ lösen.
Hierfür müssen wir zunächst die Existenz einiger Polynome aus $K[x]$ mit bestimmten Teilbarkeits- und Reziprozitätseigenschaften sicherstellen. Wir beginnen mit einem wohlbekannten Satz, der für endliche Körper den Zusammenhang zwischen Irreduzibilität in $F[x]$ und in $K[x]$ klärt. (Einen Beweis findet man zum Beispiel in dem Buch 'Finite Fields' von D. Jungnickel [45] Kapitel 1, §3, Korollar 1.3.12, S.23.)

Satz 4.2.1 *Seien q eine Primzahlpotenz und $k, n \in \mathbb{N}$. Ein normiertes irreduzibles Polynom $p \in \mathrm{F}_q[x]$ vom Grad n ist genau dann irreduzibel in $\mathrm{F}_{q^k}[x]$, wenn k und n teilerfremd sind.* ■

In unserer Situation bedeutet dies: Ist K ein endlicher Körper, so ist ein normiertes Polynom $p \in F[x]$ vom Grad n genau dann irreduzibel in $K[x]$, wenn n ungerade und p irreduzibel in $F[x]$ ist.
Es ist eine wohlbekannte Tatsache, daß jeder endliche Körper normierte irreduzible Polynome beliebigen Grades besitzt. Weniger bekannt ist der

Satz 4.2.2 *Sei L ein endlicher Körper und $n \in \mathbb{N}$ gerade. Dann gibt es normierte irreduzible symmetrische Polynome vom Grad n in $L[x]$.*

Für einen Beweis verweisen wir wieder auf [45] Kapitel 2, §7, Theorem 2.7.4, S. 77, oder auf die dort zitierte Originalarbeit von Carlitz [14].
Mit diesen Hilfsmitteln können wir jetzt bequem die nächsten zwei Bemerkungen beweisen.

Bemerkung 4.2.3 *Seien $m \in \mathbb{N}_{\geq 2}$ und $\alpha \in F^*$. Dann gibt es ein Polynom $p \in K[x]$ vom Grad m mit $p(0) = \alpha$, so daß p teilerfremd zu p^* und pp^* symmetrisch ist.*

Beweis. Wir unterscheiden die Fälle A: $|F| = 2$ (i.e. $F = \mathrm{F}_2$) und B: $|F| > 2$.

A. Ist m ungerade, so wähle $p \in F[x]$ normiert und irreduzibel vom Grad m. Wegen $m \geq 2$ muß trivialerweise $0 \neq p(0) \in F^* = \{\alpha\}$ gelten. Nach 4.2.1 ist p irreduzibel in $K[x]$. Dies trifft dann auch auf $p^* = p^\times$ zu. Weil symmetrische Polynome $\neq x \pm 1$ einen geraden Grad haben, sind p und p^* verschieden und damit teilerfremd.
Ist m gerade so finden wir nach 4.2.2 ein normiertes irreduzibles symmetrisches Polynom p in $K[x]$. Wie im Vorigen sehen wir, daß $p(0) = \alpha$ gelten muß. Weiterhin folgern wir $p^* = \overline{p^\times} = \overline{p} \neq p$ aus 4.2.1 und damit die Teilerfremdheit von p und p^*.

B. Wegen $|F| \geq 3$ gibt es ein $\mu \in K \backslash F$ mit $\mu\bar{\mu} \neq 1$. [Wähle etwa $\nu \in K \backslash F$ mit $\nu\bar{\nu} = 1$, $\omega \in F^* \backslash \{-(\nu + \bar{\nu})\} \neq \emptyset$ und setze $\mu := \omega + \nu \in K \backslash F$. Dann ist $\mu\bar{\mu} = \omega^2 + (\nu + \bar{\nu})\omega + 1 \neq 1$.] Sei $r := (x + \mu)(x + \mu^{-1})$. Dann ist r offenbar symmetrisch und teilerfremd zu $r^* = (x + \bar{\mu}^{-1})(x + \bar{\mu})$.

Für $F \neq \mathrm{F}_3, \mathrm{F}_5$ finden wir wegen $|(F^*)^2| \geq 3$ ein $\nu \in (F^*)^2 \backslash \{\pm 1\}$. Wir definieren nun

$$s := \begin{cases} (x+\nu)^2(x+\nu^{-2}) & \text{, falls } F \neq \mathrm{F}_3, \mathrm{F}_5 \text{ ist,} \\ x^3 - x + 1 & \text{, falls } F = \mathrm{F}_3 \text{ ist,} \\ x^3 + x + 1 & \text{, falls } F = \mathrm{F}_5 \text{ ist,} \end{cases} \qquad t := \begin{cases} (x+\nu)^2(x-\nu^{-2}) & \text{, falls } F \neq \mathrm{F}_3, \mathrm{F}_5 \text{ ist,} \\ x^3 - x - 1 & \text{, falls } F = \mathrm{F}_3 \text{ ist,} \\ x^3 + x - 1 & \text{, falls } F = \mathrm{F}_5 \text{ ist.} \end{cases}$$

In jedem Fall gehört s (t) zu $F[x]$. Ist $F \in \{\mathrm{F}_3, \mathrm{F}_5\}$, so ist s (t) irreduzibel in $F[x]$. Weil $\deg(s) = 3 (= \deg(t))$ ungerade ist, ist s (t) nach 4.2.1 auch irreduzibel in $K[x]$. Damit ist in jedem Fall s (t) teilerfremd zu s^* (t^*) und r^*, und $ss^* = ss^\times$ $(tt^* = tt^\times)$ ist symmetrisch.
Ist F ein endlicher Körper, so ist die Normabbildung $\mathcal{N} : K \to F, k \mapsto k\bar{k}$ ein surjektiver Gruppenhomomorphismus und es gibt ein $\zeta \in K^*$ mit $\zeta\bar{\zeta} = \alpha$. Wegen $|\ker \mathcal{N}| = |F| + 1 \geq 4 > 2$ findet man ein $\delta \in \ker \mathcal{N}$, so daß $\delta\zeta$ nicht zu $\{\bar{\nu}, \bar{\nu}^{-1}\}$ gehört. Wegen $\delta\zeta\overline{\delta\zeta} = \zeta\bar{\zeta}$ können wir o.B.d.A. $\zeta \neq \bar{\nu}, \bar{\nu}^{-1}$ annehmen. Ist F nicht endlich, so können wir ein β aus $F^* \backslash \{\pm 1, \pm\alpha\}$ wählen. Wir definieren nun

$$u := \begin{cases} (x+\zeta)(x+\bar{\zeta}) & \text{, falls } F \text{ endlich ist,} \\ (x+\beta)(x+\beta^{-1}\alpha) & \text{sonst,} \end{cases}$$

und stellen fest, daß $u \in F[x]$ für $\alpha \neq 1$ stets teilerfremd zu u^*, r^* ist. Ferner ist $uu^* = uu^\times$ symmetrisch. Setzt man

$$p := \begin{cases} r^{\frac{m-1}{2}}(x+\alpha) & \text{, falls } m \text{ ungerade und } \alpha \neq \pm 1 \text{ ist,} \\ r^{\frac{m-3}{2}}s & \text{, falls } m \text{ ungerade und } \alpha = 1 \text{ ist,} \\ r^{\frac{m-3}{2}}t & \text{, falls } m \text{ ungerade und } \alpha = -1 \text{ ist,} \\ r^{\frac{m}{2}} & \text{, falls } m \text{ gerade und } \alpha = 1 \text{ ist,} \\ r^{\frac{m-2}{2}}u & \text{, falls } m \text{ gerade und } \alpha \neq 1 \text{ ist,} \end{cases}$$

so hat p die gewünschten Eigenschaften. ■

Bemerkung 4.2.4 *Seien* $\mathrm{char}(K) \neq 2$, $\delta \in K \backslash F$ *und* $m \in \mathbb{N}_{\geq 2}$. *Für* $|F| < \infty$ *gelte* $m \geq 3$. *Dann gibt es ein normiertes Polynom* $p \in K[x]$ *vom Grad* $m-1$ *mit* $p(0) \in F^*$, *so daß* p *teilerfremd zu* p^* *und* pp^* *symmetrisch und teilerfremd zu* $(x + p(0)^{-1}\delta)$ *ist. Für* $|F| = \infty$ *kann man zusätzlich* $p(0)^2 \neq \delta\bar{\delta}$ *erreichen.*

Beweis. Fall A: $|F| < \infty$ und m ist gerade. Dann ist $m - 1 \geq 2$ ungerade und wir finden ein normiertes irreduzibles Polynom p vom Grad $m-1$ in $F[x]$. Wir haben $p(0) \in F^*$, und p ist nach 4.2.1 irreduzibel in $K[x]$. Wegen $p(0)^{-1}\delta \notin F$ ist damit pp^* insbesondere teilerfremd zu $x + p(0)^{-1}\delta$. Weil p ungeraden Grad hat, kann p nicht symmetrisch sein, i.e. p und $p^\times = p^*$ sind teilerfremd. Trivialerweise ist $pp^* = pp^\times$ symmetrisch.

Fall B: $|F| < \infty$ und m ist ungerade. Dann ist $m - 1 \geq 2$ gerade und es gibt nach 4.2.2 ein normiertes irreduzibles symmetrisches Polynom p vom Grad $m-1$ in $K[x]$, welches nach 4.2.1 nicht in $F[x]$ liegt. Damit ist p teilerfremd zu $p^* = \overline{p^\times} = \bar{p}$, $p(0) = 1$, und pp^* ist symmetrisch und teilerfremd zu $x + \delta$.

Fall C: $|F| = \infty$. Weil dann auch $|F^{2(m-1)}| = \infty$ ist, gibt es ein $\alpha \in F^*$ mit $\alpha^{2(m-1)} \notin \{1, \delta\bar{\delta}\}$.

Wähle $p := (x+\alpha)^{m-1}$. ■

Wir benötigen nun noch ein einfaches Lemma, das zeigt, wie man die Konjugiertenklasse einer zyklischen Abbildung aus $\mathrm{GL}(V)$ durch Heranmultiplizieren einer einfachen Abbildung verändern kann. (Einen Beweis findet man in [49] Lemma 10.(Simple lemma).)

Lemma 4.2.5 *Seien L ein Körper, $m \in \mathbb{N}$ und W ein m-dimensionaler L-Vektorraum. Seien weiterhin $q \in L[x]$ ein normiertes Polynom vom Grad m mit $q(0) \neq 0$ und $\pi \in GL(W)$ zyklisch. Dann gibt es eine Abbildung $\tau \in \mathrm{GL}(W)$ mit $\dim \mathrm{B}(\tau) \leq 1$, so daß $\pi\tau$ zyklisch mit Minimalpolynom $\mathrm{mip}(\pi\tau) = q$ ist. Notwendigerweise muß $\det \tau = (-1)^m q(0) \det \pi^{-1}$ gelten, so daß τ für $q(0) = (-1)^{m+1} \det \pi$ eine Involution ist.* ■

Kombiniert man 4.2.3, 4.2.4 und 4.2.5 mit dem Satz von Djoković 2.3.2, so erhält man unmittelbar die beiden folgenden Lemmata.

Lemma 4.2.6 *Der reguläre hermitesche Vektorraum (V, f) besitze maximalen Wittindex $m \geq 2$. Sei $\pi \in \mathrm{U}^{\pm}(f)$ derart, daß es einen maximalen totalisotropen Unterraum W gibt, der π-invariant und π zyklisch ist. Die Determinante von π_W gehöre zu F^*. Dann ist π ein Produkt von drei unitären Involutionen.*

Beweis: Nach 4.2.3 gibt es ein Polynom $p \in \mathrm{F}[x]$ vom Grad m mit $p(0) = (-1)^{m+1} \det \pi_W$, so daß p teilerfremd zu p^* und pp^* symmetrisch ist. Nach 4.2.5 finden wir eine Involution $\sigma \in \mathrm{GL}(W)$, so daß $\pi_W \sigma$ zyklisch ist und das Minimalpolynom p besitzt. Wir können nun σ zu einer Involution $\hat{\sigma} \in \mathrm{U}(f)$ fortsetzen (cf. 1.3.5). Sei $\phi := \pi\hat{\sigma}$. Dann gilt $\mathrm{mip}(\phi_W) = p$. Weil $\mathrm{mip}(\phi)$ $^-$-symmetrisch und $\mathrm{lcm}(p, p^*) = 1$ ist, teilt pp^* $\mathrm{mip}(\phi)$. Ist $n := \dim V$ gerade, so folgt bereits aus $\deg(pp^*) = 2m = n$ die Gleichheit $\mathrm{mip}(\phi) = pp^*$. Damit ist ϕ zyklisch und, da pp^* symmetrisch ist, auch ähnlich zu seinem Inversen. Der Satz von Djoković 2.3.2 besagt nun, daß ϕ das Produkt von zwei unitären Involutionen ρ, η ist. Also ist $\pi = \phi\hat{\sigma} = \rho\eta\hat{\sigma}$ ein Produkt von drei unitären Involutionen.

Wir können daher annehmen, daß $\dim V = 2m + 1$ ungerade ist. Wegen $\deg(pp^*) = 2m = \deg(\mathrm{char}(\phi)) - 1$, gibt es ein $\epsilon \in K^*$, so daß $\mathrm{char}(\phi) = pp^*(x - \epsilon)$ gilt. Wir berechnen

$$\begin{aligned} -\epsilon &= -\det \phi_W \overline{\det \phi_W}^{-1} \epsilon = -p(0)p^*(0)\epsilon \\ &= \mathrm{char}(\phi)(0) = (-1)^{n+1} \det \phi \in \{\pm 1\}. \end{aligned}$$

Weil p nach Voraussetzung keine $^-$-symmetrischen Primteiler besitzt, ist $(x + \epsilon)$ teilerfremd zu pp^*. Hieraus folgt $V = Y \textcircled{\perp} Z$, $Y := \mathrm{F}_\epsilon(\phi)$, $Z := Y^\perp$, $\phi = \epsilon 1_Y \textcircled{\perp} \phi_Z$ und ϕ_Z ist zyklisch mit symmetrischem Minimalpolynom pp^*. Wie im ersten Fall findet man Involutionen $\rho, \eta \in \mathrm{U}(f_Z)$ mit $\phi_Z = \rho\eta$. Dann sind $\hat{\rho} := \epsilon 1_Y \textcircled{\perp} \rho$ und $\hat{\eta} := 1_Y \textcircled{\perp} \eta$ unitäre Involutionen so, daß $\pi = \hat{\rho}\hat{\eta}$ gilt. Also ist auch in diesem Fall $\pi = \phi\hat{\sigma} = \hat{\rho}\hat{\eta}\hat{\sigma}$ ein Produkt von drei unitären Involutionen. ■

Lemma 4.2.7 *Es sei $\mathrm{char}(K) \neq 2$ und V ein hyperbolischer Raum der Dimension $2m \geq 4$, $m \in \mathbb{N}_{\geq 2}$. Falls F endlich ist, sei $m \geq 3$. Sei $\det \pi \neq 1$ derart, daß es einen maximalen totalisotropen*

Unterraum W gibt, der π-invariant ist. Nach 4.1.7 ist $\delta := \det \pi_W = \det \pi \overline{\det \pi_W} \notin F$. Ferner sei π_W zyklisch.

(i) *Es gilt $\pi = \tau\eta\rho\sigma$ für unitäre Involutionen η, ρ, σ und ein $\tau \in \mathrm{U}(f)$ mit $\det \tau = \det \pi$, für das $H := \mathrm{B}(\tau) \leq \mathrm{F}(\eta) \cap \mathrm{F}(\rho)$ eine hyperbolische Ebene ist.*

(ii) *Im Fall $|F| = \infty$ ist τ_H vom Typ I.*

(iii) *Falls es ein totalisotropes π-invariantes Komplement U von W in V gibt (diese Situation sei durch* (K) *abgekürzt), ist τ_H vom Typ I oder eine Homothetie.*

Beweis: Der Beweis verläuft ähnlich wie der von 4.2.6.
Nach 4.2.4 gibt es ein Polynom $p \in \mathrm{F}[x]$ vom Grad $m-1$ mit folgenden Eigenschaften:

(1) $p(0) \in F^*$;

(2) p ist teilerfremd zu p^*;

(3) pp^* ist symmetrisch;

(4) pp^* ist teilerfremd zu $x + p(0)^{-1}(-1)^{m+1}\delta$;

(5) Für $|F| = \infty$ gilt $p(0)^2 \neq \delta\bar{\delta}$.

Seien $\gamma := p(0)^{-1}(-1)^{m+1}\delta$, $q := (x+\gamma)(x+\bar{\gamma}^{-1})$ und $r := \mathrm{lcm}(x+\gamma, x+\bar{\gamma}^{-1})$. Nach 4.2.5 gibt es eine Involution $\sigma \in \mathrm{GL}(W)$, so daß $\mathrm{mip}(\pi_W\sigma) = (x+\gamma)p$ ist. Seien $\hat{\sigma} \in \mathrm{U}(f)$ eine Involution die σ fortsetzt und $\phi := \pi\sigma$. Im Fall (K) kann man erreichen, daß auch U $\hat{\sigma}$-invariant ist, womit dies auch auf ϕ zutrifft. Es gilt $\mathrm{mip}(\phi_W) = (x+\gamma)p = \mathrm{char}(\phi_W)$ und im Fall (K) $\mathrm{mip}(\phi_U) = (x+\bar{\gamma}^{-1})p^* = \mathrm{char}(\phi_U)$. Hieraus folgt $\mathrm{char}(\phi) = \mathrm{char}(\phi_W)\mathrm{char}(\phi_W)^* = pp^*q$ (cf. (4.1.4) in 4.1.4 mit $C = 0$ und die dortige Nummer (iv)). Weil $\mathrm{mip}(\phi)$ $^-$-symmetrisch ist, folgt aus (2),(4) daß $\mathrm{mip}(\phi)$ von pp^*r geteilt wird. Im Fall (K) gilt bereits $\mathrm{mip}(\phi) = pp^*r$. Hieraus erhalten wir die Zerlegung $V = Z \bigoplus H$, $Z := \ker pp^*(\phi)$, $H := \ker q(\phi)$. Dabei ist ϕ_Z zyklisch mit symmetrischem Minimalpolynom pp^* und H eine hyperbolische Ebene, da H regulär und $\{0\} \neq \ker(\phi_W + \gamma) \leq H \cap W$ ein eindimensionaler singulärer Unterraum von H ist. Aus der Ähnlichkeit von ϕ_Z zu seinem Inversen schließen wir mit (2) aus dem Satz von Djoković, daß ϕ_Z ein Produkt von zwei Involutionen η, ρ aus $\mathrm{U}(f_Z)$ ist. Dann sind $\hat{\eta} := \eta \bigoplus 1_H$ und $\hat{\rho} := \rho \bigoplus 1_H$ Involutionen aus $\mathrm{U}(f)$, die η bzw. ρ fortsetzen. Für $\tau := \phi_H \bigoplus 1_H$ gilt $\mathrm{B}(\tau) = H \leq \mathrm{F}(\hat{\eta}) \cap \mathrm{F}(\hat{\rho})$ und $\det \tau = q(0) = \delta\bar{\delta}^{-1} = \det \pi$. Im Fall $|F| = \infty$ schließen wir mit (5), daß τ vom Typ I ist. Im Fall (K) ist $\mathrm{mip}(\tau) = r$, so daß τ_H für $\gamma \neq \bar{\gamma}^{-1}$ vom Typ I und für $\gamma = \bar{\gamma}^{-1}$ eine Homothetie ist. Damit haben wir $\pi = \hat{\eta}\hat{\rho}\tau\hat{\sigma} = \tau\hat{\eta}\hat{\rho}\hat{\sigma}$ in der gewünschten Weise dargestellt. ■

Als nächstes fassen wir das Symmetrien-Längenproblem für hyperbolische Ebenen in der folgenden Bemerkung zusammen.

Bemerkung 4.2.8 *Sei V eine hyperbolische Ebene. Außer im Fall $F = \mathrm{F}_3$ wird $\mathrm{U}^{\pm}(f)$ von Symmetrien erzeugt (cf.3.4.22). welche sich nicht als ein Produkt von Symmetrien darstellen lassen. Schließt man diesen Fall aus, so ergibt sich die Symmetrien-Länge $\mathrm{l}(\pi)$ für ein $\pi \in \mathrm{U}^{\pm}(f)$, das keine Involution ist, wie folgt:*

(i) *Ist* $\mathrm{char}(K) \neq 2$, *so gilt*

$$\mathrm{l}(\pi) = \begin{cases} 2 & , falls\ \det\pi = 1,\ \pi\ orthogonal\ zerlegbar\ und\ -1 \in \mathcal{N}(K)\ ist, \\ 4 & , falls\ \det\pi = 1,\ \pi\ orthogonal\ zerlegbar\ und\ -1 \notin \mathcal{N}(K)\ ist, \\ 2 & , falls\ \det\pi = 1\ und\ \pi\ vom\ Typ\ I\ ist, \\ 2 & , falls\ \det\pi = 1,\ \pi\ vom\ Typ\ II\ und \\ & \mathrm{trace}(\pi)^2 - 4 = (\mathrm{trace}(\pi)+2)(\mathrm{trace}(\pi)-2) \in \mathcal{N}(K)\backslash\{0\}\ ist, \\ 4 & , falls\ \det\pi = 1,\ \pi\ vom\ Typ\ II\ und \\ & \mathrm{trace}(\pi)^2 - 4 = (\mathrm{trace}(\pi)+2)(\mathrm{trace}(\pi)-2) \notin \mathcal{N}(K)\ ist, \\ 3 & , falls\ \det\pi = -1\ und\ \pi\ keine\ Homothetie\ ist, \\ 3 & , falls \det\pi = -1,\ \pi\ eine\ Homothetie\ und\ -1 \in \mathcal{N}(K)\ ist, \\ 5 & , falls\ \det\pi = -1,\ \pi\ eine\ Homothetie\ und -1 \notin \mathcal{N}(K)\ ist. \end{cases}$$

(ii) *Ist* $\mathrm{char}(K) = 2$, *so gilt* $\mathrm{l}(\pi) = 2$.

Beweis. Wir betrachten als erstes den Fall, daß π keine Homothetie ist. Dann gibt es einen isotropen Vektor u, so daß $\mathcal{B} := (u, u\pi)$ eine geordnete Basis von V ist. Setzt man $\alpha := -\mathrm{trace}(\pi)$, $\epsilon := \det(\pi)$ und $\nu := f(u, u\pi)$, so gilt $\bar{\alpha} = \epsilon\alpha$, und man erhält folgende Koordinatendarstellung:

$$\mathcal{M}_{\mathcal{B}}(\pi) = \begin{bmatrix} 0 & 1 \\ -\epsilon & -\alpha \end{bmatrix}, \qquad \mathcal{M}_{\mathcal{B}}(f) = \begin{bmatrix} 0 & \nu \\ \bar{\nu} & 0 \end{bmatrix}.$$

Aus $\pi \in \mathrm{U}(f)$ folgt:

$$\begin{bmatrix} 0 & \nu \\ \bar{\nu} & 0 \end{bmatrix} = \mathcal{M}_{\mathcal{B}}(f) = \mathcal{M}_{\mathcal{B}}(\pi)\mathcal{M}_{\mathcal{B}}(f)\overline{\mathcal{M}_{\mathcal{B}}(f)}^t = \begin{bmatrix} 0 & -\bar{\nu}\epsilon \\ -\epsilon\nu & \epsilon(\alpha\bar{\nu} + \bar{\alpha}\nu) \end{bmatrix}.$$

Dies erzwingt $\bar{\nu} = -\epsilon\nu$.

Fall A: $\det\pi = -1$. Dann gehört ν zu F^*.

A.1. $\mathrm{char}(K) = 2$. Setze $b := v(\pi + 1)$. Es ist $q_\pi(b) = \nu \in F^*$ und die Symmetrie $\sigma := \sigma_{\nu^{-1},b}$ erfüllt $\dim \mathrm{F}(\pi\sigma) = 1$, cf. 3.2.2 (a). Also ist $\pi\sigma$ eine Symmetrie und damit $\mathrm{l}(\pi) = 2$, was (ii) beweist.

A.2. $\mathrm{char}(K) \neq 2$. Weil wir $F = \mathrm{F}_3$ ausgeschlossen haben, finden wir ein $\beta \in F^*\backslash\{\pm 1\}$. Es ist $b := v\pi - \beta v$ anisotrop und die Symmetrie σ mit Bahn $\langle b\rangle$ bildet $v\pi$ auf βv ab, so daß wir $\mathrm{mip}(\pi\sigma) = (x - \beta)(x - \beta^{-1})$ erhalten. Weil dann $\pi\sigma$ ähnlich zu seinem Inversen ist und $\mathrm{mip}(\pi\sigma)$ keine $^-$-symmetrischen Primteiler besitzt, ist $\pi\sigma$ nach 2.3.2 ein Produkt von zwei Involutionen, welche zwangsläufig Symmetrien sein müssen. Es folgt $\mathrm{l}(\pi) = 3$.

Fall B: $\det\pi = 1 \neq -1$. Dann gilt $\bar{\nu} = -\nu$. Aus 4.1.23 lesen wir $\mathrm{l}(\pi) \leq 4$ ab. Ist π vom Typ I, so gilt $\mathrm{mip}(\pi) = (x - \beta)(x - \bar{\beta}^{-1})$ für ein $\beta \in K^*$ mit $\beta\bar{\beta} \neq 1$. Aus $1 = \det\pi = \beta\bar{\beta}^{-1}$ folgt $\beta \in F^*$. Damit ist π ähnlich zu seinem Inversen und kein Primteiler von $\mathrm{mip}(\pi)$ ist $^-$-symmetrisch. Mit 2.3.2 folgt wiederum $\mathrm{l}(\pi) = 2$.

Ist $\pi = \mu 1_{\langle a\rangle} \textcircled{\perp}\ \mu^{-1}1_{\langle b\rangle}$ orthogonal zerlegbar, $a, b \in V$ anisotrop, so folgt aus $l(\pi) = 2$, daß π in $\mathrm{U}(f)$ konjugiert zu π^{-1} ist. Dies impliziert $f(a,a)\mathcal{N}(K) = f(b,b)\mathcal{N}(K)$, also $-1\mathcal{N}(K) = \mathrm{disc}(f) = f(a,a)f(b,b)\mathcal{N}(K) = f(a,a)^2\mathcal{N}(K) = \mathcal{N}(K)$ (, da $F^2 \subseteq \mathcal{N}(K)$). Ist umgekehrt diese

Bedingung erfüllt, so kann man o.B.d.A. $f(a,a) = f(b,b) = 1$ annehmen. Für $c := a - b$ gilt dann $f(c,c) = 2 \neq 0$, $a(\pi\sigma_c)^2 = a$ und $\det \pi\sigma_c = -1$. Folglich ist $\pi\sigma_c$ eine Symmetrie, so daß wir $\mathrm{l}(\pi) = 2$ schließen.
Ist π oder $-\pi$ eine Transvektion so gilt $\mathrm{trace}(\pi)^2 = 4$ und $\mathrm{l}(\pi) > 2$ (cf.2.2.3), also $\mathrm{l}(\pi) = 4$.
Ist π vom Typ II mit irreduziblem Minimalpolynom $p := x^2 + \alpha x + 1$ und

$$d : \mathrm{B}(\pi) \times \mathrm{B}(\pi),\ d(v(\pi-1), w(\pi-1)) := i \cdot f(v(\pi+1), w(\pi-1))$$

die in 3.2.3 definierte hermitische Form ($\bar{i} = -i \in K^*$), so berechnet man bezüglich der geordneten Basis $\mathcal{C} := (u(\pi-1), u\pi(\pi-1))$ von $\mathrm{B}(\pi) = V$ folgende Koordinatendarstellung:

$$\mathcal{M}_{\mathcal{C}}(d) = i\nu \begin{bmatrix} 2 & -\alpha \\ -\alpha & 2 \end{bmatrix}.$$

Somit hat d die Diskriminante $(4-\alpha^2)(i\nu)^2\mathcal{N}(K) = (2+\alpha)(2-\alpha)\mathcal{N}(K)$, da $(i\nu)^2 \in F^2 \subseteq \mathcal{N}(K)$. Weil $\mathrm{mip}(\pi) \neq (x \pm 1)^2$ irreduzibel ist, gilt $\alpha \neq \pm 2$. Folglich ist d regulär. Weil π keine Homothetie ist, ist π nach 3.1.2,3.2.4 und 3.2.2 genau dann ein Produkt von zwei Symmetrien, wenn d eine hyperbolische Ebene ist. Dies ist genau dann der Fall, wenn $\mathrm{disc}(d) = -\mathcal{N}(K)$ gilt, i.e. $(4-\alpha^2) \in -\mathcal{N}(K)$.

Sei schließlich π eine λ-Homothetie. Wegen $\pi \neq 1$ ist $\det \pi \neq 1$, also $\mathrm{char}(K) \neq 2$ und $\lambda^{-1} = \bar{\lambda} = -\lambda$. Für jede Symmetrie σ ist $\pi\sigma = -\lambda 1_{\mathrm{B}(\sigma)} \textcircled{\perp} \lambda 1_{\mathrm{F}(\sigma)}$ orthogonal zerlegbar mit $\det \pi\sigma = 1$. Aus dem bereits Bewiesenen folgern wir $\mathrm{l}(\pi\sigma) = 2$,falls $-1 \in \mathcal{N}(K)$ gilt, und $\mathrm{l}(\pi\sigma) = 4$ sonst. Dies impliziert $\mathrm{l}(\pi) = 3$,falls $-1 \in \mathcal{N}(K)$ gilt, und $\mathrm{l}(\pi) = 5$ sonst. ∎

Bemerkung 4.2.9 *Seien* $\mathrm{char}(K) = 2$, $|F| = \infty$, $\dim V = 3$ *und* $\pi \in \mathrm{SU}(f)$ *besitze das Minimalpolynom* $(x+1)^3$. *Dann hat* π *die Symmetrien-(Involutionen-) Länge* $\mathrm{l}(\pi) = 4$.

Beweis. Beachte, daß es unter den gegebenen Voraussetzungen isotrope Vektoren gibt [$V(\pi+1)^2 = \mathrm{F}(\pi) \neq \{0\}$ ist isotrop] und jede Involution $\neq 1$ eine Symmetrie ist. Wörtlich wie in 3.4.4 zeigt man

(1) $\mathrm{l}(\pi) \geq 4$.

Weil V von isotropen Vektoren erzeugt wird, gibt es ein isotropes $v \in V$ mit $\langle v \rangle_\pi = V$. Nach 2.2.4 (ii) gilt $\alpha := f(v, v\pi) = f(v, v(\pi+1)) \notin F$. Daher ist neben $p := (\alpha\bar{\alpha})^{-2}x^4 + (\alpha^{-2}\bar{\alpha}^{-1} + \bar{\alpha}^{-2}\alpha^{-1})x^3 + (\alpha^{-1} + \bar{\alpha}^{-1})x + 1$ auch $q := (\alpha^{-2}\bar{\alpha}^{-1} + \bar{\alpha}^{-2}\alpha^{-1})x^2 + (\alpha^{-1} + \bar{\alpha}^{-1})$ ein von Null verschiedenes Polynom in $F[x]$. Wegen $|F| = \infty$ können wir ein $\beta \in F^*$ finden, so daß $p(\beta) \neq 0 \neq q(\beta)$ und $\beta^2 \neq \alpha\bar{\alpha}$ erfüllt ist. Dann gilt insbesondere

(2) $\gamma := \beta\alpha^{-1} \notin F$ und $\gamma\bar{\gamma} \neq 1$

Wir wollen nun $v\pi$ auf γv 'zurückschwenken'. Dazu sei $b := v\pi + \gamma v$. Nach Konstruktion ist b isotrop, so daß die Symmetrie $\sigma := \sigma_{\beta^{-1},b}$ wohldefiniert ist. Wir berechnen:

$$v\pi\sigma = v\pi + \beta^{-1} f(v\pi, v\pi + \beta\alpha^{-1}v)(v\pi + \gamma v) = \gamma v.$$

Demnach hat $\phi := \pi\sigma$ den Eigenwert γ. Aus (2) und $\det\phi = 1$ folgt dann bereits $\mathrm{mip}(\phi) = (x+\gamma)(x+\bar{\gamma}^{-1})(x+\bar{\gamma}\gamma^{-1})$. Wähle $e_1 := v$ und Eigenvektoren e_2, e_3 von ϕ zu den Eigenwerten $\bar{\gamma}^{-1}$ und $\bar{\gamma}\gamma^{-1}$. Dann ist $H := \langle e_1, e_2\rangle$ eine hyperbolische Ebene mit isotropen Vektoren e_1, e_2 und wir können $f(e_1, e_2) = 1$ erreichen. Ferner haben wir $V = H \oplus \langle e_3\rangle$. Indem man die Form f notfalls mit einem Faktor aus F^* multipliziert, kann man o.B.d.A. $f(e_3, e_3) = 1$ annehmen. Wähle nun

$$\xi := \frac{p(\beta)}{\beta q(\beta)} \in F^*,\ \nu := \frac{\xi + \gamma^{-1} + 1}{\bar{\gamma} + \gamma^{-1}},\ (\text{cf.}(2)) \text{ und } z := e_1 + \nu e_2 \in H.$$

Man berechnet dann $f(z, z) = \nu + \bar{\nu} = 1$ und

$$\begin{aligned} f_\phi(z(\phi+1), z(\phi+1)) &= f(z, z(\phi+1)) = f(e_1 + \nu e_2, (\gamma+1)e_1 + (\bar{\gamma}^{-1}+1)\nu e_2) \\ &= \nu(\bar{\gamma} + \gamma^{-1}) + \gamma^{-1} + 1 = \xi \in F^*. \end{aligned}$$

Für $\rho := \sigma_{\xi^{-1}, z(\phi+1)}$ ist nach 3.2.2 (a) $\mathrm{F}(\phi\rho) = \langle z\rangle$ regulär. Für $y \in z^\perp \cap H$ berechnen wir $\mathcal{N}(K) = \mathrm{disc}(f_H) = f(z,z)f(y,y)\mathcal{N}(K) = f(y,y)\mathcal{N}(K)$. Für $L := \mathrm{B}(\phi\rho) = z^\perp$ bedeutet dies aber $\mathrm{disc}(f_L) = f(y,y)f(e_3,e_3)\mathcal{N}(K) = \mathcal{N}(K)$, i.e. L ist eine hyperbolische Ebene. Nach 4.2.8 (ii) ist dann $\phi\rho$ ein Produkt von zwei Symmetrien η, ζ, so daß $\pi = \eta\zeta\rho\sigma$ ein Produkt von vier Symmetrien ist. ■

Wir geben nun wie eingangs angekündigt Involutionen-Längen $\mathrm{l}_I(\pi)$ orthogonal unzerlegbarer unitärer Isometrien mit Determinante ± 1 an. Die folgende Liste ist weit davon entfernt, vollständig zu sein, und gibt in vielen Fällen nur obere Schranken an. Wir werden im Anschluß genau auf die Lücken hinweisen.

Satz 4.2.10 *Seien $\pi \in \mathrm{U}^\pm(f)$ keine Involution und V ein orthogonal unzerlegbarer π-Modul.*

(i) *Sei π vom Typ* I *mit Minimalpolynom $(pp^*)^t$, $p \in K[x]$ irreduzibel und nicht $^-$-symmetrisch, $t \in \mathbb{N}$. Dann gilt:*

$$\mathrm{l}_I(\pi) \begin{cases} = 2 & , \textit{falls } pp^* \textit{ symmetrisch ist}, \\ = 3 & , \textit{falls } pp^* \textit{ nicht symmetrisch und } \det\pi = 1 \textit{ ist}, \\ \in \{3,4\} & , \textit{falls } \det\pi = -1 \neq 1 \textit{ ist}. \end{cases}$$

(ii) *Sei π vom Typ* III *mit Minimalpolynom $(x \pm 1)^n$, $n = \dim V$. Dann gilt:*

$$\mathrm{l}_I(\pi) \begin{cases} = 2 & , \textit{falls } \mathrm{char}(K) \neq 2 \textit{ und } n \textit{ ungerade ist}, \\ = 3 & , \textit{falls } \mathrm{char}(K) \neq 2, \textit{ und } n \geq 4 \textit{ gerade ist}, \\ = 4 & , \textit{falls } \mathrm{char}(K) \neq 2,\ F \neq \mathrm{F}_3 \textit{ und } n = 2 \textit{ ist}, \\ = 2 & , \textit{falls } \mathrm{char}(K) = 2 \textit{ und } n \textit{ gerade ist}, \\ = 3 & , \textit{falls } \mathrm{char}(K) = 2 \textit{ und } n > 3 \textit{ ungerade ist}, \\ = 4 & , \textit{falls } \mathrm{char}(K) = 2,\ n = 3 \textit{ und } F \neq \mathrm{F}_2 \textit{ ist}. \end{cases}$$

(Für $F = \mathrm{F}_3$ und $n = 2$ bzw. $F = \mathrm{F}_2$ und $n = 3$ haben wir in 3.4.22 bzw. 3.5.8 (b) gesehen, daß π kein Produkt von Involutionen ist.)

(iii) *Sei* π *vom Typ* III *mit Minimalpolynom* p^{2t}*, wobei* $p \in K[x]\backslash\{x \pm 1\}$ $^-$*-symmetrisch und* $t \in \mathbb{N}$ *sei. Dann gilt:*

$$\mathrm{l}_I(\pi) \begin{cases} = 3 & , falls\ |K| < \infty,\ \dim V \geq 6\ und\ \det \pi = 1\ ist, \\ \leq 3 & , falls\ |K| = \infty,\ \dim V \geq 4\ und\ \det \pi = 1\ ist, \\ \in \{3,4\} & , falls\ [\dim V = 4\ oder\ F \neq \mathrm{F}_3]\ und\ \det \pi = -1 \neq 1\ ist, \\ = 3 & , falls\ \dim V = 2\ und\ F \neq \mathrm{F}_3\ ist. \end{cases}$$

(Für $F = \mathrm{F}_3$ *und* $n = 2$ *zeigt 3.4.22, daß* π *kein Produkt von Involutionen ist.)*

Beweis: Für $\dim V = 2$ haben wir das Behauptete in 4.2.8 bewiesen, so daß wir $\dim V \geq 3$ annehmen können. [Beachte: Im Fall $\dim V = 2$, $F = \mathrm{F}_3$ gibt es keine Isometrien vom Typ I mit Determinante ± 1.]
(i) Falls pp^* symmetrisch ist, muß insbesondere $\det \pi = 1$ sein (, weil $x \pm 1$ kein Teiler von p ist). Ferner ist dann π ähnlich zu π^{-1}, da π zyklisch ist, und es folgt $\mathrm{l}_I(\pi) = 2$ aus dem Satz von Djoković. Ist pp^* nicht symmetrisch, so ist π nicht ähnlich zu π^{-1} und damit trivialerweise $\mathrm{l}_I(\pi) \geq 3$. Es sind $W := \ker p^t(\pi)$ und $U := \ker p^{*t}(\pi)$ totalisotrope π-zyklische Moduln mit $V = U \oplus W$. Nach 4.1.7 haben wir:

$$\overline{\det \pi_W} = \begin{cases} \det \pi_W & \text{, falls } \det \pi = 1 \text{ ist,} \\ -\det \pi_W & \text{, falls } \det \pi = -1 \text{ ist.} \end{cases}$$

Im Fall $\det \pi = 1$ folgt $l(\pi) = 3$ aus 4.2.6. Ist $\det \pi = -1 \neq 1$, so kann man π nach 4.2.7 als ein Produkt $\tau\eta\rho\sigma$ darstellen, wobei η, ρ, σ unitäre Involutionen sind, $\tau \in \mathrm{U}(f)$ die Determinante -1 hat und $H := \mathrm{B}(\tau) \leq \mathrm{F}(\eta) \cap \mathrm{F}(\rho)$ eine hyperbolische Ebene ist. Für $|F| = \infty$ ist τ_H außerdem keine Homothetie (cf.4.2.7 (ii)) und für $|F| < \infty$ ist τ_H entweder vom Typ I oder eine Homothetie (cf.4.2.7 (iii)). Nach 4.2.8 (für $F \neq \mathrm{F}_3$) und 3.4.22 (für $F = \mathrm{F}_3$) gilt $\tau_H = \zeta_1\zeta_2\zeta_3$ für Symmetrien $\zeta_1, \zeta_2, \zeta_3 \in \mathrm{U}(f_H)$. Die Abbildungen $\hat{\zeta} := \zeta_1 \mathbin{\bigcirc\!\!\!\!\perp}\ 1_H$, $\hat{\eta} := \zeta_2 \mathbin{\bigcirc\!\!\!\!\perp}\ \eta_H$, $\hat{\rho} := \zeta_1 \mathbin{\bigcirc\!\!\!\!\perp}\ \rho_H$ sind unitäre Involutionen und erfüllen $\pi = \hat{\zeta}\hat{\eta}\hat{\rho}\sigma$. Es folgt $\mathrm{l}_I(\pi) \leq 4$.

(ii) Nach 2.2.3 und 4.2.9 müssen wir nur noch $\mathrm{l}_I(\pi) \leq 3$ für $\mathrm{char}(K) \neq 2$ und gerades $t = 2m$, $m \geq 2$ bzw. für $\mathrm{char}(K) = 2$ und ungerades $t = 2m+1$, $m \geq 2$ nachweisen. Dies folgt jedoch sofort aus 4.2.6 mit $W := V(\pi - 1)^m$.

(iii) Beachte, daß $\dim V$ gerade ist, und deshalb aus der eingangs gemachten Voraussetzung $\dim V > 2$ bereits $\dim V \geq 4$ folgt. Falls K endlich und $\dim V = 4 (= \dim \mathrm{B}(\pi))$ ist, ist π in jedem Fall eine kurze Abbildung im Sinne der Definitionen 3.4.1, 3.4.20, 3.5.1 und 3.5.7. Nach den Sätzen 3.4.5 (a), 3.4.21 (a), 3.5.5 (a) und 3.5.8 (a) gilt $l_I(\pi) \leq 4$. Falls K endlich ist können wir daher $\dim V \geq 6$ annehmen. Ferner halten wir fest, daß p für $|K| < \infty$ nicht symmetrisch sein kann, sonst hätte $p = p^* = \overline{p^\times} = \bar{p} \in \mathrm{F}[x]\backslash\{x \pm 1\}$ geraden Grad und wäre deshalb nach 4.2.1 nicht irreduzibel in $K[x]$. In diesem Fall ist daher π nicht ähnlich zu π^{-1}, was $\mathrm{l}_I(\pi) \geq 3$ impliziert. Wir müssen also nur noch $\mathrm{l}_I(\pi) \leq 3$ für $\det \pi = 1$ und $\mathrm{l}_I(\pi) \leq 4$ für $\det \pi = -1 \neq 1$ und $F \neq \mathrm{F}_3$ beweisen. Dies folgt jedoch mit analogen Schlüssen wie in (i) mit $W := Vp^t(\pi)$. [Man beachte hierbei, daß es kein π-invariantes totalisotropes Komplement zu W in V gibt, wie es in (i) der Fall war. Dies haben wir jedoch nur für $F = \mathrm{F}_3$ und $\det\pi = -1$ wirklich benötigt. Dieser Fall ist hier gerade ausgeschlossen.]

Folgende Fragen zu Involutionen-Längen $\mathrm{l}(\pi)$ orthogonal unzerlegbarer Isometrien $\pi \in \mathrm{U}^{\pm}(f)$ sind offen:

- $\mathrm{char}(K) \neq 2$, $\dim V \geq 4$, π ist vom Typ I und $det\pi = -1$. Gilt $\mathrm{l}_I(\pi) = 3$? (Wir weisen darauf hin, daß π nach einem Satz von C.S. Ballantine (cf.[3] Abschnitt 2, Theorem 3) stets ein Produkt von drei Involutionen aus $\mathrm{GL}(V)$ ist.)
- $F = \mathrm{F}_3$, $\dim V \geq 6$ und π ist vom Typ III mit $\det\pi = -1$ und Minimalpolynom p^{2t}, wobei $p \in K[x]\backslash\{x \pm 1\}$ irreduzibel und $^{-}$-symmetrisch und $t \in \mathbb{N}$ sei.
- π ist vom Typ III mit Minimalpolynom p^{2t+1}, wobei $p \in K[x]\backslash\{x \pm 1\}$ irreduzibel und $^{-}$-symmetrisch und $t \in \mathbb{N}$ sei. Dies scheint das schwierigste aller genannten Probleme zu sein, da es in dieser Allgemeinheit eng mit der ungelösten Frage verknüpft ist, ob auch für anisotropes f (und $\mathrm{char}(K) \neq 2$) $\mathrm{U}^{\pm}(f)$ von Involutionen erzeugt wird.

4.3 Körper mit surjektiver Normabbildung

Als eine einfache Konsequenz der Sätze 4.1.21, 4.1.23, 3.4.5 und 3.5.5 ergibt sich der

Satz 4.3.1 *Es gelte $\mathcal{N}(K) = F$ und $|F| > 3$. Dann ist $\mathrm{U}^{\pm}(f)$ 5-spiegelig, i.e. jedes $\pi \in \mathrm{U}^{\pm}(f)$ ist ein Produkt von fünf unitären Involutionen.*

Zum Beweis von 4.3.1 benötigen wir die

Beobachtung 4.3.2 *Es gelte $\mathcal{N}(K) = F$ und $|F| > 3$. Sei $\pi \in \mathrm{U}(f)$ keine Homothetie derart, daß $\mathrm{F}(\pi) = \{0\} = \mathrm{F}_{-1}(\pi)$ und*

($*$) $\deg(\mathrm{mip}(\pi)) > 2$ *oder* $\mathrm{mip}(\pi)(0) \neq -1$

gilt. Dann gibt es einen anisotropen Vektor $v \in V$ mit $q_\pi(v(\pi - 1)) \in F^*$.

Beweis: Seien s, d die in 3.2.3 auf $\mathrm{B}(\pi) = V$ definierten hermiteschen Formen. Wir setzen

$$g := \begin{cases} d & \text{, falls char}(K) \neq 2 \text{ ist,} \\ s & \text{, falls char}(K) = 2 \text{ ist,} \end{cases} \quad \text{und } h := \begin{cases} s & \text{, falls char}(K) \neq 2 \text{ ist,} \\ d & \text{, falls char}(K) = 2 \text{ ist.} \end{cases}$$

Nach Voraussetzung gehört $\phi := (\pi - 1)$ zu $\mathrm{GL}(V)$. Also ist $t := f \circ (\phi^{-1} \times \phi^{-1})$ eine wohldefinierte $^{-}$-hermitesche Form auf V. Annahme: Für alle $v \in V$ folgt aus $g(v, v)$ bereits $h(v, v) = 0$ oder $t(v, v) = 0$. Wegen $|F| > 3$ ergibt 3.1.6:

(a) $g(v, v) = 0$ impliziert $h(v, v) = 0$ für alle $v \in V$

oder

(b) $g(v, v) = 0$ impliziert $t(v, v) = 0$ für alle $v \in V$.

Aus g-rad $V = \mathrm{F}_{-1}(\pi) = \{0\}$ (cf.3.2.3), $\dim V \geq 2$ und $\mathcal{N}(K) = F$ schließen wir, daß V eine g-hyperbolische Ebene enthält. Lemma 3.1.2 zeigt nun, daß $h \in Fg$ oder $t \in Fg$ gilt. Weil π nach Voraussetzung keine Homothetie ist, folgt $h \notin Fg$ aus 3.2.3 und 3.2.4. Somit erhalten wir $t = \lambda g$ für ein $\lambda \in F^*$ (,da $t \neq 0$). Hieraus berechnet man

$$\begin{aligned} f(v\pi, w\pi) &= f(v,w) = \lambda g(v(\pi-1), w(\pi-1)) \\ &= \begin{cases} \lambda i f(v\pi, w(\pi^2-1)) & \text{, falls char}(K) \neq 2 \text{ ist,} \\ \lambda f(v\pi, w(\pi^2+1)) & \text{, falls char}(K) = 2 \text{ ist.} \end{cases} \end{aligned}$$

Aus der Regularität von f folgert man hieraus, daß mip(π) entweder $x^2 + (\lambda i)^{-1}x - 1$ (char(K) $\neq 2$) oder $x^2 + \lambda^{-1}x + 1$ (char(K) $= 2$) teilt. In jedem Fall ist dies ein Widerspruch zu $(*)$.

Es gibt daher ein $a \in V$ mit $g(a,a) = 0$ und $h(a,a) \neq 0 \neq t(a,a)$. Der Vektor $v := a\phi^{-1}$ hat dann die gewünschten Eigenschaften. ■

Wir beweisen nun 4.3.1.

Ist π eine Homothetie so ist π nach 4.1.21 ein Produkt von vier unitären Involutionen, da V wegen $\mathcal{N}(K) = F$ eine Orthonormalbasis besitzt. Wir können daher diesen Fall außer Acht lassen. Seien $U := \ker(\pi^2-1)^\infty$ und $W := V(\pi^2-1)^\infty$. Dann gilt $V = U \bigoplus W$, mip(π_U) hat nur Teiler der Form $(x \pm 1)^j$, $j \in \mathbb{N} \cup \{0\}$, und es ist $\mathrm{F}(\pi_W) = \{0\} = \mathrm{F}_{-1}(\pi_W)$. Nach 4.2.10 (ii) ist π_U ein Produkt von vier unitären Involutionen aus $\mathrm{U}(f_U)$, so daß wir $U = \{0\}$ annehmen können.
Fall A. deg(mip(π)) > 2 oder mip(π)(0) $\neq \pm 1$. Sei $\delta := -\det \pi \in \{\pm 1\}$. Dann sind die Voraussetzungen von 4.3.2 für $\delta\pi$ erfüllt. Wir finden deshalb einen anisotropen Vektor $v \in V$, so daß $q_\pi(v(\pi-1))$ in F^* liegt. Nach 3.2.2 (a) gibt es dann eine Symmetrie σ, so daß $\langle v \rangle = \mathrm{F}_\delta(\pi\sigma)$ ist. Sei $\psi := \pi\sigma$. Dann ist $\psi = \psi_{\langle v \rangle} \bigoplus \psi_{v^\perp}$ und $\det \psi_{v^\perp} = 1$. Nach 4.1.23 ist $\psi_{v^\perp}$ ein Produkt von vier unitären Involutionen aus $\mathrm{U}(f_{v^\perp})$. Hieraus folgt nun unmittelbar, daß auch ψ ein Produkt von vier unitären Involutionen ist. Also ist $\pi = \psi\sigma$ ein Produkt von fünf unitären Involutionen.

Fall B. deg(mip(π)) $= 2$ und mip(π)(0) $\in \{\pm 1\}$. Wir können dann $V = (\bigoplus_{i \in I} C_i) \bigoplus D$ als orthogonale Summe von π-Moduln C_i und D schreiben, so daß mip(π_{C_i}) $=$ mip(π) und π_D eine Homothetie ist. Nach 3.4.5 (a) und 3.5.5 (a) ist π_{W_i} ein Produkt von höchstens drei Symmetrien. Wegen $\det \pi_D = \pm 1$ ist π_D nach 4.1.21 ein Produkt von vier Involutionen aus $\mathrm{U}(f_D)$, da D wegen $\mathcal{N}(K) = F$ eine Orthonormallbasis besitzt. Orthogonales Zusammensetzen ergibt nun, daß π ein Produkt von vier unitären Involutionen ist. ■

4.4 Algebraisch abgeschlossene Körper

Radjavi [59] hat für den Fall $K = \mathbb{C}$ und anisotropes f gezeigt, daß jede unitäre Transformation mit Determinante ± 1 ein Produkt von vier unitären Involutionen ist (cf. 4.1.21). Bekanntlich gibt es in diesem Fall zu jeder unitären Transformation π eine Orthogonalbasis, die aus Eigenvektoren von π besteht. Im allgemeinen Fall werden Abbildungen mit dieser Eigenschaft Quasi-Involutionen

genannt.
Als Hauptergebnis der folgenden Untersuchungen erhält man, daß jede unitäre Transformation mit Determinante ± 1 ein Produkt von fünf und in Analogie zu obigem Spezialfall jede Quasi-Involution mit Determinante ± 1, welche keine Homothetie ist, ein Produkt von vier unitären Involutionen ist, vorausgesetzt K ist algebraisch abgeschlossen. Weiterhin zeigen wir unter dieser Voraussetzung, daß $\mathrm{U}^{\pm}(f)$ genau dann 4-spiegelig ist, wenn f anisotrop ist.

4.4.1 Artins Charakterisierung reell abgeschlossener Körper und der Trägheitssatz von Sylvester für hermitesche Formen

Definition 4.4.1 *Ein Körper heißt formal reell, wenn -1 nicht Summe von Quadraten ist. Ein Körper heißt reell abgeschlossen, wenn er formal reell, und jede nichttriviale algebraische Körpererweiterung algebraisch abgeschlossen ist.*

Satz 4.4.2 *Jeder reell abgeschlossene Körper R besitzt genau einen Positivbereich, nämlich die Menge R^2 aller Quadrate von R.*

Beweis. Siehe [53] Teil 2, S.8, F5.

Satz 4.4.3 (Artin) *Sei C ein algebraisch abgeschlossener Körper und R ein echter Teilkörper von C , so daß C eine endliche Körpererweiterung von R ist. Dann ist R reell abgeschlossen und es gilt $C = R(\iota)$ für ein $\iota \in K$ mit $\iota^2 + 1 = 0$.*

Beweis : Siehe [53] Teil 2, S.10, Satz 8.

Korollar 4.4.4 *Ist K algebraisch abgeschlossen, so ist F reell abgeschlossen und es gibt ein $\iota \in K$ mit $\iota^2 + 1 = 0$ und $\bar{\iota} = -\iota$. Weiterhin besitzt F genau eine Ordnung $\leq$, die durch $a \leq b \leftrightarrow_{def} b - a \in F^2$ definiert ist.*

Satz 4.4.5 (Trägheitssatz von Sylvester für hermitesche Formen) *Es sei $(F, \leq)$ ein geordneter Körper und es gelte $K = F(\iota)$ für ein $\iota \in K$ mit $\iota^2 < 0$. Seien $(v_1, \ldots, v_n)$ und $(w_1, \ldots, w_n)$ Orthogonalbasen von V. Dann gilt*

$$p := |\{i \in \mathbb{N}_{\leq n}; f(v_i, v_i) > 0\}| = |\{i \in \mathbb{N}_{\leq n}; f(w_i, w_i) > 0\}|$$

und

$$q := |\{i \in \mathbb{N}_{\leq n}; f(v_i, v_i) < 0\}| = |\{i \in \mathbb{N}_{\leq n}; f(w_i, w_i) < 0\}|.$$

Die Zahl $\mathrm{sgn}(f) := p - q$ *heißt die Signatur von f.*

Beweis. [64], S.351, Beispiel 1.6. (iii).

Bemerkung 4.4.6 *In der Situation von* 4.4.5 *ist f durch die dort definierten Größen p und q eindeutig bestimmt. In diesem Fall wird deshalb* $\mathrm{U}(f)$ *auch mit* $\mathrm{U}(p, q)$ *bezeichnet.*
Die Voraussetzungen von 4.4.5 sind insbesondere dann erfüllt, wenn K algebraisch abgeschlossen ist (cf.4.4.4).

4.4.2 $\mathrm{U}^{\pm}(p,q)$ ist 5-spiegelig

Lemma 4.4.7 *Seien K algebraisch abgeschlossen und $\pi \in \mathrm{U}(p,q)$. Dann gibt es eine unitäre Involution σ derart, daß $V = H \bigoplus W$ für $\pi\sigma$-Moduln H und W mit folgenden Eigenschaften gilt:*

- $\mathrm{B}(\sigma) \leq W$ *und* $H \leq F(\sigma)$*:*
- *Falls* $\dim W > 1$ *ist, ist* $(\pi\sigma)_W$ *eine Quasi-Involution und keine Homothetie;*
- *Falls* $H \neq \{0\}$ *ist, ist* H *ein hyperbolischer Raum und* $(\pi\sigma)_H = \pi_H$ *keine Homothetie.*

Beweis. Sei

$$V = (\bigoplus{}_{i\in I} H_i) \bigoplus (\bigoplus{}_{j\in J} W_j)$$

eine Zerlegung von V in orthogonal unzerlegbare π-Moduln H_i, W_j derart, daß $\dim H_i$ gerade und $\dim W_j$ ungerade ist für alle $(i,j) \in I \times J$. Falls $I \neq \emptyset$ ist, ist $H := \bigoplus H_i$ ein hyperbolischer Raum und π_H keine Homothetie. Sei $W := \bigoplus{}_{j\in J} W_j$. Falls $\dim W \leq 1$ oder π_W eine Quasi-Involution und keine Homothetie ist, wähle $\sigma := 1$. Falls $\dim W \geq 2$ und π_W eine Homothetie ist, wähle eine beliebige Symmetrie σ mit $\mathrm{B}(\sigma) \leq W$. Dann ist $(\pi\sigma)_W$ eine Quasi-Involution und keine Homothetie. Falls $\dim W \geq 2$ und π_W keine Quasi-Involution ist, gibt es zu jedem $j \in J$ ein $t_j \in \mathbb{N}$ und $\lambda_j \in K^*$ mit $\lambda_j\bar{\lambda_j} = 1$ und $\mathrm{mip}(\pi_{W_j}) = (x-\lambda_j)^{2t_j-1}$. Folglich gilt $\mathrm{mip}(\overline{\lambda_j}\pi_{W_j}) = (x-1)^{2t_j-1}$ und W_j ist ein orthogonal unzerlegbarer $\overline{\lambda_j}\pi$-Modul vom Typ III. Nach 2.2.3 (i) gilt $(\overline{\lambda_j}\pi)_{W_j} = \rho_j\sigma_j$ für unitäre Involutionen $\rho_j, \sigma_j \in \mathrm{U}(f_{W_j})$, die im Fall $t_j > 1$ ungleich $\pm 1_{W_j}$ sind. Folglich ist $\pi_{W_j}\sigma_j = \lambda_j\rho_j$ eine Quasi-Involution und keine Homothetie, falls $t_j > 1$ ist. Orthogonales Zusammensetzen liefert die Involutionen $\sigma := \bigoplus{}_{j\in J}\sigma_j \in \mathrm{U}(f_W)$ und die Quasi-Involution $\eta := \bigoplus{}_{j\in J}\lambda_j\rho_j$, die keine Homothetie ist, da mindestens ein $t_j > 1$ ist, und die $\pi_W\sigma = \eta$ erfüllt. ∎

Lemma 4.4.8 *Seien $|F| \geq 9$, V ein hyperbolischer Raum und $\pi \in \mathrm{U}(f)\backslash\mathrm{SU}(f)$. Falls* $\dim V > 2$ *ist, sei π keine Homothetie. Dann gibt es unitäre Involutionen $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ derart, daß für $\phi := \sigma_4\sigma_3\sigma_2\sigma_1\pi$ gilt :* $\det\phi = \det\pi$ *und* $\mathrm{B}(\phi) \leq \mathrm{F}(\sigma_3) \cap \mathrm{F}(\sigma_4)$ *ist eine hyperbolische Ebene und ein orthogonal unzerlegbarer ϕ-Modul vom Typ I.*

Beweis. Sei $m := \frac{\dim V}{2}$. Wähle gemäß 4.1.13 eine Basis $\mathcal{B}$ von V, so daß (4.1.4) für ein $A \in \mathrm{GL}_m(K)$, das im Fall $m > 1$ keine Homothetie ist, und geeignete $B, C, D \in K^{m\times m}$ gilt. Setze $d := \det A$. Nach 4.1.7 und wegen $\det\pi \neq 1$ folgt $d \notin F$. Wegen $|F| \geq 9$ gibt es ein $a, b \in F^*$ mit $a^2 \neq 1$ und $b^2 \notin \{1, a^2, d\bar{d}\}$. Setze $p := (x-a)^{m-1}(x-b)$ und $q := (x-a^{-1})^{m-1}(x-b^{-1}d)$. Die Polynome p und q erfüllen die Voraussetzungen von 4.1.17, und es gilt $\gcd(p,p^*) = 1 = \gcd(q,q^*)$. Folglich gibt es zyklische unitäre Transformationen ϕ und ψ mit

$$\mathrm{mip}(\phi) = pp^* = (x-a)^m(x-a^{-1})^m$$

und

$$\mathrm{mip}(\psi) = (x-a)^{m-1}(x-a^{-1})^{m-1}(x-a^{-1}d)(x-a\bar{d}^{-1}),$$

deren Produkt π ist. Setzt man

$$W := \ker(\psi-a)^{m-1}(\psi-a^{-1})^{m-1} \text{ und } H := (\psi-a^{-1}d)(\psi-a\bar{d}^{-1}),$$

so gilt $V = W \textcircled{\perp} H$, $\dim H = 2$, und ψ_W ist zyklisch mit Minimalpolynom $(x-a)^{m-1}(x-a^{-1})^{m-1}$. Wegen $a^2 \neq d\bar{d}$ ist ψ_H vom Typ I mit $\det \psi_H = d\bar{d}^{-1} = \det \pi$ und damit H insbesondere eine hyperbolische Ebene. Weil sowohl ϕ als auch ψ_W zyklisch sind und symmetrische Minimalpoynome besitzen, die keine $^{-}$-symmetrischen Primteiler haben, gibt es nach 2.3.2 Involutionen $\sigma_1, \sigma_2 \in \mathrm{U}(f)$ und $\sigma_3', \sigma_4' \in \mathrm{U}(f_W)$ so, daß $\phi = \sigma_1\sigma_2$ und $\psi_W = \sigma_3'\sigma_4'$ ist. Setzt man $\sigma_i := \sigma_i' \textcircled{\perp} 1_H$, $i \in \{3, 4\}$, so hat $\sigma_4 \cdots \sigma_1 \pi = \psi_H \textcircled{\perp} 1_W$ die gewünschten Eigenschaften. ■

Lemma 4.4.9 *Seien V eine hyperbolische Ebene und $\pi \in \mathrm{U}(f)$ mit $\det(\pi) \neq -1$ derart, daß V ein orthogonal unzerlegbarer π-Modul vom Typ I ist. Sei ferner $\epsilon \in \{\pm 1\}$. Dann gibt es eine Symmetrie σ und eine Quasi-Symmetrie η mit $f(a, a) \in \epsilon\mathcal{N}(K)$ für $a \in \mathrm{B}(\eta)$ und $\pi = \sigma\eta$.*

Beweis. Es gilt $\mathrm{mip}(\pi) = (x - \alpha)(x - \bar{\alpha}^{-1})$ für ein $\alpha \in K^*$ mit $\bar{\alpha}^{-1} \neq \alpha$ und $V = \ker(\pi - \alpha) \oplus \ker(\pi - \bar{\alpha}^{-1})$, wobei $\ker(\pi - \alpha)$ und $\ker(\pi - \bar{\alpha}^{-1})$ totalisotrop sind. Seien $u \in \ker(\pi - \alpha)$ und $v \in \ker(\pi - \bar{\alpha}^{-1})$ mit $f(u, v) = 1$. Wegen $\det \pi \neq -1$ ist $\alpha \neq -\bar{\alpha}$ und somit $y := \alpha + \bar{\alpha} - \alpha^{-1} - \bar{\alpha}^{-1} = (\alpha - \bar{\alpha}^{-1})(\bar{\alpha}\alpha^{-1} + 1) \neq 0$. Für $z := \epsilon(\alpha - \alpha^{-1})y^{-1}$ und $w := zu + v$ gilt $f(w, w) = z + \bar{z} = \epsilon$. Sei ρ die Quasisymmetrie mit $\mathrm{B}(\rho) = \langle w \rangle$ und $\det \rho = -\det \pi$. Dann gilt:

$$\begin{aligned}
\mathrm{trace}(\pi\rho^{-1}) &= \mathrm{trace}(\pi) + \frac{f(w\pi, w)}{f(w, w)}(\det \rho^{-1} - 1) \\
&= \alpha + \bar{\alpha}^{-1} - \epsilon(z\alpha + \bar{z}\bar{\alpha}^{-1})(\bar{\alpha}\alpha^{-1} + 1) \\
&= \alpha + \bar{\alpha}^{-1} - \epsilon(z\alpha + (\epsilon - z)\bar{\alpha}^{-1})(\bar{\alpha}\alpha^{-1} + 1) \\
&= \alpha - \bar{\alpha}^{-1} - \epsilon z(\alpha - \bar{\alpha}^{-1})(\bar{\alpha}\alpha^{-1} + 1) = 0
\end{aligned}$$

Wegen $\det \pi\rho^{-1} = -1$ ist $\pi\rho^{-1}$ eine Symmetrie. ■

Bemerkung 4.4.10 *Ist $(L, \leq)$ ein geordneter Körper, so gibt es zu jedem normierten Polynom $p \in L[x]$, dessen Grad $\neq 0$ ist, ein $z \in L_{\geq 1}$ mit $p(z) > 0$.*

Beweis. Für $a \in L$ sei

$$|a| := \begin{cases} a & \text{, falls } a \geq 0 \text{ ist,} \\ -a & \text{, falls } a < 0 \text{ ist.} \end{cases}$$

Sei $p = x^m + p_{m-1}x^{m-1} + \cdots + p_1x + p_0 \in L[x]$ ein normiertes Polynom vom Grad $m \in \mathbb{N}$. Setze $z := 1 + \sum_{i=0}^{m-1} |a_i|$. Dann ist $z \geq 1$ und somit $z^j \leq z^m$ für alle $j \in \mathbb{N}_{\leq m} \cup \{0\}$. Hieraus folgt $p(z) = z^{m-1} + \sum_{i=0}^{m-1}(|a_i|z^{m-1}) + \sum_{i=0}^{m-1} a_i z^i \geq z^{m-1} + \sum_{i=0}^{m-1}(|a_i| + a_i)z^i \geq z^{m-1} \geq 1 > 0$. ■

Das folgende Lemma zeigt, wie in einer hyperbolischen Ebene über einem algebraisch abgeschlossenen Körper das Spektrum einer Quasi-Involution durch Verknüpfung mit einem Zweierprodukt von Symmetrien geändert werden kann.

Lemma 4.4.11 *Seien K algebraisch abgeschlossen, V eine hyperbolische Ebene und $\pi \in \mathrm{U}(f)$ eine Quasi-Involution und keine Homothetie. Seien weiterhin $\alpha, \beta \in K$ mit $\alpha \neq \beta$, $\alpha\bar{\alpha} = 1 = \beta\bar{\beta}$ und $\det \pi = \alpha\beta$. Es gibt dann Symmetrien ρ, σ und eine Orthogonalbasis (v, w) von V mit $f(v, v) = 1 = -f(w, w)$, $v\pi\sigma = \alpha v$ und $w\pi\sigma = \beta w$.*

Beweis. Seien ζ, ξ die zwei verschiedenen Eigenwerte von π und a, b zugehörige Eigenvektoren mit $f(a,a) = 1 = -f(b,b)$. Seien $\mu, \nu \in K$ derart, daß $v := \mu a + \nu b$ den Formwert $f(v,v) = \mu\bar{\mu} - \nu\bar{\nu} = 1$ hat. Setzt man $w := \bar{\nu} a + \bar{\mu} b$, so gilt $f(w,w) = \bar{\nu}\nu - \bar{\mu}\mu = -1$ und $f(v,w) = \mu\nu - \nu\mu = 0$. Seien ρ, η die Quasi-Symmetrien mit $\mathrm{B}(\rho) = \langle v \rangle$, $\det \rho = \alpha$, $\mathrm{B}(\eta) = \langle w \rangle$ und $\det \eta = \beta$. Man berechnet

$$
\begin{aligned}
\operatorname{trace}(\pi\rho^{-1}\eta^{-1}) &= \operatorname{trace}(\pi) + \frac{f(v\pi, v)}{f(v,v)}(\bar{\alpha} - 1) + \frac{f(w\pi, w)}{f(w,w)}(\bar{\beta} - 1) \\
&= (\zeta + \xi) + (\zeta\mu\bar{\mu} - \xi\nu\bar{\nu})(\bar{\alpha} - 1) - (\zeta\nu\bar{\nu} - \xi\mu\bar{\mu})(\bar{\beta} - 1) \\
&= (\zeta + \xi) + (\zeta\mu\bar{\mu} + \xi(1 - \mu\bar{\mu}))(\bar{\alpha} - 1) + (\zeta(1 - \mu\bar{\mu}) + \xi\mu\bar{\mu})(\bar{\beta} - 1) \\
&= (\zeta + \xi) + \xi(\bar{\alpha} - 1) + \zeta(\bar{\beta} - 1) + \mu\bar{\mu}(\zeta - \xi)(\bar{\alpha} - \bar{\beta}) \\
&= \xi\bar{\alpha} + \zeta\bar{\beta} + \nu\bar{\nu}(\zeta - \xi)(\bar{\alpha} - \bar{\beta}).
\end{aligned}
$$

Wegen $c := \xi\bar{\alpha} + \zeta\bar{\beta} = \xi\bar{\alpha} + \bar{\xi}\alpha \in F$ und $d := (\zeta - \xi)(\bar{\alpha} - \bar{\beta}) = \zeta\bar{\alpha} + \bar{\zeta}\alpha - c \in F^*$ ist $s := dx^2 + c$ ein Element von $F[x]$. Nach 4.4.10 gibt es ein $z \in F_{\geq 1}$, so daß $(s(z)^2 - 4)d^{-2} > 0$ ist, i.e. $s(z)^2 > 4$. Weil dann $z^2 - 1 \in F_{\geq 0} = F^2$ gilt, gibt es ein $y \in F$ mit $z^2 - y^2 = 1$. Man kann daher $\mu = z$ und $\nu = y$ wählen und erhält $(\operatorname{trace}(\pi\rho^{-1}\eta^{-1}))^2 > 4$. Hieraus folgt, daß V ein orthogonal unzerlegbarer $\pi\rho^{-1}\eta^{-1}$-Modul vom Typ I ist, denn sonst würde für $\kappa := \pi\rho^{-1}\eta^{-1}$ bereits $\operatorname{char}(\kappa) = (x - \gamma)(x - \bar{\gamma})$ für ein $\gamma \in K$ mit $\gamma\bar{\gamma} = 1$ gelten. Für ι wie in 4.4.4 und $g, h \in F$ mit $\gamma = g + \iota h$ berechnet man $1 = \gamma\bar{\gamma} = g^2 + h^2$ und

$$
\operatorname{trace}(\kappa)^2 = (\gamma + \bar{\gamma})^2 = \gamma^2 + \bar{\gamma}^2 + 2 = 2(g^2 - h^2) + 2 \leq 2(g^2 + h^2) + 2 \leq 4,
$$

ein Widerspruch. Wegen $\det \kappa = 1 \neq -1$ ist κ nach 4.4.9 ein Produkt von zwei unitären Symmetrien. ∎

Definition 4.4.12 *Es seien die Voraussetzungen von 4.4.5 erfüllt. Seien* $\pi \in \mathrm{U}(p,q)$ *und* α *ein Eigenwert von* π *zum Eigenvektor* v. *Nenne* α *einen Form-positiven (Form-negativen) Eigenwert von* π, *falls* $f(v,v) > 0$ ($f(v,v) < 0$) *ist. [Beachte, daß* α *sowohl ein Form-positiver als auch ein Form-negativer Eigenwert von* π *sein kann.] Es seien*

$$
\begin{aligned}
\operatorname{spec}^+(\pi) &:= \{\beta \in K; \beta \text{ ist ein Form-positiver Eigenwert von } \pi\}, \\
\operatorname{spec}^-(\pi) &:= \{\beta \in K; \beta \text{ ist ein Form-negativer Eigenwert von } \pi\}, \\
n_\alpha^+ &:= \dim\langle w; w\pi = \alpha w, f(w,w) > 0\rangle, \\
n_\alpha^- &:= \dim\langle w; w\pi = \alpha w, f(w,w) < 0\rangle.
\end{aligned}
$$

Lemma 4.4.13 *Seien* K *algebraisch abgeschlossen und* $v \in V$ *anisotrop. Falls* $W := \langle v \rangle^\perp$ *anisotrop ist, sei auch* V *anisotrop. Weiterhin sei* $\pi \in \mathrm{U}^\pm(p,q)$ *eine Quasi-Involution mit folgenden Eigenschaften :*

(i) $v\pi = \alpha v$ *für ein* $\alpha \in K \backslash \{\pm 1\}$

(ii) *Falls* W *isotrop ist, sei* π_W *keine Homothetie, i.e. es gibt* $(\xi, \zeta) \in \operatorname{spec}^+(\pi) \times \operatorname{spec}^-(\pi)$ *mit* $\xi \neq \zeta$. *In diesem Fall gelte*

$$
f(v,v) = \begin{cases} 1 & , \textit{falls } \alpha\xi^{-1} \prod_{\beta \in \operatorname{spec}^+(\pi_W)} \beta^{n_\beta^+} \neq \det \pi \zeta^{-1} \prod_{\beta \in \operatorname{spec}^-(\pi_W)} \beta^{n_\beta^-} \textit{ ist,} \\ -1 & \textit{sonst.} \end{cases}
$$

Dann gibt es unitäre Involutionen $\iota_1, \iota_2, \iota_3, \iota_4$ derat, daß $v \in \mathrm{F}(\iota_1) \cap \mathrm{F}(\iota_2)$ und $\pi = \iota_1\iota_2\iota_3\iota_4$ ist.

Beweis. Fall A : W ist anisotrop. Seien $(e_1, \dots, e_n)$ eine Orthogonalbasis von V mit $e_1 = v$ und $\alpha_1, \dots, \alpha_n \in K$, so daß $\epsilon := f(e_1, e_1) = f(e_i, e_i)$ und $e_i\pi = \alpha_i e_i$ für alle $i \in \mathbb{N}_{\leq n}$ gilt. Insbesondere ist dann $\alpha_1 = \alpha$. Definiert man $\beta_i, \gamma_i, \beta, \gamma, \iota_1, \dots, \iota_4$ wie im Beweis von 4.1.21, so gilt $\pi = \beta\gamma$, $\beta = \iota_1\iota_2$, $\mathrm{B}(\iota_1), \mathrm{B}(\iota_2) \leq \mathrm{B}(\beta)$, $\gamma = \iota_3\iota_4$ und $\mathrm{B}(\iota_3), \mathrm{B}(\iota_4) \leq \mathrm{B}(\gamma)$. Wegen $\beta_1 = 1$ erhält man $\langle v \rangle = \langle e_1 \rangle \leq \mathrm{F}(\beta) \leq \mathrm{F}(\iota_1) \cap \mathrm{F}(\iota_2)$.

Fall B: W ist isotrop. Seien ζ, ξ wie in (ii) und $d := \det \pi$.

Fall B1: $f(v, v) = 1$. Seien $(e_1, \dots, e_n)$ eine Orthogonalbasis von V und $\alpha_1, \dots \alpha_n \in K$ mit $\langle v \rangle = \langle e_1 \rangle$,

$$f(e_i, e_i) = \begin{cases} 1 & \text{falls } i \leq p \text{ ist,} \\ -1 & \text{sonst,} \end{cases},$$

$e_i\pi = \alpha_i e_i$ und $\alpha_p = \xi \neq \zeta = \alpha_{p+1}$. Für $i \in N_{\leq p-1}$ seien

$$\beta_i := \begin{cases} \prod_{k=1}^{i-1} \bar{\alpha_k} & \text{, falls } i \text{ ungerade ist,} \\ \prod_{k=1}^{i} \alpha_k & \text{, falls } i \text{ gerade ist} \end{cases} \quad \textit{und } \gamma_i := \begin{cases} \prod_{k=1}^{i} \alpha_k & \text{, falls } i \text{ ungerade ist,} \\ \prod_{k=1}^{i-1} \bar{\alpha_k} & \text{, falls } i \text{ gerade ist.} \end{cases}$$

Falls $q \geq 2$ ist, definiere für $i \in \mathbb{N}_{\leq q-1}$

$$\delta_{p+1+i} := \begin{cases} d\prod_{k=p+2}^{p+i} \bar{\alpha_k} & \text{, falls } i \text{ ungerade ist,} \\ \prod_{k=p+2}^{p+1+i} \alpha_k & \text{, falls } i \text{ gerade ist,} \end{cases} \quad \textit{und } \omega_{p+1+i} := \begin{cases} \prod_{k=p+2}^{p+1+i} \alpha_k & \text{, falls } i \text{ ungerade ist,} \\ \prod_{k=p+2}^{p+i} \bar{\alpha_k} & \text{, falls } i \text{ gerade ist.} \end{cases}$$

Dann gilt $\beta_i\gamma_i = \alpha_i$ für alle $i \in \mathbb{N}_{\leq p-1}$ und $\delta_j\omega_j = \alpha_j$ für alle $j \in \{p+2, \dots, n\}$. Setze $\beta := \bigoplus_{i=1}^{p-1} \beta_i 1_{\langle e_i \rangle}$, $\gamma := \bigoplus_{i=1}^{p-1} \gamma_i 1_{\langle e_i \rangle}$, $\delta := \bigoplus_{i=p+2}^{n} \delta_i 1_{\langle e_i \rangle}$, $\omega := \bigoplus_{i=p+2}^{n} \omega_i 1_{\langle e_i \rangle}$,

$$(\rho, \sigma) := \begin{cases} (\beta, \gamma) & \text{, falls } p-1 \text{ ungerade ist,} \\ (\gamma, \beta) & \text{, falls } p-1 \text{ gerade ist,} \end{cases} \quad \textit{und } (\phi, \psi) := \begin{cases} (\delta, \omega) & \text{falls } q-1 \text{ ungerade ist,} \\ (\omega, \delta) & \text{falls } q-1 \text{ gerade ist,} \end{cases}$$

und $\eta := \sigma \bigoplus \alpha_p 1_{\langle e_p \rangle} \bigoplus \alpha_{p+1} 1_{\langle e_{p+1} \rangle} \bigoplus \psi$. Für $j \in \mathbb{N}_{\leq n}$ sei η_j der Eigenwert von η zum Eigenvektor e_j. Weiterhin seien $\eta_0 := 1$, $\eta_{n+1} := d$ und $m := \max\{p+2, n\}$. Es gilt dann $\eta_{p-1} = \alpha_1 \cdots \alpha_{p-1}$, $\eta_p = \alpha_p = \xi \neq \zeta = \alpha_{p+1} = \eta_{p+1}$ und $\eta_m = d\alpha_{p+2} \cdots \alpha_m$, also $\eta_{p-1} \neq \eta_m$ wegen (ii) und $\overline{\eta_{p-1}\eta_m} = \eta_p\eta_{p+1}$. Nach 4.4.11 gibt es Symmetrien ν_1, ν_2 und eine Orthogonalbasis (e'_p, e'_{p+1}) von $H := \langle e_p, e_{p+1} \rangle$, so daß $\mathrm{B}(\nu_1), \mathrm{B}(\nu_2) \leq H$, $f(e'_p, e'_p) = 1 = -f(e'_{p+1}, e'_{p+1})$, $e'_p\nu_1\nu_2\eta = \overline{\eta_{p-1}}e'_p$ und $e'_{p+1}\nu_1\nu_2\eta = \overline{\eta_m}e'_{p+1}$. Seien $\kappa := \rho \bigoplus (\nu_2\nu_1)_H \bigoplus \phi$, $\eta' := \nu_1\nu_2\eta = \sigma \bigoplus \overline{\eta}_{p-1} 1_{\langle e'_p \rangle} \bigoplus \overline{\eta}_m 1_{\langle e'_{p+1} \rangle}$, $U := \langle e_1, \dots, e_{p-1} \rangle$, $W := \langle e_{p+2}, \dots, e_n \rangle$, $U' := \langle e_1, \dots, e_{p-1}, e'_p \rangle$ und $W' := \langle e'_{p+1}, e_{p+2} \dots, e_n \rangle$. Dann gilt $\pi = \kappa\eta'$ und $\kappa_U, \kappa_W, \eta'_{U'}, \eta'_{W'}$ sind Quasi-Involutionen, welche ähnlich zu ihren Inversen sind. Weil U, W, U', W' anisotrop sind, findet man wie im Fall A unitäre Involutionen $\mu_1, \mu_2 \in \mathrm{U}(f_U)$, $\mu_3, \mu_4 \in \mathrm{U}(f_W)$, $\theta_1, \theta_2 \in \mathrm{U}(f_{U'})$ und $\theta_3, \theta_4 \in \mathrm{U}(f_{W'})$, so daß $\kappa = \mu_1\mu_2$, $\mathrm{B}(\mu_1), \mathrm{B}(\mu_2) \leq \mathrm{B}(\kappa_U)$, $\kappa_W = \mu_3\mu_4$, $\mathrm{B}(\mu_3), \mathrm{B}(\mu_4) \leq \mathrm{B}(\kappa_W)$, $\eta'_{U'} = \theta_1\theta_2$, $\mathrm{B}(\theta_1), \mathrm{B}(\theta_2) \leq \mathrm{B}(\eta'_{U'})$, $\eta'_{W'} = \theta_3\theta_4$ und $\mathrm{B}(\theta_3), \mathrm{B}(\theta_4) \leq \mathrm{B}(\eta'_{W'})$. Orthogonales Zusammensetzen liefert unitäre Involutionen $\iota_1 := \mu_1 \bigoplus (\nu_2)_H \bigoplus \mu_3$, $\iota_2 := \mu_2 \bigoplus (\nu_1)_H \bigoplus \mu_4$, $\iota_3 := \theta_1 \bigoplus \theta_3$ und $\iota_4 := \theta_2 \bigoplus \theta_4$ aus $\mathrm{U}(f)$, für die $\kappa = \iota_1\iota_2$, und $\eta' = \iota_3\iota_4$ gilt. Ist $p-1$ ungerade, so folgt $\langle v \rangle = \langle e_1 \rangle \leq \mathrm{F}(\beta) = \mathrm{F}(\rho) \leq \mathrm{F}(\iota_1) \cap \mathrm{F}(\iota_2)$. Ist $p-1$ gerade, so folgt $\langle v \rangle = \langle e_1 \rangle \leq \mathrm{F}(\beta) = \mathrm{F}(\sigma) \leq \mathrm{F}(\iota_3) \cap \mathrm{F}(\iota_4)$.

Fall B2. f(v,v)=-1. Es ist dann

$$\alpha \prod_{\beta \in \operatorname{spec}^-(\pi_W)} \beta^{n_\beta^-} \zeta^{-1} \neq \det \pi \prod_{\beta \in \operatorname{spec}^+(\pi_W)} \beta^{n_\beta^+} \xi^{-1}, \tag{4.4.9}$$

da sonst

$$\alpha \prod_{\beta \in \operatorname{spec}^-(\pi_W)} \beta^{n_\beta^-} \zeta^{-1} = \det \pi \prod_{\beta \in \operatorname{spec}^+(\pi_W)} \beta^{n_\beta^+} \xi^{-1} = \alpha^{-1} \prod_{\beta \in \operatorname{spec}^-(\pi_W)} \beta^{n_\beta^-} \zeta^{-1}$$

und damit $\alpha = \alpha^{-1}$ gelten würde, im Widerspruch zu (i). Indem man f durch $-f$ ersetzt, erhält man, daß die Situation des Falles B1 vorliegt. ■

Wir handeln nun zunächst den zweidimensionalen Fall ab.

Satz 4.4.14 *Seien K algebraisch abgeschlossen,* $\dim V = 2$ *und* $\pi \in \mathrm{U}^{\pm}(p,q)$ *keine Involution. Ist V anisotrop, so gilt:*

$$\mathrm{l}_I(\pi) = \begin{cases} 2 & , falls \ \det \pi = 1 \ ist, \\ 3 & , falls \ \det \pi = -1 \ ist. \end{cases}$$

Ist V eine hyperbolische Ebene, so gilt:

$$\mathrm{l}_I(\pi) = \begin{cases} 2 & , falls \ \det \pi = 1 \ und \ \pi \ vom \ Typ \ I \ ist, \\ 4 & , falls \ \det \pi = 1 \ und \ \pi \ nicht \ vom \ Typ \ I \ ist, \\ 3 & , falls \ \det \pi = -1 \ und \ \pi \ keine \ Homothetie \ ist, \\ 5 & , falls \ \det \pi = -1 \ und \ \pi \ eine \ Homothetie \ ist. \end{cases}$$

Beweis. Fall A. V ist anisotrop. Seien $\alpha, \beta \in K^*$ die Eigenwerte von π zu Eigenvektoren $u, v \in V$. Weil F^* nur die Normnebenklassen $F_{\geq 0} = F^2$ und $F_{\leq 0} = -F^2$ besitzt und weil f anisotrop ist, kann man o.B.d.A. $f(u,u) = 1 = f(v,v)$ annehmen. Ist $\det \pi = 1$, so gilt $\beta = \bar{\alpha}$. Aus (4.1.8) in 4.1.21 folgt, daß π ein Produkt von zwei unitären Involutionen ist. Ist $\det(\pi) = -1$, wähle eine beliebige Symmetrie σ. Wegen $\det(\pi\sigma) = 1$ ist $\pi\sigma$ nach Obigem ein Produkt von zwei unitären Symmetrien.

Fall B. V ist eine hyperbolische Ebene. Es ist $-1 \notin \mathcal{N}(K) = F_{\geq 0}$. Sei $\pi \in \mathrm{SU}(f)$ nicht vom Typ I. Ist π orthogonal zerlegbar, so folgt $\mathrm{l}_I(\pi) = 4$ aus 4.2.8. Ist π vom Typ III, so gilt $\operatorname{mip}(\pi) = (x + \lambda^2)$ für ein $\lambda \in K^*$, da K algebraisch abgeschlossen ist. Wegen $\lambda^2 = \det \pi = 1$ muß $\lambda = \pm 1$ gelten. Wegen $\operatorname{trace}(\pi)^2 - 4 = 0$ folgt wiederum $\mathrm{l}_I(\pi) = 4$ aus 4.2.8. Die anderen Fälle liest man unmittelbar in 4.2.8 ab. ■

Wir kommen nun zu den Hauptergebnissen.

Satz 4.4.15 *Seien K algebraisch abgeschlossen und $\pi \in \mathrm{U}^{\pm}(p,q)$ eine Quasi-Involution. Falls* $\operatorname{Ind}(V) \geq 1$ *ist, sei π keine Homothetie. Dann ist π ein Produkt von vier unitären Involutionen.*

Beweis. Falls $\dim V = 2$ ist, folgt die Behauptung aus 4.4.14. Man kann daher annehmen, daß $\dim V \geq 3$ und ± 1 kein Eigenwert von π ist. Sei α ein Eigenwert von π und $c := \max\{n_\beta^+, n_\gamma^-; \beta \in$

$\mathrm{spec}^+(\pi), \gamma \in \mathrm{spec}^-(\pi)\}$. Falls $c \geq 2$ ist, kann man, indem man gegebenenfalls f durch $-f$ ersetzt, o.B.d.A. annehmen, daß $c = n_\alpha^+$ ist. Falls $c = 1$ ist, kann man o.B.d.A. annehmen, daß $p \geq q$ und $\alpha \in \mathrm{spec}^+(\pi)$ gilt. Seien v ein Eigenvektor von π zum Eigenwert α mit $f(v,v) = 1$ und $W := \langle v \rangle^\perp$. Wegen $\dim V \geq 3$ gilt $\dim W \geq 2$. Nach Wahl von α sind die Voraussetzungen von 4.4.13 erfüllt. Folglich ist π ein Produkt von vier unitären Involutionen. ■

Satz 4.4.16 *Seien K algebraisch abgeschlossen und $\pi \in \mathrm{U}^\pm(p,q)$. Dann ist π ein Produkt von fünf unitären Involutionen.*

Beweis. Ist $\dim V = 2$, so folgt die Behauptung aus 4.4.14. Man kann daher $\dim V \geq 3$ annehmen. Nach 4.4.7 gibt es eine unitäre Involution σ und Unterräume H, W von V, so daß mit der Abkürzung $\phi := \pi\sigma$ gilt: $H\phi = H$, $W\phi = W$, $V = H \oplus W$, $B(\sigma) \leq W$ und $H \leq \mathrm{F}(\sigma)$. Falls $H \neq \{0\}$ ist, ist H ein hyperbolischer Raum und ϕ_H keine Homothetie. Falls $W \neq \{0\}$ ist, ist ϕ_W eine Quasi-Involution, welche im Fall $\dim W \geq 2$ keine Homothetie ist. Ist $\det \phi_H \in \{\pm 1\}$ oder $\det \phi_W \in \{\pm 1\}$, so ist ϕ_H nach 4.1.23 ein Produkt von fünf unitären Involutionen $\sigma_1, \ldots, \sigma_5 \in \mathrm{U}(f_H)$ und ϕ_W wegen 4.4.15 in jedem Fall ein Produkt von vier unitären Involutionen $\rho_1, \ldots, \rho_4 \in \mathrm{U}(f_W)$. Folglich ist $\pi = (\sigma_1 \oplus \rho_1) \cdots (\sigma_4 \oplus \rho_4)(\sigma_5 \oplus \sigma)$ ein Produkt von fünf unitären Involutionen. Man kann daher o.B.d.A. $\det \phi_H, \det \pi_W \notin \{\pm 1\}$ annehmen. Insbesondere gilt dann $H \neq \{0\} \neq W$. Nach 4.4.8 und 4.4.9 findet man Involutionen $\sigma_1, \ldots, \sigma_4 \in \mathrm{U}(f)$, eine Symmetrie η und eine Quasi-Symmetrie ρ mit $\det \rho = -\det \phi_H \notin \{\pm 1\}$, so daß $\phi_H = \sigma_1 \cdots \sigma_4 \eta \rho$ und $\mathrm{B}(\eta) + \mathrm{B}(\rho)$ ist eine hyperbolische Ebene, die in $\mathrm{F}(\sigma_3) \cap \mathrm{F}(\sigma_4)$ enthalten ist. Dabei läßt sich vorschreiben, ob

$(*)$ $f(v,v) \leq 0$ oder $f(v,v) \geq 0$ für alle $v \in \mathrm{B}(\rho)$

gelten soll. Setze $\zeta := \rho_{\mathrm{B}(\rho)} \oplus \phi_W \in \mathrm{U}(f_{\mathrm{B}(\rho) \oplus W})$. Bei geeigneter Wahl der Diskriminante von $f_{B(\rho)}$ (cf. $(*)$) findet man ein $v \in \mathrm{B}(\rho)$ derart, daß die Vorausetzungen von 4.4.13 für $V' := \langle v \rangle \oplus W$ anstelle von V, ζ anstelle von π und $\det \rho$ anstelle von α erfüllt sind. Man findet daher Involutionen $\kappa_1, \ldots, \kappa_4 \in U(f_{V'})$ derart, daß $\mathrm{B}(\kappa_1), \mathrm{B}(\kappa_2) \leq W$ und $\zeta = \kappa_1 \cdots \kappa_4$ gilt. Setzt man $Z := V'^\perp$, so folgt:

$$\begin{aligned}
\pi\sigma &= \phi_H \oplus \phi_W = (\sigma_1\sigma_2\sigma_3\sigma_4\eta\rho) \oplus \phi_W \\
&= ((\sigma_1\sigma_2\sigma_3\sigma_4\eta) \oplus 1_W)(\rho \oplus \phi_W) \\
&= ((\sigma_1\sigma_2\sigma_3\sigma_4\eta) \oplus 1_W)(1_Z \oplus \rho_{\mathrm{B}(\rho)} \oplus \phi_W) \\
&= ((\sigma_1\sigma_2\sigma_3\sigma_4\eta) \oplus 1_W)(1_Z \oplus \zeta) \\
&= ((\sigma_1\sigma_2\sigma_3\sigma_4\eta) \oplus 1_W)(1_Z \oplus (\kappa_1\kappa_2\kappa_3\kappa_4)) \\
&= (\sigma_1 \oplus (\kappa_1)_W)(\sigma_2 \oplus (\kappa_2)_W)(\eta \oplus 1_W)((\sigma_3)_Z \oplus \kappa_3)((\sigma_4)_Z \oplus \kappa_4).
\end{aligned}$$

Weil $\iota_1 := (\sigma_1 \oplus (\kappa_1)_W)$, $\iota_2 := (\sigma_2 \oplus (\kappa_2)_W)$, $\iota_3 := \eta \oplus \sigma_W$, $\iota_4 := (\sigma_3)_Z \oplus \kappa_3$ und $\iota_5 := (\sigma_4)_Z \oplus \kappa_4$ unitäre Involutionen sind, ist $\pi = \iota_1\iota_2\iota_3\iota_4^\sigma\iota_5^\sigma$ ein Produkt von fünf unitären Involutionen. ■

Abschließend zeigen wir nun, daß $\mathrm{U}^\pm(p,q)$ genau dann vierspiegelig ist, wenn f anisotrop ist, i.e. $p = 0$ oder $q = 0$ gilt.

Beispiel 4.4.17 *Sei K ein algebraisch abgeschlossener Körper. Sei $\lambda \in K^*$ eine primitive $2n$-te Einheitswurzel (cf. [53] §9, F8). Dann gilt $\lambda\bar{\lambda} = 1$ und die Abbildung $\lambda \cdot 1_V$ ist ein Element von* $\mathrm{U}(p,q)$ *mit Determinante* -1. *Sie ist genau dann ein Produkt von vier unitären Involutionen, wenn f anisotrop ist.*

Beweis. Es gilt $\lambda\bar{\lambda} \in F_{>0}$. Wegen $(\lambda\bar{\lambda})^{2n} = 1$ folgt $\lambda\bar{\lambda} = 1$. Nach 4.4.15 ist nur zu zeigen, daß f anisotrop ist, falls $\lambda 1_V$ ein Produkt von vier unitären Involutionen ist.
Seien $\rho, \sigma, \tau, \omega$ unitäre Involutionen, so daß $\lambda 1_V = \rho\sigma\tau\omega$ ist. Seien weiterhin $\alpha := \rho\sigma$, $\beta := \tau\omega$ und $\phi := \rho\tau \in \mathrm{U}(p,q)$. Man berechnet:

$$\alpha = \lambda\beta^{-1} = (\lambda\beta)^\tau = (\lambda^2\alpha^{-1})^\tau = (\lambda^2\alpha)^{\rho\tau} = (\lambda^2\alpha)^\phi.$$

Hieraus folgt

(1) $\alpha = (\lambda^{2i}\alpha)^{\phi^i}, i \in \mathbb{N}$.

Für jeden Eigenwert a von α und jedes $i \in \mathbb{N}$ ist dann auch $\bar{\lambda}^{2i}a$ ein Eigenwert von α und nach (1) gilt

(2) $\ker(\alpha - a) = \ker((\lambda^{2i}\alpha)^{\phi^i} - a) = (\ker(\alpha - \bar{\lambda}^{2i}a))\phi^i$.

Seien nun $i, j \in \mathbb{N}_{\leq n-1} \cup \{0\}$, so daß $i > j$ ist. Wegen $2(i-j) < 2n$ gilt dann

$$\lambda^{2(i-j)} \neq 1 \Leftrightarrow \bar{\lambda}^{2j}a \neq \bar{\lambda}^{2i}a.$$

Folglich sind alle Polynome $x - \bar{\lambda}^{2i}a$, $i \in \mathbb{N}_{\leq n-1} \cup \{0\}$, paarweise teilerfremd. Dies liefert

$$V = \oplus_{i=0}^{n-1} \ker(\alpha - \bar{\lambda}^{2i}a)$$

und

(3) $\dim\ker(\alpha - \bar{\lambda}^{2i}a) = 1$.

Weil α ähnlich zu seinem Inversen ist, gibt es ein $i \in \mathbb{N}_{\leq n-1} \cup \{0\}$, so daß $a^{-1} = \bar{\lambda}^{2i}a$ ist. Dies liefert $a \in \{\pm\lambda^i\}$. Weil dann insbesondere $a\bar{a} = 1$ ist, folgt

(4) $V = \bigoplus\!\!\!\!\!\!\bigcirc\ {}_{i=0}^{n-1} \ker(\alpha - \bar{\lambda}^{2i}a)$.

Sei nun $v \in \ker(\alpha - a)\backslash\{0\}$. Aus (3) und (4) folgt, daß v anisotrop ist. Aus (2) und (4) erhält man, daß $(v, v\phi^{-1}, \ldots, v\phi^{1-n})$ eine Orthogonalbasis von V mit $f(v,v) = f(v\phi^{-1}, v\phi^{-1}) = \cdots = f(v\phi^{1-n}, v\phi^{1-n})$ ist. Folglich ist f anisotrop. ■

4.5 Quasi-Involutionen

Wir geben zuerst einen Beweis des in der Einleitung erwähnten Ergebnisses von E.W. Ellers [28] an.

Satz 4.5.1 (Ellers) *Sei V anisotrop. Dann ist jedes $\pi \in \mathrm{U}(f)$ ein Produkt von zwei Quasi-Involutionen.*

Beweis. Seien $\pi \in \mathrm{U}(f)$ und $M := \{(\alpha,\beta)|\alpha,\beta$ Quasi-Involutionen mit $(*)\}$, wobei wir die Eigenschaft $(*)$ definieren als: Es gibt eine Quasi-Symmetrie ρ so, daß

(1) $\mathrm{B}(\alpha\pi\beta) \leq \mathrm{F}(\rho\alpha) \cap \mathrm{F}(\beta)$ und $\mathrm{F}(\alpha) \leq \mathrm{F}(\rho\alpha)$, oder

(2) $\mathrm{B}(\alpha\pi\beta) \leq \mathrm{F}(\alpha) \cap \mathrm{F}(\beta\rho)$ und $\mathrm{F}(\beta) \leq \mathrm{F}(\beta\rho)$.

Offenbar ist $M \neq \emptyset$ (wähle $\alpha = \rho^{-1}$ und $\beta = 1_V$). Seien $(\alpha,\beta) \in M$, so daß $\dim \mathrm{B}(\alpha\pi\beta)$ minimal ist. Angenommen $\phi := \alpha\pi\beta \neq 1$. Sei dann ρ die Quasi-Symmetrie, die in $(*)$ auftritt. Man kann o.B.d.A. annehmen, daß α,β,ρ die Bedingung (1) erfüllen (andernfalls gelten analoge Argumente). Ist $\mathrm{B}(\rho) \nsubseteq \mathrm{F}(\phi)$, so wähle $u \in \mathrm{B}(\rho)\backslash\mathrm{F}(\phi)$, andernfalls wähle $u \in V\backslash\mathrm{F}(\phi)$. Weil $a := u(\phi-1)$ anisotrop ist, ist $\sigma : V \to V, v \mapsto v + f(a,u)^{-1}f(v,a)a$ eine Quasi-Symmetrie mit $\mathrm{B}(\sigma) = \langle a\rangle \leq \mathrm{F}(\beta)$ und $\mathrm{B}(\phi\sigma) = \mathrm{B}(\phi)\cap\langle u\rangle^{\perp} \leq \mathrm{F}(\rho\alpha)\cap\mathrm{F}(\rho)\cap\mathrm{F}((\beta\sigma)\sigma^{-1}) = \mathrm{F}(\alpha)\cap\mathrm{F}((\beta\sigma)\sigma^{-1})$. Folglich ist $\beta' := \beta\sigma$ eine Quasi-Involution, $(\alpha,\beta') \in M$ (da $\alpha,\beta',\sigma^{-1}$ (2) erfüllen) und $\dim \mathrm{B}(\alpha\pi\beta') < \dim \mathrm{B}(\alpha\pi\beta)$, ein Widerspruch. ■

Von nun an setzen wir $\mathrm{char}(K) \neq 2$ voraus.

Lemma 4.5.2 (a) *Sind $S,T \leq V$ totalisotrope Unterräume, so daß $S \oplus T$ regulär ist, und gilt $m := \dim S = \dim T$, so gibt es eine Involution $\sigma \in \mathrm{U}(f)$ mit $S\sigma = T$ und $\mathrm{B}(\sigma) \leq S \oplus T$.*
(b) *Seien $A,B \leq V$ maximale totalisotrope Unterräume von V. Dann gilt $A\sigma = B$ für eine Involution $\sigma \in \mathrm{U}(f)$.*

Beweis. (a) Es gibt eine Basis $s_1,\ldots,s_m$ von S und eine Basis $t_1,\ldots,t_m$ von T, so daß

$$f(s_i,t_j) = \begin{cases} 0 & \text{, falls } i \neq j \text{ ist,} \\ 1 & \text{, falls } i = j \text{ ist.} \end{cases}$$

Die Vektoren $t_i - s_i$ sind anisotrop und paarweise orthogonal. Folglich ist der von ihnen erzeugte Unterraum M regulär. Weiterhin gilt $2s_i = (t_i+s_i)-(t_i-s_i)$ und $t_i+s_i \perp t_j - s_j$ für alle i,j. Demnach bildet die Involution $\sigma \in \mathrm{U}(f)$, deren Bahn M ist, s_i auf t_i ab.
(b) Schreibe $A = (A\cap B)\oplus S$ and $B = (A\cap B)\oplus T$. Dann haben S und T die in (a) geforderten Eigenschaften. Es folgt $S\sigma = T$ und $\mathrm{B}(\sigma) \leq S \oplus T$ für eine Involution $\sigma \in \mathrm{U}(f)$. Wegen

$$A\cap B \leq A^{\perp}\cap B^{\perp} = (A+B)^{\perp} \leq (S\oplus T)^{\perp} \leq \mathrm{F}(\sigma)$$

erhalten wir $A\sigma = B$. ■

Lemma 4.5.3 *Seien $\pi \in \mathrm{GL}(V)$ und $a \in K^*$. Für $p := (x-a)(x-\bar{a}^{-1})$gelte*

$$V = \ker p(\pi)^{\infty}.$$

Es gebe einen totalisotropen π-Modul $T \leq \ker p(\pi)$, dessen Dimension mit dem Witt-Index von V übereinstimmt. Falls $a \neq \bar{a}^{-1}$ ist, ist $\mathrm{mip}(\pi)$ ein Teiler von p^2. Falls $a = \bar{a}^{-1}$ ist, ist $\mathrm{mip}(\pi)$ ein Teiler von $(x-a)^5$.

Beweis. Seien $q := \mathrm{lcm}(x-a, x-\bar{a}^{-1})$ und

$$V = \textcircled{\perp}_{i=1}^{m} V_i$$

eine Zerlegung von V in orhtogonal unzerlegbare π-Moduln, $m \in \mathbb{N}$. Für jedes $i \in \mathbb{N}_{\leq m}$ sei $n_i := \deg \operatorname{mip}(\pi_{V_i})$, i.e. $\operatorname{mip}(\pi_{V_i}) = q^{n_i}$. Die V_i seien so angeordnet, daß $n_1 \geq \cdots \geq n_m$ gilt. Seien

$$A := \{v \in V_1 | \text{Es gibt ein } w \in V_1^{\perp} \text{ so, daß } v + w \in T.\}$$

und

$$B := \{w \in V_1^{\perp} | \text{Es gibt ein } v \in V_1 \text{ so, daß } v + w \in T.\}$$

Man sieht leicht, daß A und B π-invariante Unterräume von $V_1 \cap \ker p(\pi)$ bzw. $V_1^{\perp} \cap \ker p(\pi)$ sind und daß $T \leq A \bigoplus B$ gilt.
Angenommen die Konklusion des Lemmas ist falsch. Dann ist $A \subseteq \ker p(\pi) \cap V_1$ totalisotrop. Sei $w \in B$. Es gibt dann ein $v \in V_1^{\perp}$, so daß $v + w \in T$ ist. Folglich ist $v \in A$ und $f(w, w) = f(v + w, v + w) = 0$. Also ist auch B und damit $A \bigoplus B$ totalisotrop. Weil T ein maximaler totalisotroper Unterraum ist, impliziert dies $T = A \bigoplus B$.
Falls $a \neq \bar{a}^{-1}$ ist, setze $C := \ker(\pi - a)^{n_1} \cap V_1$. Dann ist C ein totalisotroper Unterraum mit

$$\dim C = n_1 \geq 3 > 2 = \dim \ker p(\pi) \cap V_1 \geq \dim A.$$

Falls $a = \bar{a}^{-1}$ ist, wähle $\frac{n_1}{2} \leq s < \frac{n_1}{2} + 1$ und setze $C := V_1(\pi - a)^s$. Wegen $n_1 \geq 6$ gilt $\frac{n_1}{2} + 3 \leq n_1$, i.e. $s + 2 < n_1$. Demnach ist $\ker p(\pi) \cap V_1$ und damit A echt in dem totalisotropen Unterraum C enthalten.
Folglich ist $C \bigoplus B$ in jedem Fall ein totalisotroper Unterraum, dessen Dimension größer als die von T ist, ein Widerspruch. ∎

Bemerkung 4.5.4 *Sei $H \leq V$ ein nichttrivialer totalisotroper Unterraum von V. Jedes $\alpha \in \mathrm{GL}(H)$ läßt sich zu einer Isometrie $\hat{\alpha} \in \mathrm{U}(f)$ fortsetzen, so daß $\operatorname{mip}(\hat{\alpha})$ ein Teiler von*

$$\operatorname{lcm}((x-1), \operatorname{mip}(\alpha), \operatorname{mip}(\alpha)^*)$$

ist. Falls α eine Involution ist, trifft dies damit auch auf $\hat{\alpha}$ zu.

Beweis: Wähle einen totalisotropen Unterraum L von V so, daß $L \oplus H$ regulär ist und setze $Z := (L \oplus H)^{\perp}$. Nach 1.3.5 gibt es eine Fortsetzung $\alpha' \in \mathrm{U}(f_{L \oplus H})$ von α so, daß $\operatorname{mip}(\alpha') = \operatorname{lcm}(\operatorname{mip}(\alpha), \operatorname{mip}(\alpha)^*)$ ist. Die Isometrie $\hat{\alpha} := \alpha' \bigoplus 1_Z$ hat dann die gewünschten Eigenschaften. ∎

Als nächstes betrachten wir unitäre Transformationen mit kleiner Bahn.

Lemma 4.5.5 *Sei $\pi \in \mathrm{U}(f)$.*

(a) *Falls $\dim \mathrm{B}(\pi) \leq 2$ und $\mathrm{B}(\pi)$ nicht totalisotrop ist, so ist π ein Produkt von zwei Quasi-Symmetrien.*

(b) *Ist V ein orthogonal unzerlegbarer π-Modul mit $\operatorname{mip}(\pi) = (x + \epsilon)^k$, wobei $\epsilon \in \{\pm 1\}$ sei, und ist $1 \leq k \leq 5$, so ist π ein Produkt von zwei Quasi-Involutionen.*

Beweis. Behauptung (a) ist ein Spezialfall von Dieudonnés Ergebnis, welches besagt, daß im Fall $\mathrm{char}(K) \neq 2$ jedes $\pi \in \mathrm{U}(f)$, dessen Bahn nicht totalisotrop ist, ein Produkt von $\dim \mathrm{B}(\pi)$ Quasi-Symmetrien ist.

(b) Sei zunächst $\epsilon = -1$ angenommen. Ist $k = 2$, so folgt $\dim V = 2$ und π ist eine Transvektion. Weil auch $-\pi$ ein Element aus $\mathrm{U}(f)$ mit $\mathrm{B}(-\pi) = V$ ist, liefert (a) Quasi-Symmetrien ρ, σ, so daß $-\pi = \rho\sigma$ ist. Demnach ist π das Produkt der beiden Quasi-Involutionen $-\rho$ und σ. Falls $k \in \{3, 5\}$ ist, ist π nach 2.2.3 sogar ein Produkt von zwei unitären Involutionen.

Sei nun $\mathrm{mip}(\pi) = (x-1)^4$ angenommen.
Es genügt folgendes zu zeigen: Es gibt kommutierende Quasi-Symmetrien ρ, σ so, daß $\mathrm{B}(\pi\rho\sigma)$ 1-dimensional und regulär ist.
Denn dann ist $\pi\rho\sigma$ eine Quasi-Symmetrie und damit $\pi = (\pi\rho\sigma)(\rho\sigma)^{-1}$ ein Produkt von zwei Quasi-Involutionen.

Sei $\phi := \pi - 1$. Wir zeigen zunächst:

(i) Es gibt ein $v \in V$ mit folgenden Eigenschaften:
(1) $V = \langle v, v\phi, v\phi^2, v\phi^3 \rangle$,
(2) $v\phi$ ist anisotrop,
(3)
$$\lambda := -\frac{f(v\phi, v\phi)}{f(v\phi^2, v\phi)} \text{ und } \mu := -\frac{f(v\phi + \lambda v\phi^2, v)}{f(v\phi^3, v)}$$
erfüllen $\mu + \bar{\mu} \neq \lambda^2$.

Beweis von (i). Wähle ein $v \in V$, so daß (1) und (2) gelten. Man kann dann $\mu + \bar{\mu} = \lambda^2$ annehmen, wobei μ und λ wie in (3) definiert seien. Setze $\hat{v} := v + v(\pi - 1)^2$. Dann sind (1) und (2) für $\hat{v}$ erfüllt. Weiterhin gilt
$$-\frac{f(\hat{v}\phi, \hat{v}\phi)}{f(\hat{v}\phi^2, \hat{v}\phi)} = \lambda \qquad \text{und} \qquad -\frac{f(\hat{v}\phi + \lambda\hat{v}\phi^2, \hat{v})}{f(\hat{v}\phi^3, \hat{v})} = \mu - 2,$$
also $\mu - 2 + \overline{\mu - 2} = \lambda^2 - 4 \neq \lambda^2$. Folglich erfüllt $\hat{v}$ die Bedingungen (1), (2) und (3).

(ii) Seien
$$\rho : V \to V,\ u \mapsto u + \frac{f(u, v\phi)}{f(v\phi, v)} v\phi, \quad y := \lambda v\phi + \mu v\phi^2, \quad z := v + y, \quad \sigma : V \to V,\ u \mapsto u + \frac{f(u, z\phi)}{f(z\phi, z)} z\phi$$
Dann gilt $f(v\phi, z\phi) = 0$, i.e. ρ und σ kommutieren. Weiterhin gilt:
$$\mathrm{F}(\pi\rho) = \mathrm{F}(\pi) \oplus \langle v \rangle, \qquad \mathrm{F}(\pi\rho\sigma) = \mathrm{F}(\pi) \oplus \langle v \rangle \oplus \langle z \rangle.$$
Beachte, daß $f(y, y) = (-\lambda^2 + \mu + \bar{\mu}) f(v\phi, v\phi) \neq 0$ ist. Setze
$$\nu := -\frac{f(y, y)}{f(v\phi^2, y)}, \qquad \xi := -\frac{f(y + \nu v\phi^2, v)}{f(v\phi^3, v)}, \qquad b := y + \nu v\phi^2 + \xi v\phi^3.$$
Dann gilt $b \in \mathrm{B}(\pi) \cap \langle v \rangle^\perp \cap \langle z \rangle^\perp = \mathrm{B}(\pi\rho\sigma)$ und $f(b, b) = \nu f(v\phi^2, y) \neq 0$. Damit haben wir das Gewünschte bewiesen.

Falls $\epsilon = 1$ ist, gilt $\mathrm{mip}(-\pi) = (x-1)^k$ und $-\pi = \sigma\rho$ für Quasi-Involutionen σ, ρ nach dem zuerst betrachteten Fall. Weil $-\sigma$ eine Quasi-Involution ist, erhalten wir das gewünschte Ergebnis. ■

Bemerkung 4.5.6 *Seien $\pi \in \mathrm{U}(f)$ und $a_1, \ldots, a_s, b_1, \ldots, b_t \in K^*$ verschiedene Elemente so, daß $a_i\bar{a_i} = 1$ und $b_j\bar{b_l} \neq 1$ für $i \in \mathbb{N}_{\leq s}$ und $j, l \in \mathbb{N}_{\leq t}$. Falls $\mathrm{mip}(\pi)$ ein Teiler von*

$$\prod_{i=1}^{s}(x-a_i)^5 \prod_{j=1}^{t}(x-b_j)(x-b_j)^*$$

ist, ist π ein Produkt von zwei Quasi-Involutionen.

Beweis. Sei $V = \bigoplus_{l=1}^{k} U_l$ eine Zerlegung von V in orthogonal unzerlegbare π-Moduln U_l. Es gilt dann $\dim U_l = 2$, falls $\mathrm{mip}(\pi_{U_l})$ keinen $^-$-symmetrischen Primteiler besitzt. Folglich liefert 4.5.5 (a), daß π_{U_l} ein Produkt von zwei Quasi-Involutionen ist. Andernfalls gilt $\mathrm{mip}(\pi_{U_l}) = (x-a)^m$ für ein $a \in K$ mit $a\bar{a} = 1$ und ein $m \in \mathbb{N}_{\leq 5}$. In diesem Fall ist U_l ein orthogonal unzerlegbarer $(\bar{a}\pi)$-Modul mit $\mathrm{mip}(\bar{a}\pi_{U_l}) = (x-1)^m$. Nach 4.5.5 (b) ist $\bar{a}\pi_{U_l}$ ein Produkt von zwei Quasi-Involutionen $\alpha, \beta \in \mathrm{U}(f_{U_l})$. Weil auch $a\alpha$ eine Quasi-Involution ist, ist auch $\pi_{U_l} = (a\alpha)\beta$ ein Produkt von zwei Quasi-Involutionen. Orthogonales Zusammensetzen liefert das Gewünschte. ■

Lemma 4.5.7 *Seien $\pi \in \mathrm{GL}(V)$ und $p := \mathrm{mip}(\pi)$. Weiterhin sei V is π-zyklisch. Es gibt dann $\rho, \sigma \in \mathrm{GL}(V)$ so, daß $\mathrm{mip}(\rho)$ ein Teiler von x^2-1, $\mathrm{mip}(\sigma)$ ein Teiler von $(x^2-1)(x+p(0))$ ist, und $\pi = \rho\sigma$ gilt.*

Beweis. Seien $n := \dim V$ und $v \in V$ so, daß $(v, v\pi, ..., v\pi^{n-1})$ eine Basis von V ist. Definiere $\rho, \sigma \in \mathrm{GL}(V)$ durch $v\pi^i\rho := v\pi^{n-i-1}$ für $0 \leq i \leq n-1$ und $v\pi^i\sigma := v\pi^{n-i}$ für $0 \leq i \leq n-1$. Dann gilt $\pi = \rho\sigma$, $\rho^2 = 1$ und $(\sigma^2-1)(\sigma+p(0)) = 0$, i.e. $\mathrm{mip}(\sigma)$ teilt $(x^2-1)(x+p(0))$. ■

Lemma 4.5.8 *Sei $\phi \in \mathrm{U}(f)$ derart, daß $H\phi = H$ für einen maximalen totalisotropen Unterraum H von V gilt. Jeder Primteiler von $\mathrm{mip}(\phi_H)$ sei $^-$-symmetrisch. Dann ist ϕ ein Produkt von einer unitären Involution und zwei Quasi-Involutionen.*

Beweis. Sei $H = \oplus_{i\in I} H_i$ eine Zerlegung von H in ϕ-zyklische ϕ-Moduln. Für jedes $i \in I$ sei $a_i := \mathrm{mip}(\phi_{H_i})(0)$. Weil jeder Primteiler von $\mathrm{mip}(\phi_H)$ $^-$-symmetrisch ist, gilt insbesondere $a_i\overline{a_i} = 1$. Nach 4.5.7 gibt es $\alpha_i, \beta_i \in \mathrm{GL}(H_i)$ derart, daß $\mathrm{mip}(\alpha_i)$ ein Teiler von x^2-1, $\mathrm{mip}(\beta_i)$ ein Teiler von $(x^2-1)(x+a_i)$ ist, und $\phi_{H_i} = \alpha_i\beta_i$ gilt. Setze $\alpha := \oplus_{i\in I}\alpha_i, \beta := \oplus_{i\in I}\beta_i \in \mathrm{GL}(H)$. Dann ist α eine Involution und $\mathrm{mip}(\beta)$ teilt $(x^2-1)\cdot \mathrm{lcm}\{x+a_i, i \in I\}$. Seien $m := |\{a_i; i \in I\}\backslash\{\pm 1\}|$, $b_1, \ldots b_m \in K$ derart, daß $\{a_i; i \in I\}\backslash\{\pm 1\} = \{b_i; i \in \mathbb{N}_{\leq m}\}$ gilt, und $b_{m+1} := 1$, $b_{m+2} := -1$. Mit diesen Bezeichnungen erhält man

$$\mathrm{mip}(\beta) \text{ teilt } \prod_{i=1}^{m+2}(x+b_i)^2.$$

Setzt man $A_i := \ker(\beta+b_i)^2$, $i \in \mathbb{N}_{\leq m+2}$, so erhält man

$$H = \oplus_{i=1}^{m+2} A_i.$$

Nach 4.5.4 kann man α zu einer unitären Involution $\hat{\alpha} \in \mathrm{U}(f)$ fortsetzen. Damit ist $\psi := \hat{\alpha}\phi$ eine Fortsetzung von β. Setzt man $\hat{A}_i := \ker(\psi + b_i)^\infty$, so gilt $A_i \leq \hat{A}_i$ für alle $i \in \mathbb{N}_{\leq m+2}$. Weil

$$E := \textcircled{\perp}\,{}_{i=1}^{l} \hat{A}_i$$

ein regulärer ψ-Untermodul von V ist, gilt

$$\dim H = \mathrm{Ind}(V) \geq \mathrm{Ind}(E) \geq \sum_{i=1}^{m+2} \mathrm{Ind}(\hat{A}_i) \geq \sum_{i=1}^{m+2} \dim(A_i) = \dim H,$$

also $\mathrm{Ind}(\hat{A}_i) = \dim A_i$ für alle $i \in \mathbb{N}_{\leq m+2}$. Aus 4.5.3 erhält man nun, daß $\mathrm{mip}(\psi_{\hat{A}_i})$ ein Teiler von $(x - b_i)^5$ ist. Nach 4.5.6 ist ψ_E ein Produkt von zwei Quasi-Involutionen $\gamma', \delta' \in \mathrm{U}(f_E)$. Weil $E^\perp$ ein anisotroper ψ- Modul ist, ist $\psi_{E^\perp}$ nach 4.5.1 ein Produkt von zwei Quasi-Involutionen $\gamma'', \delta'' \in \mathrm{U}(f_{E^\perp})$, so daß ψ das Produkt der Quasi-Involutionen $\gamma := \gamma' \textcircled{\perp}\ \gamma''$ und $\delta := \delta' \textcircled{\perp}\ \delta''$ ist. Folglich ist $\phi = \alpha\gamma\delta$ das Produkt der unitären Involutionen α und der beiden Quasi-Involutionen γ und δ. ■

Lemma 4.5.9 *Sei $\pi \in \mathrm{U}(f)$ derart, daß kein Primteiler von $\mathrm{mip}(\pi)$ $^-$-symmetrisch ist. Dann ist π ein Produkt von einer unitären Involution und zwei Quasi-Involutionen.*

Beweis. Eine orthogonale Zerlegung von V in orthogonal unzerlegbare π-Moduln enthält ausschließlich Moduln vom Typ I. Man kann daher annehmen, daß V selbst ein orthogonal unzerlegbarer π-Modul vom Typ I ist. Dann gilt $V = U \oplus W$ für totalisotrope zyklische π-Moduln U und W. Sei $p := \mathrm{mip}(\pi_W)$. Gemäß 4.5.7 findet man $\rho, \sigma \in \mathrm{GL}(W)$ so, daß $\pi_W = \rho\sigma$, $\mathrm{mip}(\rho)$ ein Teiler von $x^2 - 1$ und $\mathrm{mip}(\sigma)$ ein Teiler von $q := (x^2 - 1)(x + p(0))$ ist. Seien $\hat{\rho}, \hat{\sigma} \in \mathrm{U}(f)$ die nach 1.3.5 eindeutig bestimmten Fortsetzungen von ρ bzw. σ mit $U\hat{\rho} = U = U\hat{\sigma}$. Nach 1.3.5 ist $\hat{\rho}$ eine Involution und $\mathrm{mip}(\hat{\sigma})$ ein Teiler von $\mathrm{lcm}(q, q^*)$. Dieses Polynom teilt $(x^2-1)(x+p(0))(x-\bar{p(0)}^{-1})$, so daß $\hat{\sigma}$ nach 4.5.6 ein Produkt von zwei Quasi-Involutionen ist. ■

Durch Kombination von 4.5.1, 4.5.8 und 4.5.9 können wir nun den entscheidenden Satz dieses Abschnittes beweisen, aus dem mit 4.5.2 sofort das Hauptergebnis folgt.

Satz 4.5.10 *Jedes $\phi \in \mathrm{U}(f)$, das einen maximalen totalisotropen Unterraum H invariant läßt, ist ein Produkt von einer unitären Involution und zwei Quasi-Involutionen. Insbesondere ist ϕ damit ein Produkt von drei Quasi-Involutionen.*

Beweis. Sei $\mathrm{mip}(\phi_H) = rs$, wobei r und s normierte Polynome seien, so daß jeder Primteiler von r jedoch keiner von s $^-$-symmetrisch ist. Setze $A := \ker r(\phi_H)$, $\hat{A} := \ker r(\phi)^\infty$, $B := \ker s(\phi_H)$, $\hat{B} := \ker(ss^*)(\phi)^\infty$ und $C := (\hat{A}+\hat{B})^\perp$. Dann gilt $H = A \oplus B$, $A \leq \hat{A}$, $B \leq \hat{B}$ und $V = \hat{A} \textcircled{\perp}\ \hat{B} \textcircled{\perp}\ C$. Wegen

$$\dim H = \mathrm{Ind}(V) \geq \mathrm{Ind}(\hat{A}) + \mathrm{Ind}(\hat{B}) \geq \dim A + \dim B = \dim H$$

gilt $\mathrm{Ind}(\hat{A}) = \dim A$, und C ist ein anisotroper ϕ-Modul. Nach 4.5.8 ist $\phi_{\hat{A}}$ ein Produkt von einer unitären Involution σ_1 und zwei Quasi-Involutionen α_1, β_1. Nach 4.5.9 ist auch $\phi_{\hat{B}}$ ein Produkt von einer unitären Involution σ_2 und zwei Quasi-Involutionen α_2, β_2. Nach 4.5.1 ist ϕ_C ein Produkt von zwei Quasi-Involutionen α_3, β_3. Folglich ist ϕ das Produkt der unitären Involution $\sigma := \sigma_1 \textcircled{\perp}\ \sigma_2 \textcircled{\perp}\ 1_C$ und der Quasi-Involutionen $\alpha := \alpha_1 \textcircled{\perp}\ \alpha_2 \textcircled{\perp}\ \alpha_3$, $\beta := \beta_1 \textcircled{\perp}\ \beta_2 \textcircled{\perp}\ \beta_3$. ■

Satz 4.5.11 *Jedes $\pi \in \mathrm{U}(f)$ ist ein Produkt von zwei unitären Involutionen und zwei Quasi-Involutionen. Insbesondere ist π ein Produkt von vier Quasi-Involutionen.*

Beweis. Sei H ein maximaler totalisotroper Unterraum. Weil auch $H\pi^{-1}$ ein solcher ist, gibt es nach 4.5.2 eine unitäre Involution σ, so daß $H\sigma = H\pi^{-1}$ ist, i.e. $H\sigma\pi = H$. Nach 4.5.10 gibt es eine unitäre Involution α und Quasi-Involutionen β, γ, so daß $\sigma\pi = \alpha\beta\gamma$ ist, i.e. $\pi = \sigma\alpha\beta\gamma$. ■

Korollar 4.5.12 *Besitzt $\pi \in \mathrm{U}(f)$ keinen Elementarteiler der Form p^{2t-1}, $t \in \mathbb{N}$, $p \in K[x]$ irreduzibel, $^{-}$-symmetrisch und $\deg(p) > 1$, so ist π ein Produkt von einer unitären Involution und zwei Quasi-Involutionen. Insbesondere ist π ein Produkt von drei Quasi-Involutionen.*

Beweis. Jeder reguläre, orthogonal unzerlegbare π- Untermodul von V enthält einen maximalen totalisotropen Unterraum, der π-invariant ist, so daß die Behauptung aus 4.5.10 folgt. ■

Eine triviale Konsequenz dieses Korollars ist der

Satz 4.5.13 *Ist K ein algebraisch abgeschlossener Körper, so ist jedes $\pi \in \mathrm{U}(f)$ ein Produkt von einer unitären Involution und zwei Quasi-Involutionen, also insbesondere ein Produkt von drei Quasi-Involutionen.* ■

4.6 Offene Fragen

(1) Lassen sich analoge 'Block-Zerlegungssätze' zu den im Abschnitt 4.1 hergeleiteten auch für hermitesche Räume ungerader Dimension mit maximalem Witt-Index $\frac{1}{2}(\dim V - 1)$ formulieren? Kann man auf diese Weise die Vermutungen von Thompson und Ore für die endlichen einfachen Gruppen $\mathrm{PSU}_{2m+1}(\mathrm{F}_{q^2})$, $(m, q) \neq (1, 2)$, studieren?

(2) Man versuche, die Sätze aus dem Abschnitt 4.1 einheitlich für hyperbolische symmetrische, symplektische und hermitesche Formen zu formulieren und zu beweisen.

(3) Unter der Voraussetzung $\mathcal{N}(K) = F$ und $|F| > 3$ beweise oder widerlege man durch ein Gegenbeispiel, daß $\mathrm{U}^{\pm}(f)$ vierspiegelig ist, i.e. jedes $\pi \in \mathrm{U}(f)$ ein Produkt von vier unitären Involutionen ist (cf. 4.3.1).

(4) Beispiel 4.4.17 zeigt, daß $\mathrm{U}^{\pm}(p, q)$ für $p, q \geq 1$ stets Homothetien enthält, welche kein Produkt von vier unitären Involutionen sind. Gibt es in $\mathrm{U}^{\pm}(p, q)$ Elemente mit dieser Eigenschaft, die nicht im Zentrum liegen?

(5) Ist $\pi \in \mathrm{U}(f)$ im Fall $\mathrm{char}(K) \neq 2$ ein Produkt von 3 oder sogar 2 Quasi-Involutionen ? (Zum Nachweis der 3-Quasispiegeligkeit könnte man nach 4.5.12 o.B.d.A. annehmen, daß π vom Typ III ist und daß $\mathrm{mip}(\pi) = p^{2t-1}$ für ein irreduzibles, $^{-}$-symmetrisches $p \in K[x]$ mit $\deg(p) \geq 2$ gilt.)

(6) Wie in der Einleitung angesprochen sind für $\mathrm{char}(K) = 2$ unitäre Involutionen ($\neq 1$) keine Quasi-Involutionen. Dies wirft natürlich die Frage auf, ob Quasi-Involutionen im bisherigen

Sinne das geeignete unitäre Analogon zu Involutionen in orthogonalen Gruppen repräsentieren. Eine naheliegende, neue Definition wäre, solche unitären Transformationen, welche ein Produkt von beliebigen paarweise kommutierenden einfachen unitären Transformationen [also sowohl Quasi-Symmetrien als auch unitären Transvektionen] sind, als Quasi-Involutionen zu bezeichnen. Jede Quasi-Involution im alten Sinne wäre dann natürlich auch eine im neuen. Quasi-Involutionen wären dann in jeder unitären Gruppe ein Erzeugendensystem. Lassen sich die obigen Techniken verfeinern, oder bieten sich neue zur Lösung des Längenproblems bezüglich dieser Quasi-Involutionen an?

Anhang

Der Satz von Lev

A.Lev beweist in [51] folgenden Satz (Theorem 2) über Produkte zyklischer Konjugiertenklassen in allgemeinen linearen Gruppen:

Satz 4.6.1 (Lev) *Seien F ein Körper, $n \in \mathbb{N}_{\geq 2}$ und $A, B, M \in \mathrm{GL}_n(F)$. Es sei M keine Homothetie und die Matrizen A, B seien zyklisch,* $\mathrm{mip}(A)$ *zerfalle in $F[x]$ in Linearfaktoren und es gelte* $\det M = \det A \det B$. *Weiterhin seien $\Omega_1 := A^{\mathrm{GL}_n(F)}$ und $\Omega_2 := B^{\mathrm{GL}_n(F)}$ die zu A bzw. B gehörigen Konjugiertenklassen in* $\mathrm{GL}_n(F)$. *Falls $n \geq 3$ und $|F| \geq 4$ ist, gilt $M \in \Omega_1\Omega_2$. Im Fall $n = 2$ gilt*

$$\{N \in \mathrm{GL}_2(K) | \det N = \det AB \textit{ und } N \textit{ ist keine Homothetie}\} \subseteq \Omega_1\Omega_2$$

genau dann, wenn die Eigenwerte von A verschieden sind, oder $\mathrm{mip}(B)$ *in $F[x]$ in Linearfaktoren zerfällt.*

In der oben zitierten Arbeit wird außer 4.6.1 noch eine Aussage über Produkte zyklischer Konjugiertenklassen in speziellen linearen Gruppen gemacht (Theorem 3). Weil der Beweis dieser fehlerhaft ist (so ist etwa für $n = 5$ und $k = 3$ die Gleichung

$$Y_n^{-1}(t)\rho = \rho \mathrm{diag}(1, Y_{n-1}(-t))$$

am Ende des Beweises von Lemma 5 falsch), beide Sätze aber in weiten Teilen gemeinsam behandelt werden, erschien es mir aus Gründen der Nachprüfbarkeit meiner eigenen Ergebnisse notwendig, den Satz 4.6.1 separat zu beweisen. Der Beweis vereinfacht sich für $n \geq 3$ wesentlich, wenn man voraussetzt, daß die zyklische Matrix A aus 4.6.1 einen Eigenwert mit einfacher Vielfachheit besitzt. Es stellt sich dabei heraus, daß man dann die Forderung $|F| \geq 4$ zu $|F| \geq 3$ abschwächen kann. Es wird diese leichtere Version bewiesen, da sie für die Anwendungen im Kapitel 4 ausreichend ist. Es sei angemerkt, daß sich mit ihr die Vermutung von Thompson auch für die einfachen Gruppen $\mathrm{PSL}_{2m+1}(\mathrm{F}_3)$, $m \in \mathbb{N}$, beweisen läßt (cf. 4.6.15 unten).

Satz 4.6.2 *Seien F ein Körper, $|F| \geq 3$, $n \in \mathbb{N}_{\geq 2}$, $A, B \in \mathrm{GL}_n(F)$ zyklisch und $M \in \mathrm{GL}_n(F)$ keine Homothetie mit* $\det M = \det A \det B$. *Weiterhin seien $\Omega_1 := A^{\mathrm{GL}_n(F)}$ und $\Omega_2 := B^{\mathrm{GL}_n(F)}$ die zu A bzw. B gehörigen Konjugiertenklassen in* $\mathrm{GL}_n(F)$.

(i) *Sei* $n = 2$ *und* A *besitze die Eigenwerte* $\mu, \nu \in F^*$. *Es gilt* $M \in \Omega_1\Omega_2$ *genau dann, wenn* $\mu \neq \nu$ *oder* $\mathrm{trace}(M) \neq \mu\mathrm{trace}(B)$ *oder wenn* $\mathrm{mip}(B)$ *in* $F[x]$ *in Linearfaktoren zerfällt.*

(ii) *Sei* $n \geq 3$. *Das charakteristische Polynom von* A *zerfalle in Linearfaktoren, und* A *besitze einen Eigenwert mit einfacher Vielfachheit. Dann gilt* $M \in \Omega_1\Omega_2$.

Ich möchte hervorheben, daß die Ideen für den angegebenen Beweis von 4.6.2 von A. Lev stammen und aus [51] übernommen wurden.
Als erstes beweisen wir kurz die Aussage (i).
Seien $\gamma := \mathrm{trace}(B)$, $\delta := -\det B$, $\zeta := \mathrm{trace}(M)$ und

$$B' := \begin{bmatrix} & 1 \\ \delta & \gamma \end{bmatrix} \in \Omega_2$$

$\Leftarrow$. Setze $z := (\zeta - \nu\gamma)\delta^{-1}$. Falls $\mu \neq \nu$ oder $z \neq 0$ ist, gilt

$$A' := \begin{bmatrix} \mu & z \\ & \nu \end{bmatrix} \in \Omega_1.$$

Es folgt

$$M' := A'B' = \begin{bmatrix} z\delta & \mu + z\gamma \\ \nu\delta & \nu\gamma \end{bmatrix} \in \Omega_1\Omega_2.$$

Wegen $\mathrm{trace}(M') = \zeta$ und weil M' wegen $\nu\delta \neq 0$ keine Homothetie ist, ist M' ähnlich zu M. Man kann daher $\mu = \nu$ und $z = 0$ annehmen. Nach Voraussetzung besitzt B dann Eigenwerte $\eta, \theta \in F^*$. Wegen $|F| \geq 3$ gibt es ein $r \in F^* \backslash \{\mu\}$. Setze $s := r\eta^{-1} \in F^*$ und

$$A'' := \begin{bmatrix} \mu + r & -s \\ r^2 s^{-1} & \mu - r \end{bmatrix}.$$

Wegen $s \neq 0$ ist A'' keine Homothetie und damit zyklisch. Man berechnet $\mathrm{mip}(A'') = x^2 - 2\mu x + \mu^2 = \mathrm{mip}(A)$. Es folgt $A'' \in \Omega_1$ und

$$A''B' = \begin{bmatrix} \mu + r & -s \\ r^2 s^{-1} & \mu - r \end{bmatrix} \begin{bmatrix} & 1 \\ \delta & \gamma \end{bmatrix} = \begin{bmatrix} -s\delta & \mu + r - s\gamma \\ (\mu - r)\delta & r^2 s^{-1} + (\mu - r)\gamma \end{bmatrix} \in \Omega_1\Omega_2.$$

Wegen $\mu \neq r$ ist $M'' := A''B'$ keine Homothetie. Aus

$$\begin{aligned} \mathrm{trace}(M'') &= r^2 s^{-1} - r\gamma - s\delta + \mu\gamma = s(\eta^2 - \eta\gamma - \delta) + \mu\gamma \\ &= s\ \mathrm{mip}(B)(\eta) + \zeta = \mathrm{trace}(M). \end{aligned}$$

folgt, daß M'' ähnlich zu M ist.

$\Rightarrow$. Sei $M \in \Omega_1\Omega_2$. Es gelte $\mu = \nu$ und $\zeta = \mu\gamma$. Für $r \in F$ und $s \in F^*$ sei

$$A(r, s) := \begin{bmatrix} \mu + r & -s \\ r^2 s^{-1} & \mu - r \end{bmatrix}.$$

Wegen $s \neq 0$ gilt $\mathrm{mip}(A(r,s)) = \mathrm{char}(A(r,s)) = x^2 - 2\mu x + \mu^2 = \mathrm{mip}(A)$, also $A(r,s) \in \Omega_1$. Ist umgekehrt

$$C = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

ein Element von Ω_1, so gilt $x^2 - 2\mu x + \mu^2 = \mathrm{mip}(A) = \mathrm{mip}(C) = x^2 - (a+d)x + ad - bc$, i.e. $r := a - \mu = \mu - d$ und $r^2 = -cb$. Weil C zyklisch ist und nur einen Eigenwert besitzt, ist $b \neq 0$ oder $c \neq 0$. Es folgt $C = A(r, -b)$ oder $C = A(r, -c)^t$ und somit $\Omega_1 = \{A(r,s), A(r,s)^t; r \in F, s \in F^*\}$. Es gibt daher eine zu M ähnliche Matrix N, ein $r \in F$ und ein $s \in F^*$ so, daß

$$(1)\ \ N = A(r,s)B' = \begin{bmatrix} -s\delta & \mu + r - s\gamma \\ (\mu - r)\delta & r^2 s^{-1} + (\mu - r)\gamma \end{bmatrix}$$

oder

$$(2)\ \ N = A(r,s)^t B' = \begin{bmatrix} r^2 s^{-1}\delta & \mu + r + r^2 s^{-1}\gamma \\ (\mu - r)\delta & (\mu - r)\gamma - s \end{bmatrix}$$

gilt. Im Fall (1) erhält man

$$\mu\gamma = \mathrm{trace}(M) = \mathrm{trace}(N) = s((rs^{-1})^2 - \gamma(rs^{-1}) - \delta) + \mu\gamma = s\ \mathrm{mip}(B)(rs^{-1}) + \mu\gamma.$$

Wegen $s \neq 0$ ist rs^{-1} ein Eigenwert von B. Im Fall (2) erhält man

$$\mu\gamma = \mathrm{trace}(M) = \mathrm{trace}(N) = s\delta^{-1}((r\delta s^{-1})^2 - \gamma(r\delta s^{-1}) - \delta) + \mu\gamma = s\delta^{-1}\mathrm{mip}(B)(r\delta s^{-1}) + \mu\gamma.$$

Wegen $s\delta^{-1} \neq 0$ ist $r\delta s^{-1}$ ein Eigenwert von B. In jedem Fall zerfällt $\mathrm{mip}(B)$ in $F[x]$ in Linearfaktoren. ■

Für das weitere seien F ein Körper und $n \in \mathbb{N}_{\geq 2}$.

Notation 4.6.3 *Seien $l \in \mathbb{N}_{\geq 2}$ und $m \in \mathbb{N}_{\leq l}$. Die Permutation $(1 \dots m)$ der symmetrischen Gruppe S_l sei mit $\rho_{(l,m)}$ bezeichnet. Für $l = m$ schreiben wir ρ_l statt $\rho_{(l,l)}$. Weiterhin sei $\rho := \rho_n$. Für eine Permutation $\sigma \in \mathrm{S}_l$ sei die zugehörige Permutationsmatrix $(\delta_{i,j\sigma^{-1}})_{1 \leq i,j \leq l} \in F^{l \times l}$ ebenfalls mit σ bezeichnet.*

Definition 4.6.4 (Begleitmatrix) *Seien $p = x^n + \sum_{i=0}^{n} p_i x^i$ ein normiertes Polynom aus $F[x]$ und $q := (-p_1, \dots, -p_{n-1}) \in F^{n-1}$. die Matrix*

$$\begin{bmatrix} & I_{n-1} \\ -p_0 & q \end{bmatrix} \in \mathrm{GL}_n(F)$$

nennen wir die Begleitmatrix zum Polynom p.

Lemma 4.6.5 *Seien $A \in F^{n \times n}$ und $f_{1,1}, \dots, f_{n,n} \in F$ mit $\prod_{i=1}^{n} f_{i,i} = 1$. Es gibt dann $f_{i,j} \in F^*$, $(i,j) \in \mathbb{N}_{\leq n} \times \mathbb{N}_{\leq n} \backslash \{(i,i); i \in \mathbb{N}_{\leq n}\}$ so, daß für $B := (f_{i,j} A_{i,j})_{1 \leq i,j \leq n}$ die Matrix ρB ähnlich zu ρA ist.*

Beweis. Für $i \in \mathbb{N}_{\leq n}$ setze $c_i := \prod_{j=2}^{i} f_{j,j}^{-1}$. Dann gilt $c_i c_{i+1}^{-1} = f_{i+1,i+1}$ für $i \in \mathbb{N}_{\leq n-1}$ und $c_n c_1 = \prod_{i=2}^{n} f_{i,i}^{-1} = f_{1,1}$. Wähle $C := \mathrm{diag}(c_1, \dots, c_n)$ und $f_{i,j} := c_{i\rho^{-1}} c_j^{-1} \in F^*$ für $(i,j) \in \mathbb{N}_{\leq n} \times \mathbb{N}_{\leq n} \backslash \{(i,i); i \in \mathbb{N}_{\leq n}\}$. Dann gilt $B := \rho^{-1} C \rho A C^{-1} = (f_{i,j} A_{i,j})_{1 \leq i,j \leq n}$. ■

Korollar 4.6.6 *Seien* $A \in \mathrm{GL}_n(F)$ *eine Begleitmatrix mit* $\mathrm{mip}(A) = x^n + \sum_{i=0}^{n-1} a_i x^i$ *und* $f_1, \ldots f_n \in F$ *mit* $\prod_{i=1}^n f_i = 1$. *Dann gibt es* $a'_1, \ldots, a'_n \in F$ *so, daß für*

$$B := \begin{bmatrix} -a_0 f_1 & a'_1 \ldots & a'_{n-1} \\ & \ddots & \\ & & f_n \end{bmatrix}$$

die Matrix ρB *ähnlich zu* A *ist.* ■

Lemma 4.6.7 *Seien* A *und* B *wie in 4.6.6. Seien weiterhin* $r \in \mathbb{N}_{\leq n-1}$, $B_1 \in \mathrm{GL}_r(F)$ *und* $B_2 \in \mathrm{GL}_{n-r}(F)$ *obere Dreiecksmatrizen so, daß* $(B_1)_{i,i} = B_{i,i}$ *für* $i \in \mathbb{N}_{\leq r}$ *und* $(B_2)_{i,i} = B_{r+i,r+i}$ *für* $i \in \mathbb{N}_{\leq n-r}$ *gilt. Dann gibt es ein* $C \in F^{r \times n-r}$ *so, daß* A *ähnlich zu der Matrix*

$$\rho \begin{bmatrix} B_1 & C \\ & B_2 \end{bmatrix}$$

ist.

Beweis. Siehe [10] Satz 5.13. ■

Lemma 4.6.8 *Seien* $a_1, \ldots, a_n \in F^*$ *und* $A \in \mathrm{GL}_n(F)$ *zyklisch mit Jordan' scher Normalform*

$$\tilde{A} = \begin{bmatrix} a_1 & \epsilon_1 & & \\ & \ddots & \ddots & \\ & & a_{n-1} & \epsilon_{n-1} \\ & & & a_n \end{bmatrix},$$

$\epsilon_1, \ldots, \epsilon_{n-1} \in \{0, 1\}$. *Sei* $B \in \mathrm{GL}_n(F)$ *eine obere Dreiecksmatrix mit* $B_{i,i} = a_i$ *für alle* $i \in \mathbb{N}_{\leq n}$, *und für* $i \in \mathbb{N}_{\leq n-1}$ *gelte* $B_{i,i+1} \neq 0$, *falls* $\epsilon_i = 1$ *ist. Dann ist* B *ähnlich zu* A.

Beweis. Siehe [10] Hilfssatz 4.9. ■

Satz 4.6.9 *Seien* $|F| \geq 3$, $n \in \mathbb{N}_{\geq 3}$ *und* $A, B, M \in \mathrm{GL}_n(F)$ *zyklisch mit* $\det M = \det A \det B$. *Das Minimalpolynom von* A *zerfalle in* $F[x]$ *in Linearfaktoren . Seien* $\Omega_1 := A^{\mathrm{GL}_n(F)}$ *und* $\Omega_2 := B^{\mathrm{GL}_n(F)}$ *die zu* A *bzw.* B *gehörigen Konjugiertenklassen in* $\mathrm{GL}_n(F)$. *Dann gilt* $M \in \Omega_1 \Omega_2$.

Beweis. Seien $\mathrm{mip}(M) = x^n + \sum_{i=0}^{n-1} p_i x^i$, $\mathrm{mip}(B) = x^n + \sum_{i=0}^{n-1} b_i x^i$ und $a_1, \ldots, a_n \in F^*$ die Eigenwerte von A so, daß

$$\begin{bmatrix} a_1 & \epsilon_1 & & \\ & \ddots & \ddots & \\ & & a_{n-1} & \epsilon_{n-1} \\ & & & a_n \end{bmatrix}$$

eine Jordan'sche Normalform von A für geeignete $\epsilon_1, \ldots, \epsilon_{n-1} \in \{0, 1\}$ ist. O.B.d.A. gelte

$$M = \rho \left[\begin{array}{c|c} -p_0 & -p_1 \cdots - p_{n-1} \\ \hline & I_{n-1} \end{array} \right].$$

Setze

$$C := \begin{bmatrix} a_2 & 1 & & & \\ & \ddots & \ddots & & \\ & & a_{n-1} & 1 \\ & & & a_n \end{bmatrix} \in \mathrm{GL}_{n-1}(F),$$

$f_1 := \prod_{i=2}^n a_i$ und $f_i := a_i^{-1}$ für $2 \le i \le n$. Dann gilt $\prod_{i=1}^n f_i = 1$ und

$$-b_0 f_1 = (-1)^{n+1} a_1^{-1} \det B \det A = (-1)^{n+1} a_1^{-1} \det M = -p_0 a_1^{-1}.$$

Nach 4.6.6 und 4.6.7 gibt es ein $u \in F^{n-1}$ so, daß

$$B' := \rho \begin{bmatrix} -p_0 a_1^{-1} & u \\ & C^{-1} \end{bmatrix} \in \Omega_2$$

gilt.

Fall A: $p_1 \neq -a_2 u_1$. Sei $v := ((p_1, \ldots, p_{n-1}) + uC) a_1 p_0^{-1} \in F^{n-1}$. Dann gilt $v_1 = (p_1 + a_2 u_1) a_1 p_0^{-1} \neq 0$ und nach 4.6.8

$$A' := \begin{bmatrix} a_1 & v \\ & C \end{bmatrix} \in \Omega_1.$$

Es folgt $M = B'A' = (B'A'B'^{-1})B' \in \Omega_1 \Omega_2$.

Fall B. $p_1 = -a_2 u_1$. Wegen $|F| \ge 3$ gibt es ein $t \in F^* \backslash \{-a_2^{-1}\}$. Setze

$$S := \begin{bmatrix} 1 & t & \\ & 1 & \\ & & I_{n-2} \end{bmatrix} \in \mathrm{SL}_n(F) \text{ und } T := \begin{bmatrix} 1 & -t & \\ & 1 & \\ & & I_{n-3} \end{bmatrix} \in \mathrm{SL}_{n-1}(F).$$

Dann gilt :

$$\rho \operatorname{diag}(1, T) \rho^{-1} = \begin{bmatrix} & I_{n-1} \\ 1 & \end{bmatrix} \begin{bmatrix} 1 & \\ & T \end{bmatrix} \begin{bmatrix} & 1 \\ I_{n-1} & \end{bmatrix} = \operatorname{diag}(T, 1) = S^{-1},$$

i.e. $S^{-1}\rho = \rho \operatorname{diag}(1, T)$. Es folgt

$$\begin{aligned} B'' := S^{-1} B' S &= \rho \begin{bmatrix} 1 & \\ & T \end{bmatrix} \begin{bmatrix} -p_0 a_1^{-1} & u \\ & C^{-1} \end{bmatrix} \begin{bmatrix} 1 & t & \\ & 1 & \\ & & I_{n-2} \end{bmatrix} \\ &= \rho \left[\begin{array}{c|c} -p_0 a_1^{-1} & -p_0 a_1^{-1} t + u_1, u_2, \ldots, u_{n-1} \\ \hline & TC^{-1} \end{array} \right]. \end{aligned}$$

Setze $u' := (-p_0 a_1^{-1} t + u_1, u_2, \ldots, u_{n-1}) \in F^{n-1}$,

$$
\begin{aligned}
C' := CT^{-1} &= \begin{bmatrix} a_2 & 1 & & \\ & a_3 & \ddots & \\ & & \ddots & 1 \\ & & & a_n \end{bmatrix} \begin{bmatrix} 1 & t & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \\
&= \begin{bmatrix} a_2 & a_2 t + 1 & & & \\ & a_3 & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & a_n \end{bmatrix}
\end{aligned}
$$

und $v' := ((p_1, \ldots, p_{n-1}) + u'C') a_1 p_0^{-1} \in F^{n-1}$. Dann gilt $v_1' = (p_1 + a_2 u_1') a_1 p_0^{-1} = -a_2 t \neq 0 \neq a_2 t + 1 = C'_{1,2}$ und nach 4.6.8

$$
A'' := \begin{bmatrix} a_1 & v' \\ & C' \end{bmatrix} \in \Omega_1.
$$

Es folgt $M = B''A'' = (B''A''B''^{-1})B'' \in \Omega_1 \Omega_2$. ∎

Lemma 4.6.10 *Seien $a_1, \ldots, a_n \in F^*$ und $A \in \mathrm{GL}_n(F)$ zyklisch mit Jordan'scher Normalform*

$$
\begin{bmatrix} a_1 & \epsilon_1 & & \\ & \ddots & \ddots & \\ & & a_{n-1} & \epsilon_{n-1} \\ & & & a_n \end{bmatrix}.
$$

$\epsilon_1, \ldots, \epsilon_{n-1} \in \{0, 1\}$ *Seien $s \in \mathbb{N}_{<n}$ und $q_0, \ldots, q_{s-1} \in F$ so, daß $\prod_{i=1}^{s}(x - a_i) = x^s + \sum_{i=0}^{s-1} q_i x^i$ gilt, und*

$$
A_1' := \begin{bmatrix} & & & -q_0 \\ 1 & & & \vdots \\ & \ddots & & \\ & & 1 & -q_{s-1} \end{bmatrix}.
$$

Sei weiterhin $A_2 \in \mathrm{GL}_{n-s}(F)$ eine obere Dreiecksmatrix mit $(A_2)_{i,i} = a_{s+i}$ für alle $i \in \mathbb{N}_{\leq n-s}$ und $(A_2)_{i,i+1} \neq 0$ für alle $i \in \mathbb{N}_{\leq n-s-1}$, für die $\epsilon_i = 1$ ist. Dann gibt es zu jedem $c = (c_1, c_3, \ldots, c_s) \in F^{s-1}$ ein $d_c \in F$ so, daß für alle $c_2 \in F \backslash \{d_c\}$ und alle $C \in F^{s \times n-s-1}$ die Matrix

$$
A' := \begin{bmatrix} A_1' & C' \\ & A_2 \end{bmatrix}
$$

ähnlich zu A ist, wobei $C' := ((c_1, c_2, c_3, \ldots, c_s)^t, C) \in F^{s \times n-s}$ sei.

Beweis. Seien

$$A_1 := \begin{bmatrix} a_1 & 1 & & & \\ & \ddots & \ddots & & \\ & & & & \\ & & a_{s-1} & 1 \\ & & & a_s \end{bmatrix} \in \mathrm{GL}_s(F)$$

und $e := (0, \ldots, 0, 1) \in F^s$ der s-te Standardbasis-Vektor des F^s. Für $0 \leq j \leq s-1$ sei

$$r_j := A_1^j e^t = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ * \end{bmatrix} \begin{array}{l} \\ \\ \\ \leftarrow s-j \\ \\ \end{array}$$

Folglich ist $\{r_j^t; 0 \leq j \leq s-1\}$ eine Basis von F^s und damit $R := ((r_{j-1})_i)_{1 \leq i,j \leq s} = (r_0| \ldots |r_{s-1}) \in \mathrm{GL}_s(F)$. Es gilt

$$R = \begin{bmatrix} & & & 1 \\ & & \cdot & \\ & \cdot & * & \\ 1 & a_s & & \end{bmatrix} \in \mathrm{GL}_s(F)$$

und bekanntlich $R^{-1}A_1R = A_1'$. Setze

$$d_c := a_s^{-1}(-c_1 - \sum_{i=3}^{s} R_{s,i}c_i) = a_s^{-1}(-c_1 - \sum_{i=3}^{s} R_{s,i}c_i)$$

und $S := \mathrm{diag}(R, I_{n-s})$. Man berechnet

$$A'' := SA'S^{-1} = \begin{bmatrix} A_1 & RC' \\ & A_2 \end{bmatrix}.$$

Wegen $R_{s,2} = a_s$ und $(C')_{2,1} = c_2 \neq d_c$ gilt $(RC')_{s,1} = a_s(c_2 - d_c) \neq 0$. Nach 4.6.8 ist A'' ähnlich zu A. ■

Die beiden folgenden Bemerkungen beinhalten einfache Rechnungen mit speziellen Permutationen.

Bemerkung 4.6.11 *Seien $n \geq 3$, $m \in \mathbb{N}_{\geq 2}$, $n_1 \in \mathbb{N} \cup \{0\}$, $n_2, \ldots, n_m \in \mathbb{N}$ so, daß $n = \sum_{i=1}^{m} n_i$ gilt, und $\sigma := \mathrm{diag}(I_{n_1}, \rho_{n_2}, \ldots, \rho_{n_m}) \in \mathrm{GL}_n(F)$. Bezeichnet man die zur Permutationsmatrix σ gehörige Permutation von $\mathbb{N}_{\leq n}$ ebenfalls mit σ und setzt $p_i := \sum_{j=1}^{i} n_j$ für $j \in \mathbb{N}_{\leq m}$, so gilt $\sigma = \prod_{j=1}^{m-1}(p_j + 1 \ldots p_{j+1})$. Die Menge $\mathcal{S} := \mathbb{N}_{\leq n_1} \cup \{p_i + 1; i \in \mathbb{N}_{\leq m-1}\}$ hat die Mächtigkeit $s := n_1 + m - 1 \leq \min\{n-1, p_{m-1}+1\}$. Sei*

$$\psi' : \mathbb{N}_{\leq s} \to \mathcal{S}, i \mapsto \begin{cases} i & , \textit{falls } i \leq n_1 \textit{ ist,} \\ p_{i-n_1} + 1 & , \textit{falls } i > n_1 \textit{ ist.} \end{cases}$$

die anordnungserhaltende Bijektion von $\mathbb{N}_{\leq s}$ auf $\mathcal{S}$. Dann gilt $\mathbb{N}_{\leq n_1+1} \subseteq \mathrm{Fix}(\psi')$. Es läßt sich ψ' zu einer Permutation ψ'' von $\mathbb{N}_{\leq s} \cup \mathcal{S}$ fortsetzen. Diese induziert dann eine Permutation ψ von

$\mathbb{N}_{\leq n}$ *mit* $\mathbb{N}_{\leq n} \backslash (\mathbb{N}_{\leq s} \cup \mathcal{S}) \subseteq \mathrm{Fix}(\psi)$. *Wegen* $\max \mathbb{N}_{\leq s} \cup \mathcal{S} = p_{m-1} + 1$ *gilt insbesondere* $\mathbb{N}_{\leq n_1+1} \cup \{p_{m-1}+2, \ldots, n\} \subseteq \mathrm{Fix}(\psi)$. *Weiterhin gilt*

$$\sigma^{-1}\rho = \psi^{-1}\rho_{(s,n)}\psi.$$

Beweis. Es ist nur die Gültigkeit der letzten Gleichung nachzuweisen. Falls $i \in \mathbb{N}_{\leq n_1} \subseteq \mathrm{Fix}(\sigma) \cap \mathbb{N}_{<s}$ ist, gilt $i, i+1 \in \mathrm{Fix}(\psi)$ und

$$i\psi\sigma^{-1}\rho = i\rho = i+1 = i\rho_{(s,n)} = i\rho_{(s,n)}\psi.$$

Falls $i \in \{n_1+1, \ldots s\}$ ist, gilt

$$i\psi\sigma^{-1}\rho = (p_{i-n_1}+1)\sigma^{-1}\rho = p_{i-n_1+1}\rho = \begin{cases} n\rho = 1 & \text{falls } i = s \text{ ist,} \\ p_{i+1-n_1}+1 = (i+1)\psi & \text{falls } i < s \text{ ist,} \end{cases}$$

und

$$i\rho_{(s,n)}\psi = \begin{cases} 1\psi = 1 & \text{falls } i = s \text{ ist,} \\ (i+1)\psi & \text{falls } i < s \text{ ist.} \end{cases}$$

Falls $i \in \mathbb{N}_{>s} \subseteq \mathrm{Fix}(\rho_{(s,n)})$ ist, gilt $i\psi \notin \mathcal{S} = \mathbb{N}_{\leq s}\psi$, also
$i\psi\sigma^{-1}\rho = (i\psi-1)\rho = i\psi = i\rho_{(s,n)}\psi$ ■

Bemerkung 4.6.12 *Es seien die Bezeichnungen wie in 4.6.11. Seien* $\mathcal{T} := \{s+1, \ldots, p_{m-1}+1\}$ *und* ϕ' *diejenige Permutation von* $\mathcal{T}\psi$, *für die* $(s+1)\psi\phi' < \cdots < (p_{m-1}+1)\psi\phi'$ *gilt. Die Permutation* ϕ *von* $\mathbb{N}_{\leq n}$, *die auf* $\mathcal{T}\psi$ *mit* ϕ' *übereinstimmt und auf* $\mathbb{N}_{\leq n}\backslash\mathcal{T}\psi$ *die Identität ist, genügt dann den folgenden Bedingungen:*

(i) $1\psi\phi < \cdots < s\psi\phi$,

(ii) $(s+1)\psi\phi < \cdots < n\psi\phi$,

(iii) $(\sigma^{-1}\rho)\phi = \phi(\sigma^{-1}\rho)$,

(iv) *Es gilt* $1 \in \mathrm{Fix}(\psi\phi)$ *und, falls* $n_m \geq 2$ *ist, auch* $n \in \mathrm{Fix}(\psi\phi)$.

Beweis. (i). Wegen $\mathbb{N}_{\leq s}\psi \subseteq \mathbb{N}_{\leq n}\backslash\mathcal{T}\psi \subseteq \mathrm{Fix}(\phi)$ gilt $(1\psi\phi, \ldots, s\psi\phi) = (1\psi, \ldots, s\psi) = (1, \ldots, n_1, p_1+1, \ldots, p_j+1, \ldots, p_{m-1}+1)$, $j \in \mathbb{N}_{\leq m-1}$.
(ii). Nach 4.6.11 gilt $\{p_{m-1}+2, \ldots n\} \subseteq \mathrm{Fix}(\psi)$, $\{p_{m-1}+2, \ldots, n\} = \{p_{m-1}+2, \ldots, n\}\psi \subset \mathbb{N}_{\leq n}\backslash\mathcal{T}\psi \subseteq \mathrm{Fix}(\phi)$. Es folgt $((s+1)\psi\phi, \ldots, n\psi\phi) = ((s+1)\psi\phi', \ldots, (p_{m-1}+1)\psi\phi', p_{m-1}+2, \ldots, n)$. Nach Wahl von ϕ' sind die Einträge dieses $(n-s)$-Tupels wachsend angeordnet.
(iii). Nach 4.6.11 gilt $\sigma^{-1}\rho = \rho^{\psi}_{(s,n)}$. Es gilt $\mathbb{N}_{\leq n}\backslash\mathcal{T}\psi \subseteq \mathrm{Fix}(\phi)$ und wegen $\mathcal{T} \subseteq (\mathbb{N}_{\leq n})_{>s} \subseteq \mathrm{Fix}(\rho_{(s,n)})$ auch $T\psi \subseteq \mathrm{Fix}(\psi^{-1}\rho_{(s,n)}\psi) = \mathrm{Fix}(\sigma^{-1}\rho)$. Somit kommutieren ϕ und $\sigma^{-1}\rho$.
(iv). Wegen $1 \leq n_1+1$ liegt 1 nach 4.6.11 in $\mathrm{Fix}(\psi)$. Wegen $1 < s+1$, gehört $1 = 1\psi^{-1}$ nicht zu $\mathcal{T}$, i.e. $1 \in \mathbb{N}_{\leq n}\backslash\mathcal{T}\psi \subseteq \mathrm{Fix}(\phi)$. Sei $n_m \geq 2$. Dann ist $p_{m-1}+2 \leq n$, so daß n nach 4.6.11 in $\mathrm{Fix}(\psi)$ liegt. Wegen $n > p_{m-1}+1$, gilt $n\psi^{-1} = n \notin \mathcal{T}$, also $n \in \mathbb{N}_{\leq n}\backslash\mathcal{T}\psi \subseteq \mathrm{Fix}(\phi)$. ■

Hilfssatz 4.6.13 *Es seien die Bezeichnungen wie in 4.6.11 und 4.6.12. Seien* $R \in \mathrm{GL}_s(F)$, $S \in \mathrm{GL}_{n-s}(F)$ *obere Dreiecksmatrizen,* $T \in F^{s \times n-s}$ *mit* $T_{i,j} = 0$*, falls* $i\psi\phi > (j+s)\psi\phi$, $(i,j) \in \mathbb{N}_{\leq s} \times \mathbb{N}_{\leq n-s}$*, und*

$$Q := \begin{bmatrix} R & T \\ & S \end{bmatrix} \in \mathrm{GL}_n(F).$$

Dann ist $U := Q^{\psi\phi} = (Q_{i(\psi\phi)^{-1},j(\psi\phi)^{-1}})_{1 \leq i,j \leq n}$ *eine obere Dreiecksmatrix mit Diagonalelementen* $U_{i\psi\phi,i\psi\phi} = Q_{i,i}$*. Ist* $n_m \geq 2$*, so sind* $U_{i\psi\phi,n} = Q_{i,n}$, $i \in \mathbb{N}_{\leq n}$ *die Einträge der letzten Spalte von* U.

Beweis. Seien $i,j \in \mathbb{N}_{\leq n}$. Weil für eine Permutationsmatrix P stets $P^t = P^{-1}$ gilt, erhält man $U_{i,j} = e_i U e_j^t = e_i(\psi\phi)^{-1}Q(\psi\phi)e_j^t = e_{i(\psi\phi)^{-1}}Qe^t_{j(\psi\phi)^{-1}} = Q_{i(\psi\phi)^{-1},j(\psi\phi)^{-1}}$, i.e. $U_{i\psi\phi,j\psi\phi} = Q_{i,j}$. Falls $n_m \geq 2$ ist, wird n nach 4.6.3 (iv) von $\psi\phi$ festgelassen. Dies beweist die letzte Aussage der Behauptung.
Annahme: Es gilt $i\psi\phi > j\psi\phi$ und $0 \neq U_{i\psi\phi,j\psi\phi} = Q_{i,j}$. Weil Q eine obere Dreiecksmatrix ist, ist dann $i \leq j$. Nach 4.6.12 (i) und (ii) gilt dann $(i,j) \in \mathbb{N}_{\leq s} \times \mathbb{N}_{\geq s+1}$, also $0 \neq Q_{i,j} = T_{i,j-s}$, ein Widerspruch zur Definition von T. ■

Wir kommen nun zum Beweis von 4.6.2 (ii).
Nach 4.6.9 kann man annehmen, daß M nicht zyklisch ist. Weiterhin kann man o.B.d.A. annehmen, daß M in Frobenius-Normalform ist. Weil M nicht zyklisch und keine Homothetie ist, gibt es ein $m \in \mathbb{N}_{\geq 2}$, ein $n_1 \in \mathbb{N} \cup \{0\}$ mit $n_1 > 0$, falls $m = 2$ ist, $n_2, \ldots, n_m \in \mathbb{N}_{\geq 2}$, Begleitmatrizen $M_i \in F^{l_i \times l_i}$, $2 \leq i \leq m$, derart, daß für $2 \leq j \leq m-1$ $\mathrm{char}(M_j)$ ein Teiler von $\mathrm{char}(M_{j+1})$ ist, und ein $\mu \in F^*$ so, daß

$$M = \mathrm{diag}(\mu I_{n_1}, M_2, \ldots, M_m)$$

gilt. Es seien $(p_i)_{i \in \mathbb{N}_{\leq m}}, s, \sigma, \psi, \phi$ wie in 4.6.11 und 4.6.12 definiert. Beachte daß $s = n_1 + m - 1 \geq 2$ ist. Wir unterscheiden die beiden Fälle A: '$n - s \geq 2$' und B: '$n - s = 1$'.

Fall A. Für $2 \leq i \leq m$ sei $U_i := \rho_{n_i}^{-1} M_i$. Setze $U := \mathrm{diag}(\mu I_{n_1}, U_2, \ldots, U_m)$. Dann ist U eine obere Dreiecksmatrix, und es gilt $M = \sigma U$. Seien $C \in F^{s \times n-s}$, $c := (C_{1,1}, C_{1,3}, \ldots, C_{s,1}) \in F^{s-1}$ und $\epsilon_{n-1}, A_1', A_2, d_c$ wie in 4.6.10. Nach Voraussetzung besitzt A einen Eigenwert α mit einfacher Vielfachheit. Daher kann man $(A_2)_{n-s,n-s} = \alpha$ und $\epsilon_{n-1} = 0$ annehmen. Es gelte

(a1) $C_{i,j} = 0$, falls $i\rho_s^{-1}\psi\phi > (j+s)\psi\phi$ ist.

Nach 4.6.12 (iv) gilt $1 \in \mathrm{Fix}(\phi\psi)$, und daher

$$2\rho_s^{-1}\psi\phi = 1\psi\phi = 1 \leq (s+1)\psi\phi.$$

Die Forderung $C_{2,1} \neq d_c$ steht daher nicht im Widerspruch zu (a1). Nach 4.6.10 gilt

$$A' := \begin{bmatrix} A_1' & C \\ & A_2 \end{bmatrix} \in \Omega_1.$$

Weil $n_m \geq 2$ ist, schließen wir weiterhin mit 4.6.12 (iv), daß $i\rho_s^{-1}\psi\phi \leq n = n\psi\phi$ für alle $i \in \mathbb{N}_{\leq s}$ gilt. Dies besagt, daß wegen $n - s \geq 2$ die Einträge der letzten Spalte von C frei wählbar sind (cf.

(a1)). Setze

$$D := \rho_s A_1' = \begin{bmatrix} 1 & & & -q_1 \\ & \ddots & & \\ & & 1 & -q_{s-1} \\ & & & -q_0 \end{bmatrix}$$

und $E := \rho_s C$. Dann sind die Einträge der letzten Spalte $E_{i,n-s} = C_{i\rho_s,n-s}$, $i \in \mathbb{N}_{\leq s}$, von E frei wählbar, und nach Wahl von C gilt $E_{i,j} = C_{i\rho_s,j} = 0$, falls $i\psi\phi > (j+s)\psi\phi$ ist. Es ist

$$G := \rho_{(s,n)} A' = \begin{bmatrix} D & E \\ & A_2 \end{bmatrix} \in \mathrm{GL}_n(F)$$

eine obere Dreiecksmatrix mit $\det G = (-1)^{s+1} \det A$. Weil E die in 4.6.13 geforderten Eigenschaften besitzt, ist $H := G^{\psi\phi}$ eine obere Dreiecksmatrix mit Diagonalelementen $H_{i\psi\phi,i\psi\phi} = G_{i,i}$ und letzter Spalte $H_{i\psi\phi,n} = G_{i,n}$, $i \in \mathbb{N}_{\leq n}$ wegen $n_m \geq 2$. Weil wegen $\epsilon_{n-1} = 0$ nach 4.6.10 auch die Einträge $(A_2)_{i,n-s}$, $i \in \mathbb{N}_{\leq n-s-1}$ beliebig aus F gewählt werden können, erhalten wir:

(a2) Die Einträge $H_{i\psi\phi,n} = G_{i,n}$, $i \in \mathbb{N}_{\leq n-1}$, dürfen beliebig aus F gewählt werden.

[Zwischenbemerkung: In (a2) besteht die wesentliche Vereinfachung der allgemeinen Situation des Satzes von A.Lev 4.6.1. Dort kann $\epsilon_{n-1} = 1$ auftreten, so daß nach 4.6.8 nur die Einträge $H_{i\psi\phi,n}$, $i \neq n-1$ beliebig aus F gewählt werden dürfen. Der Eintrag $H_{(n-1)\psi\phi,n} = (A_2)_{n-s-1,n-s}$ hingegen muß zu F^* gehören.]
Mit Hilfe von 4.6.11 und 4.6.12 (iii) berechnet man:

$$\begin{aligned} A'' &:= A'^{\psi\phi} = \phi^{-1}\psi^{-1}\rho_{(s,n)}^{-1} G\psi\phi = \phi^{-1}{\rho_{(s,n)}^{-1}}^{\psi} G^{\psi}\phi \\ &= \phi^{-1}(\rho^{-1}\sigma)G^{\psi}\phi = (\rho^{-1}\sigma)\phi^{-1}G^{\psi}\phi = \rho^{-1}\sigma H \in \Omega_1. \end{aligned}$$

Seien $H' := (H_{i,j})_{1\leq i,j\leq n-1}$, $h_i := H_{i,n}$, $1 \leq i \leq n$, $h := (h_1, \ldots, h_{n-1})^t$ und analog $U' := (U_{i,j})_{1\leq i,j\leq n-1}$, $u_i := U_{i,n}$, $1 \leq i \leq n$, $u := (u_1, \ldots, u_{n-1})^t$. Dann gilt

$$H = \begin{bmatrix} H' & h \\ & h_n \end{bmatrix} \text{ und } U = \begin{bmatrix} U' & u \\ & u_n \end{bmatrix}.$$

Setze $L' := H'^{-1}U'$ und $l_n := h_n^{-1}u_n$. Für $i \in \mathbb{N}_{\leq n}$ sei

$$f_i := \begin{cases} L'_{1,1}(-1)^{n+1} \det B^{-1} & \text{, falls } i = 1 \text{ ist,} \\ L'_{i,i} & \text{, falls } 2 \leq i \leq n-1 \text{ ist,} \\ l_n & \text{, falls } i = n \text{ ist.} \end{cases}$$

Aus

$$\begin{aligned} \det\sigma &= (-1)^{n-n_1+m-1}, \\ \det\sigma \det U &= \det M = \det A \det B, \\ \det H &= \det G = (-1)^{s+1} \det A = (-1)^{n_1+m} \det A \end{aligned}$$

folgt:

$$\begin{aligned}\prod_{i=1}^{n} f_i &= (-1)^{n+1}\det B^{-1}\det H^{-1}\det U = (-1)^{n+1}\det B^{-1}(-1)^{s+1}\det A^{-1}\det\sigma\det M\\ &= (-1)^{(n+1)+(n_1+m)+(n-n_1+m-1)} = 1.\end{aligned}$$

Nach 4.6.6 gibt es $r_1,\ldots,r_{n-1}\in F$ so, daß

$$N := \begin{bmatrix} (f_1(-1)^{n+1}\det B) & r_1 & \ldots & r_{n-1}\\ & f_2 & & \\ & & \ddots & \\ & & & f_n \end{bmatrix} \in \rho^{-1}\Omega_2$$

gilt. Nach 4.6.7 [das dortige Variablen-Tupel (A,B,B_1,B_2) ist mit (B,N,L',l_n) zu belegen] gibt es ein $l\in F^{n-1}$ so, daß

$$L := \begin{bmatrix} L' & l^t\\ & l_n\end{bmatrix} \in \rho^{-1}\Omega_2$$

gilt. Setzt man $\tilde h := (l_n^{-1}(u^t - H'l^t))^t$, so berechnet man

$$\begin{bmatrix} H' & \tilde h^t\\ & h_n\end{bmatrix} L = \begin{bmatrix} H' & \tilde h^t\\ & h_n\end{bmatrix}\begin{bmatrix} L' & l^t\\ & l_n\end{bmatrix} = \begin{bmatrix} U' & H'l^t + \tilde h^t l_n\\ & u_n\end{bmatrix} = U.$$

Nach (a2) kann man $h=\tilde h$, i.e. $HL=U$ annehmen. Dies bedeutet

$$M = \sigma U = \rho(\rho^{-1}\sigma H)\rho^{-1}(\rho L) = A''^{\rho^{-1}}\rho L \in \Omega_1\Omega_2.$$

Fall B. In diesem Fall gilt $1 = n - s = \sum_{i=1}^{m} n_i - (n_1 + m - 1) = \sum_{i=2}^{m} n_i - m + 1 \geq 2(m-1) - m + 1 = m - 1$ und wegen $m\geq 2$ bereits $m=2$. Dies impliziert wiederum $1 = n - s = n_2 - 1$, i.e. $n_2 = 2$. Wegen $3\leq n = n_1 + n_2 = n_1 + 2$ ist $n_1\neq 0$. Weil M in Frobeniusnormalform ist, bedeutet dies $M_1 = \mu I_{n-2}$ und $\mathrm{mip}(M_2) = (x-\mu)(x-\nu)$ für geeignete $\mu,\nu\in F^*$. Somit besteht die Konjugiertenklasse Ω von M aus den Matrizen $N\in \mathrm{GL}_n(F)$, welche der Bedingung

(b1) $\dim\ker(N-\mu) = n-1$ und $\mathrm{mip}(N) = (x-\mu)(x-\nu)$

genügen. Seien $\mathrm{mip}(A) = x^n + \sum_{i=0}^{n-1}\alpha_i x^i$, $\mathrm{mip}(B) = x^n + \sum_{i=0}^{n-1}\beta_i x^i$, $a := (-\alpha_1,\ldots,-\alpha_{n-1})$, $b := (-\beta_1,\ldots,-\beta_{n-1})$. Dann gilt

$$R := \begin{bmatrix} I_{n-1} & a^t\\ & -\alpha_0\end{bmatrix} \in \rho\Omega_1 \text{ und } S := \begin{bmatrix} I_{n-1} & b^t\\ & -\beta_0\end{bmatrix} \in \rho\Omega_2.$$

Setze

$$L := (\delta_{i,n-j})_{1\leq i,j\leq n-1} = \begin{bmatrix} & & & 1\\ & & \cdot & \\ & \cdot & & \\ 1 & & & \end{bmatrix} \in \mathrm{GL}_{n-1}(F)$$

und $J := \operatorname{diag}(L, 1)$. Die Matrizen L und J sind involutorisch, und es gilt

$$\begin{aligned} J\rho &= \begin{bmatrix} L & \\ & 1 \end{bmatrix} \begin{bmatrix} & I_{n-1} \\ 1 & \end{bmatrix} = \begin{bmatrix} & L \\ 1 & \end{bmatrix} \\ &= \begin{bmatrix} & 1 \\ L & \end{bmatrix} = \begin{bmatrix} & 1 \\ I_{n-1} & \end{bmatrix} \begin{bmatrix} L & \\ & 1 \end{bmatrix} = \rho^{-1} J, \end{aligned}$$

i.e. $(\rho^{-1})^J = \rho$. Hieraus folgt $\rho R^J = (\rho^{-1} R)^J \in \Omega_1$. Man berechnet

$$R' := R^J = \begin{bmatrix} I_{n-1} & La^t \\ & -\alpha_0 \end{bmatrix}.$$

Setzt man $f_{i,i} := \mu$ für $i \in \mathbb{N}_{\leq n-1}$ und $f_{n,n} = \nu \alpha_0^{-1} \beta_0^{-1}$, so gilt

$$\prod_{i=1}^{n} f_{i,i} = \mu^n \nu \alpha_0^{-1} \beta_0^{-1} = \det M \det A^{-1} \det B^{-1} = 1.$$

Nach 4.6.5 angewandt auf $A = R'$ gibt es ein $c \in F^{n-1}$ so, daß

$$R'' = \begin{bmatrix} \mu I_{n-1} & c^t \\ & -\nu \beta_0^{-1} \end{bmatrix} \in \rho^{-1} \Omega_1.$$

Dies impliziert

$$T := (\rho R'')^\rho \rho^{-1} S = R'' S = \begin{bmatrix} \mu I_{n-1} & \mu b^t - \beta_0 c^t \\ & \nu \end{bmatrix} \in \Omega_1 \Omega_2.$$

Falls $\nu \neq \mu$ oder $z := \mu b - \beta_0 c \neq 0$ ist, erfüllt T die Bedingung (b1) anstelle von N, so daß die Behauptung für diesen Fall bewiesen ist. Man kann daher $\nu = \mu$ und $z = 0$ annehmen. Dies bedeutet $\mu I_n \in \Omega_1 \Omega_2$ und somit $\operatorname{mip}(B) = \prod_{i=1}^{n} (x - \mu a_i^{-1})$. Wegen $|F| \geq 3$ gibt es ein $\epsilon \in F^* \backslash \{a_2^{-1} \mu\}$. Dann ist $\delta := a_1^{-1}(\epsilon - a_2^{-1} \mu) \neq 0$. Aus (b1) erhält man

$$N := \begin{bmatrix} \mu & 1 & & \\ & \mu & & \\ & & \ddots & \\ & & & \mu \end{bmatrix} \in \Omega.$$

Es seien die a_i so angeordnet, daß die in 4.6.8 definierte Matrix $\tilde{A}$ eine Jordan' sche Normalform von A ist. Seien $\epsilon_1, \ldots, \epsilon_{n-1}$ wie dort. Aus 4.6.8 schließt man:

$$Y := \begin{bmatrix} a_1 & 1 & & \\ & \ddots & \ddots & \\ & & a_{n-1} & 1 \\ & & & a_n \end{bmatrix} \in \Omega_1.$$

Man berechnet

$$Z := Y^{-1}N = \begin{bmatrix} a_1^{-1} & -a_1^{-1}a_2^{-1} & & * \\ & \ddots & \ddots & \\ & & a_{n-1}^{-1} & -a_{n-1}^{-1}a_n^{-1} \\ & & & a_n^{-1} \end{bmatrix} \begin{bmatrix} \mu & \epsilon & & \\ & \mu & & \\ & & \ddots & \\ & & & \mu \end{bmatrix}$$

$$= \begin{bmatrix} a_1^{-1}\mu & \delta & & & * \\ & a_2^{-1}\mu & (-a_2^{-1}a_3^{-1}\mu) & & \\ & & \ddots & \ddots & \\ & & & a_{n-1}^{-1}\mu & (-a_{n-1}^{-1}a_n^{-1}\mu) \\ & & & & a_n^{-1}\mu \end{bmatrix}.$$

Wegen $Z_{i,i+1} \neq 0$ für alle $i \in \mathbb{N}_{\leq n}$ und weil

$$\begin{bmatrix} a_1^{-1}\mu & \epsilon_1 & & \\ & \ddots & \ddots & \\ & & a_{n-1}^{-1}\mu & \epsilon_{n-1} \\ & & & a_n^{-1}\mu \end{bmatrix}$$

eine Jordan'sche Normalform von B ist, ist Z nach 4.6.8 ein Element von Ω_2. Es folgt $N = YZ \in \Omega_1\Omega_2$. ■

Korollar 4.6.14 (Lev) *Seien $|F| \geq 4$ und $n \in \mathbb{N}_{\geq 2}$. Dann besitzt $\mathrm{PSL}_n(F)$ eine Konjugiertenklasse Ω, die $\mathrm{PSL}_n(F) = \Omega^2$ erfüllt.*

Beweis. Wegen $|F| \geq 4$ gibt es ein $a \in F^*\backslash\{\pm 1\}$. Sei Ω die zyklische $\mathrm{GL}_n(F)$-Konjugiertenklasse mit $\mathrm{mip}(\Omega) = (x-a)(x-a^{-1})(x-1)^{n-2}$. Diese ist bekanntlich eine in $\mathrm{SL}_n(F)$ enthaltene $\mathrm{SL}_n(F)$-Konjugiertenklasse. Sie hat zwei verschiedene Eigenwerte a und a^{-1} mit einfacher Vielfachheit. Nach 4.6.2 gilt $M \in \Omega^2$ für jedes $M \in \mathrm{SL}_n(F)$, das keine Homothetie ist. Die Symmetrie von $\mathrm{mip}(\Omega)$ ergibt $\Omega = \Omega^{-1}$, also $1_V \in \Omega^2$. ■

Korollar 4.6.15 *Seien $|F| = 3$ und $n \in \mathbb{N}_{\geq 3}$ ungerade. Dann besitzt $\mathrm{PSL}_n(F)$ eine Konjugiertenklasse Ω, die $\mathrm{PSL}_n(F) = \Omega^2$ erfüllt.*

Beweis. Sei $t \in \mathbb{N}$ mit $n = 2t+1$. Sei Ω die zyklische $\mathrm{GL}_n(F)$-Konjugiertenklasse mit $\mathrm{mip}(\Omega) = (x+1)^{2t}(x-1)$. Diese ist wiederum eine in $\mathrm{SL}_n(F)$ enthaltene $\mathrm{SL}_n(F)$-Konjugiertenklasse. Sie besitzt die beiden verschiedenen Eigenwerte 1 und -1, und der Eigenwert 1 hat einfache Vielfachheit. Nach 4.6.2 gilt wiederum $M \in \Omega^2$ für jedes $M \in \mathrm{SL}_n(F)$, das keine Homothetie ist, und aus der Symmetrie von $\mathrm{mip}(\Omega)$ folgert man $1_V \in \Omega^2$. ■

Literaturverzeichnis

[1] Z. Arad und M. Herzog (Hrsg.), Products of conjugacy classes in groups, Lecture Notes in Mathematics 1112 (1985).

[2] F. Bachmann, Aufbau der Geometrie aus dem Spiegelungsbegriff, Springer-Verlag (1973).

[3] C.S. Ballantine, Products of involutory matrices I, Linear and Multilinear Algebra 5 (1977), 53-62.

[4] S.D. Berman and K. Buzaši, Representations of the infinite dihedral group, Publ. Math. Debrecen 28 (1981), 173-187.

[5] V.M. Bondarenko, Representations of dihedral groups over a field of characteristik 2, Mathematiceskij Sbornik 96 (1975), 63-74.

[6] O. Bonten, Aachener Beiträge zur Mathematik Band 7 (Dissertation 1992).

[7] N. Bourbaki, Algebra I, Chapters 1-3, Springer Verlag (1989).

[8] N. Bourbaki, Formes sesquilinéaires (Éléments de Mathématiques I, livres II, chapitre 9), Hermann, Paris (1959).

[9] J.L. Brenner, Covering theorems for finasigs X. The group $G = \mathrm{PSL}(n, q)$ had a class C such that $CC = G$, Ars Combinatoria 16 (1983), 57-67.

[10] F.Bünger, Produkte von Konjugiertenklassen in den Gruppen $\mathrm{GL}(V)$ und $\mathrm{SL}(V)$, Diplomarbeit Kiel (1994).

[11] F. Bünger, F. Knüppel, K. Nielsen, Products of symmetries in unitary groups, Linear Algebra and its Applications, to appear.

[12] F. Bünger, F.Knüppel, Products of quasi-involutions in unitary groups, erscheint in Geometriae Dedicata.

[13] D. Callan, The generation of $\mathrm{Sp}(\mathrm{F}_2)$ by transvections, J. Algebra 42 (1976), 378-390.

[14] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, Journal für die reine und angewandte Mathematik 227 (1967), 212-220.

[15] E. Cartan, La géométrie des groupes simples, Ann. Mat. Pura Appl. 4 (1927), 209-256.

[16] Cleuvers, Neubüser, Pahlings , Abstracts AMS 6 (34) (1984), 84T-20-415, p.395.

[17] J. Dieudonné, Sur les groupes classiques, Actualités Scientifiques et industrielles, no. 1040, Hermann, Paris (1948).

[18] J. Dieudonné, Orthogonal and unitary groups over the rational field, Amer. J. Math., Vol.73 (1951), 940-948.

[19] J. Dieudonné, On the structure of unitary groups, Trans. Amer. Math. Soc. 72 (1952), 367-385.

[20] J. Dieudonné, On the structure of unitary groups (II), Amer. J. Math. 75 (1953), 665-678.

[21] J. Dieudonné, Sur les generateurs des groupes classiques, Summa Brasil. Math. 3 (1955), 149-179.

[22] J. Dieudonné, La géométrie des groupes classiques, Springer-Verlag (1955).

[23] D.Ž. Djoković, The product of two involutions in the unitary group of a hermitian form, Indiana Univ. Math. J. 21 (1971), 449-456.

[24] D.Ž. Djoković, Product of two involutions, Arch. Math. 18 (1967), 582-584.

[25] D.Ž. Djoković, Pairs of involutions in the general linear group, J. Algebra 100 (1986), 214-223.

[26] D.Ž. Djoković and J.Malzan, Products of reflections in the unitary group, Proceedings of the American Mathematical Society, Vol. 73, no. 2 (1979), 157-160.

[27] D.Ž. Djoković and J.Malzan, Products of reflections in $\mathrm{U}(p,q)$, Memoirs of the American Mathematical Society, Vol. 259 (1982), 1-82.

[28] E.W. Ellers, Bireflectionality in classical groups. Can. J. of Math. XXIX (1977), 1157-1162.

[29] E.W. Ellers and W. Nolte, Bireflectionality of orthogonal and symplectic groups, Arch. Math., Vol. 39 (1982), pp.113-116.

[30] E.W. Ellers, Classical Groups, 'Generators and relations in groups and geometries' edited by A.Barlotti, E.W.Ellers, P.Plaumann and K. Strambach, Kluwer Academic Publishers (1991), 1-45.

[31] E.W. Ellers, The reflection length of a transformation in the unitary group over a finite field, Linear and Multilinear Algebra, Vol. 35 (1993), 11-35.

[32] E.W. Ellers, N. Gordeev, Gauss decomposition with prescribed semisimple part in chevalley groups, Communications in Algebra 22 (1994), 5935-5950.

[33] E.W. Ellers, N. Gordeev, Gauss decomposition with prescribed semisimple part in chevalley groups II exceptional cases, Communications in Algebra 23 (1995), 3085-3098.

[34] M. Götzky, Eine Kennzeichnung der orthogonalen Gruppen unter den unitären Gruppen, Arch. Math. 15 (1964), 261-265.

[35] M. Götzky, Eine Kennzeichnung der unitären Gruppen über einem Schiefkörper der Charakteristik $\neq 2$, Dissertation, Kiel (1965).

[36] M. Götzky, Unverkürzbare Produkte und Relationen in unitären Gruppen, Math. Z. 104 (1968), 1-15.

[37] D. Gorenstein, R. Lyons, R. Solomon, The classification of the finite simple groups, Mathematical Surveys and Monographs, Volume 40, Number I, American Mathematical Society (1994).

[38] R. Gow, Products of two involutions in classical groups of characteristic 2, J.Algebra 71 (1981), 583-591.

[39] R. Gow, Commutators in the symplectic group, Archiv der Mathematik 50 (1988), 204-209.

[40] O.v.Grudzinski, Funktionalanalysis, Vorlesungsmitschrift (Sommersemester 1994).

[41] A.J.Hahn O.T. O'Meara, The Classical Groups and K-Theory, Springer-Verlag (1989).

[42] B. Huppert, Endliche Gruppen. Springer-Verlag (1983), zweiter Nachdruck der ersten Auflage.

[43] B. Huppert, Angewandte lineare Algebra. de Gruyter, Berlin New York (1990).

[44] N. Ito, A theorem on the alternating group A_n $(n \geq 5)$, Mathematica Japonicae 2 (1950-52), 59-60.

[45] D. Jungnickel, Finite fields, BI Wissenschaftsverlag (1993).

[46] S. Karni, Covering numbers of groups of small order and sporadic groups, Kapitel 2 des Springer Lecture Note Bandes 1112 (1985): Products of conjugacy classes in groups.

[47] F. Knüppel, Products of involutions in orthogonal groups. Ann. of Discr. Math. 37 (1988), 231-248.

[48] F. Knüppel, K. Nielsen, On products of two involutions in the orthogonal group of a vector space, Linear Algebra and its Applications 94 (1987), 209-216.

[49] F. Knüppel, K. Nielsen, SL(V) is 4-reflectional, Geometriae Dedicata 38 (1991), 301-308.

[50] A.Lev, Products of cyclic conjugacy classes in the groups PSL(n, F), Lin. Alg. Appl. 179 (1993), 59-83.

[51] A.Lev, Products of cyclic similarity classes in the groups $\mathrm{GL}_n(F)$, Lin. Alg. Appl. 202 (1994), 235-266.

[52] S. Lang, Algebra, Addison Wesley (1984).

[53] F. Lorenz, Einführung in die Algebra Teil 1 u. 2. BI Wissenschaftsverlag, Mannheim/Wien/Zürich (1991, 1992).

[54] D.Ž. Djoković and J. Malzan, Products of reflections in U(p, q). Mem. Amer. Math. Soc. 37(259) (1982), 1-82.

[55] J. Milnor, On isometries of inner product spaces, Inventiones math., Vol. 8 (1969), 83-97.

[56] K.Nielsen, Products of involutions in symplectic groups, Geom. Ded., to appear.

[57] K.Nielsen, Products of conjugacy classes in symplectic groups, (preprint 1995).

[58] O. Ore, Some remarks on commutators, Proc. Amer. Math. Soc. 2 (1951), 307-314.

[59] H. Radjavi, Products of hermitian matrices and symmetries. Proc. Amer. Math. Soc. 21 (1969), 369-375.

[60] C. Riehm, The equivalence of bilinear forms, J. Algebra, Vol. 31 (1974), 45-66.

[61] C. Riehm and M.A. Shrader-Frechette, The equivalence of sesquilinear forms, J. Algebra, Vol. 42 (1976), 495-530.

[62] C.M. Ringel, The indecomposable representations of the dihedral 2-groups, Math. Analen 214 (1975), 19-34.

[63] R. Scharlau, Zur Klassifikation von Bilinearformen und von Isometrien über Körpern, Math. Z. 178 (1981), 359-373.

[64] W. Scharlau, Quadratic and hermitian forms, Springer-Verlag, Berlin Heidelberg New York (1985).

[65] P. Scherk, On the decomposition of orthogonalities into symmetries, Proc. Amer. Math. Soc. 1 (1950), 481-491.

[66] A.R. Sourour, A factorization theorem for matrices, Linear and Multilinear Algebra 19 (1986), 141-147.

[67] T.A. Springer, Over symplektische transformaties, Thesis, University of Leiden (1951).

[68] A. Borel R. Carter C.W. Curtis N. Iwahori T.A. Springer R. Steinberg, Seminar on algebraic groups and related finite groups, Lecture Notes in Mathematics, Springer-Verlag (1986).

[69] D.E. Taylor, The geometry of the classical groups, Heldermann Verlag (1992).

[70] R.C. Thompson, Commutators in the special and general linear groups, Trans. Amer. Math. Soc. 101 (1961), 16-33.

[71] R.C. Thompson, On matrix commutators, Portugal. Math. 21 (1962), 143-153.

[72] R.C. Thompson, Commutators of matrices with coefficients from the field of two elements, Duke Math. J. 29 (1962), 367-373.

[73] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J.Austral. Math. Soc. III (1963), 1-62.

[74] J. Williamson, The equivalence of non-singular pencils of hermitian matrices in an arbitrary field., Amer. J. Math., Vol. 57 (1935), 475-490.

[75] J. Williamson, On the algebraic problem concerning the normal forms of linear dynamical systems., Amer. J. Math., Vol. 58 (1936), 141-163.

[76] J. Williamson, On the normal forms of linear canonical transformations in dynamics., Amer. J. Math., Vol. 59 (1937), 599-617.

[77] J. Williamson, Normal matrices over an arbitrary field of characteristic zero., Amer. J. Math., Vol. 61 (1939), 335-356.

[78] J. Williamson, Note on the equivalence of nonsingular pencils of hermitian matrices., Bull. Amer. Math. Soc., Vol. 61 (1945), 894-897.

[79] M.J. Wonenburger, Transformations which are products of two involutions, J. Math. Mech. 16 (1966), 327-338.

[80] Cheng-Hao Xu, The commutators of the alternating group, Sci. Sinica 14 (1965), 339-342.

[81] H. Zassenhaus, On a normal form of the orthogonal transformation I, Can. Math. Bull., vol. 1, no. 1 (1958), 31-39.

[82] H. Zassenhaus, On a normal form of the orthogonal transformation II, Can. Math. Bull., vol. 1, no. 2 (1958), 101-191.